LCOS 10.94

Reference Manual

05/2026

LANCOM SYSTEMS

Contents

1 LCOS....26
2 Configuration....27
2.1 Ways and means of configuration....27
2.2 Configuration software....27
2.2.1 LANconfig....28
2.2.2 WEBconfig....28
2.2.3 LANCOM Management Cloud (LMC)....43
2.2.4 Terminal program....49
2.2.5 SNMP management program....83
2.3 LANCOM Layer 2 Management protocol (LL2M)....84
2.3.1 Introduction....84
2.3.2 Configuring the LL2M server....84
2.3.3 Commands for the LL2M client....84
2.4 Saving and loading device-configuration and script files....86
2.4.1 Configuration management with WEBconfig and the console....87
2.4.2 Script management with WEBconfig and the console....88
2.4.3 Configuration management with LANconfig....89
2.5 Alternative boot config....89
2.5.1 Introduction....89
2.5.2 Using the boot configuration....90
2.5.3 Storing and uploading the boot configurations....91
2.5.4 Deleting the boot configuration....92
2.5.5 Working with certificates....92
2.6 FirmSafe....93
2.6.1 Introduction....93
2.6.2 Configuration....93
2.6.3 Toggling the active firmware via console command....93
2.6.4 Asymmetric FirmSafe....94
2.7 Uploading firmware to the device via a client....94
2.7.1 Firmware upload via LANconfig....94
2.7.2 Firmware upload via WEBconfig....95
2.7.3 Firmware upload by terminal program....95
2.7.4 Firmware upload via outband with reset of the configuration....96
2.8 LANCOM Auto Updater....97
2.8.1 Configuring the Auto Updater....98
2.9 Loading files directly from/to the device via TFTP, HTTP(S) or SCP....100
2.9.1 Loading a file via a TFTP client....100
2.9.2 Loading a file via an SCP client....101
2.9.3 File download from a TFTP or HTTP(S) server....104
2.10 Automatic upload of firmware or configuration from USB....109

2.10.1 Automatic upload of loader and/or firmware files....110
2.10.2 Automatic upload of configuration and/or script files....110
2.10.3 Configuring automatic uploads via USB....111
2.11 Resetting the device....112
2.11.1 Configuring the reset button....112
2.12 Managing rights for different administrators....113
2.12.1 Rights for the administrators....113
2.12.2 Configuring SNMP read-only access....116
2.13 Device-internal SSH/SSL keys....117
2.13.1 Automatic generation of device-specific SSH/SSL keys....117
2.13.2 Manually create custom SSH keys....118
2.14 SSH authentication using a public key....119
2.14.1 Certificate check on SSH access....120
2.14.2 Generating an SSH keypair with PuTTY....120
2.14.3 Syntax and modifying public-key users....122
2.14.4 Setting up a device for public-key authentication....122
2.14.5 Public-key authentication with PuTTY....123
2.14.6 Public-key authentication with LANconfig....124
2.15 SSH and Telnet client in LCOS....125
2.15.1 Introduction....125
2.15.2 Syntax of SSH clients....125
2.15.3 Syntax of the Telnet client....126
2.15.4 Public keys for authentication....127
2.15.5 Creating SSH keys in LCOS....128
2.15.6 Priorities for SSH authentication....129
2.15.7 Rights for operating the SSH/Telnet client....129
2.16 Importing files by copy & paste on the CLI....129
2.17 Basic HTTP file server for external storage media....132
2.17.1 Introduction....132
2.17.2 Preparing the USB storage medium....133
2.17.3 Determine the mount point of the USB medium in the LCOS....133
2.17.4 Accessing the files on a USB medium....133
2.17.5 Rules for directory access....133
2.17.6 Supported content type....134
2.18 Rollout Wizard....134
2.18.1 Default Rollout Wizard....134
2.18.2 Custom Rollout Wizard....135
2.18.3 Activating the Rollout Wizard in WEBconfig....149
2.18.4 Configuration with LANconfig....150
2.18.5 Receiving LSR information via DHCP server (zero-touch rollout)....151
2.19 TCP port tunnel....155
2.19.1 Configuring the TCP/HTTP tunnel....155
2.19.2 Create the TCP/HTTP tunnel....155
2.19.3 Create a TCP-/HTTP Tunnel via CLI....156

2.19.4 Deleting the TCP/HTTP tunnel before it expires....157
2.20 The LANCOM High Availability Clustering Option....157
2.20.1 Setting up configuration synchronization....157
2.20.2 1-Click WLC High Availability Clustering Wizard....162
2.21 CPE WAN Management Protocol (CWMP)....165
2.21.1 Setting up CWMP with LANconfig....166
2.21.2 Device configuration via CWMP....168
2.22 Setting known loopback addresses....170
2.23 Configuration option for IPv4/IPv6 resolution with DNS resolutions....171
2.24 Customize the management ports for device access....171
2.25 Changing the SIM card PIN....172
3 LANtools....173
3.1 LANconfig – configuring devices....173
3.1.1 Start LANconfig....174
3.1.2 Working with LANconfig....176
3.1.3 LANconfig menu structure....206
3.1.4 Toolbar icons....240
3.1.5 LANconfig context menu....241
3.1.6 LANconfig keyboard shortcuts....241
3.1.7 LANconfig command line parameters....242
3.1.8 LANconfig application concepts....243
3.1.9 Pairing devices with the LANCOM Management Cloud....244
3.2 LANmonitor – monitoring devices on the LAN....247
3.2.1 Start LANmonitor....248
3.2.2 QuickFinder in LANmonitor....248
3.2.3 Display functions in LANmonitor....249
3.2.4 The menu structure in LANmonitor....249
3.2.5 The toolbar in LANmonitor....268
3.2.6 LANmonitor context menu....269
3.2.7 LANmonitor keyboard shortcuts....269
3.2.8 LANmonitor application concepts....269
3.3 WLANmonitor – monitoring wireless devices....273
3.3.1 Start WLANmonitor....275
3.3.2 QuickFinder in WLANmonitor....275
3.3.3 Rogue detection....275
3.3.4 The menu structure in WLANmonitor....278
3.3.5 The toolbar in WLANmonitor....287
3.3.6 WLANmonitor context menu....288
3.3.7 WLANmonitor keyboard shortcuts....288
3.3.8 WLANmonitor application concepts....288
3.4 LANtracer – tracing with LANconfig and LANmonitor....289
3.4.1 Starting LANtracer....290
3.4.2 Working with LANtracer....290
3.4.3 The menu structure in LANtracer....299

3.4.4 The toolbar in LANtracer....303
3.4.5 LANtracer context menu....304
3.4.6 LANtracer keyboard commands....304
4 Diagnosis....305
4.1 Trace information....305
4.1.1 How to start a trace....305
4.1.2 Overview of the keys....305
4.1.3 Parameter overview for the trace command....305
4.1.4 Combination commands....315
4.1.5 Trace filterss....315
4.1.6 Examples of traces....315
4.1.7 Recording traces....315
4.1.8 Trace to an attached USB drive....316
4.2 Tracing with LANmonitor....317
4.3 Recording and analyzing data packets....317
4.3.1 Data capture with packet capturing....317
4.3.2 Data capture with LCOSCAP....318
4.3.3 Data capture with RPCap....319
4.3.4 Output capture data to a USB drive....324
4.4 The SYSLOG module....324
4.4.1 Structure of SYSLOG messages....325
4.4.2 Configuring SYSLOG....327
4.4.3 Meaning of SYSLOG messages....333
4.5 Parameter overview for the ping command....336
4.6 Monitoring the switch....338
4.7 Cable test....339
4.8 Average value of the CPU load display....340
4.8.1 Introduction....340
4.8.2 Configuration....340
4.9 Sending attachments with the mailto command....341
4.10 Enhanced Sysinfo....342
4.10.1 Output additional ports in SYSINFO at the console....343
4.10.2 Output the configuration date....343
4.10.3 Output the configuration hashes....344
4.10.4 Output the configuration version....344
4.11 Bandwidth measurements with iPerf....345
4.11.1 Setting up iPerf with LANconfig....346
4.11.2 Temporary iPerf server and client....347
4.11.3 Analyzing iPerf results with LANmonitor....347
4.12 SLA monitoring....348
4.12.1 Configuring SLA monitoring with LANconfig....348
4.12.2 Displaying the SLA monitoring results in LANmonitor....350
4.13 Layer-7 application detection....351
4.13.1 IPv4/IPv6 traffic accounting....354

5 Security....356
5.1 Protecting the configuration....356
5.1.1 Password protection....356
5.1.2 Further administrators with restricted rights....358
5.1.3 Two-Factor Authentication (2FA) for Device Access....358
5.1.4 Login barring....361
5.1.5 Restricting access to the configuration....362
5.1.6 Management protocols....363
5.1.7 Deactivating Ethernet interfaces....365
5.2 Location verification by GPS....365
5.2.1 GPS location verification....366
5.2.2 Configuring location verification....366
5.3 Preventing password form fields in the browser from storing passwords....368
5.4 The security checklist....369
6 Routing and WAN connections....372
6.1 General information about WAN connections....372
6.1.1 Bridges for standard protocols....372
6.1.2 What happens with a request from the LAN?....372
6.2 IP routing....373
6.2.1 Routing behavior....373
6.2.2 Routing options....380
6.2.3 Prefix lists....382
6.2.4 The routing table....383
6.2.5 Policy-based routing....388
6.2.6 Dynamic routing with IP RIP....390
6.2.7 WAN RIP....394
6.2.8 SYN/ACK speedup....396
6.3 Advanced Routing and Forwarding (ARF)....396
6.3.1 Introduction....396
6.3.2 Defining networks and assigning interfaces....399
6.3.3 Assigning logical interfaces to bridge groups....399
6.3.4 Filtering protocols....400
6.3.5 Interfaces tags for remote sites....404
6.3.6 Setting the routing tag for local routes....405
6.3.7 Routing tags for DNS forwarding....405
6.3.8 Virtual routers....408
6.4 Configuring remote sites....409
6.4.1 Remote sites....409
6.4.2 Layer List....414
6.5 Generic routing encapsulation (GRE)....416
6.5.1 Understanding the generic routing encapsulation (GRE) protocol....416
6.5.2 Ethernet-over-GRE (EoGRE)....418
6.6 IP masquerading....420
6.6.1 Simple masquerading....420

6.6.2 Port forwarding (inverse masquerading)....422
6.7 Demilitarized Zone (DMZ)....424
6.7.1 Assigning network zones to the DMZ....424
6.7.2 Address check with DMZ and intranet interfaces....424
6.7.3 Unmasked Internet access for servers in the DMZ....425
6.8 Multi PPPoE....426
6.8.1 Example application: Home office with private Internet access....426
6.8.2 Configuration....426
6.9 Load balancing....427
6.9.1 DSL port mapping....428
6.9.2 Dynamic load balancing....430
6.9.3 Dynamic load balancing....434
6.9.4 Indirect bundling for LAN-LAN links via PPTP....435
6.9.5 Configuring load balancing....435
6.10 SD-WAN Dynamic Path Selection....440
6.10.1 Configuring Dynamic Path Selection....441
6.10.2 Show commands....447
6.10.3 Sample configurations....447
6.11 N:N mapping....449
6.11.1 Example applications....450
6.11.2 Configuration....452
6.12 Connection establishment with PPP....454
6.12.1 The protocol....454
6.12.2 Everything OK? Checking the line with LCP....455
6.12.3 Assigning IP addresses via PPP....456
6.12.4 Settings in the PPP list....456
6.12.5 The meaning of the DEFAULT remote site....459
6.12.6 RADIUS authentication of PPP connections....459
6.12.7 32 additional gateways for PPTP connections....460
6.13 DSL connection establishment using PPTP....461
6.13.1 Configuring PPTP....461
6.14 Permanent connection for flat rates – keep-alive....462
6.14.1 Configuring the keep-alive function....462
6.15 Data volumes on the WAN interface....462
6.15.1 Configuring data volume budgets....463
6.15.2 Budget analysis....465
6.16 Manual definition of the MTU....466
6.16.1 Configuration....466
6.16.2 Statistics....466
6.17 The Rapid Spanning Tree Protocol....467
6.17.1 Classic and rapid spanning tree....467
6.17.2 Improvements from rapid spanning tree....467
6.17.3 Configuring the Spanning Tree Protocol....468
6.17.4 Status reports via the Spanning Tree Protocol....469

6.18 The Action table....471
6.18.1 Introduction....471
6.18.2 Actions for Dynamic DNS....471
6.18.3 Further example actions....475
6.18.4 Configuration....476
6.19 Using the serial interface in the LAN....480
6.19.1 Introduction....480
6.19.2 Operating modes....480
6.19.3 Serial interface configuration....481
6.19.4 Configuring the COM port server....481
6.19.5 WAN device configuration....486
6.19.6 Serial connection status information....486
6.19.7 COM-port adapters....489
6.20 IGMP / MLD snooping....489
6.20.1 Introduction....489
6.20.2 IGMP/MLD snooping operation....490
6.20.3 IGMP/MLD snooping through multiple bridges....491
6.20.4 Configuration....494
6.20.5 IGMP/MLD status....498
6.21 eSIM....500
6.21.1 Configuration....502
6.21.2 CLI Configuration....503
6.22 Configuring WWAN access....504
6.23 Switching between mobile profiles or SIM cards....510
6.24 BGPv4....510
6.24.1 Border Gateway Protocol version 4 (BGPv4)....510
6.24.2 Best-path selection algorithm....534
6.24.3 Tutorial: Setting up BGPv4 under LANconfig....535
6.24.4 Tutorial: Setting preferences for prefixes....540
6.24.5 Tutorial: Setting the Community attribute....542
6.24.6 Tutorial: Filtering received prefixes....544
6.25 OSPF....546
6.25.1 Setting up OSPF with LANconfig....547
6.25.2 Show commands via CLI....558
6.26 Bidirectional Forwarding Detection (BFD)....559
6.26.1 Profiles....559
6.26.2 Key-Chains....560
6.26.3 Show commands via CLI....561
6.27 BGP RPKI-RTR....561
6.27.1 Configuring RPKI....562
6.27.2 The CLI show commands....563
6.28 Locator / ID Separation Protocol (LISP)....564
6.28.1 Configuration....565
6.28.2 LISP tutorial....571

6.29 Route monitor....574
6.29.1 Configuring the route monitor with LANconfig....575
6.30 DSLoL for WLAN routers....575
6.31 WWAN bridge mode....576
6.31.1 Configuration....577
6.31.2 WWAN Bridge Mode Tutorial....578
7 IPv6....582
7.1 IPv6 basics....582
7.1.1 Why use IPv6-standard IP addresses?....582
7.1.2 IP address structure according to the IPv6 standard....582
7.1.3 Stages of migration....583
7.2 Basic settings....583
7.2.1 LAN interfaces....584
7.2.2 WAN profiles....586
7.2.3 RAS templates....588
7.2.4 IPv6 addresses....589
7.2.5 IPv6 parameters....591
7.2.6 Loopback addresses....591
7.2.7 Setting up IPv6 Internet access....592
7.3 Router-Advertisement....600
7.3.1 Interface options....601
7.3.2 Prefix list....602
7.3.3 Prefix pools....603
7.3.4 DNS options....604
7.3.5 Route options....605
7.3.6 PREF64 options....605
7.3.7 Router advertisement snooping....606
7.4 DHCPv6....607
7.4.1 DHCPv6 server....608
7.4.2 DHCPv6 client....615
7.4.3 DHCPv6 Relay Agent....618
7.4.4 Lightweight DHCPv6 Relay Agent (LDRA)....619
7.5 IPv6 firewall....620
7.5.1 Feature....620
7.5.2 Configuration....620
7.5.3 IPv6 firewall log table....636
7.6 IPv6 tunnel technologies....637
7.6.1 6to4 tunnel....637
7.6.2 6in4 tunnel....638
7.6.3 6rd tunnel....639
7.6.4 Dual-Stack Lite (DS-Lite)....639
7.6.5 464XLAT....639
7.6.6 Setting up tunnels....641
8 Firewall....650

8.1 Threat analysis....650
8.1.1 The dangers....650
8.1.2 The paths of the attackers....650
8.1.3 The methods....651
8.1.4 The victims....651
8.2 What is a firewall?....652
8.2.1 The tasks of a firewall....652
8.2.2 Different types of firewalls....653
8.3 The firewall in the device....656
8.3.1 How the firewall inspects data packets....656
8.3.2 Special protocols....658
8.3.3 General settings of the firewall....660
8.3.4 Parameters of the firewall rules....666
8.3.5 Alert functions of the firewall....670
8.3.6 Strategies for configuring the firewall....672
8.3.7 Tips for setting the firewall....674
8.4 Configuring the firewall with LANconfig....676
8.4.1 Definition of firewall objects....676
8.4.2 Defining firewall rules....679
8.5 Configuring firewall rules from the command line....681
8.5.1 Rules....681
8.5.2 Object table....681
8.5.3 Action table....682
8.6 Firewall diagnosis....682
8.6.1 The firewall table....682
8.7 Firewall limitations....688
8.8 Protection against break-in attempts: Intrusion detection....688
8.8.1 Examples of attempted break-ins....688
8.8.2 Configuring the IDS....689
8.9 Protection against “Denial-of-Service” attacks....689
8.9.1 Increased DoS threshold value for central devices....689
8.9.2 Examples of Denial-of-Service attacks....690
8.9.3 Configuring DoS blocking....692
8.9.4 Configuring ping blocking and stealth mode....692
8.10 WAN policy-based NAT....693
8.10.1 Configuring policy-based NAT with firewall rules....693
9 Quality of Service....697
9.1 What is QoS used for?....697
9.2 Which data packets to prefer?....697
9.2.1 What is DiffServ?....698
9.2.2 Guaranteed minimum bandwidth....698
9.2.3 Limited maximum bandwidths....699
9.3 The queue concept....699
9.3.1 Queues in the send direction....699

9.3.2 Queues in the receiving direction....699
9.4 Reducing the packet length....700
9.5 QoS parameters for Voice-over-IP applications....701
9.6 QoS in send or receive direction....705
9.7 QoS configuration....706
9.7.1 Evaluate DiffServ Field in the Firewall....706
9.7.2 Defining minimum and maximum bandwidths....707
9.7.3 Setting transmission rates for interfaces....707
9.7.4 Sending and receiving direction....712
9.7.5 Reducing the packet length....712
9.8 Quality-of-Service (QoS) with 8 queues....713
9.8.1 Queues....714
9.8.2 Queue lists....716
9.8.3 Interfaces....717
9.8.4 Congestion Action....717
9.8.5 Example 1: Configuring a QoS concept with four classes....718
9.8.6 Example 2: Configuring a QoS concept on the VDSL connection with two QoS classes....721
9.8.7 Queue usage in the firewall....722
9.9 QoS for WLANs according to IEEE 802.11e (WMM/WME)....726
10 Multicast routing....727
10.1 General multicast show commands....727
10.2 General settings....728
10.2.1 IPv4 filter lists....728
10.2.2 IPv6 filter lists....728
10.3 IGMP (Internet Group Management Protocol)....729
10.3.1 IGMP parameters....730
10.3.2 SSM range....731
10.3.3 IGMP proxy....731
10.3.4 Static IPv4 multicast routing....732
10.3.5 SSM source IP list....733
10.3.6 Tutorial: Setting up an IGMP proxy....733
10.4 MLD (Multicast Listener Discovery)....734
10.4.1 MLD parameters....734
10.4.2 SSM range....736
10.4.3 MLD proxy....736
10.4.4 Static IPv6 multicast routing....737
10.4.5 SSM source IP list....738
10.5 PIM (Protocol Independent Multicast)....738
10.5.1 Interfaces....740
10.5.2 IPv4 RP list....742
10.5.3 IPv4 SSM list....742
10.5.4 IPv4 SSM mapping....743
10.5.5 IPv6 RP list....744

10.5.6 IPv6 SSM list....744
10.5.7 IPv6 SSM mapping....745
10.6 Further Multicast Protocols....745
10.6.1 Bonjour proxy....745
11 Virtual Private Networks – VPN....751
11.1 What does VPN offer?....751
11.1.1 Conventional network infrastructure....751
11.1.2 Networking via the Internet....752
11.1.3 Private IP addresses on the Internet?....752
11.1.4 Secure communications via the Internet?....753
11.2 The VPN module at a glance....754
11.2.1 VPN example application....754
11.2.2 Functions of the VPN module....754
11.3 VPN connections in detail....755
11.3.1 LAN-LAN links....755
11.3.2 Dial-in connections (Remote Access Service)....756
11.4 What is LANCOM Dynamic VPN?....757
11.4.1 A look at IP addressing....757
11.4.2 This is how LANCOM Dynamic VPN works....757
11.5 Configuring VPN connections....759
11.5.1 VPN tunnel: Connections between VPN gateways....759
11.5.2 Set up VPN connections with the Setup Wizard....760
11.5.3 1-Click-VPN for networks (site-to-site)....761
11.5.4 1-Click-VPN for the LANCOM Advanced VPN Client....762
11.5.5 Inspecting VPN rules....763
11.5.6 Manually setting up VPN connections....763
11.5.7 IKE config mode....764
11.5.8 Diagnosis of VPN connections....765
11.6 Working with digital certificates....766
11.6.1 Basics....766
11.6.2 Advantages of certificates....769
11.6.3 Structure of certificates....770
11.6.4 Security....771
11.6.5 Certificates for establishing VPN connections....772
11.6.6 Certificates from certificate service providers....773
11.6.7 Establishing a proprietary CA....773
11.6.8 Requesting a certificate with Stand-alone Windows CA....773
11.6.9 Export the certificate to a PKCS#12 file....775
11.6.10 Create certificates with OpenSSL....778
11.6.11 Uploading certificates to the device....780
11.6.12 Saving and uploading certificates with LANconfig....781
11.6.13 Extended certificate support....782
11.6.14 Set up VPN connections to support certificates....784
11.6.15 Set up certificate-based VPN connections with the Setup Wizard....787

11.6.16 Setting up the LANCOM Advanced VPN Client for certificate connections....789
11.6.17 Simplified RAS with certificates....792
11.6.18 Simplified network connection with certificates – proadaptive VPN....793
11.6.19 Request certificates using CERTREQ....793
11.6.20 Certificate revocation list – CRL....793
11.6.21 Wildcard matching of certificates....795
11.6.22 Diagnosis of VPN certificate connections....796
11.6.23 OCSP client for certificate validation....796
11.7 Multi-level certificates for SSL/TLS....797
11.7.1 Introduction....797
11.7.2 SSL/TLS with multi-level certificates....797
11.7.3 VPN with multi-level certificates....797
11.8 Certificate enrollment via SCEP....798
11.8.1 SCEP server and SCEP client....798
11.8.2 Distributing certificates....798
11.8.3 Configuration of SCEP....800
11.8.4 Using smart certificates....805
11.9 NAT Traversal (NAT-T)....818
11.10 Extended Authentication Protocol (XAUTH)....820
11.10.1 Introduction....820
11.10.2 XAUTH in the firmware....820
11.10.3 Configuration of XAUTH....821
11.10.4 XAUTH with external RADIUS servers....822
11.11 Backup via alternative VPN connection....823
11.11.1 Introduction....823
11.11.2 Backup-capable network infrastructure....824
11.11.3 Configuring the VPN backup....827
11.12 Automatic configuration synchronization (Config Sync) with the LANCOM VPN High Availability Clustering XL option....829
11.13 IPSec over HTTPS....830
11.13.1 Introduction....830
11.13.2 Configuring IPsec-over-HTTPS technology....830
11.13.3 Status displays of the IPsec-over-HTTPS technology....832
11.14 MPPE for PPTP tunnels....832
11.15 Layer-2 tunneling protocol (L2TP)....833
11.15.1 Configuring the L2TP tunnel....834
11.15.2 Authentication via RADIUS....838
11.15.3 Operation as an L2TP access concentrator (LAC)....840
11.15.4 Operation as an L2TP network server (LNS) with authentication via RADIUS....842
11.15.5 Operation as the L2TP network server (LNS) for RAS clients....844
11.15.6 Configuring a WLAN scenario for bridging payload data to the central site....845

11.16 VPN connections: High availability with “load balancing”....848
11.16.1 Multiple VPN gateway addresses....848
11.16.2 Grouping and prioritization of alternative gateways....849
11.17 How does VPN operate?....854
11.17.1 IPsec – the foundation of VPN....854
11.17.2 Alternatives to IPsec....855
11.18 The standards behind IPsec....855
11.18.1 IPsec modules and their tasks....856
11.18.2 Security Associations – numbered tunnels....856
11.18.3 Encryption of the packets – the ESP protocol....856
11.18.4 Key management – IKE....857
11.18.5 Replay detection....858
11.19 IKEv2....858
11.19.1 Configuring IKEv2 with LANconfig....859
11.19.2 Two-factor authentication in the VPN....900
11.19.3 RADIUS support for IKEv2....903
11.19.4 Tutorial: Setting up IKEv2 under LANconfig....909
11.19.5 Tutorial: Setting up a certificate-based IKEv2 VPN connection (RSA)....914
11.19.6 Tutorial: Setting up a certificate-based IKEv2 VPN connection (digital signature)....921
11.19.7 Tutorial – EAP client at an EAP server....928
11.20 LANconfig application concepts....930
11.20.1 1-Click-VPN for networks (site-to-site)....930
11.20.2 1-Click-VPN for the Advanced VPN Client....931
11.21 WireGuard....931
11.21.1 Licensing....932
11.21.2 Configuration....932
11.21.3 Configuration with LANconfig....933
12 Virtual LANs (VLAN)....938
12.1 What is a virtual LAN?....938
12.2 VLAN and how it works....938
12.2.1 Frame tagging....939
12.2.2 Implementation in the LAN interfaces....940
12.2.3 Example applications....940
12.3 Configuration of VLANs....942
12.3.1 General settings....943
12.3.2 The network table....945
12.3.3 The port table....945
12.4 Configurable VLAN IDs....946
12.4.1 Different VLAN IDs per WLAN client....946
12.4.2 VLAN IDs for DSL interfaces....947
12.4.3 Special VLAN IDs for DSLoL interfaces....947
12.5 VLAN tags on layer 2/3 in the Ethernet....948
12.5.1 Introduction....948

12.5.2 Configuring VLAN tagging on layer 2 / 3....948
13 Wireless LAN – WLAN....950
13.1 Introduction....950
13.2 Application scenarios....950
13.2.1 Infrastructure mode....951
13.2.2 Hotspot or guest access....951
13.2.3 Managed mode....952
13.2.4 WLAN bridge (point-to-point)....952
13.2.5 WLAN bridge in relay mode....953
13.2.6 WLAN bridge to the AP – managed and unmanaged mixed....953
13.2.7 Wireless distribution system (point-to-multipoint)....954
13.2.8 Client mode....954
13.2.9 Client mode with mobile objects in industry....955
13.3 WLAN standards....955
13.4 WLAN security....956
13.4.1 Basics....956
13.4.2 WPA3 (Wi-Fi Protected Access 3)....957
13.4.3 IEEE 802.11i / WPA2....959
13.4.4 TKIP and WPA....962
13.4.5 WEP....963
13.4.6 LANCOM Enhanced Passphrase Security (LEPS)....963
13.4.7 Background WLAN scanning....967
13.4.8 Starting an environment scan at a configurable time....967
13.4.9 Replay-attack recognition....968
13.4.10 WLAN protected management frames (PMF)....969
13.5 LANCOM Active Radio Control (ARC)....971
13.5.1 Adaptive RF Optimization....972
13.5.2 Airtime Fairness....975
13.5.3 WLAN band steering....977
13.5.4 Client Management....978
13.5.5 Adaptive noise immunity for reducing interference on the WLAN....982
13.5.6 Spectral scan....983
13.6 Dynamic frequency selection (DFS)....987
13.6.1 DFS configuration....988
13.7 APSD – Automatic Power Save Delivery....990
13.7.1 Introduction....990
13.7.2 Configuration....990
13.7.3 Statistics....991
13.8 WLAN routing (isolated mode)....991
13.9 IEEE 802.11e user priority converted into VLAN tags....992
13.10 Establishing WLAN bridges....992
13.10.1 Configuring WLAN bridges....992
13.10.2 Setting up WLAN bridges with LANmonitor....993
13.10.3 Geometric dimensioning of outdoor wireless network links....994

13.10.4 Antenna alignment for P2P operations....997
13.10.5 Surveys for wireless bridges....999
13.10.6 Activating point-to-point operation mode....999
13.10.7 Configuration of P2P connections....1000
13.10.8 LEPS-MAC for P2P connections....1002
13.10.9 Access points in relay mode....1003
13.11 Adaptive transmission power....1004
13.12 Opportunistic key caching (OKC)....1004
13.12.1 Encrypted OKC via IAPP....1004
13.13 Fast roaming....1005
13.13.1 Fast roaming with IAPP....1006
13.14 Bandwidth limitations in the WLAN....1007
13.14.1 Operating as an access point....1007
13.14.2 Operating as a Client....1008
13.14.3 Bandwidth restriction of the LAN interfaces....1009
13.15 Automatic adjustment of multicast and broadcast transmission rates....1010
13.16 LANCOM "Wireless Quality Indicators" (WQI)....1010
13.17 Configuring the WLAN parameters....1011
13.17.1 General WLAN settings....1011
13.17.2 The physical WLAN interfaces....1012
13.17.3 The logical WLAN interfaces....1023
13.17.4 Point-to-point....1038
13.17.5 Point-to-point partners....1039
13.17.6 Expert WLAN settings....1040
13.17.7 Configurable data rates per WLAN module....1045
13.17.8 RTLS (real-time location system)....1047
13.17.9 IEEE 802.11k Roaming Targets....1050
13.17.10 WLAN data trace....1051
13.17.11 Client Management....1052
13.17.12 WLAN security....1056
13.17.13 Selecting approved stations for the WLAN....1064
13.17.14 Encryption settings....1069
13.17.15 IEEE 802.1X / EAP....1072
13.17.16 IEEE 802.11u and Hotspot 2.0....1076
13.17.17 Static WLAN controller....1094
13.17.18 Advanced WLAN parameters....1095
13.17.19 Location-based services (LBS)....1098
13.18 Configuring the client mode....1103
13.18.1 Enabling client mode with LANconfig....1104
13.18.2 Client settings....1104
13.18.3 Radio settings....1105
13.18.4 Setting the SSID of the available network....1106
13.18.5 Encryption settings....1106
13.18.6 PMK caching in the WLAN client mode....1107

13.18.7 Pre-authentication in WLAN-client mode....1108
13.18.8 Multiple WLAN profiles in client mode....1108
13.18.9 Roaming....1109
14 WLAN management....1112
14.1 Initial situation....1112
14.2 Technical concepts....1112
14.2.1 WLC features in the LANCOM vRouter....1112
14.2.2 The CAPWAP standard....1113
14.2.3 Smart controller technology....1113
14.2.4 Communication between access point and WLAN controller....1115
14.2.5 Zero-touch management....1117
14.2.6 Split management....1117
14.2.7 Protection against unauthorized CAPWAP access from the WAN....1117
14.3 Basic configuration of the WLAN controller function....1118
14.3.1 Setting the time information for the WLAN controller....1118
14.3.2 Example: Default configuration....1118
14.3.3 Assigning the default configuration to the new access points....1122
14.3.4 Configuring the access points....1123
14.4 Configuration....1124
14.4.1 General settings....1124
14.4.2 Profiles....1124
14.4.3 Access point configuration....1142
14.4.4 IP-dependent auto configuration and tagging of APs....1177
14.5 Access point administration....1179
14.5.1 Accepting new access points into the WLAN infrastructure manually....1179
14.5.2 Manually removing access points from the WLAN infrastructure....1181
14.5.3 Deactivating access points or permanently removing them from the WLAN infrastructure....1181
14.6 Central firmware and script management....1182
14.6.1 General settings for firmware management....1183
14.7 RADIUS....1186
14.7.1 Checking WLAN clients with RADIUS (MAC filter)....1187
14.7.2 External RADIUS server....1188
14.7.3 Dynamic VLAN assignment....1190
14.7.4 Activating RADIUS accounting for logical WLANs in the WLAN controller...1191
14.8 Displays and commands in LANmonitor....1193
14.9 RF optimization....1194
14.9.1 Group-related radio field optimization....1195
14.10 Client steering by WLC....1196
14.10.1 Configuration....1197
14.11 Channel-load display in WLC mode....1200
14.12 Backing up the certificates....1201
14.12.1 Create backups of the certificates....1201
14.12.2 Uploading a certificate backup into the device....1202

14.12.3 Backing up and restoring further files from the SCEP-CA....1203
14.12.4 One-click backup of the SCEP-CA....1203
14.12.5 Using LANconfig to backup and restore certificates....1204
14.13 Backup solutions....1205
14.13.1 WLC cluster....1205
14.13.2 Backup with redundant WLAN controllers....1209
14.13.3 Backup with primary and secondary WLAN controllers....1211
14.13.4 Primary and secondary controllers....1211
14.13.5 Automatic search for alternative WLCs....1212
14.13.6 One-click backup of the SCEP-CA....1212
14.14 Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option....1213
14.14.1 Special LANconfig icon for devices in a cluster or using Config Sync....1214
14.14.2 Special LANmonitor icon for devices in a cluster or using Config Sync....1215
15 Public Spot....1216
15.1 Introduction....1216
15.1.1 What is a Public Spot?....1216
15.1.2 Application scenarios....1217
15.1.3 Overview of the Public Spot module....1224
15.2 Setup and operation....1226
15.2.1 Basic configuration....1227
15.2.2 Security settings....1250
15.2.3 Extended functions and settings....1252
15.2.4 Alternative login methods....1274
15.2.5 Internal and customized voucher and authentication pages (templates)....1307
15.2.6 Viewing Public Spot clients....1328
15.2.7 Displaying advertising to Public Spot users....1328
15.3 Access to the Public Spot....1329
15.3.1 Requirements for logging in....1329
15.3.2 Logging in to the Public Spot....1330
15.3.3 Session information....1331
15.3.4 Logging out of the Public Spot....1331
15.3.5 Advice and help....1332
15.4 Tutorials for setting up and using Public Spots....1333
15.4.1 Virtualization and guest access via WLAN controller with VLAN....1333
15.4.2 Virtualization and guest access via WLAN controller without VLAN....1343
15.4.3 Setting up a secure hotspot with Enhanced Open....1357
15.4.4 Setting up an external RADIUS server for user administration....1357
15.4.5 Internal and external RADIUS servers combined....1358
15.4.6 Checking WLAN clients with RADIUS (MAC filter)....1362
15.4.7 Setting up an external SYSLOG server....1363
15.5 XML interface....1364
15.5.1 Feature....1365
15.5.2 Setting up the XML interface....1366

15.5.3 Analyzing the XML interface using cURL....1367
15.5.4 Commands....1368
15.6 Appendix....1374
15.6.1 Commonly transmitted RADIUS attributes....1374
15.6.2 RADIUS attributes transmitted via WISPr....1379
16 Voice over IP – VoIP....1380
16.1 Introduction....1380
16.2 VoIP implementation in LANCOM VoIP routers....1381
16.2.1 Example applications....1381
16.2.2 The central position of the LANCOM VoIP router....1384
16.3 Call switching: Call routing....1386
16.3.1 SIP proxy and SIP gateway....1387
16.3.2 User registration at the SIP proxy....1387
16.3.3 Number translation at network transitions....1390
16.3.4 The Call Manager....1390
16.3.5 Telephony with LANCOM VoIP routers....1391
16.3.6 Hold call, swap call, transfer call....1394
16.3.7 Transmission of DTMF tones....1394
16.4 Configuring the VoIP parameters....1396
16.4.1 General settings....1396
16.4.2 Line configuration....1397
16.4.3 Configuration of users....1416
16.5 Call Manager Configuration....1428
16.5.1 Process of call routing....1428
16.5.2 Handling the calling party ID....1428
16.5.3 Call-routing table parameters....1430
16.5.4 Signaling parallel calls in the ISDN....1436
16.5.5 Extended settings....1437
16.6 Telephony (PBX) functions in LANCOM VoIP routers....1438
16.6.1 Transfer and forward call....1439
16.6.2 Spontaneous call management by the user....1442
16.6.3 Configure permanent call forwarding....1444
16.6.4 Call forwarding (call deflection / partial rerouting) at the SIP trunk (SIP 302)....1445
16.6.5 Fax via T.38 – Fax over IP (FoIP)....1445
16.6.6 Hunt groups with call distribution....1446
16.6.7 Multiple logins (multi login)....1448
16.7 VoIP media proxy – Optimized management for SIP connections....1448
16.8 SIP-ID as switchboard number with trunk lines....1450
16.9 Switching at the SIP provider....1451
16.10 SIP Application Layer Gateway (SIP ALG)....1452
16.10.1 Properties....1452
16.10.2 Configuration....1452
16.11 Restricting or preventing SIP registration over WAN....1453

16.12 Certificates for encrypted telephony....1453
16.13 Handling canonical telephone numbers....1455
16.14 Processing Destination Domains....1455
16.14.1 Registration at upstream exchanges....1455
16.14.2 Switching internal calls....1456
16.15 Configuring the ISDN interfaces....1456
16.15.1 Point-to-multipoint and point-to-point connections....1456
16.15.2 Bus termination....1457
16.15.3 Protocol settings....1457
16.15.4 ISDN connection timing....1457
16.16 Configuration examples....1458
16.16.1 VoIP telephony in stand-alone operation....1458
16.16.2 Using VoIP telephony to enhance the upstream ISDN PBX....1464
16.16.3 Connecting to an upstream SIP PBX....1471
16.16.4 VoIP connectivity between sites without a SIP PBX....1475
16.16.5 SIP trunking....1479
16.16.6 Block outgoing calls to service numbers....1481
16.16.7 Rejecting incoming calls....1482
16.16.8 Reject calls without a calling number....1483
16.16.9 Forwarding calls without a calling number....1484
16.17 Diagnosis of VoiP connections....1484
16.17.1 SIP traces....1484
16.17.2 Connection diagnosis with LANmonitor....1484
16.18 VoSIP support in the Voice Call Manager....1486
16.19 Auto provisioning LANCOM DECT 510 IP....1487
16.19.1 Configuring DECT base stations and handsets with LANconfig....1487
17 Backup solutions....1490
17.1 High availability of networks....1490
17.1.1 How is a network-connection disturbance detected?....1490
17.1.2 High-availability of lines – backup connections....1494
17.1.3 High-availability of gateways – redundant gateways with VPN load balancing....1496
17.1.4 High availability Internet access – Multi-PPPoE....1496
17.1.5 Example applications....1496
17.2 Backup solutions and load balancing with VRRP....1499
17.2.1 Introduction....1499
17.2.2 Virtual Router Redundancy Protocol....1499
17.2.3 Application scenarios....1504
17.2.4 Interaction with internal services....1506
17.2.5 VRRP in the WAN....1509
17.2.6 Interaction with the WAN backup module....1510
17.2.7 Control of WAN/WAN backup by VRRP....1510
17.2.8 Configuration of VRRPv3....1510
17.2.9 Status Information....1514

17.3 Interface bundling with LACP....1515
17.3.1 Configuring the LACP interfaces....1516
17.4 Support for vRouter redundancy in Amazon AWS....1517
17.4.1 Configuration....1518
17.4.2 Commands....1518
17.4.3 Configuring the IAM role in AWS....1519
18 RADIUS....1520
18.1 How RADIUS works....1521
18.2 Using RADIUS to login to the LCOS management GUI....1521
18.3 RADIUS as authenticator or network access server (NAS)....1522
18.3.1 General settings....1523
18.3.2 Dial-in using PPP and RADIUS....1523
18.3.3 Dial-in using WLAN and RADIUS....1525
18.3.4 Dial-in using a public spot and RADIUS....1527
18.3.5 Dial-in using 802.1X and RADIUS....1530
18.3.6 Additional source ports for access requests....1533
18.4 RADIUS server....1533
18.4.1 RADIUS service....1533
18.4.2 RADIUS / RADSEC clients....1534
18.4.3 User database....1536
18.4.4 Forwarding....1544
18.4.5 EAP authentication....1548
18.4.6 User-defined attributes....1550
18.4.7 Options....1551
18.5 RADIUS attributes....1551
18.5.1 RADIUS attributes configurable....1554
18.5.2 RADIUS attribute extensions for IPv6 RAS services....1555
18.6 Dynamic Peer Discovery....1556
18.7 Dynamic authorization by RADIUS CoA (Change of Authorization)....1557
18.7.1 Configuring dynamic authorization with LANconfig....1558
18.7.2 RADIUS CoA for 802.1X Authenticator Ethernet Ports....1559
18.8 RADSEC....1560
18.8.1 Configuring RADSEC for the client....1560
18.8.2 Certificates for RADSEC....1561
19 IoT – the Internet of Things....1562
19.1 Wireless ePaper....1562
19.1.1 Settings for Wireless ePaper....1564
19.2 iBeacon....1566
19.3 BLE scanner and beacon....1567
19.3.1 Settings for BLE....1567
19.3.2 Monitoring....1570
20 Other services....1571
20.1 Automatic IP address administration with DHCP....1571
20.1.1 Introduction....1571

20.1.2 Configuring DHCPv4 parameters with LANconfig....1572
20.1.3 Configuring DHCP clients....1585
20.1.4 DHCP-client option Classless Static Route....1585
20.1.5 DHCP relay server....1585
20.1.6 Displaying status information from the DHCP server....1586
20.1.7 DHCP cluster....1587
20.1.8 Alternative DHCP server for forwarding....1588
20.1.9 DHCP snooping and DHCP option 82....1588
20.1.10 Assigning IP addresses based on DHCP option 82....1589
20.1.11 Delivering LANCOM Management Cloud parameters with the DHCP server....1591
20.2 Domain Name Service (DNS)....1591
20.2.1 What does a DNS server do?....1592
20.2.2 DNS forwarding....1592
20.2.3 Setting up the DNS server....1593
20.2.4 Logging DNS queries with SYSLOG....1595
20.2.5 URL blocking....1596
20.2.6 DNS filter for DNS data tunnels....1597
20.2.7 Dynamic DNS....1598
20.3 Accounting....1599
20.3.1 Operating principles....1600
20.3.2 Switching accounting on or off on the fly....1601
20.3.3 Data traffic counting....1601
20.3.4 Configuring accounting....1601
20.4 Call charge management....1602
20.4.1 Connection limits for DSL and cable modem....1603
20.4.2 Settings in the charge module....1604
20.5 Time server for the local net....1604
20.5.1 Configuring the time server under LANconfig....1604
20.5.2 Configuring the NTP client....1607
20.5.3 Retrieving Device Time via GPS....1608
20.6 Scheduled Events....1609
20.6.1 Regular Execution of LCOS-Commands....1609
20.6.2 CRON jobs with time delay....1610
20.6.3 Configuring the scheduler....1610
20.7 PPPoE server....1611
20.7.1 VLAN Support....1612
20.7.2 Multiple Logins....1612
20.7.3 LCP Polling....1612
20.7.4 IPv6....1612
20.7.5 Supported Standard RADIUS Attributes....1613
20.7.6 Supported Vendor-Specific RADIUS Attributes....1614
20.7.7 Tutorial: Setting Up a PPPoE Server with a Local User Table for IPv4 and IPv6....1616

20.7.8 Tutorial: Setting Up a PPPoE Server with RADIUS for IPv4 and IPv6.....1621
20.7.9 Configuration.....1627
20.7.10 PPPoE snooping.....1629
20.8 Simple Network Management Protocol (SNMP).....1629
20.8.1 SNMPv3 basics.....1630
20.8.2 Configuring SNMP.....1631
20.9 Netflow / IPFIX.....1641
20.9.1 Configuring NetFlow / IPFIX.....1641
20.10 Operating printers at the USB connector of the device.....1644
20.10.1 Configuring the printer server in the device.....1644
20.10.2 Printer configuration at the computer.....1646
20.11 LANCOM Security Essentials.....1649
20.11.1 Introduction.....1649
20.11.2 Requirements for using LANCOM Security Essentials.....1650
20.11.3 Quick start.....1650
20.11.4 Standard settings in the Content Filter.....1651
20.11.5 General Settings.....1652
20.11.6 Settings for blocking.....1654
20.11.7 Override settings.....1658
20.11.8 Profiles in the Content Filter.....1660
20.11.9 Options for the Content Filter.....1665
20.11.10 Additional settings for the Content Filter.....1667
20.12 BPjM module.....1670
20.12.1 Recommendations for use.....1671
20.12.2 Menu action to delete the BPjM signature definition.....1672
20.13 TACACS+.....1672
20.13.1 Introduction.....1672
20.13.2 Configuring the TACACS+ parameters.....1673
20.13.3 Configuring the TACACS+ server.....1676
20.13.4 Login to the TACACS+ server.....1677
20.13.5 Assigning rights under TACACS+.....1679
20.13.6 Authorizing functions.....1679
20.13.7 Bypassing TACACS+.....1681
20.14 LLDP.....1682
20.14.1 How it works.....1682
20.14.2 Structure of LLDP messages.....1683
20.14.3 Supported operating systems.....1684
20.15 Sending and receiving SMS text messages.....1684
20.15.1 Receiving SMS text messages.....1684
20.15.2 Basic configuration of the SMS module.....1685
20.15.3 Managing SMS text messages with LANmonitor.....1685
20.15.4 Sending SMS text messages with LANmonitor.....1686
20.15.5 URL placeholder for sending SMS.....1686
20.15.6 Character set for sending SMS.....1687

20.15.7 Execute actions on incoming SMS....1688
20.16 Deactivating device LEDs – boot-persistent....1689
20.17 802.1X authenticator for Ethernet ports....1690
20.18 xDSL Interface....1692
20.18.1 ADSL/VDSL modem operation (bridge mode)....1692
20.18.2 Further XDSL settings....1694
20.19 GPON support....1695
20.20 ACME-Client....1696
20.20.1 ACME client configuration....1697
20.21 Operations, Administration, and Management (OAM)....1698
20.21.1 Ethernet Link OAM (IEEE 802.3ah)....1699
20.21.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731)....1700
20.22 Alive Test....1705
21 Appendix....1707
21.1 CRON syntax....1707
21.2 Factory default active services according to EN 18031 GEC-4....1707

Copyright

© 2026 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control, and AirLancer are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from LANCOM Systems include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 LCOS

The LANCOM Operating System (LCOS) is the firmware specifically developed for LANCOM routers, SD-WAN gateways, and WLAN controllers, forming the core of LANCOM Systems's reliable and secure network infrastructures. As a proprietary operating system, LCOS is continuously enhanced and regularly updated with new features and improvements.

LCOS stands for the highest security standards, backed by comprehensive quality assurance and independent certifications. The development and quality assurance of LANCOM Systems' solutions take place in Germany in accordance with high security standards. The "IT Security made in Germany" quality label of the German IT Security Association, as well as certifications from the Federal Office for Information Security (BSI), attest to the level of security achieved. Continuous evaluations and frequent updates ensure the highest level of security.

With future-proof hardware scalability, LANCOM products are designed for long-term use. Regular software updates—including security patches, feature updates, and major releases—ensure that even older devices can be operated securely and reliably for many years.

LCOS embodies the LANCOM core values:

- **Security**

  Every LCOS version is developed and tested with the utmost care. Additionally, LCOS undergoes regular security testing and external audits.

- **Reliability**

  Through continuous development and frequent updates, LCOS delivers maximum stability and availability throughout the entire product lifecycle.

- **Future-Proofing**

  In alignment with LANCOM's lifecycle policies, LCOS supports the long-term secure operation and evolution of network infrastructures through continuous feature and security updates.

With LCOS, businesses receive a proven, high-performance, and trustworthy foundation for professional networking solutions—developed and maintained in Germany.

2 Configuration

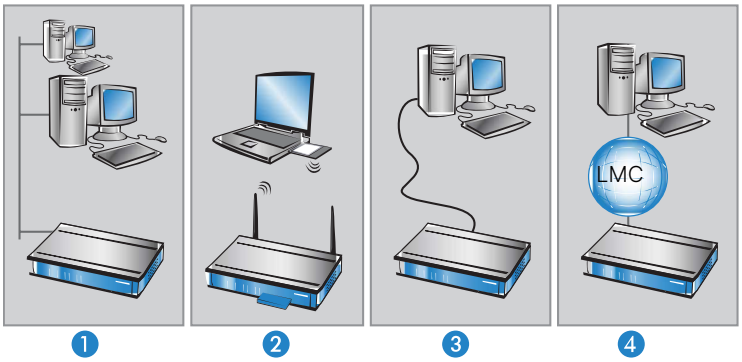
This chapter gives you an overview of the ways and means by which you can access the device and adjust its settings. It contains descriptions for the following topics:

- Configuration tools
- Control and diagnostic functions of the device and software
- Backing up and restoring complete configurations
- Installing new firmware on the device

2.1 Ways and means of configuration

The device supports different ways (i.e. interfaces) and means (i.e. software) of configuration. Depending on the available connections, the device can be accessed in different ways:

- Via the connected network ([W]LAN and [W]WAN; also named "inband") [1, 2];
- Via the serial configuration interface (config interface; also named "outband") [3];
- Via the LANCOM Management Cloud (LMC) (License required) [4].



How do these paths differ?

The access paths listed above differ in how they are accessed and in their hardware and software requirements:

- Inband configuration requires a suitable computer in the LAN, WAN or WLAN along with the appropriate software, such as LANconfig or a web browser when configuring with WEBconfig or LMC (cf. *Configuration software* on page 27). However, inband configuration will not work if the network is malfunctioning.
- Outband configuration is always available because it is a physical connection. Along with the configuration software, it also requires a computer with a serial interface.

2.2 Configuration software

There is no end of different situations in which configurations have to be carried out, or ways in which operators prefer to work. This is why the device offers a wide range of ways to set up the configuration:

- **LANconfig** – the menu-driven, clearly structured and easy way to set almost all parameters for a device. LANconfig requires a configuration PC with a current Windows operating system. Please refer to section *LANconfig – configuring devices* on page 173 for further information.
- **WEBconfig** – this software is an integral part of the device LCOS. This makes WEBconfig operating-system agnostic; all you need is a web browser on the configuration PC. Please refer to section *WEBconfig* on page 28 for further information.
- **LANCOM Management Cloud** – is the cloud-based management system that intelligently organizes, optimizes and controls your entire network architecture in WAN, LAN, WLAN and SECURITY. Please refer to section *LANCOM Management Cloud (LMC)* on page 43.
- **Terminal program** – as an alternative to LANconfig, you can also use terminal programs (such as HyperTerminal or PuTTY) to configure a device from the command line interface (CLI). Depending on the program's range of functions, either via the serial interface or an IP network can be used for communications. The protocols available within IP networks are Telnet, SSH and TFTP.
- **SNMP management program** – as an alternative to LANconfig, you can also use device-independent IP network management programs based on the SNMP protocol.

The following table shows the various ways that you can access the configuration:

Table 1: Overview of the configuration means in relation to the configuration paths

Used software	[W]LAN, [W]WAN (inband)	Config interface (outband)
LANconfig	Yes	Yes
WEBconfig	Yes	No
LANCOM Management Cloud	Yes	No
Serial client	No	Yes
Telnet client	Yes	No
SSH client	Yes	No
TFTP client	Yes	No
SNMP management program	Yes	No

Please note that all methods access the same configuration data. For example, any changes you make to the settings in LANconfig also directly effect the values under WEBconfig and Telnet.

2.2.1 LANconfig

Information on configuring the devices with LANconfig is available separately in the LANtools chapter *LANconfig – configuring devices* on page 173,

2.2.2 WEBconfig

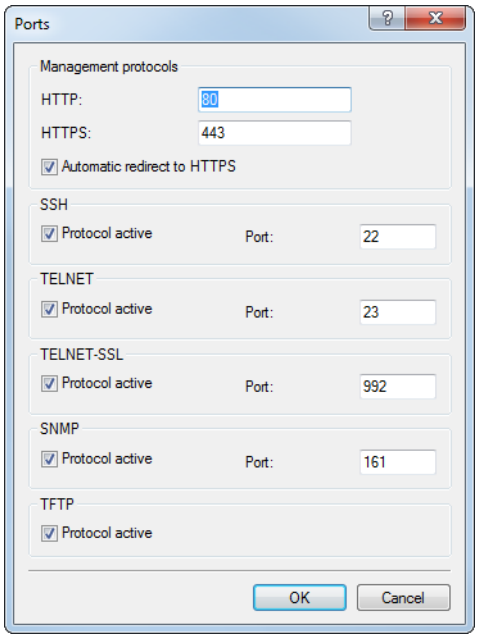
WEBconfig is the graphical user interface that offers direct access to the LCOS integrated into the device. This allows you to configure the devices remotely and irrespective of the operating system used on your computer. All you need to work with WEBconfig is a web browser.

2.2.2.1 Accessing the device with WEBconfig

To carry out a configuration with WEBconfig, you need to know how to contact the device. Device behavior and accessibility for configuration via a Web browser depend on whether the DHCP server and DNS server are active in the LAN already, and whether these two server processes share the assignment in the LAN of IP addresses to symbolic names. WEBconfig accesses the device either via its IP address, the device name (if configured), or by means of any name if the device has not yet been configured.

The browser uses the IP address or name to make an unencrypted connection request to the LANCOM device. This then automatically switches to an encrypted HTTPS connection. As a result, confidential data such as the login password or the configuration itself are secured with the encrypted connection.

If this feature has not been activated, you can enable it under **Management** > **Admin** > **Management protocols** > **Settings** > **Automatic redirect to HTTPS**.



Following power-on, unconfigured devices first check whether a DHCP server is already active in the LAN. Depending on the situation, the device can either enable its own DHCP server or enable DHCP client mode. In the second operating mode, the device can retrieve an IP address for itself from a DHCP server in the LAN.

If a WLAN device is centrally managed by a WLAN controller, the device switches the DHCP mode from auto to client mode when it is provisioned with the WLAN configuration.

2.2.2.2 Network without a DHCP server

In a network without a DHCP server, unconfigured devices enable their own DHCP server service when switched on and assign IP addresses, information on gateways, etc. to other computers in the LAN (provided they are set to automatic retrieval of IP addresses – auto DHCP). In this constellation, the device can be accessed by every computer with the auto DHCP function enabled with a web browser under IP address **172.23.56.254**.

With the factory settings and an activated DHCP server, the device forwards all incoming DNS requests to the internal web server. This means that a connection can easily be made to set up an unconfigured device by entering any name into the address bar of a web browser.



If the configuration computer does not retrieve its IP address from the DHCP server, determine the current IP address of the computer (with **Start** > **Run** > **cmd** and command **ipconfig** at the prompt under Windows 7 or higher, or with command **ifconfig** in the CLI under Linux). In this case, the device can be accessed with address **x.x.x.254** (the "x"s stand for the first three blocks in the IP address of the configuration computer).

2.2.2.3 Network with DHCP server

If a DHCP server for the assignment of IP addresses is active in the LAN, an unconfigured device disables its own DHCP server, switches to DHCP client mode and retrieves an IP address from the DHCP server in the LAN. However, this IP address is initially unknown and accessing the device depends on the name resolution:

- If the LAN also has a DNS server for name resolution and this communicates the IP address/name assignment to the DHCP server, the device can be reached by entering its MAC address, e.g. `00a057xxxxxx`.

  The MAC address on a sticker on the base of the device.

- If there is no DNS server in the LAN, or if it is not linked to the DHCP server, the device cannot be reached via the name. In this case you have the following options to determine the IP address of the device:
  - From another accessible device, use the WEBconfig function **Show/search other devices**, or alternatively the LANconfig function **Find devices**.
  - Find the IP address assigned by DHCP to the device with the aid of suitable tools, and try to access the device directly using this IP address.
  - Connect a computer to the device by means of the serial configuration interface and run a terminal program.

2.2.2.4 Logging in to the device

Call WEBconfig by using the IP address assigned by the DHCP server or the name assigned by the DNS server. When prompted for user name and password when accessing the device, enter your personal data in the appropriate fields. Observe the use of upper and lower case.

If you used the general configuration access (“root”), you only need to enter the corresponding **password**. The **login** box for the user name is preset in this case.

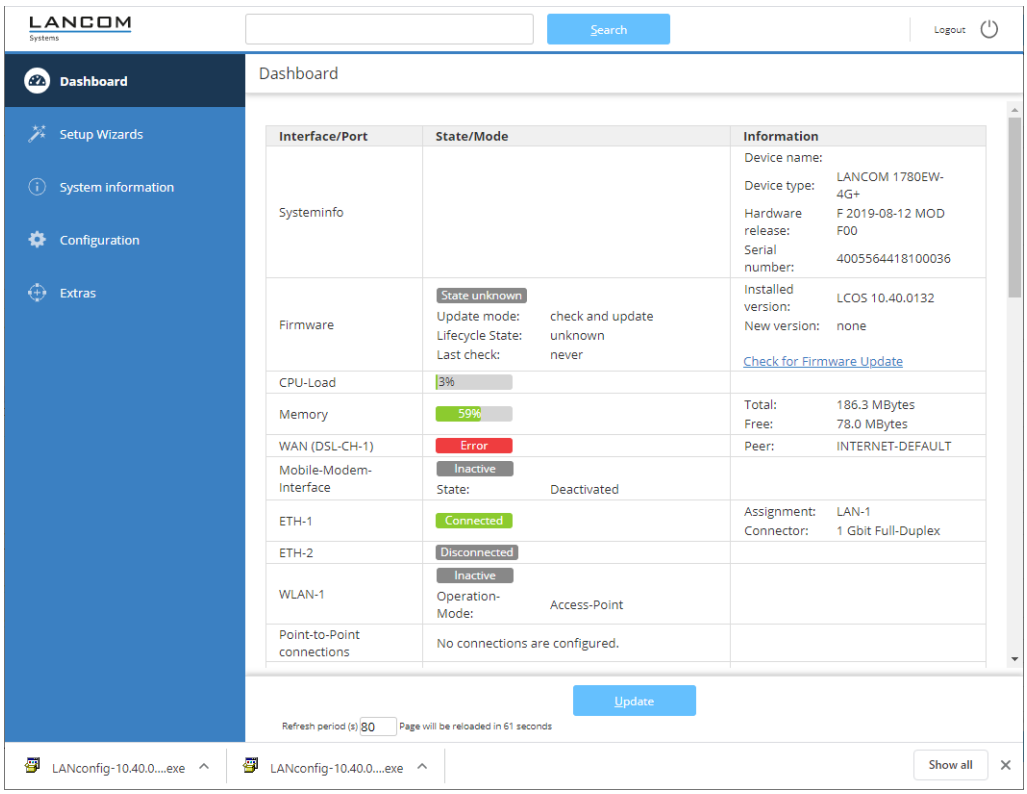
Always use the latest version of your browser to ensure maximum security. Also check that your browser is still in the current development branch, as some browsers only perform automatic updates in certain version ranges. Also, updates may be stopped when support for specific operating systems has expired. In this case, we strongly recommend that you switch to an alternative web browser.

2.2.2.5 Search

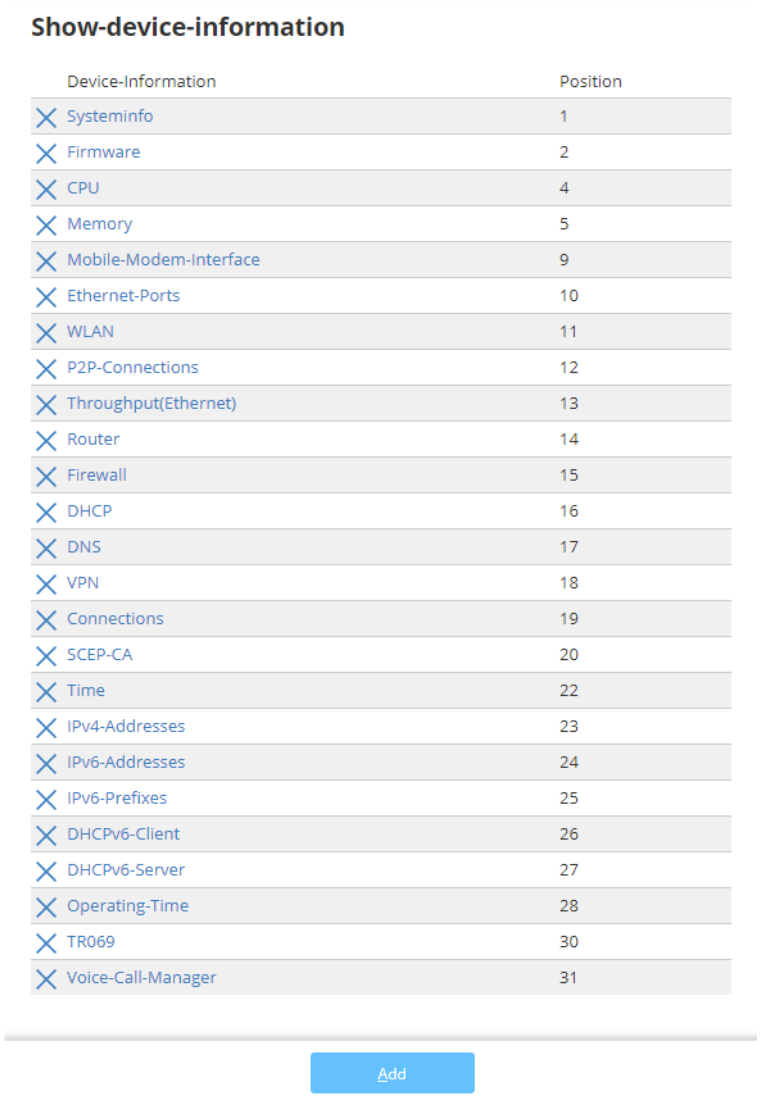
Use the search function in the upper area to search the entire menu tree for the word you enter. If you know the name for a particular status- or configuration parameter, but do not know which menu it is to be found in, you can quickly locate it in this way.

2.2.2.6 Dashboard

Here you will find comprehensive information on the current operating state of the device. This includes, for example, a visual representation of the interfaces with information on the networks active on them. Appropriate links can be used to call up further relevant statistics (such as DHCP table). For significant configuration deficiencies (such as invalid time setting), a direct link to the appropriate configuration parameters is provided.

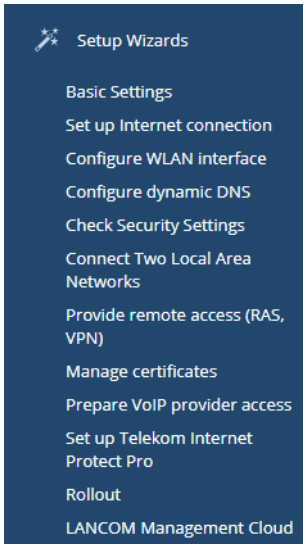


The amount of information shown on this screen can be defined under **Extras** > **LCOS menu tree** > **Setup** > **HTTP** > **Show-device-information**. An index number is also used to specify the display sequence.



2.2.2.7 Setup wizards

The setup wizards help you to make frequently used settings on a device quickly and easily. Select the wizard and enter the appropriate data on the following screens. The individual setup steps are identical to those in LANconfig.



The device does not save any settings until you confirm the entries on the final page of a wizard. Which wizards are available depends on the individual device type (access point, WLAN controller, etc.).

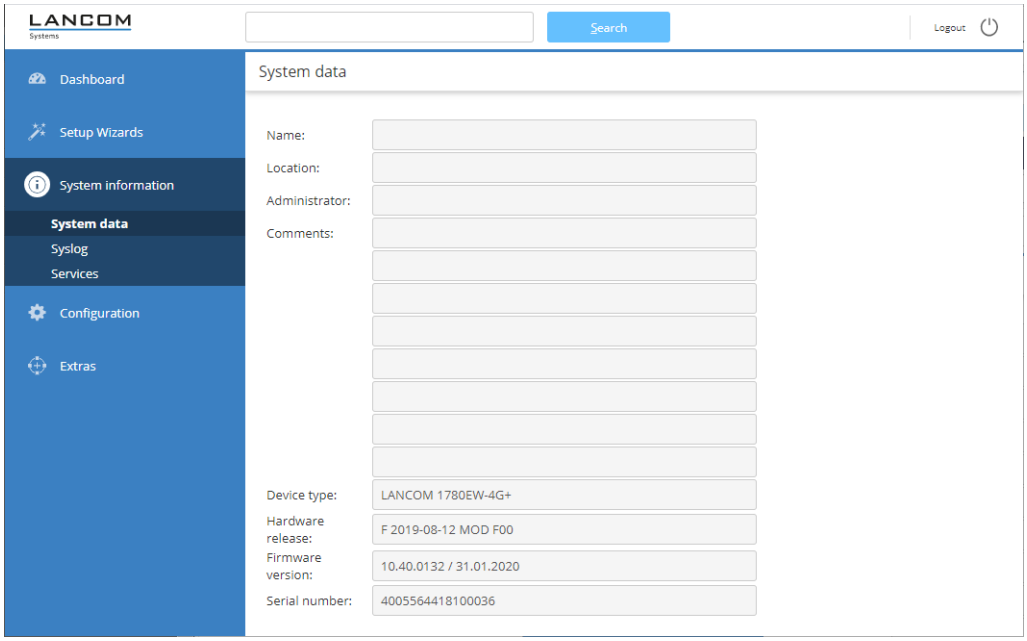
On devices featuring VPN, VPN client dial-in access accounts for the Advanced VPN Client can also be created with WEBconfig. The 1-Click VPN configuration is not available in WEBconfig due to restrictions on browser access.

2.2.2.8 System information

Your device features the menu area **System information**, which displays various important facts about the software and hardware of your device, the syslog table, and the services.

System data

Under **System information** > **System data** you will find general information about the device, its location, firmware version, serial number, etc.



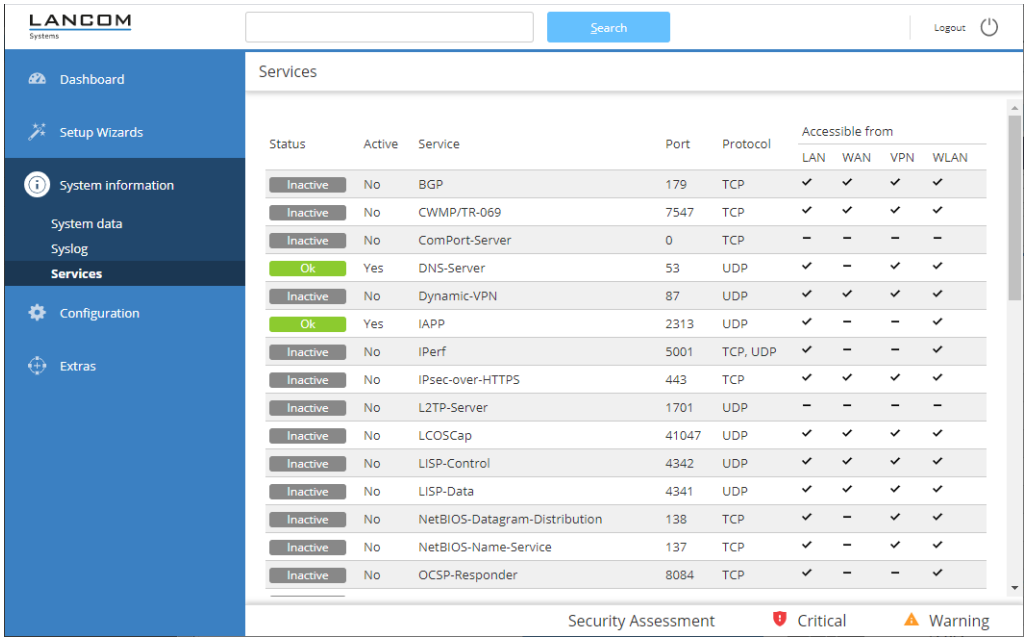
Syslog

The device stores syslog information in its main memory (see *The SYSLOG module* on page 324).

Timestamps starting with '1900- ...' indicate that the time has not been set or is set incorrectly.

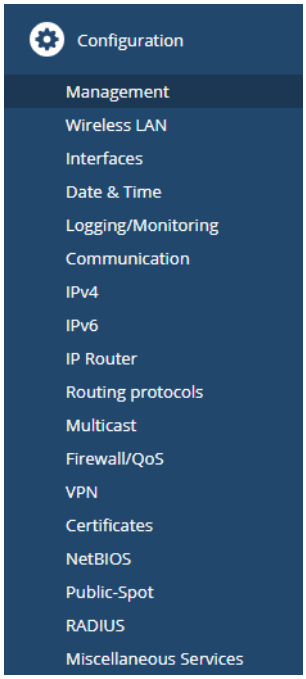
Services

Here you have an overview of the internal LCOS services, their ports and protocols, whether they are active, and how they can be reached.



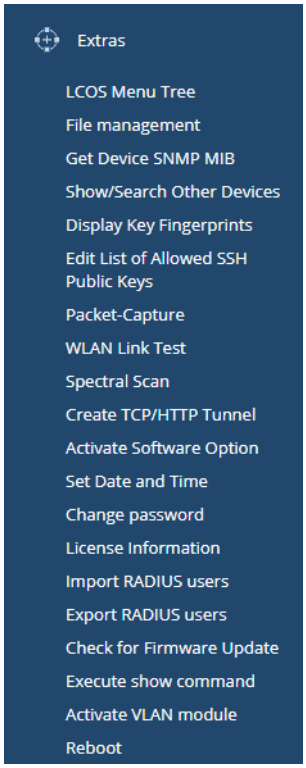
2.2.2.9 Configuration

The **Configuration** menu section provides the configuration parameters in the same structure as seen in LANconfig.



2.2.2.10 Extras

The **Extras** section contains various features that help to configure the device and, depending on the device at hand, it also provides some features and analysis modules that do not logically fit to the other menu items.



The scope of functions of this menu area varies depending on the device type.

LCOS menu tree

The **LCOS menu tree** sections presents the configuration and status parameters in the same structure as the command line. Each branch of the menu tree is divided into menu items, tables, parameters and actions. Tables contain sets of parameters, while menu items contain tables, individual parameters and actions.

Furthermore, the menu tree has a context-sensitive help system: Clicking on the question mark next to an entry calls up a separate help page for each menu item, table and parameter. You will find information about the individual entries in the Menu Reference Guide.

Status

The **Status** menu contains all of the status values stored by the device. Status values are stored in the corresponding status parameters and are for information purposes only. Values can be read out but not adjusted.

Some of the status values are directly or indirectly influenced by the parameter settings in the Setup menu and only actually contain values under certain setups. For example, the DHCP table only contains any values if the DHCP server in the device is enabled and in use. Other parts are not influenced by setup parameters, such as the hardware information, for example. Some menu items include actions or analysis functions that you need to perform manually before the device displays any results.

Setup

The **Setup** menu is used to modify and save all of the adjustable parameters in the device. The setup parameters are the most basic aspect of a device configuration: Any settings you make in LANconfig or WEBconfig are ultimately saved in the parameters of the Setup menu.

A large number of parameters are required for the proper operation of the device, but many of them never need to be adjusted: for example, standards and regulations require fixed upper and lower limits. For this reason, this menu also contains parameters which cannot be adjusted in LANconfig. Under most circumstances there is no need to change these parameters. However, in some cases it may be useful or even necessary to adjust certain default values to meet individual needs.

These "expert settings" often require deep background knowledge about the functionality and interrelationships of the different modules in the LCOS, and also of the technical standards. It is not unusual to have to change parameters in several places in the setup menu to reach a specific configuration. We therefore recommend that you only make changes in the Setup menu if the documentation or our Support explicitly requests this or if you are familiar with the technical standards and regulations behind a feature.

Firmware

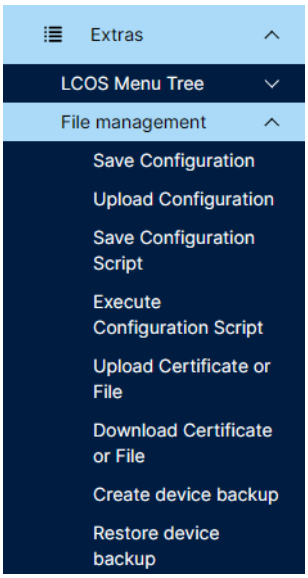
The **Firmware** menu provides information about the current firmware version, configures the Firmsafe feature and switches to an alternative firmware version if necessary (also read *FirmSafe* on page 93), and it allows new firmware to be uploaded to the device. Alternatively, you can use *File management* to load a different firmware into the device.

Other

Using this menu, you can manually set up or terminate the connection to a remote site, restart the device, and (from the CLI) upload a new firmware version.

File management

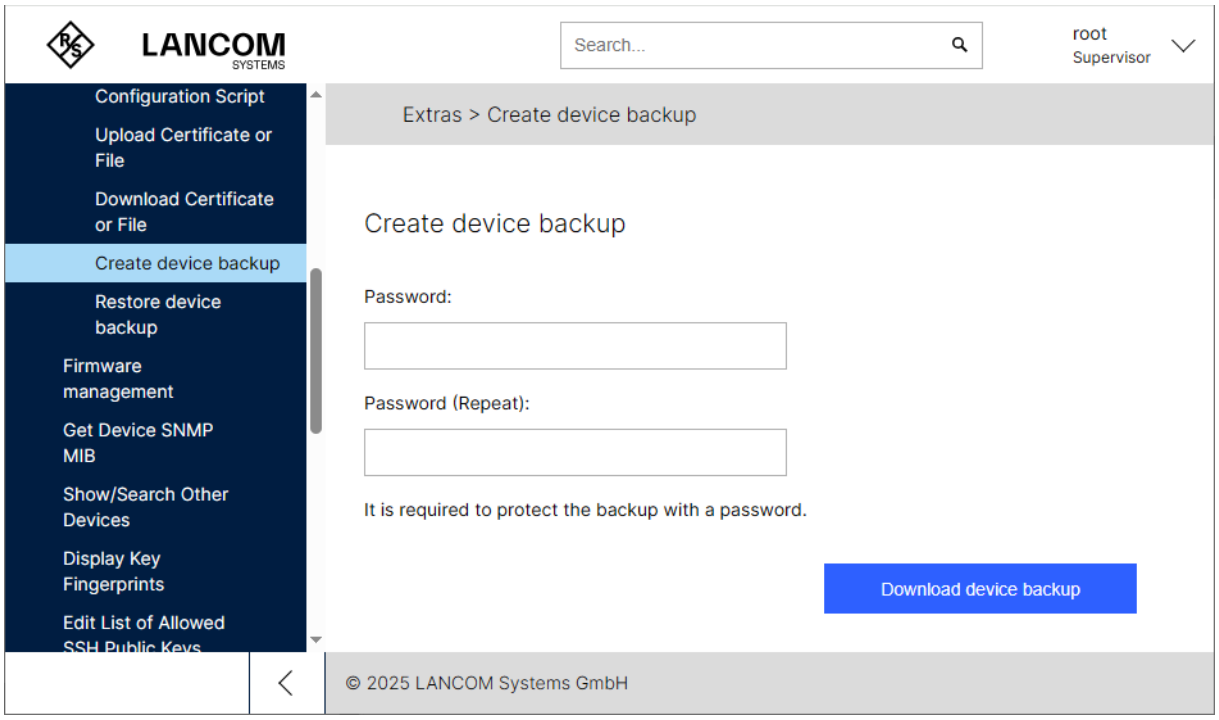
The **File management** section contains the various actions for uploading files to or downloading files from the device (i.e. configuration files and scripts, certificates, templates and logos). You can also use this to perform a backup or restore of the device.



Certificates or files that were uploaded to the device can be viewed in the Status menu under **File system**.

Device backup

Under **Extras** > **File management** > **Create device backup** or **Extras** > **File management** > **Restore device backup**, you can save important files in a password-protected ZIP archive. This file can later be uploaded back to the device for restoration.



The following functions/features, depending on the feature scope of the respective device, are included in the ZIP archive:

- encrypted configuration
- allowed SSH public keys
- known SSH hosts
- additional VPN CA certificates
- RADIUS accounting totals
- certificate list of the CA
- certificate serial number counter of the CA
- all Public Spot templates
- all Hotspot 2.0 provider icons
- WLC scripts (treated like regular files and stored unencrypted!)
- additional CA certificates for the alternate rollout configuration
- rollout wizard including template and logo
- custom wizards
- issue text
- SMS inbox and outbox
- IPerf TCP and UDP results

The following files are included, depending on the feature scope of the respective device:

- ssh_authkeys
- ssh_known_hosts
- vpn_add_cas
- radiuss_accnt_total
- scep_cert_list

- scep_cert_serial
- pbspot_template_welcome
- pbspot_template_login
- pbspot_template_error
- pbspot_template_start
- pbspot_template_status
- pbspot_template_logoff
- pbspot_template_help
- pbspot_template_noproxy
- pbspot_template_voucher
- pbspot_template_agb
- pbspot_template_reg_email
- pbspot_template_login_email
- pbspot_template_reg_sms
- pbspot_template_login_sms
- pbspot_formhdrimg
- pbspot_voucherimg_1
- pbspot_voucherimg_2
- pbspot_voucherimg_3
- pbspot_voucherimg_4
- pbspot_voucherimg_5
- pbspot_boxhdrimg
- pbspot_template_fallback
- pbspot_branding_logo
- hs20_prov_icon_1
- hs20_prov_icon_2
- hs20_prov_icon_3
- hs20_prov_icon_4
- hs20_prov_icon_5
- hs20_prov_icon_6
- hs20_prov_icon_7
- hs20_prov_icon_8
- hs20_prov_icon_9
- hs20_prov_icon_10
- hs20_prov_icon_11
- hs20_prov_icon_12
- hs20_prov_icon_13
- hs20_prov_icon_14
- hs20_prov_icon_15
- hs20_prov_icon_16
- WLC_Script_1.lcs
- WLC_Script_2.lcs
- WLC_Script_3.lcs
- default_add_cas
- rollout_wizard
- rollout_template
- rollout_logo
- user_wizard_1
- user_wizard_2

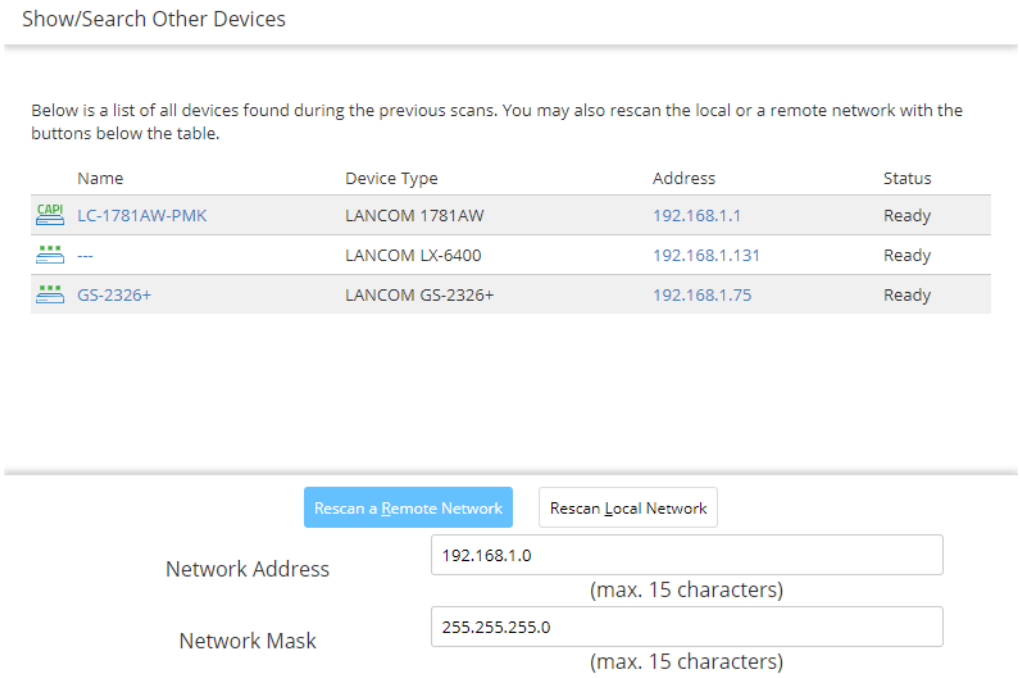
- user_wizard_3
- user_wizard_4
- issue
- shortmessaging_inbox
- shortmessaging_outbox
- iperf_tcp_last_result
- iperf_tcp_result_history
- iperf_udp_last_result
- iperf_udp_result_history

Retrieving the SNMP device MIB

This menu item allows you to download the device-specific *.mib file (management information base), which is required by alternative SNMP management software to monitor and manage the device. More information is available under *SNMP management program* on page 83.

Show / search other devices

Using the Show/Search function, you can search for other devices in your network and switch directly to the configuration page of the found devices via a corresponding link. This function is similar to the **Find devices** option in LANconfig.



Show key fingerprints

This page provides an overview of the fingerprints of all of the cryptographic keys in the device. Learn more about under *Device-internal SSH/SSL keys* on page 117.

Allowed SSH public keys

This page gives you an overview of the SSH public keys for public-key authentication that are accepted by the device. WEBconfig outputs the overview as a text field, which at any time can also be used to add additional keys and / or edit existing ones as an alternative to uploading a file in the File management section.

More about this topic and key syntax can be found in the chapter *Syntax and modifying public-key users* on page 122.

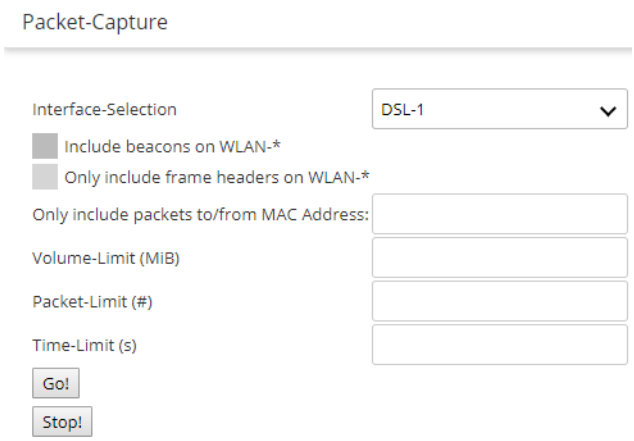
Enter new keys on a separate line; line breaks are not permitted in key strings.

Packet capturing

The command line tool `lcoscap` allows you to capture data packets to analyze any errors or problems. This command enables the capture of packets and writes the results to a file that you can open and analyze with a tool like "Wireshark".

LCOS offers you an additional, significantly more convenient method: In WEBconfig, go to **Extras** > **LCOS menu tree** > **Setup** > **WLAN** > **Packet-Capture** > **WLAN-Capture-Format** to select a file format used by the device to capture data packets on the selected interfaces and save them to a results file.

After setting the parameters, navigate to **Extras** > **Packet-Capturing** and click on **Go!** to start capturing packets. You can then open the generated file with a tool such as "Wireshark".



This method offers you several advantages:

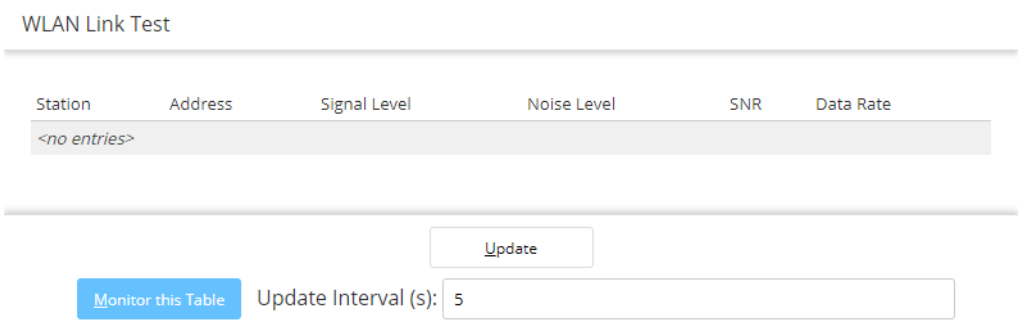
- You do not need any special software, because you can run WEBconfig on any Web browser.
- There is no need to input any CLI commands. Instead, you work with a convenient menu.
- If you use WEBconfig over HTTPS, the confidentiality and security of captured traffic is guaranteed.

Packet capturing works with IPv4 and IPv6 connections.

WLAN link test

This menu item is only available on devices with a WLAN module.

This page displays the results of the WLAN link test. The WLAN link test verifies the connection to connected WLAN clients.



Spectral Scan

This menu item is only available on certain devices.

Opens the configuration page for the Spectral Scan. Learn more about this feature under *Spectral scan* on page 983.

Create TCP/HTTP tunnel

Opens the configuration page for HTTP tunneling via TCP/IP. Learn more about this feature under *TCP port tunnel* on page 155.

Uploading firmware to a managed access point

This menu item is only available on WLAN controllers (WLCs).

On this page, you have the option of using remote access to manually update the firmware on an access point managed by the WLC. For example, this can be useful for testing firmware on selected access points before using it productively. Select an access point based on its MAC address and select the appropriate firmware file. Next click on **Start upload** to load the firmware in the access point.

Please note that this process disables the firmware management in the access point table for the selected access point. This prevents the WLC from automatically uploading a different firmware version. Firmware management can be re-enabled at any time in the setup menu under **WLAN-Management** > **AP-Configuration** > **Manage-firmware**.

In order for the access point to use the loaded firmware, you must subsequently perform a restart. By enabling the setting **Restart AP after updating the firmware** you trigger an automatic restart as soon as the firmware upload is completed.

Activate software option

Additional software option(s) available for your device are unlocked on this page after you have purchased the corresponding activation or registration key.

Registry keys are always device-specific and are not transferable to other devices. Be sure to keep a record of your key(s) in case you have to enable the option again (e.g. after a repair).

Set date and time

This page allows you to manually set the current date and time. Alternatively, you can use a time server to keep the time updated automatically. Learn more about this under *Time server for the local net* on page 1604.

A correct date and time setting is essential for some of the modules to function properly (e.g. syslog or the Public Spot module).

Change password

Use this page to change the password for your user account.

Reboot

From this page, you can restart the device after clicking on the Reboot button. This command is identical to **Extras** > **LCOS menu tree** > **Other** > **Cold-Boot**.

2.2.2.11 Logout from the device

With a click on the menu item **Logout** you end your current WEBconfig session and return to the login screen of the device.

2.2.3 LANCOM Management Cloud (LMC)

You have the option of connecting to the public LANCOM Management Cloud (public LMC) or to set up a privately hosted Management Cloud (private cloud).

2.2.3.1 Basics of the LANCOM Management Cloud

The LANCOM Management Cloud is capable of managing any size of "software-defined" networks. The LMC handles the configuration of all of the network components to minimize the amount of work involved in monitoring and configuration.

Further information about the LANCOM Management Cloud is available from *www.lancom-systems.com/cloud*.

If you wish to use the LANCOM Management Cloud for the configuration and monitoring of your device, the device needs to be paired with the LMC.

2.2.3.2 Pairing devices with the LANCOM Management Cloud

This chapter describes the different ways of pairing LANCOM devices with the LMC. Existing devices are paired in a different way than Cloud-ready devices.

Cloud-ready devices are LANCOM devices that the manufacturer has already equipped with LCOS version 10.0 or higher (LANCOM switches: Switch OS 3.30) and that have a PIN for pairing with the LMC. You will find the PIN on the enclosed product information.

Existing devices are LANCOM devices that have been updated from an older LCOS version to version 10.0 (LANCOM switches: Switch OS 3.30) or higher, which readies them for management by the LMC.

If you have a Cloud-ready device, no pairing is required. All you have to do in this case is to add your device to your account in the LANCOM Management Cloud and enter the serial number and PIN. If you wish, you can alternatively perform a pairing for Cloud-ready devices as well.

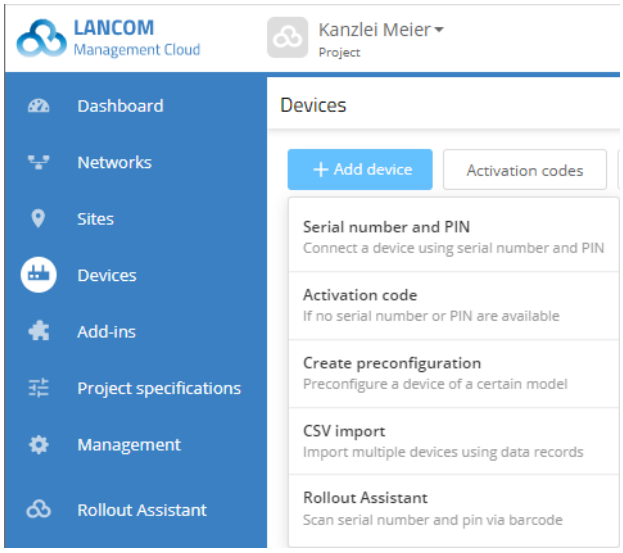
Some pairing possibilities are described below.

Integration into the LMC by serial number and Cloud PIN

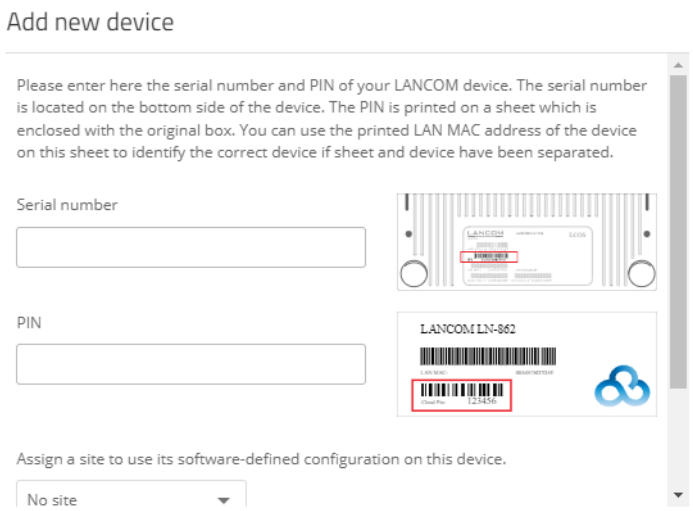
You can easily add your new device to a project in the LANCOM Management Cloud (Public). You will need the serial number of the device and the associated Cloud PIN. You can find the serial number on the bottom of the device or in LANconfig or WEBconfig. The Cloud PIN can be found on the Cloud-ready flyer, supplied with the device.



1. In the LANCOM Management Cloud, open the **Devices** view and click **Add new device**, then select the desired method, here **Serial number and PIN**.



2. In the next window, enter the serial number and Cloud PIN of the device. Then confirm with the button **Add new device**.



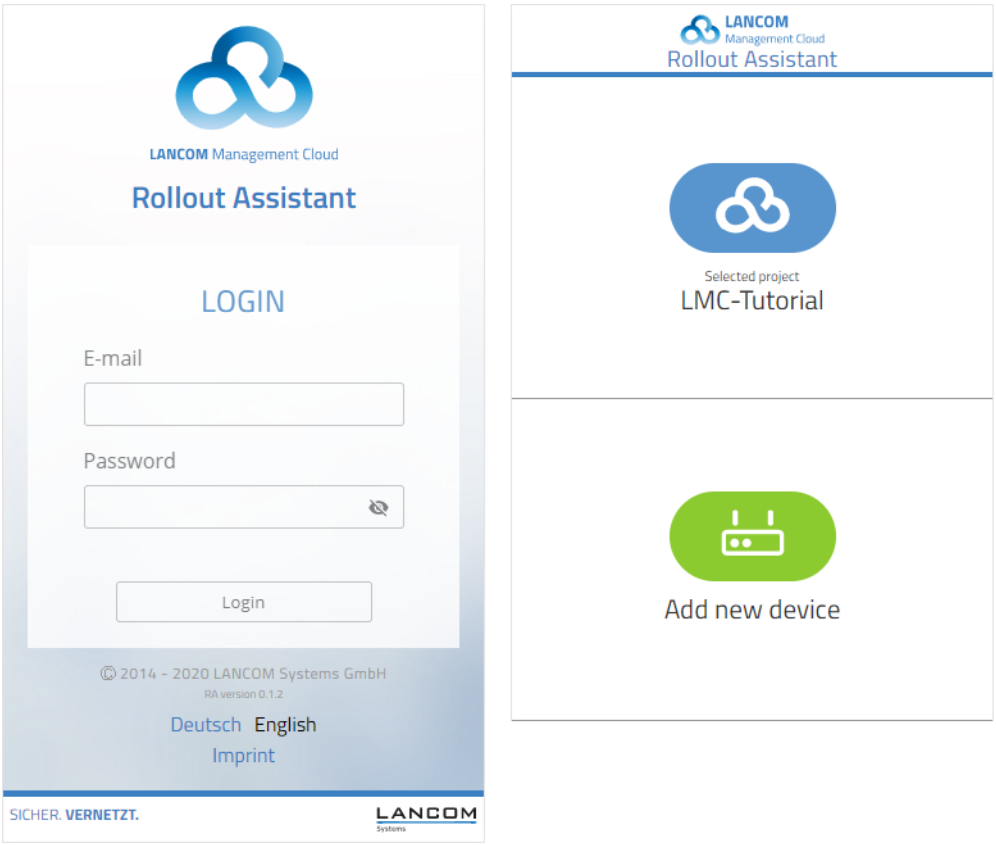
The next time the LANCOM device has contact with the LANCOM Management Cloud (Public), it will be paired automatically.

Integration into the LMC by LMC Rollout Assistant

The Rollout Assistant is a web application. It uses a device equipped with a camera and Internet access, such as a smartphone, tablet or notebook, to read the serial number and PIN. It offers an extremely easy way to connect the device to the LMC.

1. Enter the URL *cloud.lancom.de/rollout* into a browser.

The Rollout Assistant opens with this login screen:



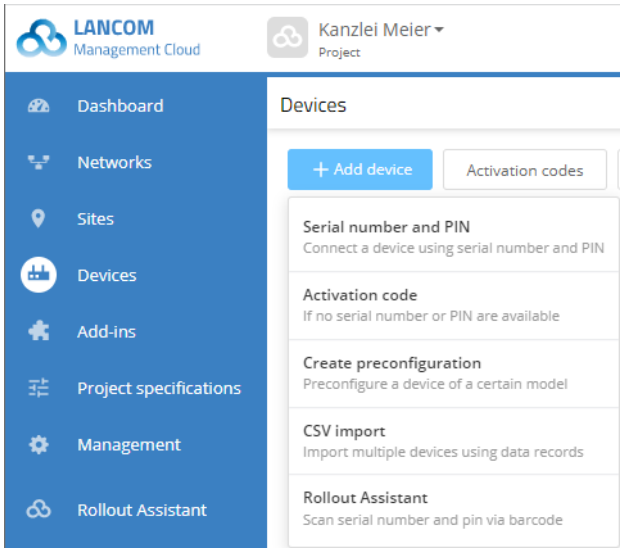
2. You select the desired language and login to the LMC using your credentials.
3. On the next page, you select the project that new devices are added to. Do this by tapping the green button and scanning the serial number. The Rollout Assistant may request access to the camera on the device to do this. You scan the serial number either on the underside of the device or alternatively from the barcode on the packaging box. Otherwise, you can enter the serial number manually.
4. Next, scan the cloud PIN from the information sheet enclosed with the device. Here, too, you have the option of entering the PIN manually. Now you can select one of the locations available in the project, or optionally use **No location** to leave this item open. Bear in mind that the location is an important setting for the configuration by SDN (Software-defined Networking).
5. In the next step, you assign various properties to the device. You give the device a name, enter an address, and take a photo of the installation. The address can be determined with the GPS information from your device.
6. In the final step, the information is displayed once again for checking. If you find any errors, simply go back and correct the corresponding entry.
7. Click or tap **Add device** to pair the device with the LMC. You will immediately see it in your project and can make other settings if necessary. As soon as you connect the device and it connects with the LMC, it is provisioned with an initial operating configuration based on the SDN settings, and the status changes to “online”.

Integration into the LMC by activation code

This method uses LANconfig and just a few steps to integrate one or more LANCOM devices simultaneously into the LANCOM Management Cloud.

Create an activation code

1. In the LANCOM Management Cloud, open the **Devices** view and click **Add new device**, then select the desired method, here **Activation code**.



2. Create an activation code by following the instructions in the dialog. This activation code allows you to integrate the LANCOM device into this project at a later time.

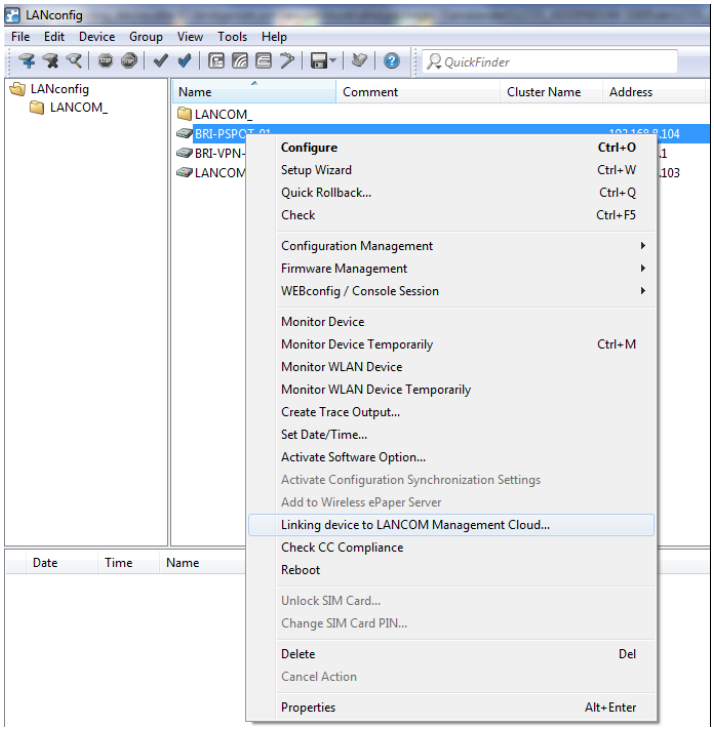
The **Activation code** button displays all of the activation codes for this project in the Devices view.

You can use the activation code in LANconfig, WEBconfig, or on the console for pairing with the LANCOM Management Cloud.

Pairing existing devices via LANconfig

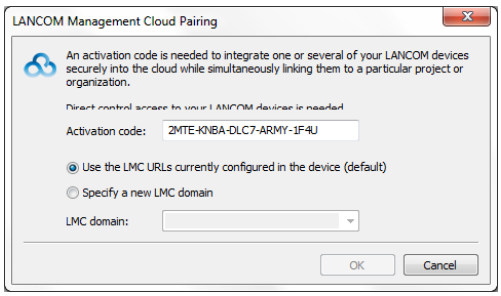
1. In the first step, you need to generate an activation code in the LANCOM Management Cloud.
2. Click on the corresponding LANCOM device with the right-hand mouse button.

3. In the context menu, select the entry **Link device to the LANCOM Management Cloud**.



4. Follow the Wizard's instructions to enter the activation code.
   Three options are available:

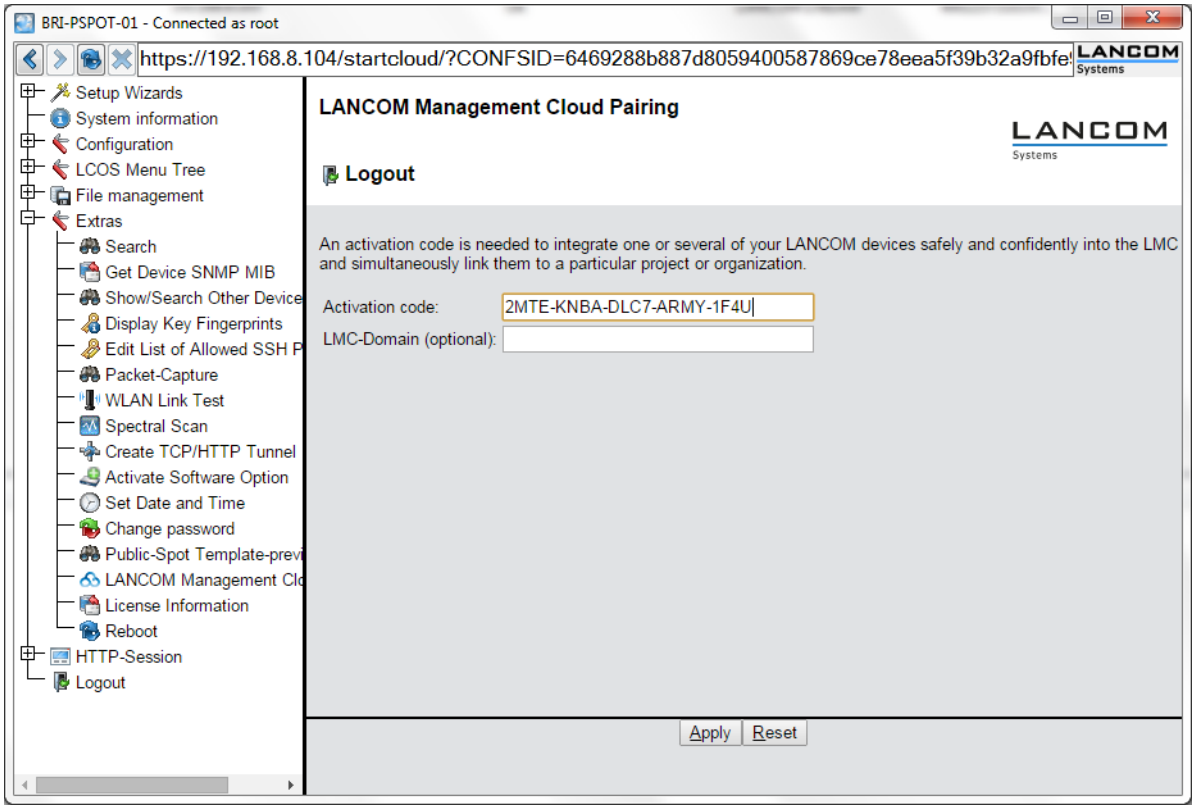
   - Public Cloud (default): You use the LANCOM Management Cloud.
   - Private Cloud: You use your own Cloud.
   - Use the settings currently stored in the device: A public or private cloud is used depending on the existing configuration in the device.



Pairing existing devices via WEBconfig

1. Start WEBconfig.

2. Under **Extras** > **LANCOM Management Cloud Pairing** you enter your activation code.



3. Click on the **Send** button.

Pairing existing devices via the command line

To conduct pairing from the command line, enter the command `startlmc`.

1. Launch a command line utility.
2. Enter the pairing command using the activation code as a parameter, e.g. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

An on-screen message will inform you if the pairing process has started successfully, or you will see an error message.

2.2.3.3 Delivery of the LMC domain by the LCOS DHCP server

As of LCOS version 10.0, LCOS devices that automatically receive their IP address from the DHCP server now additionally receive a DHCP option 43 in their DHCP packets.

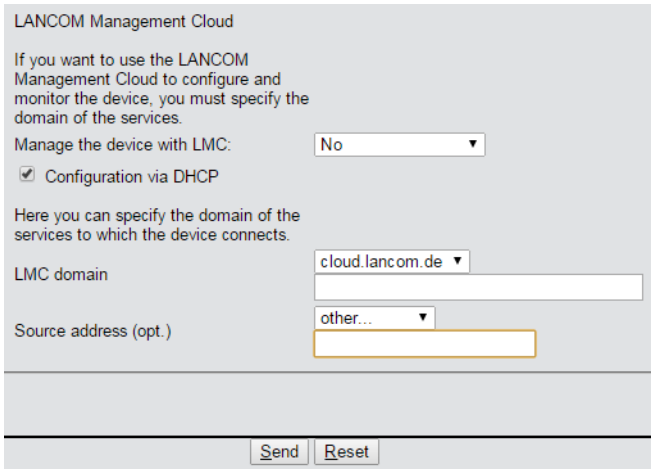
See *Delivering LANCOM Management Cloud parameters with the DHCP server* on page 1591.

2.2.3.4 Manual upfront configuration of your device for management by the LANCOM Management Cloud

This section informs you about the steps necessary in order for your device to be configured and monitored by the LANCOM Management Cloud.You specify:

- Whether your device is to be managed by the LMC.
- Whether the LMC domain is to be retrieved from a DHCP server.
- Which domain your device connects to.
- The source address (optional).

1. Navigate to **Management** > **LMC**.



2. Select one of the three options under **Manage the device with LMC:**
   - **No**: The device does not connect to the LMC.
   - **Yes:** The LMC manages the device. (Default for devices without a WLAN interface)
   - **Only without WLC**: Devices within a network managed by a WLC do not connect to the LANCOM Management Cloud. (Default for devices with a WLAN interface)
3. To obtain the LMC domain from a DHCP server, place a check mark in **Configuration via DHCP**.

   In order for the DHCP server to provide the LMC domain, the DHCP server requires sub-option 18 of the DHCP option 43 to be set to the LMC domain. For more information about the configuration of LMC parameters, see the section *Delivery of the LMC domain by the LCOS DHCP server* on page 48.
4. Under **LMC domain** you set the domain of the LANCOM Management Cloud that the device should connect to.
5. Enter an optional **Source address (opt.)** to be used instead of the one otherwise automatically selected for the source address. If you have configured a loopback address, you can specify it here as the source address.

2.2.4 Terminal program

Your device supports access via the command line of a terminal program via different interfaces (e.g. [W]LAN, [W]WAN or serial) and protocols (such as Telnet, SSH, or TFTP). A suitable client allows you to access the LCOS CLI to read-out device data, to change and analyze it, and to use your own scripts to automate these operations for multiple devices in one go, such as for the remote servicing of multiple devices—and all without the need of a graphical user interface.

In Windows, there is no Telnet client as part of the operating system. You can of course use alternative software such as the free, multi-protocol client PuTTY. PuTTY is available for Windows and Linux operating systems.

2.2.4.1 Start terminal session

On many operating systems, you start a terminal session from the command line with a combination of the protocol to be used and the IP address to connect to. There may be deviations depending on the protocol or client. For the precise syntax, refer to the relevant system or program documentation.

The following contains some of the common commands for various protocols and systems:

Telnet

From the Windows command line or the Linux terminal, start a Telnet session with the command `telnet <host>`.

Telnet establishes an (unencrypted) connection to the device with the IP address entered. After entering the password (assuming one has been set to protect the configuration) all of the configuration commands are available to you.

Linux also support Telnet sessions via SSL-encrypted connections. Depending on the distribution it may be necessary to replace the standard Telnet application with an SSL-capable version (e.g. telnet-ssl). For distributions that support Telnet-over-SSL, start an encrypted Telnet connection with the command `telnet -z ssl <host> <port>`.

SSH

Windows does not feature an SSH client by default. On Linux systems, use the command `ssh <login-name>@<host>` to set up an encrypted connection to the device and thus prevent the data being transferred during configuration from being intercepted within the network.

2.2.4.2 Change the language of the CLI

The command-line interface of your device works in different languages. The factory setting for the console language is "English". . To change the language of the CLI temporarily, i.e. for the duration of the session only, use the CLI command `lang` followed by the language or its initial letter(s), e.g. `lang Deutsch` or `long de`.

The following languages are currently supported by the CLI:

- `Deutsch`
- `English`

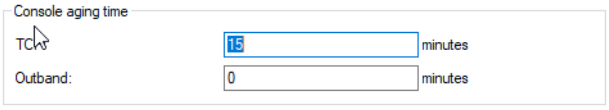
To change the default language **permanently**, select the desired language in the setup menu under **Config** > **Language**. The languages presented in the drop-down menu represent all of the possible input languages that your device currently supports.

2.2.4.3 Terminate or cancel terminal session

To close a Telnet session, enter the command `exit` at the command prompt:

If it is not possible to terminate a session by entering `exit`, for example during the login process with password entry, then Linux systems and some clients (such as PuTTY) allow terminal sessions to be canceled using the keyboard shortcut `Ctrl+c`.

The connection also terminates automatically if no activity is detected over a period of time. You can set this period under **Management** > **Advanced** in the section **Console aging time**.



TCP

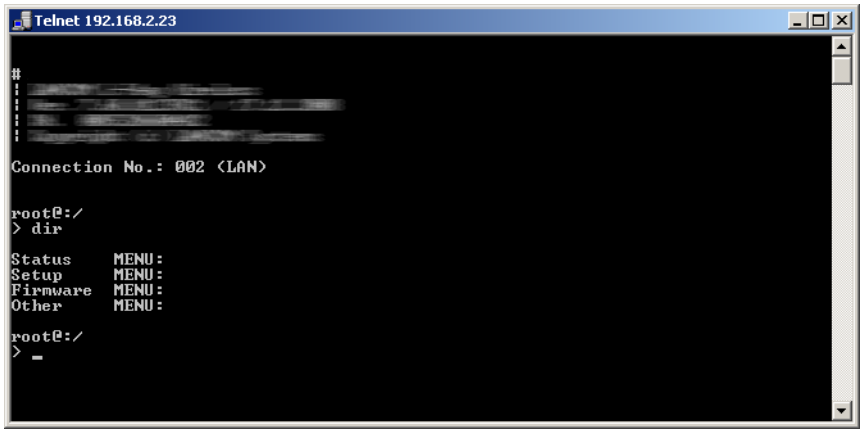
Specify here the number of minutes without activity before an inactive TCP connection (e.g. via SSH) is automatically terminated.

Outband

Specify here the number of minutes without activity before a serial connection (e.g. via Hyper Terminal) is automatically terminated.

2.2.4.4 Structure of the command-line interface

The LCOS command-line interface is structured as follows:



Status

Contains the states and statistics of all internal modules in the device and the direct access to the file system

Setup

Contains all adjustable parameters of all internal modules in the device

Firmware

Contains the firmware management

Other

Contains actions for establishing and terminating connections, reset, reboot and upload

2.2.4.5 Commands for the CLI

The LCOS command-line interface is operated with the following commands. Some of the available menu commands can be displayed using the HELP command.

Which commands are available depends upon the equipment of the device.

Some commands require special privileges in order to run, and these are listed along with the respective command. Commands that do not specify any rights have no restrictions.

Table 2: Overview of all commands available at the command line

Command	Description
`add|set [<Path>] <Value(s)>`	Sets a configuration parameter to a particular value. If the configuration parameter is a table value, a value must be specified for each column. Entering the `*` character leaves any existing table entry unchanged. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`add|set [<Path>] ?`	Lists all possible input values for a configuration parameter. If no specific path is entered, the possible input values for all configuration parameters in the current directory are listed. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write

Command	Description
`beginscript [-u] [-C d] [-s <password>]`	Resets the CLI session to script mode. In this state, commands entered are not transferred directly to the device's configuration RAM but initially to its script memory. Possible arguments are: › `-u`: Forces the **u**nconditional execution of a script or a configuration. › `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used. › `-s`: Decrypts the script with the password used for `readscript -s`. **Access rights**: Supervisor-Write
`bootconfig [-s (1|2|all)] [-r (1|2|all)]`	Enables you to save and delete boot configurations. Options: › `-s`: Stores the current configuration of a device either as a custom default setting (1), rollout configuration (2), or both (all). › `-r`: Optionally deletes the current custom default setting (1), the rollout configuration (2), or both (all). **Access rights**: Supervisor-Write For further information on boot configurations refer to the chapter *Alternative boot config* on page 89
`cd <Path>`	Switch to the current directory. Various abbreviations can be used, such as replacing `cd ../..` with `cd ...`, etc.
`clear`	Clears the current CLI output. All previously entered commands can be viewed by means of the log.
`default [-r] [<Path>]`	Resets individual parameters, tables or entire menu trees back to their default configuration. If `<PATH>` indicates a branch of the menu tree, then the option `-r` (recursive) must be entered. **Access rights**: Supervisor-Write
`del|delete|rm [<Path>] <Row>|*`	Deletes the table row `<Row>` in the current table or the table referenced in the branch of the menu tree with `<Path>`. Enter the line number for the `<Row>`. The wildcard symbol `*` deletes a table, for example, `del Config/Cron-Table *`. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`deletebootlog`	Clears the contents of the persistent boot log memory.
`dir|list|ls|llong|l [-a] [-r] [-s] [<Path>] [<Filter>]`	Displays the current directory content. Possible arguments are: › `-a`: In addition to the content of the query, this also lists the SNMP IDs. The output begins with the SNMP ID of the device followed by the SNMP ID of the current menu. The SNMP IDs of the subordinate items can be read from the individual entries. › `-r`: Also lists all subdirectories as well as the tables they contain. › `-s`: Sorts the display of the current directory; grouped by sub directories, tables, values, and actions; in ascending alphabetical order.
`dnsquery [-t <type>] [-d <destination>] name[@rtg-tag]`	Resolves DNS requests. Possible parameters: › `name`: The DNS name to resolve. › `@rtg-tag`: Optional routing tag for reaching the DNS server. › `-t <type>`: Type: A, AAAA, PTR, SRV, NAPTR

Command	Description

	› `-d <destination>`: Destination used for reaching the DNS servers. As in the forwarding table, a routing tag can also be specified if the forwarding destination is an IP address (e.g. 8.8.8.8@4095). You can also specify two comma-separated IP addresses (with an optional routing tag) (e.g. 8.8.4.4@4095,8.8.8.8@4095). The DNS client switches between servers if one does not respond
	
	If the command is entered without options, i.e. with the mandatory domain name only, then a request of type AAAA as well as a request of type A will be issued. Example:
	`> dnsquery www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	The AAAA-type response is only issued if the IPv6 address can also be reached.
	
	The type can also be specified explicitly using the option `-t`. The available types are AAAA, A, PTR, SRV and NAPTR. In the case of a PTR request, the requested IP address must be specified directly and may not be converted in the "ARPA" string:
	`> dnsquery -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	
	Because the dnsquery command uses the DNS client of the LANCOM device, its behavior is determined by the DNS configuration of the device (i.e. forwarding, loopback addresses, etc.). Since the DNS configuration may differ depending on the routing tag, the dnsquery command can be used to append the requested name (or to the requested address in the case of PTR requests) by means of an @ extension:
	`> dnsquery www.lancom.de@4095`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	It is also possible to send the requests while bypassing the forwarding configuration by specifying the -d parameter. Anything that can be specified as a destination in the forwarding table can also be specified as a destination here. With the destination set manually, the loopback address is set according to the loopback configuration. Example: AAAA+A request via WAN connection INTERNET
	`> dnsquery -dinternet www.lancom.de`
	
	`DNS result:`
	`==========`
	`www.lancom.de: type A, class IN, ttl 1 hour, addr 176.9.82.168`
	`www.lancom.de: type AAAA, class IN, ttl 1 hour, addr 2a01:4f8:151:20a3::2`
	
	To do this, a DNS server must of course have been assigned to the INTERNET WAN connection, e.g. via PPP, DHCP, or manually in the IP parameter list.
	
	Example: PTR request via Google server
	`> dnsquery -d8.8.8.8 -tptr 176.9.82.168`
	
	`DNS result:`
	`==========`
	`168.82.9.176.in-addr.arpa: type PTR, class IN, ttl 5 hours, 32 minutes, 30 seconds, www.lancom-systems.de`
	
	If no server responds, the client retries three times at increasing intervals, i.e. after each request, it waits 1, 2, 4, and finally 8 seconds. If there is no answer by then, the request is canceled. Pressing <CR> while a request is ongoing causes it to be canceled.

Command	Description
`do <Path> [<Parameter>]`	Executes the action in the current or the referenced directory, for example, do `Other/Coldstart`. If the action has additional parameters, they can be added at the end.
`echo <Argument>`	Displays the commands on the CLI.
`enable <Parameter>`	Extends the rights of authenticated TACACS+ users. Possible parameters are: › `0`: No rights › `1`: Read-only › `3`: Read-write › `5`: Read-only-limited Admin › `7`: Read-write-limited Admin › `9`: Read-only Admin › `11`: Read-write Admin › `15`: Supervisor (root)
`ethping -i <interface> [-?] [-c count] [-v vlan] [-s size] [-l mdlevel] <target address>`	CFM Ethernet Ping.See also *Commands on the Console* on page 1704.
`exit|quit|x`	Ends the terminal session.
`feature <Code>`	Activates the software option with the specified activation code. **Access rights**: Supervisor-Write **Command line options:** **Feature <activation-code>** Activation using activation code **Feature -Q** Query status of current and past remote activation requests **Feature -q** <query-id> Query status of a single request Feature -l <license-key> -t <license-type> [-i <license-index>] [-a <source-address>] [-u <server-url>] [-c <contact-data>] start a new remote activation request. Progress can be tracked using -q/-Q **-a <source-address>** source IP address or interface, e.g. INT, DMZ, LBx **-l <license-key>** 16/19 character license key **-t <license-type>** type of license, e.g. VPN25 **-i <license-index>** index of existing license for extension, 0 for additional license **-u <server-url>** URL of the license server **-c <contact-data>** comma separated list of contact details
`find <term>`	Looks for the search <term> and outputs all menu items containing it.
`flash yes|no`	Regulates the storing of configuration changes using the command line. By default, changes to the configuration using commands in the command line are written directly to the boot-resistant Flash memory of the devices (`yes`). If updating the configuration is suppressed in the Flash memory (`no`), changes are only stored in RAM (deleted on booting). **Access rights**: Supervisor-Write
`getenv <Name>`	Lists the respective environmental variables (without line feed). Please also note the command "printenv".

Command	Description
`history [options][<count>]`	Displays a list of the last executed commands. With the command `!#`, commands from the list can be called directly by their number (#): For example, `!3` executes the third command in the list. The history is saved persistently across reboots. See also *2.11.99 Persistent-History*. › `-c`: Clears the stored history. › `-w`: Writes the current history to a file. › `-a`: Appends the commands from this session's history to the end of a file. › `<count>`: Outputs only the number of commands specified in <count> on the command line.
`ikectl [-[r|d|D] <peer-name-list>] [-[e|r|d] <ipsec-name-list>] [-[r|d] [<ike-cookies-list>|<esp-spi-list>]] [-R <peer-name-list> <redirect-target>]`	This command widens the range of analysis options, for example by executing targeted actions to isolate the problem in the event of an error. This function allows you to quickly and automatically modify and test a VPN, among other things. › `-e <ipsec-name-list>`: Creates a Phase 2-SA/CHILD_SA when entered with the VPN rule name › `-r <peer-name-list>`: Performs a rekeying of the Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer › `-r <ike-cookies-list>`: Performs rekeying when entered with the IKE cookie › `-r <ipsec-name-list>`: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the name of the VPN rule › `-r <esp-spi-list>`: Performs a rekeying of the Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI › `-d <peer-name-list>`: Deletes a Phase 1-SA/IKE_SA when entered with the name of the VPN remote peer › `-d <ike-cookies-list>`: Deletes a Phase 1-SA / IKE_SA when entered with IKEv1 cookies / IKEv2 SPIs › `-d <ipsec-name-list>`: Deletes a Phase 2-SA/CHILD_SA when entered with the VPN rule name › `-d <esp-spi-list>`: Deletes a Phase 2-SA/Child_SA when entered with the incoming or outgoing ESP-SPI › `-D <peer-name-list>`: Starts the liveness check (Dead Peer Detection – DPD) when entered with the name of the VPN remote peer › `-R <peer-name-list> <redirect-target`: Redirects IKEv2 remote sites to a new destination using the IKEv2 redirect. If the list of remote sites is empty, all remote sites are redirected. This command can be used for maintenance purposes to move VPN remote sites from the current VPN gateway to another gateway securely. › `<peer-name-list>`: List of remote peer names separated by spaces and consisting of max. 16 characters › `<ipsec-name-list>`: Space-separated list of VPN rule names, as displayed in "show vpn" as ipsec-0-PEER-pr0-l0-r0. ⓘ To find a certain CHILD_SA/Phase 2-SA for a road warrior, it is important to also specify the remote station name as follows: `"peer-name ipsec-name"`. › `<ike-cookies-list>`: Consists of a list of 16 hexadecimal values separated by spaces, e.g 0x000102030405060708090A0B0C0D0E0F

Command	Description
	› `<esp-spi-list>`: Consists of a list of 4 hexadecimal values separated by spaces, e.g. 0x00010203 › `<redirect-target>`: Target to which the remote site(s) are to be redirected. The target can be an IPv4 address, IPv6 address or a DNS name Example: `ikectl -r peer ipsec-name-peer-2 -D peer3 -d peer4 0x12345678 -e "RoadWarrior IPSEC-0-DEFAULT-PR0-L0-R0"`
`importfile -a <application> [-p <passphrase>] [-n] [-h <Hash> -f <Fingerprint>] [-c] [-r]`	Your device supports the loading of files into file slots from the console and also by means of a script. This offers the convenience of using a script to roll-out files together with the configuration or, for example, to import SSH keys and VPN certificates. **Required parameters:** **-a <application>** <application> specifies the storage location and thus the usage for the entered data. For a complete list of the storage locations on your device, enter importfile -?. **Optional parameters:** **-n** -n starts the non-interactive mode. There are no prompts or other outputs on the CLI. The non-interactive mode is intended for use with scripts. **-p <passphrase>** <passphrase> is the password required to decrypt an entered private key. **-h <hash>** The hash algorithm used to determine the fingerprint of the root CA certificate. **-f <fingerprint>** The fingerprint of the root CA certificate, created with –h. The fingerprint can be entered either with or without colons. **-c** Only CA certificates are uploaded. **-r** Uploaded CA certificates replace any existing ones.
`iperf [-s|-c <Host>] [options]`	Starts iPerf on the device to perform a bandwidth measurement with an iPerf2 counterpart. Possible options include: › **Client/Server** › `-u, --udp`: Uses UDP instead of TCP. › `-p, --port <Port>`: Connects to or expects data packets on this port (default: 5001). › `-q, --quiet`: Activates the quiet mode, suppressing CLI output since the command can also be invoked via the action table. Also prevents interruption of the execution in client mode. › **Server-specific** › `-s, --server`: Starts iPerf in server mode and waits for a connection from an iPerf client.

Command	Description
	› **Client-specific** › `-c, --client <Host>`: Starts iPerf in client mode and connects to the iPerf server <Host> (IP address or DNS name). › `-b, --bandwidth [<Bandwidth>/]<Bandwidth>{kKmM}`: Limits bandwidth for analyzing a UDP connection in the [Down-]/Up-Stream. The value is specified in kilobytes (kK) or megabytes (mM) per second (default: 1 Mbps). › `-l, --len <Length>`: Specifies the length of UDP data packets. › `-t, --time <Time>`: Specifies the duration of the connection in seconds (default: 10 seconds). › `-d, --dualtest`: Conducts a bidirectional test: iPerf server and client simultaneously send and receive. › `-r, --tradeoff`: Conducts a sequential test: iPerf server and client alternately send and receive. › `-R, --reverse`: Reverses the measurement direction. › `-L, --listenport <Port>`: Specifies the port on which the device expects data packets from the remote iPerf server in bidirectional mode (default: 5001). › `-P, --parallel <Number>`: Specifies the number of parallel client tasks (maximum: 20). › `-B, --bind <Interface>`: Restricts the connection to the specified interface (IP address or interface name). › `-E, --peer <Interface>`: Establishes a connection using the interface specified by the peer name and sets rx/tx thresholds based on the result(s). If not executed in dual or tradeoff mode, the value of the unmeasured direction is set based on the last measurement if available. The result is recorded in the status table **Status** > **Iperf** > **Last-Results** > **Peer-Result** (1.96.1.3) under the values **Peer**, **Server-Bandwidth-kbps**, and **Client-Bandwidth-kbps**. › `--retry #`: Number of retry attempts if a connection cannot be established. Maximum: 99. › `--force`: If another client instance is already running, the system will wait until it is finished before proceeding. › `--ratediffperc #`: Maximum permitted rate deviation in percent in peer mode. Maximum: 99. › `--expbandwidth #/#{kKmM}`: Expected down/up stream bandwidth in peer mode. Values for unmeasured directions are ignored. Example: 10/10M › `--minbandwidth #{kKmM}`: Sets the specified value if the measurement returned a lower result. › **Miscellaneous** › `-h, --help`: Displays the help text.
`killscript <Name>`	Deletes the remaining unprocessed content of a script session Select the script session using its name. **Access rights**: Supervisor-Write
`language`	Selects a language for the CLI display. The command `language ?` lists the available languages.

Command	Description
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) is a command-line tool specified in RFC 6835 to query LISP mappings on a map resolver. Possible arguments are: › `-i <instance>`: Name of the LISP instance used for the destination query › `-m <server>`: LISP map server used for the destination query › `-id <num>`: LISP Instance ID [0-16777215] used for the destination query › `destination-eid`: Requested destination EID › `-retries <num>`: LISP retries to the map server [0-10] › `-rtg-tag <num>`: Routing tag used › `-source-eid <num>`: Source EID used Example: `lig -i LISP-INST 172.16.200.1`
`linktest`	Only available on WLAN devices. It displays the results of the WLAN link test. **Access rights**: Supervisor-Write **Execution right**: WLAN link test
`ll2mdetect`	Searches for devices via LL2M in the LAN. For further information on this command refer to the section *Commands for the LL2M client* on page 84. **Access rights**: Supervisor-Write
`ll2mexec`	Sends one command per LL2M to a device in the LAN. For further information on this command refer to the section *Commands for the LL2M client* on page 84. **Access rights**: Supervisor-Write
`loadconfig (-s <server IP address> -f <filename>)|<URL>`	Uploads a configuration file to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. For further information on this command refer to the section *File download from a TFTP or HTTP(S) server* on page 104. The cron table works with the user configured for it, meaning that if "loadconfig" is executed via the cron table, it will only be able to read the configuration completely if it is run with the root administrator. **Access rights**: Supervisor-Write

`loadfile [-a <Address>] [-s <Server-IP-address>] [-n] [-f <File-name>] [-o <File-name>] [-c <File-name>] [-p <File-name>] [-d <Passphrase>] [-C n|d] [-m <Version>] [-u] [-x <File-name>] [-i]`	Uploads a certificate file to the device. Possible arguments are:
	› `-a`: Specifies the source address of the file:
	  › `a.b.c.d`: Source IP address
	  › `INT`: Use the address of the first intranet interface as the source address
	  › `DMZ`: Use the address of the first DMZ interface as the source address
	  › `LBx`: Use the loopback address x (0..f) as the source address
	  › `<Interface>`: Use the address of the LAN interface <interface> as the source address
	› `-s`: Address of the TFTP server
	› `-n`: Ignore server name on SSL/TLS connections
	› `-f`: <File name> of the configuration file on the TFTP server
	› `-o`: Destination file <file name>for file download
	› `-c`: File <file name> with the root certificate for HTTPS
	› `-p`: File <file name> with unencrypted PKCS#12 container for HTTPS CA certificates and / or client-side authentication

Command	Description
	› -d: <Passphrase> to decrypt downloaded encrypted PKCS#12 containers › -C: Checks whether firmware is newer than (n) or different from (d) the current firmware › -m: Set a minimum <version> of the firmware › -u: Download firmware file unconditionally; skip the version check. › -x: File <file name> with additional CA certificates for HTTPS checks; the value ' none' prevents the default certificates from being downloaded › -i: Send Sysinfo as a POST request (for HTTP(S) only) The options [-f] and [-s] and the URL cannot be used simultaneously. For HTTP(S) downloads, you must specify the source by means of a URL. The maximum length of the URL is 252 characters. **Access rights**: Supervisor-Write
`loadfirmware [-e] (-s <server IP address> -f <filename>)|<URL>`	Uploads firmware to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. The `-e` option switch causes the firmware file to be saved completely in the local file system first before the firmware update starts. For further information on this command refer to the section *File download from a TFTP or HTTP(S) server* on page 104. **Access rights**: Supervisor-Write
`loadscript (-s <server IP address> -f <filename>)|<URL>`	Uploads a configuration script to the device via TFTP. You can optionally enter the server address and the file name, or the entire URL. For further information on this command refer to the section *File download from a TFTP or HTTP(S) server* on page 104. The cron table works with the user configured for it, meaning that if "loadscript" is executed via the cron table, it will only be able to read the configuration completely if it is run with the root administrator. **Access rights**: Supervisor-Write
`lspci`	Output of information via PCI devices **Access rights**: Supervisor-Read
`ping <IPv4-Address|Hostname>` `ping -6 <IPv6-Address>%<Scope>`	Sends an ICMP echo request to the IP address specified. For more information about the command and the specifics of pinging IPv6 addresses, see the section *Parameter overview for the ping command* on page 66.
`printenv`	Shows an overview of all environmental variables and their values.
`readconfig [-h] [-s <password>]`	Shows the complete configuration in the format of the device syntax. › -h: Adds a checksum to the configuration file. › -s <password>: Encrypts the configuration file with the use of the specified password. **Access rights**: Supervisor-Read
`readmib`	Display of the SNMP Management Information Base. Available only on devices without a unified MIB. **Access rights**: Supervisor-Read,Local-Admin-Read

Command	Description
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	The readscript command generates a text dump of all commands and parameters required to configure the device in its current state. You can use the following option switches for this: › `-n`: The text output is only numerical without identifiers. The output only contains the current status values of the configuration as well as the associated SNMP IDs. › `-d`: The default values are included in the text output. › `-i`: The table designations are included in the text output. › `-c`: Includes any comments contained in the script file. › `-m`: The text is output to the screen in a compact but difficult to read format (no indentations). › `-h`: Adds a checksum to the script file. › `-s <password>`: Encrypts the script file with the use of the specified password. › `-o`: Replaces the passwords with a "*" to obfuscate them in the text output. **Access rights**: Supervisor-Read
`readstatus`	Outputs the status of all SNMP IDs for the device.
`release [-x] *|<Interface_1…Interface_n>`	The DHCPv6 client returns its IPv6 address and / or its prefix to the DHCPv6 server. It then submits a new request for an address or prefix to the DHCPv6 server. Depending on the provider, the server assigns a new address to the client, or reassigns the previous one. Whether the client receives a different address or prefix is determined solely by the server. The option switch `-x` suppresses the confirmation message. The `*` wildcard applies the command on all of the interfaces and prefix delegations. Alternatively, you can specify one or more specific interfaces.
`repeat <Interval> <Command>`	IPv6 address release: Repeats the specified command every `<Interval>` seconds until the process is ended with new input.
`rollout (-r|-remove) <RelatedFile>`	Deletes the files of the user-specific rollout wizard from the file system of the device. Possible files are: › `wizard`: Deletes the wizard › `template`: Deletes the template › `logo`: Deletes the logo › `all`: Deletes the wizard, the template and the logo **Access rights**: Supervisor-Write
`setenv <Name> <Value>`	Sets an environmental variable to the specified value. **Access rights**: Supervisor-Write, Local-Admin-Write, Limited-Admin-Write
`setpass|passwd [-u <User>][-n <new> <old>]`	Changes the password of the current user account. In order to change the password without a subsequent input prompt, use the option switch `-n` while entering the new and old password. The password can have a maximum of **128 characters** and use the following characeter set: #@ABDEFGHIJKLMNOPQRSTUWXYZ[{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz `

Command	Description
	If the command `passwd` is deployed in a script and a `$` is used in the password, an additional `$` has to be prepended, as it would otherwise be interpreted as a variable and setting the password would fail. In order to change the password of the local user account when authentication by TACACS+ is enabled, use the option switch `-u` with the name of the corresponding user. If the local user does not exist or the user name is missing, the command aborts. The user must also have supervisor rights, or authorization by TACACS must be enabled.
`show <Options> <Filter>`	Shows selected internal data, such as › `admin-distance` – shows the administrative (routing) distance of all internal applications or routing protocols › `bootlog` – the last boot processes › `filter` – firewall filtering rules › `Fw-dns-destinations` – Optionally accepts a space-separated list of names of the firewall's DNS destinations. All DNS destinations or the ones specified in the parameter are listed sequentially. For each destination, the counter from **Status** > **Firewall** > **DNS-Database** > **Destination-Usage** is displayed, followed by the list of wildcard expressions. For each wildcard expression, the currently resolved addresses and the data records that are a direct or indirect match are displayed. › `ip-addresses` – displays all IPv4 and IPv6 addresses for the device for the LAN and WAN interfaces, along with advanced status information › `ipv4-addresses` – displays all IPv4 addresses for the device for the LAN and WAN interfaces, along with advanced status information › `lisp instance` – displays status information about all configured LISP instances › `lisp instance [instance]` – displays status information about the LISP instance named [instance] › `lisp map-cache` – displays status information about the map cache entries available for all instances › `lisp map-cache [instance]` – displays status information about the map cache entries for the instance named [instance] › `lisp registrations` – displays status information about the EIDs/RLOCs of all instances registered with the map server › `lisp registrations [instance]` – displays status information about the EIDs/RLOCs of the instance named [instance] registered with the map server › `lta` – shows information about groups or users of the LANCOM Trusted Access. This is set up and managed via the LANCOM Management Cloud. › `mem`, `heap` – memory usage › `netflow collectors` – displays information about the configured NetfFlow collectors › `netflow interfaces` – displays information about interfaces and the corresponding NetFlow parameters › `netflow metering-profiles` – displays information about the metering profiles of NetFlow/IPFIX For more information about NetFlow/IPFIX, please see *Netflow / IPFIX* on page 1641.

Command	Description
	› `pppoe-user-detail <user-name>` – displays status information about the respective active user or the peer on the PPPoE server. › `VLAN` – dynamically added VLANs and VLAN memberships, e.g. added to the static configuration at runtime by CAPWAP or WLAN/802.1X › `VPN` – VPN rules › `wg-connection` – Displays information about WireGuard connections › `wg-detail` – Displays detailed information about WireGuard connections › `wg-peer` – Displays information about configured WireGuard peers With additional filter arguments you can further limit the output. For an overview of all possible options, enter `show ?`. The filters available with an option are displayed by `show <option> ?`. For example, `show VPN ?` shows the filters available for the VPN rules. For information on displaying IPv6-specific data, read the section *Overview of IPv6-specific show commands* on page 77. **Access rights**: Supervisor-Read, Local-Admin-Read
`sleep [-u] <Value><Suffix>`	Delays the processing of configuration commands by a particular time or terminates them at a particular time. Applicable values for `<SUFFIX>` are `s`, `m` and `h` for seconds, minutes and hours. If no suffix is defined, the command uses milliseconds. With option switch `-u`, the `sleep` command accepts times in format `MM/DD/YYYY hh:mm:ss` (English) or in format `TT.MM.JJJJ hh:mm:ss` (German). Times will only be accepted if the system time has been set.
`smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)`	Available only on devices with 3G/4G WWAN module: Sends a text message to the destination number entered. › `-s <SMSC-Number>`: Alternative SMSC phone number (optional). If you omit this part of the command, the device uses the phone number stored on the USIM card or that configured under SNMP ID 2.83. › `-d <Destination>`: Destination phone number › `-t <Text>`: Contents of the message with <=160 characters. For an overview of available characters, see the section *Character set for sending SMS* on page 1687. Special characters must be in UTF8 encoded form.
`ssh [-?|h] [-o "option=value"] [-<a|b> Loopback-Address] [-p Port] [-C] [-j Keepalive-Interval] <Host>`	Establishes an SSH connection to the <Host>. Possible arguments are: › `-?|h`: Outputs the help text. › `-o "option=value"`: additional options with corresponding values can be specified. › `-a|b`: Allows a route or loopback address to be specified for the device to use if the destination can be reached via multiple routes. The function of `-a` and `-b` is identical. `-b` is the usual option used by an OpenSSH client on UNIX systems, whereas some other commands integrated into LCOS use `-a` to specify a loopback address. › `-p`: Sets the <Port> of the host › `-C`: Enforces compressed data transfer › `-j`: Specifies how frequently the client sends a keepalive.

Command	Description
`sshcopyid`	To store your SSH public key using SSH **Access rights**: Supervisor-Write

`sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <file-name>] [-R <host-name>]`	Creates or deletes the SSH key in the device. Possible arguments are:
	› `-h`: Displays a brief help text about the available parameters
	› `-q`: The device overrides existing keys without a prompt (quiet mode)
	› `-t`: This parameter specifies what type of key is generated. SSH supports the following types of keys:
	  › RSA
	  › DSA
	  › ECDSA
	  › ED25519
	  › ED448
	› `-b`: This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.
	› `-f`: These parameters specify the file name of the generated key file in the device file system. The choice of the file name depends on the type key you are generating. The choices available to you are:
	  › **ssh_rsakey** for RSA keys
	  › **ssh_dsakey** for DSA keys
	  › **ssh_ecdsakey** for ECDSA keys
	  › **ssl_privkey** for SSL-RSA keys
	  › **ssh_ed25519key** for Ed25519 keys
	  › **ssh_ed448key** for Ed448 keys
	› `-R`: Removes all keys for a specific hostname. Optionally, specify a key type.
	For further information on SSH / SSL keys used in the device refer to the chapter *Device-internal SSH/SSL keys* on page 117

`ssldefaults [-y]`	This command resets the SSL / TLS settings in all submenus of the current configuration to the default values after a security prompt. In LCOS, each module comes with its own submenu for SSL / TLS settings. This provides a way to reset all settings in these various submenus to the current secure default settings. The parameter `-y` ensures that the security prompt is automatically answered so that the command can be used non-interactively in scripts.
`stop`	Ends the ping command
`sysinfo`	Shows the system information (e.g., hardware release, software version, MAC address, serial number, etc.).
`tab`	For use in script files: For the command that follows, this sets the order of the columns for the arguments in the case that the columns in the table differ from the default (e.g. a column was added). **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`telnet <Address>`	Establishes a Telnet connection to the given <address>.
`testmail <From> <To_1…To_n> [<Realname> <Subject> <Body>]`	Sends a test e-mail. A sender address and receiver address are necessary; real name, subject line and message content are optional. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write

Command	Description
`time <DateTime>`	Sets a time in format `MM/DD/YYYY hh:mm:ss`. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write **Execution right**: Time Wizard
`trace <Parameter> <Filter>`	Starts a trace command for output of diagnosis data. With additional filter arguments you can further limit the output. For further information on this command refer to the section *Parameter overview for the trace command* on page 68. **Access rights**: Supervisor-Read,Limited-Admin-Read,Limited-Admin-Write
`unmount [-?][-f] <Volume>`	Outputs the current volume table. › `-f`: Releases the specified volume. <Volume> may be the volume ID or any mount point. › `-?`: Outputs the help text.
`unsetenv <Name>`	Deletes the specified environmental variable. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`wakeup [MAC]`	Performs a Wake On LAN for the device with the MAC address [MAC]. **Access rights**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`who`	Lists active configuration sessions.
`writeconfig [-u] [-C d] [-s password] [-b index]`	Writes a new configuration on the device in the syntax format for the device. The system interprets all of the following lines as configuration values until two empty lines are read. Possible arguments are: › `-u`: Forces the **u**nconditional execution of a script or a configuration. › `-C d`: Skips the default **"C**heck for **d**ifference. Also applies when the `-u` option is used. › `-s password`: Decrypts the configuration file with the use of the specified password. › `-b index`: Writes the configuration as an alternative boot configuration. Index must be `1`, `2` or `all`. **Access rights**: Supervisor-Write
`writeflash`	Load a new firmware file (only via TFTP). **Access rights**: Supervisor-Write
`!!`	Repeat last command
`!<num>`	Repeat command <num> times
`!<prefix>`	Repeat last command beginning with <prefix>
`#<blank>`	Comment

Legend

› Characters and brackets:
  › Objects, in this case dynamic or situation-dependent, are in angle brackets.
  › Round brackets group command components, for a better overview.
  › Vertical lines (pipes) separate alternative inputs.
  › Square brackets describe optional switches.

It follows that all command components that are not in square brackets are necessary information.

- `<Path>`:
  - Describes the path name for a menu or parameter, separated by "/" or "\".
  - `..` means: one level higher
  - `.` means: the current level
- `<Value>`:
  - Describes a possible input value.
  - `""` is a blank input value
- `<Name>`:
  - Describes a character sequence of [0…9] [A…Z] [a…z] [_].
  - The first character cannot be a digit.
  - There is no difference between small letters and capital letters.
- `<Filter>`:
  - The output of some commands can be restricted by entering a filter expression. Filtering does not occur line by line, but in blocks, depending on the command.
  - A filter expression starts with the "@" symbol by itself and ends either at the end of the line or at a ";" (semicolon) to end the current command.
  - A filter expression also consists of one or more search patterns, which are separated by blank spaces and preceded either by no operator (OR pattern), a "+" operator (AND pattern) or a "-" operator (NOT pattern).
  - For the execution of the command, an information block is output exactly when at least one of the "OR" patterns, all "AND" patterns or none of the "NOT" patterns matches. Capitalization is ignored.
  - For a search pattern to contain characters for structuring in the filter syntax (e.g., blank characters), then the entire search pattern can be enclosed in "". Alternatively, the symbol "\" can be placed before the special characters. If you want to search for a quotation mark (") or "\", another "\" symbol has to be placed in front of it.

    Entering the start of the word, if it is unique, is sufficient.
  - For examples of the usage of the output filter, see the section *Filtering trace output* on page 293.

Explanations for addressing, syntax and command input

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, the command `sysinfo` can be shortened to `sys` and `cd Management` to `c ma`. The input `cd /s` is not valid, however, since it corresponds to both `cd /Setup` and `cd /Status`.
- Directories can be addressed with the corresponding SNMP ID. For example, the command `cd /2/8/10/2` has the same effect as `cd /Setup/IP-router/Firewall/Rules`.
- Multiple values in a table row can be changed with **one** command, for example in the rules table of the IPv4 firewall:
  - `set WINS UDP` sets the protocol of the WINS rule to UDP
  - `set WINS UDP ANYHOST` sets the protocol of the WINS rule to UDP and the destination to ANY-HOST
  - `set WINS * ANYHOST` also sets the destination of the WINS rule to ANYHOST; the asterisk means that the protocol remains unchanged
- The values in a table row can alternatively be addressed via the column name or the position number in curly brackets. The command `set ?` in the table shows the name, the possible input values and the position number for each column. For example, in the rules table of the firewall, the destination has the number 4:

- `set WINS {4} ANYHOST` sets the destination of the WINS rule to ANYHOST
- `set WINS {destination} ANYHOST` also sets the destination of the WINS rule to ANYHOST
- `set WINS {dest} ANYHOST` sets the destination of the WINS rule to ANYHOST, because specifying `dest` here is sufficient to uniquely identify the column name.

- Names that contain spaces must be enclosed within quotation marks ("").

Command-specific help

- A command-specific help function is available for actions and commands (call the function with a question mark as the argument). For example, `ping ?` shows the options of the integrated ping command.
- Enter `help` or `?` on the command line for a complete listing of the available shell commands.

Parameter overview for the ping command

The ping command entered at the command prompt of a Telnet or terminal connection sends an "ICMP echo-request" packet to the destination address of the host to be checked. If the receiver supports the protocol and it is not filtered out in the firewall, the destination host will respond with an "ICMP echo reply". If the target computer is not reachable, the last device before the host responds with a "network unreachable" or "host unreachable" message.

The syntax of the ping command is as follows:

```
ping [-46dfnoqrmb] [-s n] [-i n] [-c n] [-x x][-p <dscp>][-a ...] destination [%scope] [%scope@rtg-tag]
[%%interface] [@rtg-tag]
```

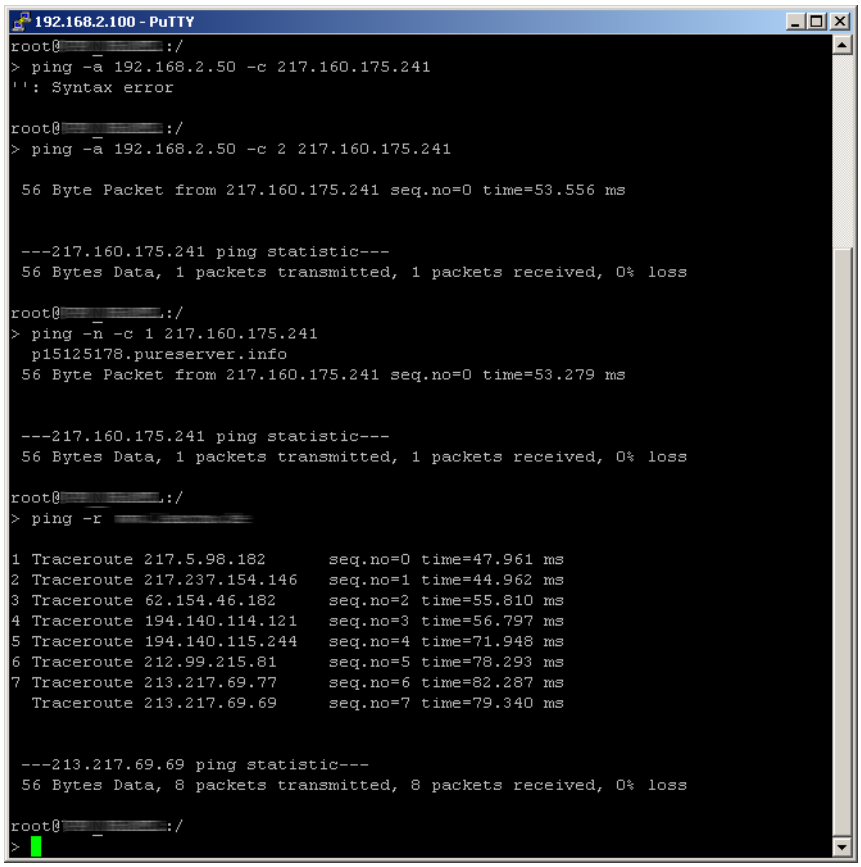
The meaning of the optional parameters is explained in the following table:

Table 3: Overview of optional parameters for the ping command

Parameter	Meaning
`-4`	Force IPv4
`-6`	Force IPv6
`-d`	Forbid fragmentation
`-f`	flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example. It is easy for flood ping to be misinterpreted as a denial-of-service (DoS) attack.
`-n`	Returns the computer name of a specified IP address.
`-o`	Immediately sends another request after a response.
`-q`	Ping command returns no output to the CLI (quiet).
`-r`	Switches to the traceroute mode. The path taken by the data packets to the target computer is displayed with all intermediate stations.
`-m`	Switches to the tracepath mode to determine the path MTU to the specified IP address.
`-b`	Do not stop pinging after receiving a PacketTooBig (DF), in order to achieve "Path MTU Discovery".
`-s n`	Sets the packet size to n bytes (max. 65500).
`-i n`	Time between packets in seconds.
`-c n`	Send n pings.

Parameter	Meaning
`[-x x]`	Atomic fragments: (n)ever, (f)orce, (a)utomatic
`[-p <dscp>]`	Use a specific DSCP value for this ping. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible DSCP values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF
`-a a.b.c.d`	Sets the ping's sender address (default: IP address of the device.
`-a <name>`	Uses a named network, interface, or loopback address as the sender address
`-l <Load-Balancer-Policy>`	If the ping target is reached via a load balancer, the policy makes a load-balancer decision when the pings are sent. Possible values are default, traffic, bandwidth, round-robin, mst-used and all defined Dynamic Path Selection policies. If an invalid policy is specified, no pings are sent It is not possible to use this CLI option in combination with the specification of a scope or an interface binding in the destination.
`-6 <IPv6-Address>%<Scope>`	Performs a ping command to the link-local address via the interface specified by <scope>. For IPv6, the scope of parameters is of central importance: IPv6 requires a link-local address (fe80::/10) to be assigned to every network interface (logical or physical) on which the IPv6 protocol is enabled, so you must specify the scope when pinging a link-local address. This is the only way that the ping command knows which interface it should send the packet to. A percent sign (%) separates the name of the interface from the IPv6 address. **Examples:** › `ping -6 fe80::1%INTRANET` Pings the link-local address “fe80::1”, which is accessible via the interface and/or the network “INTRANET”. › `ping -6 2001:db8::1` Pings the global IPv6 address “2001:db8::1”.
`destination`	Address or host name of the target computer
`%scope`	Name of the interface used to send the packet when link-local addresses are used as the destination.
`%scope@rtg-tag`	Name of the interface used to send the packet when link-local addresses are used as the destination, with additional specification of the routing tag.
`%%interface`	Name of the destination interface. The packet is sent directly to the interface without taking the routing table into account.
`@rtg-tag`	Routing tag used to send the packet.

Parameter	Meaning
`stop /<RETURN>`	Entering `stop` or pressing the RETURN button terminates the ping command.



Parameter overview for the trace command

The traces available for a particular model can be displayed by the CLI by entering `trace` without any arguments.

Table 4: Overview of some executable traces

This parameter ...	...causes the following message in the trace:
`ACME`	Automatic Certificate Management Environment (ACME) client
`ADSL-CTRL`	Output of all management packets for the internal ADSL interface
`ADSL-DATA`	Output of all packets transmitted via the internal ADSL interface
`ADSL-Modem`	Extended status information regarding the internal ADSL interface
`ADSL-Status`	Information regarding the connection status as well as the connection and disconnection of the internal ADSL interface
`ARP`	Address resolution protocol
`ATM-cell`	ATM packet layer
`ATM-error`	ATM error

This parameter ...	...causes the following message in the trace:
Autoload	Information regarding the automatic firmware and configuration load during a device rollout
Automatic-Firmware-Updater	Information regarding the automatic firmware update
B-Analog	Status information regarding the analog audio channel
BGP-Adj-RIB-In	Information regarding Border Gateway Protokoll Updates received from neighbors (BGP-Adj-RIB-In)
BGP-Adj-RIB-Out	Information regarding Border Gateway Protokoll Updates sent to neighbors (BGP-Adj-RIB-Out)
BGP-Connection	Event processing and State changes of the individual Statemachines as well as readably formatted BGP messages sent / received by the Statemachine
BGP-Control	Information regarding the processing of the BGP configuration
BGP-Message	Internal messages between the BGP threads (Note: Creates a lot of messages, usually only the number of the State Machine)
BGP-Network	Information regarding the creation of an outgoing BGP connection and accepting or rejecting of incoming BGP connections
BGP-Packet	Shows received and sent BGP packets as a hexdump (associated State Machine can only be resolved by number at the time of data retrieval)
BGP-Phase-Two	Shows, why BGP Phase 2 prefers or ignores a prefix (Note: Can create a lot of messages)
BGP-Policy	Information regarding the processing of Border Gateway Protokoll routes when using rules
Bonjour-Proxy-Packet	Packets of the Bonjour-Proxy
Bonjour-Proxy-Status	Status information of the Bonjour-Proxy
Bridge	Information on the LAN bridge
BT-Status	Status information regarding the BLE interface
Callmanager	Status information regarding the Voice Call Manager
CAPWAP-CTRL	Status information regarding the control channel between a WLAN-Controller and managed access point
CAPWAP-DATA	Packets transmitted via the Layer3-Tunnel between the WLAN-Controller and a managed access point
CAPWAP-RF-Opt	Status information regarding the WLC-based radio field optimization
CAPWAP-Firmware	Informationen zum zentralen Firmwaremanagement auf WLAN-Controllern
CF-Status	Status information regarding the Content-Filter
CF-Urls	Status information regarding URLs in the Content-Filter
COM-Port-Server	Status information about the Com-Port-Server
Config-Sync:	Status information regarding Config-Sync (automatic configuration synchronisation)
Connact	Messages from the activity protocol
CRL-Client	Status information regarding the Certificate Revocation List (CRL) Client
Cron	Activities of the scheduler (cron table)

This parameter ...	...causes the following message in the trace:
D-channel	Shows communication via ISDN D-Channel (Call setup and termination)
DFS-Pulse	Shows radar pulses in the 5 GHz band (DFS - Dynamic Frequency Selection)
DFS-Status	Shows ecvents which are related to dynamic frequency detection and radar detection
DHCP	Dynamic host configuration protocol
DHCPv6-Client	Status information regarding the DHCPv6-Client
DHCPv6-Relay-Agent	Status information regarding the DHCPv6-Relay-Agent
DHCPv6-Server	Status information regarding the DHCPv6-Server
DNS	Domain name service protocol
DS-Lite	Status information regarding Dual Stack Lite (DS-Lite)
DSLoL	Status information regarding DSLoL (DSL over LAN)
DSR-CTRL	Status information regarding the setup and termination of connections to Analog/ISDN devices
DSR-IPT	Shows received and sent voice packets between SIP and Analog/ISDN (Note: Similar to the MEDIA-PCM trace, but more specialised towards Analog/ISDN devices)
DTLS	Status information regarding DTLS connection (is used by CAPWAP)
DYN-AUTH-Client	Status information regarding the client for dynamic authorization by RADIUS CoA (Change of Authorization)
DYN-AUTH-Server	Status information regarding the server for dynamic authorization by RADIUS CoA (Change of Authorization)
EAP	Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1X
Error	Connection error messages
Ethernet	Information on the Ethernet interfaces
Filesystem	Status information regarding the filesystem
Firewall	Displays firewall events
Firmware-Upload	Status information regarding the firmware upload
FPing	Status information regarding the FPing command
FRONTPANEL-Serial	Information regarding the display monitor controller on WLC-1000/WLC-2000/ISG series
FW-DNS	Changes to the firewall database of DNS destinations: › If a DNS packet arrives, it outputs the packet along with the affected wildcard expressions and destinations. › If the TTL (time-to-live) of an entry expires, it outputs the associated record along with the relevant wildcard expressions and destinations. › If one of the two firewalls registers or de-registers a DNS destination because its configuration has changed. › If there is a change to the table **Set up** > **Firewall** > **DNS-Destinations** or **Set up** > **Firewall** > **DNS-Destination-List**.
GRE	Messages to GRE tunnels

This parameter ...	...causes the following message in the trace:
hnat	Information on hardware NAT
HTTP-Client	Status information regarding HTTP-Client events
HTTP-Client-DNS	Status information regarding DNS-based HTTP-Client events
HTTP-Server	Status information regarding HTTP-Server events
HWMON-Serial	Information regarding the Hardware Monitor Controller on WLC-1000/WLC-2000/ISG series
IAPP	Trace on inter access point protocol giving information on wireless LAN roaming.
ICMP	Internet control message protocol
ICMPv6	Status information regarding the Internet Control Message Protocol for IPv6
IGMP-Snooping	Information regarding IGMP snooping in the LAN bridge (IGMP - Internet Group Management Protocol)
Iperf-Server-Daemon	Status information regarding the iPerf server
IP-masquerading	Events in the masquerading module
IPv4-Config	Information regarding the internal IPv4-Control-Plane
IPv4-Host	Shows IPv4 packets, which the router itself sends or receives
IPv4-Interfaces	Information about the internal management of logical IPv4 interfaces
IPv4-LAN-Packet	Shows IPv4 LAN packets (without packets destined for the router itself and packets created by the router)
IPv4-Packet	Shows all IPv4 packets (without packets destined for the router itself and packets created by the router)
IPv4-RIB	Status information regarding the IPv4 Routing Information Base (RIB)
IPv4-WAN-Packet	Shows IPv4 WAN packets (without packets destined for the router itself and packets created by the router)
IPv6-config	Information about the IPv6 configuration
IPv6-firewall	IPv6 firewall events
IPv6-Interfaces	Information about the IPv6 interfaces
IPv6-LAN-Packet	Data packets over the IPv6 LAN connection
IPv6-router	Information about the IPv6 routing
IPv6-WAN-Packet	Data packets over the IPv6 WAN connection
L2TP	L2TPv2 / v3 protocol
L7-Detection	Shows the connections recognised by the Layer-7 detection
L7-Detection-Status	Shows general status information regarding the Layer-7 detection
LANAUTH	LAN authentication (e.g. Public Spot)
LACP	Information regarding the Link Aggregation Control Protocol (LACP)
LBS-Client	Information regarding the Location Based Services Client

This parameter ...	...causes the following message in the trace:
License-Management	Information regarding license files (vRouter)
LISP-Config	Information regarding the Locator / ID Separation Protocol (LISP)
LISP-Control	Information regarding the Control-Plane of the Locator / ID Separation Protocol (LISP)
LISP-Data	Shows data packets of the Locator / ID Separation Protocol (LISP)
LISP-Error	Shows error messages of the Locator / ID Separation Protocol (LISP)
LL2M	Information regarding the LANCOM Layer 2 Management Protokoll
Load-balancer	Information on load balancing
Mail-client	E-mail processing by the internal mail client
MEDIA	Status information regarding the Media Receiver (Setup/Termination of media endpoints and streams)
MEDIA-CODECS	Status information regarding the Media Receiver with focus on Codec negotiation
MEDIA-PCM	Shows data between SIP and Analog/ISDN (Note: Similar to the DSR-IPT trace, but more specialised towards the Media Receiver)
MLD	Information regarding the IPv6 Multicast Listener Discovery (MLD)
ND-CACHE	Information regarding the IPv6 Neighbor Discovery Protocol Cache
ND-DAD	Information regarding the Duplicate Address Detection of the IPv6 Neighbor Discovery Protocol
NETFLOW-Common	For more information about NetFlow/IPFIX, please see *Netflow / IPFIX* on page 1641.
NETFLOW-Error	
NETFLOW-Export	
NETFLOW-Metering	
NTP	Timeserver trace
OAM	Information regarding Ethernet OAM
OCSP-Client	Information regarding the Online Certificate Status Protocol (OCSP) Client
OCSP-Server	Information regarding the Online Certificate Status Protocol (OCSP) Server / Responder
OSPF-Expert	Expert information regarding the Open Shortest Path First (OSPF) protocol
OSPF-LSA	Information regarding the Open Shortest Path First (OSPF) Link State Advertisements (LSA)
OSPF-Neighbor	Information regarding the Open Shortest Path First (OSPF) neighbors
OSPF-Packet	Shows Open Shortest Path First (OSPF) packets
OSPF-Redistribution	Information regarding the Open Shortest Path First (OSPF) redistribution of routes with a different routing protocol source
OSPF-Router	Information regarding the Open Shortest Path First (OSPF) Router
Outband	Information regarding the outband interface (serial)

This parameter ...	...causes the following message in the trace:
Packet-dump	Displays the first 64 bytes of a packet in hexadecimal
PbSpot-Advertisement	Information regarding the insertion of advertising in the Public Spot
PCAP	Information regarding Packet Capture (PCAP)
PMS	Information regarding the Fidelio interface (PMS - Property Management System)
Port-Listener-Switch	Information regarding the switch between PSec and IPSec-over-HTTPS
PPP	PPP protocol negotiation
PRP	Information regarding the Parallel Redundancy Protocol (PRP)
Provisioning	Information regarding provisioning of DECT base stations
PSTN-MNGMT	Information regarding the setup and termination of connections between PSTN devices (Analog/ISDN) and betweem PSTN and SIP
Q.931	Information regarding the ISDN D-Channel Layer 3 Protocol
RADIUS-Client	Informationen about the RADIUS-Client
RADIUS-Server	Information about the RADIUS-Server
RADSEC	Information about RADSEC
RIP	IP Routing Information Protocol
Rollout-Agent	Information regarding the Rollout-Agent
Rollout-Wizard	Information regarding the Rollout-Wizard
Route-Monitor	Information regarding the Route-Monitor
SCEP-CA	Information regarding the Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA)
SCEP-Client	Information regarding the Simple Certificate Enrollment Protocol (SCEP) Client
Script	Script negotiation
Serial	Information on the state of the serial interface
SFP	Status information regarding SFP ports
SI3220	Status information regarding the SI3220 SLIC chip
SIP-ALG	Status information regarding SIP-ALG (Application Layer Gateway)
SIP-ALG-Packet	Shows packets transmitted via the SIP-ALG (Application Layer Gateway)
SIP-Connection	Status information regarding the setup and termination of SIP connections
SIP-packet	SIP information that is exchanged between a VoIP router and a SIP provider or an upstream SIP telephone system
SLIC	Status information about the analog telephony interface
SMTP-client	E-mail processing by the internal mail client
SNTP	Simple network time protocol
Spgtree	Information on spanning tree protocol

This parameter ...	...causes the following message in the trace:
Status	Connection status messages
SSH	Information regarding SSH connections to the SSH server and from the SSH client
SSL-Encapsulation	Information regarding VPN encapsulation via IPSec-over-HTTPS
T.38	Debug output for the T.38 library
Tacacs+	Information regarding the TACACS+ protocol
TCP	Information regarding TCP connections orifginating from or directed to the device
TFTP-Client	Information regarding TFTP connections initiated by the TFTP-Client
TLS	Information regarding SSL/TLS connections originating from or directed to the device
TR064-StateEngine	Information about the State-Machine in TR-064
TR069-Engine	Information regarding TR-069/CWMP
TR069-Message	Information regarding messages in TR-069/CWMP
TR069-State	Information regarding the State-Machine in TR-069/CWMP
USB	Information on the state of the USB interface
UserDef-Wizards	Information regarding the user-defined wizards in WEBconfig
VCM-DNS	Information regarding the DNS resolution of the Voice Call Manager
VDSL-CTRL	Shows all management packets of the internal VDSL modem
VDSL-DATA	Shows all packets transmitted via the internal VDSL modem
VDSL-Modem	Extended status regarding the internal VDSL modem
VDSL-Status	Information about the connection status as well as the setup and termination of the internal VDSL modem
VLAN	Information about VLAN tagging for individual packets
VLB-Packet	Packet information regarding the IKEv2 Server-Loadbalancer
VLB-Status	Status information regarding the IKEv2 Server-Loadbalancer
VPN-Debug	Extensive debug information for VPN connections
VPN-IKE	Shows IKE packets in the VPN
VPN-Mesh	Trace for *LANCOM Advanced Mesh VPN (AMVPN)* on page 886.
VPN-Packet	IPSec and IKE packets
VPN-Status	IPSec and IKE negotiations
VRRP	Information on the virtual router redundancy protocol
VRRP-Status	Information about processing the Virtual Router Redundancy Protocol (VRRP), e.g. information regarding states, roles, neigbors and errors
VRRP-Packet	Information regarding packets of the Virtual Router Redundancy Protocol (VRRP)
WISPr-PbSpot	Information about the Wireless Internet Service Provider Roaming (WISPr) protocol in the Public Spot

This parameter ...	...causes the following message in the trace:
WePaper-Coordination	Status information regarding the coordinated ePaper channel selection
WireGuard	Enables the basic WireGuard traces of negotiation packets as well as status and debug information.
WG-Packet	Displays the WireGuard payload packets.
WLAN	Information on activity in the wireless networks
WLAN-ACL	Status messages about MAC filtering rules. The display depends on how the WLAN data trace is configured. If a MAC address is specified there, the trace shows only the filter results relating to that specific MAC address.
WLAN-Adapt-RF-Opt	Information regarding Adaptive RF Optimization events
WLAN-AGGREGATION	Information regarding aggregation of WLAN packets (Note: Only works with 802.11n chipsets)
WLAN-ANI	Information regarding Adaptive Noise Immunity
WLAN-CCA	Information regarding WLAN-CCA (Clear Channel Assessment) (Note: Only works with 802.11n chipsets)
WLAN-DATA	Output of all packets transmitted via the internal WLAN interfaces
WLAN-NOISE	Status information regarding the noise level of the WLAN modules
WLAN-POWERSAVING	Status information regarding WLAN-Power-Saving (Note: Only works with 802.11n chipsets)
WLAN-OFFLOAD	Additional statis information regarding WLAN modules with 802.11ac or newer chipsets
WLAN-OWE	Status information regarding Opportunistic Wireless Encryption (Enhanced Open)
WLAN-RATE	Status information regarding rate adaption of WLAN modules with 802.11n chipset
WLAN-SAE	Status information regarding SAE authentication, which is used with WPA3
WLAN-STATUS	General WLAN status information
WLAN-STEERING	Status information regarding WLAN-Client-Management
WLAN-STRENGTH	Status information regarding the seen signal strength of connected WLAN clients or P2P connections
WLC-Steering	Status information regarding WLC-based Client-Steering
WLC-Tunnel	Information regarding Status connections between two WLAN-Controllers
WWAN-Control	Output of the management communication of the internal WWAN interface
WWAN-Data	Output of all packets transmitted via the internal WWAN interface
WWAN-Modem	Extended status information regarding the internal WWAN interface
XML-Interface-PbSpot	Messages from the Public Spot XML interface

Overview of CAPWAP parameters with the show command

The following information about the CAPWAP service can be viewed using the command line:

Table 5: Overview of all CAPWAP parameters with the show command

Parameters	Meaning
`-addresses [<IfcNum>]`	Shows the address tables of an individual or all WLC tunnels. In the case of an individual WLC tunnel, enter for the `<IfcNum>` the number of logical WLC tunnel interface, for example `10`.
`-groups`	Shows the information for an individual or all available assignment/tag groups.

You can supplement the command `show capwap groups` with the parameters listed below, which control the scope of the displayed information:

Table 6: Overview of all CAPWAP group parameters with the show command

Parameters	Meaning
`all`	Shows the names configured in the setup menu and the device's internal names for all assignment/tag groups as well as the default groups that were set up. The default group represents an internal group which contains all APs.
`<group1> <group2> <…>`	Shows all APs of the respective assignment/tag groups.
`-l <location>`	Shows all APs of the respective location.
`-c <country>`	Shows all APs of the respective country.
`-i <city>`	Shows all APs of the respective city.
`-s <street>`	Shows all APs of the respective street.
`-b <building>`	Shows all APs of the respective building.
`-f <floor>`	Shows all APs of the respective floor.
`-r <room>`	Shows all APs of the respective room description.
`-d <device>`	Shows all APs that have the specified device name.
`-v <firmware>`	Shows all APs which have the specified firmware. To do this, enter the version number for `<firmware>` followed by the build number, e.g., `9.00.0001`.
`-x <firmware>`	Shows all APs with a firmware version lower than the one installed on the current device.
`-y <firmware>`	Shows all APs with a firmware version the same or lower than the one installed on the current device.
`-z <firmware>`	Shows all APs with a firmware version higher than the one installed on the current device.
`-t <firmware>`	Shows all APs with a firmware version the same or higher than the one installed on the current device.
`-n <intranet>`	Shows all APs with an IP belonging to the specified Intranet address.
`-p <profile>`	Shows all APs that have been assigned with the specified WLAN profile.
`rmgrp <group1 intern_name> <group2 intern_name> …`	Deletes the group(s) with the specified internal names from the memory of the device. Use this command to free up the main memory if too large a number of groups is degrading the performance of the device. The entry in the setup menu is unaffected by this action.
`resetgrps`	Deletes all groups except the default group.

For location information the device evaluates the information entered under **Location** in the access point table. The following field names are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

For instance, the location entry `co=Germany, ci=Aachen` allows you to list all of the managed APs in Aachen from the console of the WLC with the command `+show capwap group -i Aachen`.

Example commands

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```

Overview of IPv6-specific show commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- *IPv6 addresses*: `show ipv6-addresses`
- *IPv6 prefixes*: `show ipv6-prefixes`
- *IPv6 interfaces*: `show ipv6-interfaces`
- *IPv6 neighbor cache*: `show ipv6-neighbour-cache`
- *IPv6 DHCP server* `show dhcp6-server`
- *IPv6 DHCP client* `show dhcpv6-client`
- *IPv6 route*: `show ipv6-route`

Additionally, IPv6 communications can be followed with the `trace` command.

IPv6 addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80:`.

The output is formatted as follows:

```
<Interface> :
<IPv6 address>, <status>, <attribute>, (<type>)
```

Table 7: Components of the command-line output `show ipv6-addresses`

Output	Comment
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	The status field can contain the following values: › TENTATIVE

Output	Comment
	Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. › PREFERRED The address is valid › DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. › INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	Shows an attribute of the IPv6 address. Possible attributes are: › None No special attributes › (ANYCAST) This is an anycast address › (AUTO CONFIG) The address was retrieved by auto-configuration › (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

IPv6 prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

Delegated prefixes

All prefixes that the router has obtained by delegation.

Advertised prefixes

All prefixes that the router announces in its router advertisements.

Deprecated prefixes

All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

IPv6-Interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

<Interface> : <Status>, <Forwarding>, <Firewall>

Table 8: Components of the command-line output `show ipv6-interfaces`

Output	Comment
Interface	The name of the interface

Output	Comment
Status	The status of the interface Possible entries are: › oper status is up › oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: › forwarding is enabled › forwarding is disabled
Firewall	The status of the firewall. Possible entries are: › forwarding is enabled › firewall is disabled

IPv6 neighbor cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

```
<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>
```

Table 9: Components of the command-line output `show ipv6-neighbor-cache`

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)
Status	The status of the connection to neighboring devices. Possible entries are: › INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. › REACHABLE The neighbor was reached in the last ten seconds. › STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. › DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols. › PROBE The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.
Source	The IPv6 address at which the neighbor was detected.

IPv6 DHCP server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

IPv6 DHCP client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and which prefixes and DNS server it is using.

IPv6 route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

2.2.4.6 Environment variables

Environment variables are device-specific global variables with predefined values that you can insert anywhere on the command line as dynamic placeholders. An overview of the environment variables and their values can be output using the appropriate CLI commands (see below).

All predefined environment variables begin with two underscores: When entering commands on the command line, the variables are preceded by a dollar sign.

Table 10: Overview of all environment variables

Variable name	Contents
`__BLDDEVICE`	The sub-project of the device. The sub-project generally consists of a string without spaces and it stands for the hardware model of the current device.
`__DEVICE`	The type of the device, for example as displayed in LANconfig or on the device type label.
`__FWBUILD`	The build number of the firmware currently used in the device. The build number is a four-digit number
`__FWVERSION`	The version number of the firmware currently used in the device, in the form 'x.yy'. The firmware version consists of the major release before the dot and the minor release after it.
`__LDRBUILD`	The build number of the firmware currently operating in the device. The build number is a four-digit number
`__LDRVERSION`	The version number of the loader currently installed in the device, in the form 'x.yy'. The loader version consists of the major release before the dot and the minor release after it.
`__MACADDRESS`	The type of the device, given as a 12-digit string of hexadecimal values with lowercase letters and no separators.
`__SERIALNO`	The device serial number.
`__SYSNAME`	The system name of the device.

Use the following commands in the CLI to display or modify environment variables:

- `printenv`: Displays all environment variables and their current values. If you have set one or more environment variables with the command `setenv`, the output of the command `printenv` shows the user-defined value at the top and the default value below it.
- `echo $__device`: Displays the current values of a single environment variable, in this example the value for the variable '__DEVICE'.

- `setenv __device MeinWert`: Sets the value of an environment variable to the desired value.
- `unsetenv __device`: Sets the value of an environment variable to the default value.

2.2.4.7 Keyboard shortcuts for the command line

The following shortcuts can be used to edit the commands on the command line. The "ESC key sequences" show (for comparison) the shortcuts used on typical VT100/ANSI terminals:

Table 11: Overview of CLI keyboard shortcuts

Shortcut	Esc key sequences	Description
Up arrow	ESC [A	In the list of commands last run, jumps one position up (in the direction of older commands).
Down arrow	ESC [B	In the list of commands last run, jumps one position down (in the direction of newer commands).
Right arrow	Ctrl-F ESC [C	Moves the insert cursor one position to the right.
Left arrow	Ctrl-B ESC [D	Moves the insert cursor one position to the left.
Home or Pos1	Ctrl-A ESC [A ESC [1~ (	Moves the insert cursor to the first character in the line.
Close	Ctrl-E ESC [F ESC OF ESC [4~	Moves the insert cursor to the last character in the line.
Ins	ESC [ESC [2~	Switches between input and overwrite modes.
Del	Ctrl-D ESC <BS> ESC [3~	Deletes the character at the current position of the insert cursor or ends the Telnet session if the line is blank.
erase	<BS><DEL>	Deletes the next character to the left of the insert cursor.
erase-bol	Ctrl-U	Deletes all characters to the left of the insert cursor.
erase-eol	Ctrl-K	Deletes all characters to the right of the insert cursor.
Tabulator		Completes the input from the current position of the insert cursor for a command or path of the LCOS menu structure: **1.** If there is only one possibility of completing the command/path, this is accepted by the line. **2.** If there is more than one possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. Pressing the Tab key again displays a list of all possibilities to complete the entry. Then enter e.g. another letter, to allow unambiguous completion of the input. **3.** If there is no possibility of completing the command/path, this is indicated by an audible sound when pressing the Tab key. No further actions are run. Further information on the special features of the Tab key for scripts can be found separately in the section *Tab command when scripting* on page 81,

Tab command when scripting

When working with scripts, the `tab` command enables the desired columns for the subsequent `set` command.

When you perform the configuration with a command line tool, you generally supplement the set command with the values for the columns of the table.

For example, you set the values for the performance settings of a WLAN interface as follows:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?
```

```
Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 Chars from: 1234567890

> set WLAN-1 Yes *
```

In this example the Performance table has three columns:

- Ifc, the desired interface
- Enable or disable QoS
- The desired value for TX bursting

With the command `set WLAN-1 Yes *` you enable the QoS function for WLAN-1, and you leave the value for TX bursting unchanged with the asterisk (*).

Working with the `set` command in this way is adequate for tables with only a few columns. However, tables with many columns can pose a major challenge. For example, the table under **Setup** > **Interfaces** > **WLAN** > **Transmission** contains 22 entries:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?

Possible Entries for columns in Transmission:
[1][Ifc]                 : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17), WLAN-1-4 (18), WLAN-1-5 (19), WLAN-1-6
(20), WLAN-1-7 (21), WLAN-1-8 (22)
[2][Packet-Size]         : 5 Chars from: 1234567890
[3][Min-Tx-Rate]         : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[9][Max-Tx-Rate]         : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M
 (12), 36M (13), 48M (14), 54M (15)
[4][Basic-Rate]          : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M
 (13), 48M (14), 54M (15)
[19][EAPOL-Rate]         : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M (11),
 24M (12), 36M (13), 48M (14), 54M (15), HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35), HT-2-13M (36), HT-2-26M (37),
HT-2-39M (38), HT-2-52M (39), HT-2-78M (40), HT-2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]       : 3 Chars from: 1234567890
[11][Soft-Retries]       : 3 Chars from: 1234567890
[7][11b-Preamble]        : Auto (0), Long (1)
[16][Min-HT-MCS]         : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[17][Max-HT-MCS]         : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13
 (6), MCS-6/14 (7), MCS-7/15 (8)
[23][Use-STBC]           : No (0), Yes (1)
[24][Use-LDPC]           : No (0), Yes (1)
[13][Short-Guard-Interval]  : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]    : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
[20][Max-Aggr.-Packet-Count]    : 2 Chars from: 1234567890
[6][RTS-Threshold]       : 5 Chars from: 1234567890
[10][Min-Frag-Len]       : 5 Chars from: 1234567890
[21][ProbeRsp-Retries]   : 3 Chars from: 1234567890
```

Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
> set WLAN-1-3 * * * * * * * * * * * * No
```

The asterisks for the values after the column for the short guard interval are unnecessary in this example, as the columns will be ignored when setting the new values.

As an alternative to this rather confusing and error-prone notation, you can use the `tab` command as the first step to determine which columns are changed with the subsequent `set` command:

```
> tab Ifc short guard-Interval
> set WLAN-1-3 No
```

The `tab` command also makes it possible to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
> tab Ifc short guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```

The tables may only contain only a selection of the columns, depending on the hardware model. The `tab` command ignores columns which do not exist for that device. This gives you the option to develop unified scripts for different hardware models. The `tab` instructions in the scripts reference the maximum number of required columns. Depending on the model, the script only performs the `set` instructions for the existing columns.

You can also abbreviate the `tab`command with curly brackets. Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
> set WLAN-1-3 {short-guard} No
```

The curly brackets also enable you to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
> set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

2.2.4.8 Function keys for the command line

The function keys (the F keys on the keyboard) allow users to save frequently used command sequences and to call them easily from the command line.

This function is configured in the Setup menu under **Config** > **Function-Keys**. Use thedrop-down menu under **Key** to select one of the function keys F1 to F12 and, under **Mapping**, enter the command sequence just as you would on the command line. You can enter any of the commands/shortcuts possible on the LCOS command line.

Special features of the caret character

When using the caret character (^) in your commands, be aware that this is also used to map special control commands with ASCII values below 32:

- ^A stands for Ctrl-A (ASCII 1)
- ^Z stands for Ctrl-Z (ASCII 26)
- ^[stands for Escape (ASCII 27)
- ^^ A double caret symbol stands for the caret symbol itself.

If a caret symbol is entered in a dialog field or editor followed directly by another character, the operating system may possibly interpret this sequence as another special character. By entering `caret + A`, the Windows operating system outputs an Â. To enter the caret character itself, enter a space in front of the subsequent characters. The sequence ^A is thus formed from `caret character + space + A`.

2.2.5 SNMP management program

The Simple Network Management Protocol (SNMP) enables devices on a network to be monitored and configured from a central instance. Since its initial release in 1988, it has continued to evolve to meet the needs of increasingly complex network infrastructures and the demands for user-friendliness, security and flexibility.

LCOS supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

Along with the LCMS tools (LANCOM Management System), there are a range of configuration and management programs that you can use to monitor or control network components that are equipped with an SNMP agent, including routers, switches, printers, firewalls, and others. These programs include commercial products, but also numerous applications available on an open-source, freeware or shareware basis.

The MIB (Management Information Base) file of the device, which is required by SNMP programs, can be conveniently generated with WEBconfig (see *Retrieving the SNMP device MIB* on page 40) or on the command-line console using the command `readmib`.

2.3 LANCOM Layer 2 Management protocol (LL2M)

2.3.1 Introduction

A basic pre-requisite for all methods device configuration is for an IP connection to exist between the configuration computer and the device. No matter whether LANconfig, WEBconfig or Telnet is used; no configuration commands can be sent to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. The only option in this case is to access the device via the serial configuration interface, which however is not available on all devices, or to reset the device to its factory settings. However, both options require physical access to the device—this may not always be the case for the concealed installation of access points and can represent considerable overhead for larger-scale installations.

The **LANCOM Layer 2 Management Protocol (LL2M)** is used to also enable configuration access to a device even without an IP connection. All this protocol requires is a connection on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server, which then responds to the requests or runs the commands. The LL2M client is integrated into LCOS and is run from the command line. The LL2M server is also integrated into LCOS and is usually only enabled for a brief period after device power-on. In this time frame, an administrator can use the LL2M client to perform changes to the configuration of the device running the LL2M server.

2.3.2 Configuring the LL2M server

Activation and configuration of the LL2M server is done exclusively via the setup menu of a device. The following steps show you which settings are required:

1. In WEBconfig or in a terminal program, switch to the menu item `Setup/Config/LL2M`.
2. Set the parameter **Operating** to **Yes**.
3. Set the **Time limit** in seconds for an LL2M client to reach the LL2M server after booting/powering up the device. The LL2M server is disabled automatically after expiry of the time limit. The value '0' disables the time limit. The LL2M server stays permanently enabled in this state.

2.3.3 Commands for the LL2M client

An encrypted tunnel is set up for every LL2M command to protect the transmitted log-in information. To use the integrated LL2M client, start a terminal session on a device that has local access to the LL2M server via the available physical medium (LAN, WLAN). The following commands can be used to contact the LL2M server in this console session:



You must have root rights on the LL2M server to run commands on the LL2M client.

LL2Mdetect

The LL2M client uses this command to send a SYSINFO request to the LL2M server. The server then sends its system information, such as hardware and serial number, back to the client for display. The LL2Mdetect command can be restricted with the following parameters:

-a <MAC-address>

Restricts the command to those devices with the specified MAC address only. Enter the MAC address in the format `00a057010203`, `00-a0-57-01-02-03` or `00:a0:57:01:02:03`.

If no MAC limitations are set, the "detect" is sent as a multicast (or alternatively using `-b` as a broadcast) to all LL2M-compatible devices. To contact groups of MAC addresses, `*` and `x` can be used as wildcards in individual MAC address positions, e.g., `00-a0-57-xx-xx-xx` for all devices' MAC addresses.

In a command line with multiple parameters, the final parameter **must** be `-a`. A different order is not allowed.

-b

Explicitly sends the LL2Mdetect request as a broadcast and not as a multicast.

-f <Version>

Restricts the command to those devices with the corresponding firmware version only.

-r <Hardware-Release>

Restricts the command to those devices with the corresponding hardware release only.

-s <Serial number>

Restricts the command to those devices with the corresponding serial number only.

-t <Hardware-Type>

Restricts the command to those devices of the corresponding hardware type only.

-v <VLAN-ID>

Only sends the LL2Mdetect request on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

The command `ll2mdetect -r A` sends a SYSINFO request to all devices of the hardware release "A". The response from the LL2M server then contains the following information:

- Device name
- Device type
- Serial number
- MAC address
- Hardware release
- Firmware version with date

LL2Mexec

The LL2M client uses this command to send a single-line command to run on the LL2M server. Multiple commands can be combined in one LL2M command by using semicolons as separators. Depending on the command, the actions are run on the remote device and the responses from the remote device are sent to the LL2M client for display. The LL2Mexec command conforms to the following syntax:

```
ll2mexec <User>[:<Password>]@<MAC address>
```

The LL2Mexec command can be restricted with the following parameters:

`-i <WLAN-Interface>`

Only sends the LL2Mexec command only on the specified WLAN interface.

`-v <VLAN-ID>`

Only sends the LL2Mexec command on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.

For example, the command line `ll2mexec root@00a057010203 set /setup/name MyDevice` logs in the LL2M client as "root" on the LL2M server with the MAC address "00a057010203". Since the password was not included, the device first looks for the corresponding username in the local database and automatically uses the password for this user. If the username is also not included, the login data of the currently registered user for the CLI session is used. Then the LL2M client sets the name of the remote device to the value 'MyDevice'.

2.4 Saving and loading device-configuration and script files

A device configuration file contains all of its settings. Script files are useful for managing the settings of a device automatically. To protect of these files against unauthorized access or transmission errors, it is possible to export them from or upload them to the device in an encrypted state and with a checksum.

There are three different file types:

- No checksum, no encryption: A text file with content readable by a text editor.
- Checksum: The text file contains information about the checksum and the hash algorithm for calculating this checksum. The contents of this text file is readable with a simple text editor.

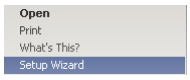
  LANconfig prior to version 9.10 recognizes files with checksums.

- Encryption: Before the file is exported it is encrypted by the device using a password chosen by the administrator. The text file contains information about the encryption algorithm used, as well as a checksum. The contents of the text file is no longer decipherable by a text editor, with the exception of the file header.

  LANconfig prior to version 9.10 cannot read encrypted files.

The file extensions of these files are `.lcf` for configuration files or `.lcs` for script files. The detection of a file that is encrypted and/or contains a checksum relies exclusively on the file header.

The following functions are available from the Windows Explorer context menu:



Open

This menu item opens the configuration in LANconfig.

This item only appears for configuration files with the extension `.lcf`.

What's this

This menu item opens a help text which gives users information about dealing with this file.

Print

This menu item enables you to print the file.

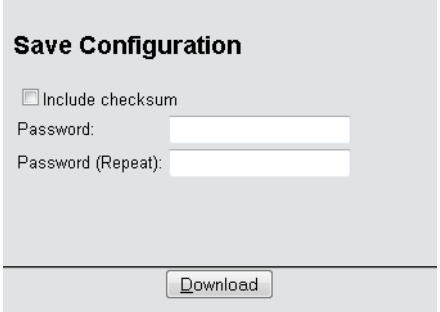
Setup Wizard

This menu item starts the LANconfig Setup Wizard.

This item only appears for configuration files with the extension `.lcf`.

2.4.1 Configuration management with WEBconfig and the console

To export a configuration file from WEBconfig, navigate to the view **Extras** > **File management** > **Save configuration**.



The following options are available:

No entries

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted configuration file without a checksum.

Include checksum

A click on **Download** invokes the dialog for downloading an unencrypted configuration file with a checksum.

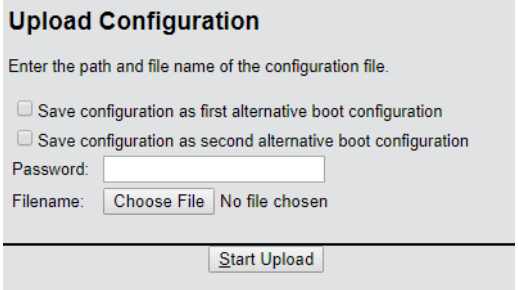
Password

Specify a password if you want to encrypt the configuration file before downloading it.

To save the configuration from the console, use the following parameters:

- `readconfig`: Backs up the configuration without checksum and encryption.
- `readconfig -h`: Adds a checksum to the configuration file.
- `readconfig -s <password>`: Encrypts the configuration file with the use of the specified password.

To upload a configuration file with WEBconfig, navigate to the view **Extras** > **File management** > **Upload configuration**.

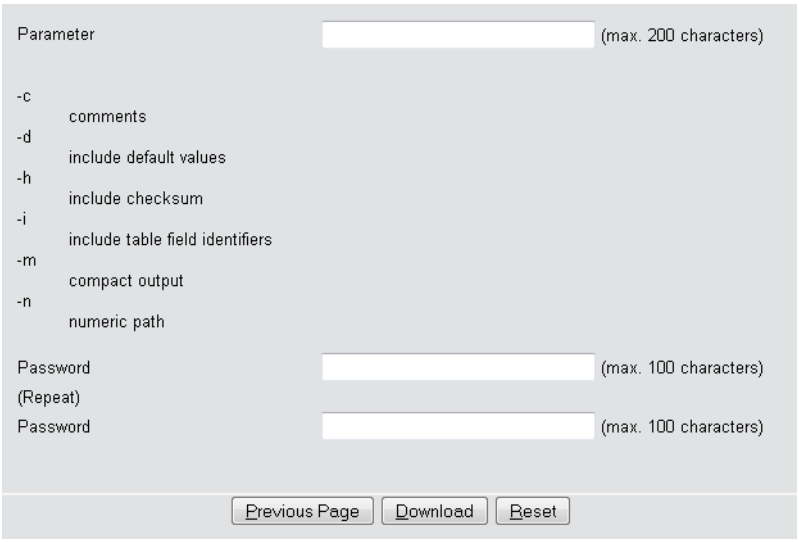


If the configuration file is encrypted, enter the appropriate password and click on **Start upload**.

For more information about alternate boot configurations, see the chapter *Alternative boot config*.

2.4.2 Script management with WEBconfig and the console

To export a script file from WEBconfig, navigate to the view **Extras** > **File management** > **Save configuration script**.



The following options are available:

Parameters

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted script file without a checksum.

Password

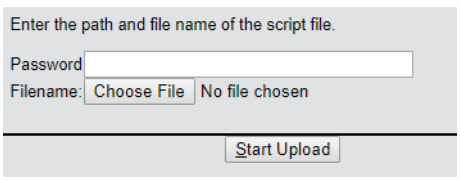
Specify a password if you want to encrypt the script file before downloading it.

To save the script file from the console, the following parameters are available:

- `readscript`: Backs up the configuration without checksum and encryption.
- `readscript -h`: Adds a checksum to the configuration file.
- `readscript -s <password>`: Encrypts the configuration file with the use of the specified password.
- `readscript -o`: Replaces the passwords with a "*" to obfuscate them in the text output.

More information about the parameters, see the chapter *Commands for the console* in the section about `readscript`.

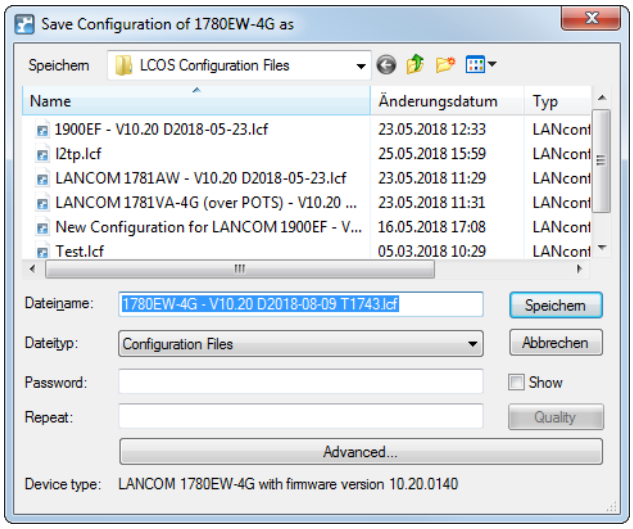
To upload a script file with WEBconfig, navigate to the view **Extras** > **File management** > **Execute configuration script**.



If the script file is encrypted, enter the appropriate password and click on **Start upload**.

2.4.3 Configuration management with LANconfig

You can use LANconfig to save a configuration file by right-clicking on the corresponding device in the list of devices. From the context dialog, open the save dialog under **Configuration management** > **Save as file**.



The following entries are available:

File name

LANconfig composes the file name from various pieces of information (including version number, date and time). Change the name to suit your needs.

File type

Choose whether this is a configuration file or something else.

Password

Specify a password if you want to encrypt the configuration file before downloading it.

Under **Advanced** you can set optional parameters that are processed by the device when a configuration file is loaded automatically (auto-load). Use this to customize the configuration.

You can use LANconfig to upload a configuration file to the device by right-clicking on the device where the configuration is to be uploaded. From the context dialog, open the restore dialog under **Configuration management** > **Restore from file**.

Select the required configuration file, enter the password (if applicable) and click **Open** to upload the configuration to the device.

2.5 Alternative boot config

2.5.1 Introduction

The way that a device operates is determined by its configuration. The configuration is defined by the user and stored to a special portion of the flash memory that remains intact even when the device is restarted (configuration memory).

When shipped, the configuration memory is empty because it does not yet have a user-defined configuration. Once in operation, the configuration memory can be deleted again by carrying out a configuration reset. If a device with an empty configuration memory is restarted or rebooted, the parameter values are taken from a boot configuration containing default values for the respective model.

A configuration is only written to the configuration memory if at least one parameter has been changed. The full configuration is written to the configuration memory. Even if only the device name is changed, current values for all of the parameters available to the device are stored to the user-defined configuration. Values for unchanged parameters are taken from a boot configuration.

The devices can work with three different boot configurations:

Factory settings

These are the default values for the model as shipped. The standard boot configuration is contained in the device's firmware.

Customer-specific standard settings

These are the customer's own default settings for the model in question. These are used when the configuration memory is empty but the factory settings should not be used. This function provides the devices with persistent settings (i.e. remaining available however many times the device is rebooted or reset) that contain customer-specific standard settings for the boot procedure. Customer-specific standard settings are **not** deleted by a configuration reset. Customer-specific standard settings are stored to the first boot memory space.

Rollout configuration

This configuration is useful for large-scale rollout scenarios where multiple devices need a boot configuration that differs from the factory settings. The rollout configuration is activated by pressing the reset key for a particular length of time. The specialized rollout configuration is stored to the second boot memory space.

2.5.2 Using the boot configuration

When started normally, the devices try to use the available configurations in a set order:

1. User-defined configuration (in the configuration memory)
2. Customer-specific standard settings (in the first boot memory space)
3. Factory settings (in firmware)

The customer-specific standard settings are taken automatically and in preference to the factory settings, assuming that the configuration memory is empty.

Special features of the rollout configuration

The rollout configuration is activated with the reset button. The reset button fulfills various functions depending upon how long the button is pressed:

› **Less than 5 seconds**:

Boot (restart), whereby the user-defined configuration is loaded from the configuration memory. If the user-defined configuration is empty, then the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. Similarly, the factory settings are loaded if the first memory space is empty.

› **Longer than 5 seconds** until the **first time** that all device LEDs light up:

Configuration reset (deletes the configuration memory) followed by a restart. In this case the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. The factory settings are loaded if the first memory space is empty.

› **Longer than 15 seconds** until the **second time** that all device LEDs light up:

Activating the rollout configuration and deleting the user-defined configuration After restarting, the rollout configuration is started from memory space 2. The loading of the rollout configuration is visible when all LEDs on the device light up twice briefly in red. The factory settings are loaded if the second memory space is empty.

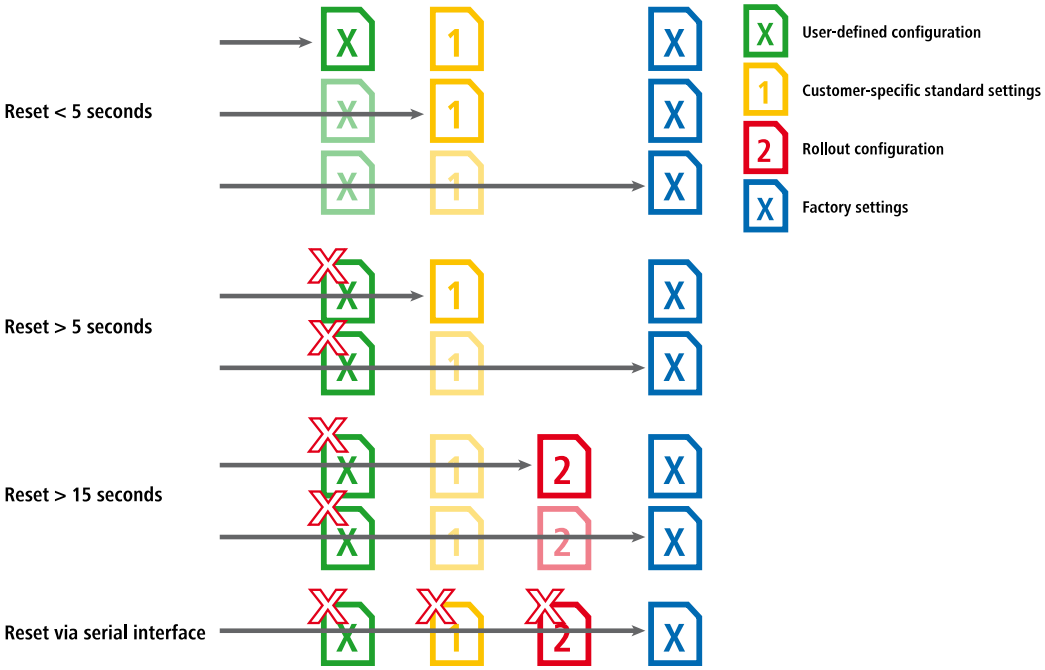
The rollout configuration is activated directly after restarting if the reset button is pressed for more than 15 seconds. The next time the device is restarted, the normal boot sequence applies again automatically, as listed above.

If the reset button has been deactivated in the configuration (set to **Ignore** or **Boot only**), it is impossible to load the rollout configuration.

Examples

The following diagram illustrates which configuration is loaded by the different reset procedures, depending on the status of the device.

- Pressing the reset button for **less than 5 seconds** loads the user-defined configuration. If no user-defined configuration exists, the device returns to the customer-specific standard settings. If these are not available either, the factory settings are loaded.
- Pressing the reset button for **longer than 15 seconds** deletes the custom configuration and loads the rollout configuration. If no rollout configuration exists, the factory settings are loaded.



2.5.3 Storing and uploading the boot configurations

Save

The customer-specific standard settings and the rollout configuration are saved in a compressed format. Using the command line, you can optionally save the current device configuration as your customer-specific standard settings or as a rollout configuration. Use one of the following commands for this:

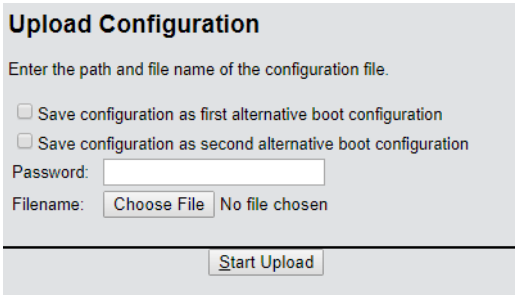
```
bootconfig --savecurrent [1,2,all]
```

```
bootconfig -s [1,2,all]
```

Entering the appropriate number ensures that either the first boot memory space for the customer-specific standard settings is selected, or the second boot memory space for the rollout configuration. The parameter `all` writes the current configuration to both memory spaces at the same time.

Upload

The customer-specific standard settings or the rollout configuration can be uploaded to the device with WEBconfig under **Extras** > **File management** > **Upload configuration**: Here you select the configuration file to be used and you activate the purpose as either customer-specific standard settings (first memory space) and/or rollout configuration. Alternative boot configurations must be available as *.lcf files.



If both memory spaces of the boot configuration are occupied (i.e. with customer-specific standard settings **and** a rollout configuration), then the device cannot be reset to the factory settings by using the reset button. Instead, reset a device as described under *Firmware upload via outband with reset of the configuration* on page 96.

For devices that only allow one boot configuration, the restriction described above does not apply. The reset button always resets these devices to their factory settings.

If the configuration file is encrypted, enter the appropriate password.

2.5.4 Deleting the boot configuration

The alternative and the special boot configurations cannot be deleted with the normal file functions. Instead you use one of the following CLI commands for this:

```
bootconfig --remove [1,2,all]
```

```
bootconfig -r [1,2,all]
```

Selecting the appropriate number ensures that the corresponding boot memory space is selected. The parameter `all` causes both memory spaces to be deleted at once.

2.5.5 Working with certificates

In order for VPN and SSL/TLS to function after a configuration reset, a **standard certificate** can be stored to the device as a **PKCS#12 container**. This standard certificate is only used by the customer-specific standard settings and the rollout configuration.

- If the customer-specific standard settings are loaded, the standard certificate is copied to the normal certificate storage location for VPN and SSL/TLS. This ensures that it remains available even after rebooting.
- If the rollout configuration is loaded, the standard certificate for VPN is used, but it is not copied. This means that in case of a restart (even without a configuration reset) the device has no access to the certificate.

You can upload the standard certificate into the device using either LANconfig or WEBconfig.

2.6 FirmSafe

2.6.1 Introduction

FirmSafe makes it safer to import new software: The firmware on the device is not simply overwritten, but a second firmware is stored in the device in addition (symmetric FirmSafe). This protects your device in case of events such as a power failure or an interrupted connection during the firmware upload.

Only one of the two firmware versions stored in the device can be active at any time. When new firmware is uploaded, the currently inactive firmware version will be overwritten. By selecting the FirmSafe mode you decide which firmware version should be activated after the upload.

2.6.2 Configuration

The firmware-upload mode is set in the Setup menu under **Firmware** > **Mode-Firmsafe**. Three different modes are available. LANconfig provides the options for uploading firmware upload either as an 'immediate' process by 'manual' means (cf. *Firmware upload via LANconfig* on page 94).

- **Immediate**: This option loads the new firmware and activates it immediately. The following situations can result:
  - The startup with the new firmware is successful and the device then operates as intended.
  - After uploading the firmware the device no longer responds. If the device does not automatically fall back to a previous firmware or if it starts with a minimal firmware, you can repeat the upload, for example via LL2M. If an error occurs during the upload, the device automatically activates the previous firmware and restarts.
- **Login**: In this mode, the device only activates the uploaded firmware temporarily in order to prevent problems from a failed upload. After activation, the device waits for a successful login via a terminal program or WEBconfig for the time (in seconds) set in the Setup menu under **Firmware** > **Timeout-Firmsafe**. Only after this login is the firmware activated.

  If the device no longer responds or it is impossible to log in, it automatically loads the previous firmware version and reboots the device with it.
- **Manual**: In this mode, the device only activates the uploaded firmware temporarily in order to prevent problems from a failed upload. The device starts with the new firmware and waits for the time period set under **Firmware** > **Timeout-Firmsafe** until the loaded firmware is manually activated and therefore becomes permanently effective.

  Using LANconfig, activate the new firmware with the menu item **Device** > **Firmware management** > **Activate firmware running in test mode**. In the Setup menu, you activate the firmware under **Firmware** > **Table-Firmsafe**. Using the CLI, enter the command line `set # active`, where '#' stands for the position of the firmware in the FirmSafe table.

  In this case, too, after the timeout has elapsed the device automatically switches back to the previous firmware and restarts.



It is only possible to upload a second firmware if the device has sufficient memory available for two complete firmware versions. Up-to-date firmware versions (with additional software options, if applicable) may take up more than half of the available memory in older hardware models. In this case these device uses the *asymmetric Firmsafe*.

2.6.3 Toggling the active firmware via console command

As of LCOS version 10.12, the current firmware can be switched over to the alternative firmware with a CLI command. The previously inactive firmware is set to "active" and the previously active firmware is set to "inactive". After entering the command, the device automatically executes a restart without further confirmation.

Under **/ Firmware**, enter the command `do switch-firmware`.

The restart is performed automatically.

2.6.4 Asymmetric FirmSafe

The large and growing range of functions in the firmware means that some models are unable to store two complete versions of the firmware at once. These devices benefit from the asymmetric FirmSafe feature.

With asymmetric FirmSafe, the device always contains a "complete version" along with a bare-bones version known as "minimal firmware". The minimal version normally remains unused, but it provides local access to the device after a failed upload of the complete firmware version (e.g. as a result of a power cut during the upload process) in order to load an executable version of the firmware onto the device (via LAN, WLAN, or the config interface).

The minimum firmware **cannot** be configured! Changes to the configuration via LANconfig, WEBconfig or Telnet are not stored to the device. Advanced functions, in particular the remote management via WAN, are **not** available as long as the minimal firmware is active. However, the LL2M server is also active in a minimal firmware version and offers access to the device provided it is reachable from an LL2M client over layer 2 (Ethernet).

2.6.4.1 Switching over to asymmetric FirmSafe

To switch devices to asymmetric FirmSafe, you first load the converter firmware onto the device. This converts the firmware currently **not activated** in the device into a minimal firmware version, creating room for new and more comprehensive firmware. This process only has to be performed once.

You can then load a new, complete firmware version onto the device, which becomes active after a successful upload. The minimal firmware remains in the device to ensure that the device can be accessed.

2.6.4.2 Firmware upgrade with asymmetric FirmSafe

The subsequent firmware upload automatically overwrites the **active** firmware with new firmware.

2.7 Uploading firmware to the device via a client

Firmware can be uploaded to the device in different ways, for example via LANconfig, WEBconfig or a terminal program. A number of different protocols are available here.

In most cases, uploading or updating the firmware does not change any of the settings in your device (exception: *Upload with reset*). Nevertheless, as a precaution you should create a complete backup of your configuration. You should also have a backup of the previous firmware version in case the update process fails and, for example, the device falls back to a minimum firmware that does not allow Internet access. If you no longer have the corresponding firmware file, look for it under *www.lancom-systems.com*.

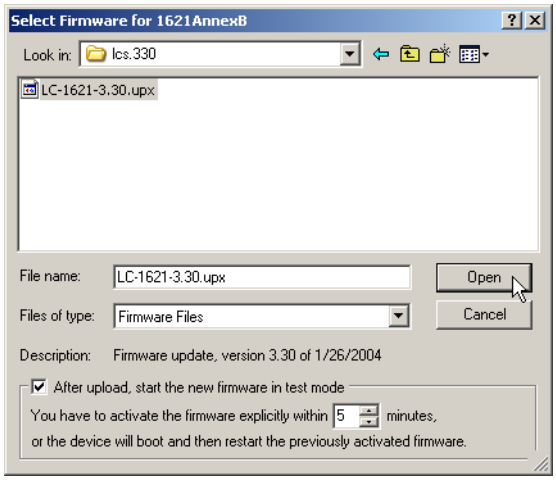
If the newly installed firmware contains parameters that are not available in the current firmware of the device, the missing values are supplemented with the default settings.

2.7.1 Firmware upload via LANconfig

This section describes how to load another firmware version into the device via LANconfig.

1. Select the device in the selection list and click on **Device** > **Firmware management** > **Upload new firmware**.
2. In the dialog box that opens, select the directory where the new version is located and mark the corresponding *.upx file.

LANconfig then displays the type, version and release date of the firmware.



3. Optional: Select whether the device should activate the firmware permanently after loading or initially operate it in a test mode. If you decide to use the test mode, specify a time period after which the device switches back to the previous firmware version if you do not activate the new firmware using the ***Configuration management***.

   This option is not available for devices that use *asymmetric FirmSafe*.

4. Click on **Open** to replace the existing firmware with the selected version.

LANconfig now starts with the firmware upload. You can track the process with the progress bar and log. After a successful upload, LANconfig restarts the device automatically.

2.7.2 Firmware upload via WEBconfig

In WEBconfig, you upload a new firmware version using the *File management* menu. Select the required firmware file and click on **Upload**. Just as with LANconfig, you have the option of uploading the firmware in test mode (see *Firmware upload via LANconfig* on page 94).

2.7.3 Firmware upload by terminal program

This section describes how to load another firmware version into the device with a terminal program. Two alternatives are available here:

- Upload via the serial configuration interface
- Upload via TFTP or SCP

Uploading via the serial connection requires a program that supports the XModem protocol, e.g. Windows HyperTerminal, Telix or the free software Tera Term. Uploading via TFTP or SCP works on a local or external network.

The following section describes a firmware upload via the serial configuration interface using HyperTerminal. Uploading firmware via TFTP or SCP is broadly very similar to any normal file upload. For more information, please see *Loading files directly from/to the device via TFTP, HTTP(S) or SCP* on page 100.

1. Use the serial configuration cable to connect the device to a computer.
2. On the computer, start a serial terminal program such as Hyperterminal.
3. Establish a connection using the following settings and login to the device with your login credentials:
   - Speed in bps: `115200`
   - Data bits: `8`
   - Stopbits: `1`
   - Parity: `None`

- Flow control: `RTS/CTS` or `RFR/CTS`

4. Change to the **Firmware** menu and use the command `set mode-firmsafe <value>` to set the desired FirmSafe mode, where `<value>` stands for one of the possible modes. If necessary, you can additionally set the time period for the firmware test under `set Timeout-firmsafe`.

   An explanation of the possible modes and the related configuration steps is available in the FirmSafe section *Configuration* on page 93.
5. The device is set to the ready-to-receive state by entering the action command `do firmware-upload`.
6. Start the upload process from your terminal program.
   - In Telix, click the button **Upload**, set **XModem** for the transfer and select the firmware file for upload.
   - In HyperTerminal, click **Transfer** > **Send file**, select the firmware file, set **XModem** as the protocol and start with **OK**.
   - In Tera Term, click **File** > **Transfer** > **XMODEM** > **Send** and select the firmware file for upload.

The firmware upload is now carried out. After a successful firmware upload, the device restarts.

2.7.4 Firmware upload via outband with reset of the configuration

If both memory spaces of the boot configuration are occupied (i.e. with customer-specific standard settings **and** a rollout configuration), then the device cannot be reset to the factory settings by using the reset button. The same applies if the function of the reset button is restricted to **Ignore** or **Boot only** and the configuration password is no longer available. In this case, you can only reset to the factory settings by means of the serial interface (outband).

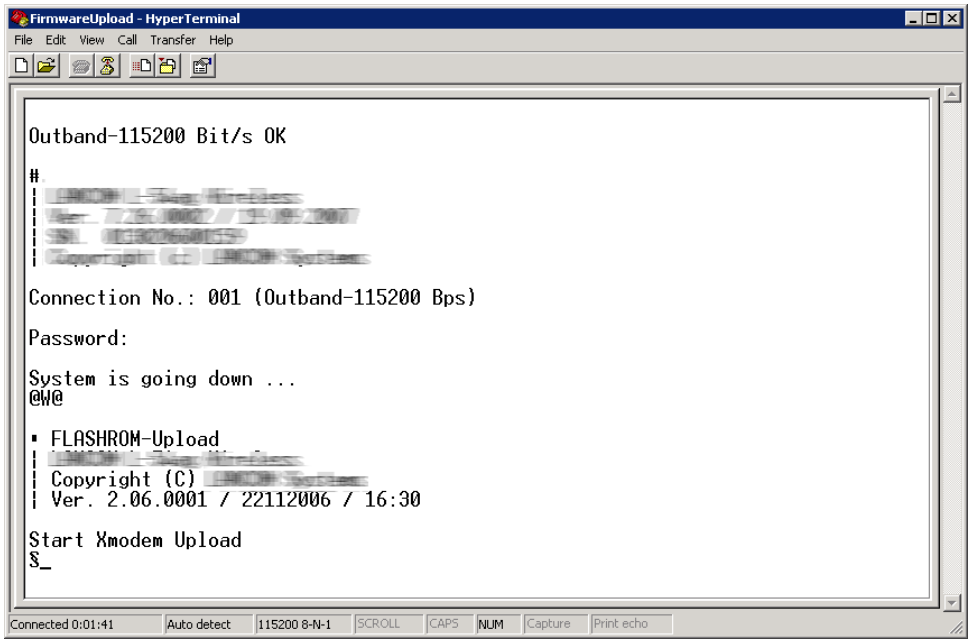
The serial interface is an optional way to upload firmware into the device. Entering the serial number of the device instead of the configuration password results in the device configuration being reset to its factory settings. In this way you can always regain access to the device if it becomes impossible to restore the factory settings in any other way.

This procedure completely deletes the configuration and the *boot configurations* stored on the device! The same applies to files stored in the device, such as any available rollout certificates. For this reason you should only use this option if you have no other way of accessing the device. The configuration and boot configuration are deleted even if the firmware upload is interrupted.

The following example application describes how to use HyperTerminal to upload firmware via the serial interface while resetting the configuration.

1. Use the serial configuration cable to connect the device to a computer.
2. On the computer, start a serial terminal program such as Hyperterminal: Windows HyperTerminal.
3. Set up a connection with the following settings:
   - Speed in bps: `115200`
   - Data bits: `8`
   - Stopbits: `1`
   - Parity: `None`
   - Flow control: `RTS/CTS` or `RFR/CTS`
4. In the terminal program's welcome screen, press the Return key until the request to enter the password appears.

5. Enter the serial number that is displayed under the firmware version and press the Return key again. The system then shuts down and is ready to receive the firmware upload.



6. In HyperTerminal, click **Transfer** > **Send file**, select the firmware file, set **XModem** as the protocol and start with **OK**.

The firmware upload is now carried out. After a successful firmware upload, the device restarts.

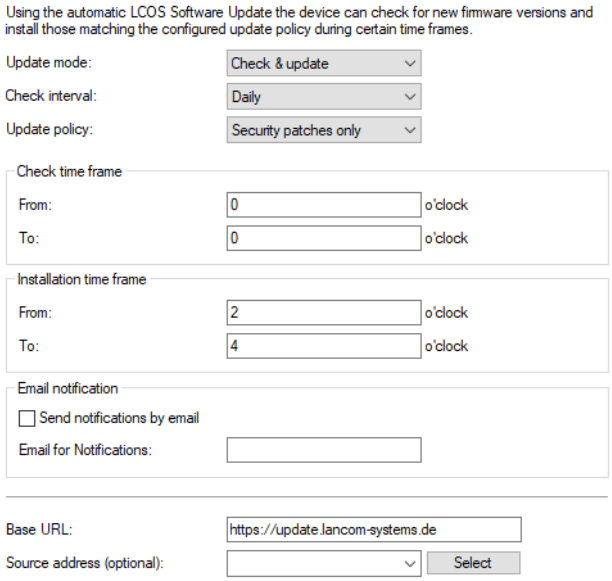
2.8 LANCOM Auto Updater

The LANCOM Auto Updater allows the automatic updating of on-site LANCOM devices without further user intervention. LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

2.8.1 Configuring the Auto Updater

The configuration for the LANCOM Auto Updater in LANconfig is located under **Management** > **Software update**.



Update mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

After booting, the Auto Updater sets a random time period within a day or a week for the check to be performed. The update itself is performed in the next time period between 02:00 - 04:00 (default).

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security patches only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest version w/o release

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 Rel.

Check time frame

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

Installation time frame

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Send notifications by e-mail

This setting determines whether the LANCOM Auto Updater sends e-mail notifications to the specified e-mail address. Administrators can use the e-mail notifications to receive information about events relating to the automatic firmware update by the Auto Updater. An e-mail is sent after the following events:

- An update was found (in the update mode “Check” only)
- An update was found and a time for automatic installation was scheduled (the in update mode “Check & Update”)
- An update has been successfully installed (including successful access check)
- An update was not successful and a fallback to the previously installed firmware was performed
- Error messages from the Auto Updater (e.g. update server could not be reached)

Notification is only given for automatically executed actions. If actions are started manually, e.g. an update check via LANmonitor or WEBconfig, then there is no e-mail notification.

E-mail address

Here you enter the e-mail address to be used when e-mail alerts are enabled.

Base URL

Specifies the URL of the server that provides the latest firmware versions.

Source address

A routing tag can be set automatically by specifying a loopback address.

2.9 Loading files directly from/to the device via TFTP, HTTP(S) or SCP

Various applications, such as loading configurations, firmware versions, scripts, and verifying server identity with certificates, require the relevant files to be stored to the device. You can to upload these files to the device with LANconfig or WEBconfig.

As an alternative you can use the command line to load the corresponding files directly into the device using TFTP, HTTP(S) or SCP. This process mainly simplifies device administration in larger installations that rely on regular updates to the firmware and/or configurations. You can choose whether to transfer a file from a computer to the device by means of a client, or to use the command line to instruct the device itself to load the file from a server.

2.9.1 Loading a file via a TFTP client

TFTP (Trivial File Transfer Protocol) is a very simple file transfer protocol for reading or writing files. It enables the easy transfer of files to other devices over the network. Other features such as those of the much more powerful FTP (e.g. rights assignment via chmod, display of existing files, user authentication) are not implemented.

LANconfig gives you the option to communicate with the device via TFTP. However, operating it is no different from using the other communication protocols. This chapter addresses alternative TFTP programs available for device communication.

Many Windows and Linux operating systems feature a command-line based TFTP client by default. In Windows 7 and later, however, the TFTP client needs to be activated first. Other clients are available, such as the free TFTP client-server application Tftpd32. Set the port to the default value `69`. The block size for data packets can be found in the parameter **Bytes-per-hashmark** in the setup menu of the device (normally `8192`).

2.9.1.1 Syntax

The syntax of the TFTP call is dependent on the operating system and program used. For the Windows-native TFTP client, for example, the syntax is as follows:

```
tftp [-i] <Host> get|put <LocalFile|Command> <RemoteFile|Command>
```

The ASCII format is preconfigured on many TFTP clients. Binary transmission therefore usually needs to be selected explicitly for the transfer of binary data (e.g. a firmware file). Under Windows this is done with the parameter `-i`.

If the device is password-protected, user name and password must be included in the TFTP command. In TFTP, the user name and password are coded in the source (TFTP read request) or target file names (TFTP write request). The file name is then composed either of the root password and the command to be executed (for supervisors), or of the combination of user name, password and then the command (for local administrators). A command sent by TFTP therefore resembles the following:

- `<Root-Password> <Command>`
- `<Username>:<Password>@<Command>`

Commands can appear as follows:

- `readmib`: Command for importing a device MIB file (SNMP management information base).
- `readconfig`: Command for reading a configuration file.
- `writeconfig`: Command for importing a configuration file.
- `writeflash`: Command for importing a firmware file.

The rights to use TFTP can be restricted for different types of administrators, see *Managing rights for different administrators* on page 113.

2.9.1.2 Example applications

- The command `writeflash` loads a firmware file into the device, and in the following example `10.0.0.1` stands for the IP address of the device and `LC-L451-8.82.0083.upx` for the file to be uploaded:

```
tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx writeflash
tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx MyAdmin:MyPasswd@writeflash
```

- Use the command `readmib` to read our the device MIB:

```
tftp 10.0.0.1 get readmib device.mib
```

- Use the command `readconfig` to read the configuration from the device using access credentials:

```
tftp 10.0.0.1 get root:MyPasswd@readconfig device.lcf
```

- Use the command `writeconfig` to write the configuration to the device using access credentials:

```
tftp 10.0.0.1 put device.lcf root:MyPasswd@writeconfig
```

The *settings made for FirmSafe* also apply to firmware uploads via TFTP.

2.9.1.3 Troubleshooting

If you are unable to connect to the device, your operating system's firewall may be blocking TFTP connections. If you have changed the firewall settings in the device, check here, too, that connections via TFTP are allowed. You can also check to see whether you have allowed access to the device from the network type that is being used for the upload (LANconfig settings are located under **Management** > **Admin** > **Access rights**).

2.9.2 Loading a file via an SCP client

SCP (Secure Copy Protocol) is a protocol for the secure transfer of data between two computers in a network. Administrators often use SCP for data exchange between servers or between a server and a workstation. Using an appropriate tool (e.g., PuTTY's additional program PSCP on Windows or Konqueror or Midnight Commander on Linux), data can also be exchanged between a machine and the device using the SCP protocol.

2.9.2.1 Syntax

The syntax of the SCP call depends on the program being used. For PSCP, the syntax on the Windows CLI is:

- **Sending files**

```
pscp.exe -scp [-pw <Password>] <LocalFile> <User>@<IP-Address>:target
```

- **Receiving files**

```
pscp.exe -scp [-pw <Password>] <User>@<IP-Address>:target <LocalFile>
```

The `target` on the remote device is inserted after a colon following the IP address. The target is either a file name (see *File Names for SCP File Transfer* on page 102) in the internal file system of the device, or it is `config`, `firmware` or `firmwarewithreset`. The targets `firmware` and `firmwarewithreset` are reserved exclusively for

importing firmware updates whereby the latter is followed by a configuration restart, while `config` is used for importing and exporting configuration files.

2.9.2.2 File Names for SCP File Transfer

In addition to the already listed `config`, `firmware`, and `firmwarewithreset`, the following table shows which files can be specifically read from the device and/or written to the device using SCP. These correspond to the files that are also available through WEBconfig file upload or download. When uploading, a password can optionally be provided using the `LCS_PASSWORD` environment variable.

Table 12: Overview of File Names for SCP File Transfer

Mount point	Read	Write	Description
ssl_cert	Yes	Yes	SSL – certificate (*.pem, *.crt. *.cer [BASE64])
ssl_privkey	No	Yes	SSL – private key (*.key [BASE64 unencrypted])
ssl_rootcert	Yes	Yes	SSL – root CA certificate (*.pem, *.crt. *.cer [BASE64])
ssl_pkcs12	No	Yes	SSL – container as PKCS#12 file (*.pfx, *.p12)
ssh_rsakey	No	Yes	SSL – RSA key (*.key [BASE64 unencrypted])
ssh_dsakey	No	Yes	SSL – DSA key (*.key [BASE64 unencrypted])
ssh_authkeys	Yes	Yes	SSH – accepted public key
ssh_ed25519key	No	Yes	SSH – ED25519 key (*.key [BASE64 unencrypted])
ssh_ed448key	No	Yes	SSH – ED448 key (*.key [BASE64 unencrypted])
vpn_rootcert	Yes	Yes	VPN – root CA certificate (*.pem, *.crt. *.cer [BASE64])
vpn_devcert	Yes	Yes	VPN – device certificate (*.pem, *.crt. *.cer [BASE64])
vpn_devprivkey	No	Yes	VPN – private device key (*.key [BASE64 unencrypted])
vpn_pkcs12	No	Yes	VPN – container (VPN1) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_2	No	Yes	VPN – container (VPN2) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_3	No	Yes	VPN – container (VPN3) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_4	No	Yes	VPN – container (VPN4) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_5	No	Yes	VPN – container (VPN5) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_6	No	Yes	VPN – container (VPN6) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_7	No	Yes	VPN – container (VPN7) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_8	No	Yes	VPN – container (VPN8) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_9	No	Yes	VPN – container (VPN9) as PKCS#12 file (*.pfx, *.p12)
vpn_add_cas	No	Yes	VPN – add additional CA certificates (*.pfx, *.p12, *.pem, *.crt. *.cer [BASE64])
eaptls_rootcert	Yes	Yes	EAP/TLS – root CA certificate (*.pem, *.crt. *.cer [BASE64])
eaptls_devcert	Yes	Yes	EAP/TLS – device certificate (*.pem, *.crt. *.cer [BASE64])
eaptls_privkey	No	Yes	EAP/TLS – private device key (*.key [BASE64 unencrypted])
eaptls_pkcs12	No	Yes	EAP/TLS – container as PKCS#12 file (*.pfx, *.p12)
radsec_rootcert	Yes	Yes	RADSEC – root CA certificate (*.pem, *.crt. *.cer [BASE64])
radsec_devcert	Yes	Yes	RADSEC – device certificate (*.pem, *.crt. *.cer [BASE64])
radsec_privkey	No	Yes	RADSEC – private device key (*.key [BASE64 unencrypted])

Mount point	Read	Write	Description
radsec_pkcs12	No	Yes	RADSEC – container as PKCS#12 file (*.pfx, *.p12)
radiuss_accnt_total	Yes	Yes	RADIUS server – summary accounting (*.csv)
scep_cert_list	Yes	Yes	SCEP-CA – certificate list
scep_cert_serial	Yes	Yes	SCEP-CA – serial number
scep_ca_backup	Yes	No	Backup for SCEP-CA – PKCS12 container
scep_ra_backup	Yes	No	Backup for SCEP-RA – PKCS12 container
scep_ca_pkcs12	No	Yes	SCEP-CA – PKCS12 container
scep_ra_pkcs12	No	Yes	SCEP-RA – PKCS12 container
pbspot_template_welcome	Yes	Yes	Public Spot – welcome page (*.html, *.htm)
pbspot_template_login	Yes	Yes	Public Spot – login page (*.html, *.htm)
pbspot_template_error	Yes	Yes	Public Spot – error page (*.html, *.htm)
pbspot_template_start	Yes	Yes	Public Spot – home page (*.html, *.htm)
pbspot_template_status	Yes	Yes	Public Spot – status page (*.html, *.htm)
pbspot_template_logoff	Yes	Yes	Public Spot – logoff page (*.html, *.htm)
pbspot_template_help	Yes	Yes	Public Spot – help page (*.html, *.htm)
pbspot_template_noproxy	Yes	Yes	Public Spot – no proxy page (*.html, *.htm)
pbspot_template_voucher	Yes	Yes	Public Spot – voucher page (*.html, *.htm)
pbspot_template_agb	Yes	Yes	Public Spot – GTC page (*.html, *.htm)
pbspot_formhdrimg	Yes	Yes	Public Spot – header image pages (*.gif, *.png, *.jpeg)
WLC_Script_1.lcs	Yes	Yes	CAPWAP – WLC_Script_1.lcs
WLC_Script_2.lcs	Yes	Yes	CAPWAP – WLC_Script_2.lcs
WLC_Script_3.lcs	Yes	Yes	CAPWAP – WLC_Script_3.lcs
default_pkcs12	No	Yes	
rollout_wizard	No	Yes	
rollout_template	No	Yes	
rollout_logo	No	Yes	
hip_cert_0	No	Yes	
issue	Yes	Yes	Text for display after command-line login (e.g.ASCII logos)
config	Yes	Yes	Importing and exporting configuration files
firmware	No	Yes	Uploading a firmware file to the passive firmware slot
firmwarewithreset	No	Yes	Like firmware, but with a subsequent configuration restart

2.9.2.3 Example applications

› For example, to transfer a file from your computer to the device, use a command as follows:

```
C:\>pscp.exe -scp -pw MyPwd c:\path\myfile.ext root@10.0.0.1:target
```

For example, to transfer a file from the device to your computer, change the order of source and destination:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:target c:\path\myfile.ext
```

Set the `target` as the name of a file with path.

- For example, to save the configuration from the device on your machine under the name `config.lcf`, use a command as follows:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:config c:\config.lcf
```

- For example, to upload new firmware from your computer to the device, use a command as follows:

```
C:\>pscp.exe -scp -pw MyPwd  c:\firmware.upx root@10.0.0.1:firmware
```

2.9.3 File download from a TFTP or HTTP(S) server

In addition to being able to use another machine to upload firmware, a configuration file, or a configuration script to the device, the device itself can also upload/download files itself from an HTTPS(S) or TFTP server in the local network or the Internet. For this purpose, the corresponding files are stored on an HTTPS(S) or TFTP server and, after a user has logged-in to the device, they are accessed by using the LCOS commands listed below.

A TFTP server is identical to an FTP server in terms of functionality, but uses a different protocol for data transmission. When using an HTTPS server, a certificate can be stored on the device which can be used to check the identity of the server later. In practice it is far simpler to provide a central HTTP(S) server with a unique Internet address (URI) than a comparable TFTP server, and, for example, an existing Web server can be modified to offer this function.

The different file types can then be called from this type of server with the following commands:

- `LoadConfig`: Uploads a configuration file (with file extension *.lcf) into the device.
- `LoadFirmware`: Uploads a firmware file (with file extension *.upx) into the device.
- `LoadScript`: Uploads a script file (file extension *.lcs) to the device, e.g., with partial configurations.
- `LoadFile`: Uploads various types of file to the device.



The `LoadFile` command only supports the protocols HTTP and HTTPS.

2.9.3.1 Syntax

The precise syntax of the load commands depends on which protocol is used (HTTP[S] or TFTP). Generally speaking, a call always consists of the command, applicable parameters, and the URL which references the file to be loaded. You can save this URL in the setup menu under **Autoload** > **Network** > **...** > **URL**. This allows you to upload firmware, configurations or script files simply by entering the command.

Connections to an HTTP(S) server

When using HTTP(S), the command can be specified in the usual URL notation. Set the protocol to either `http` or `https`:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

To access a password-protected area, you authenticate using the standard username/password notation:

```
<Command> <Parameter> <Protocol>://<Username>:<Password>@<Host>/<Directory>/<File>
```

Connections to a TFTP server

TFTP also functions with standard URL notation. Set the protocol in this case to `tftp`:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

Alternatively, you can replace the URL with appropriate parameters:

```
<Command> <Parameter> -s <Host> -f <Directory>/<File>
```

2.9.3.2 Parameters

The commands to connect to an HTTP(S) or TFTP server can be modified by specifying additional parameters. Not all parameters are available for all protocols. If certain default values can be configured from the Setup menu, the device

uses these values as long as you do not explicitly overwrite the values with the associated parameters. For example, this applies for the parameters of the version check.

Parameters for the connection

The following parameters allow you to change the way the device connects to the server.

-a <Address>

Available for protocol: HTTP, HTTPS, TFTP

Available for command: all

Use this parameter to specify an optional loopback address. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

By default, the server sends its replies back to the IP address of your device without you having to enter it here.

-f <Directory>/<File>

Available for protocol: TFTP

Available for command: all

Use this parameter to specify the path and name of the file on the server. Using this parameter in combination with `-s` means that no URL has to be specified.

-s <Host>

Available for protocol: TFTP

Available for command: all

Use this parameter to specify the DNS name or IP address of the server. Using this parameter in combination with `-f` means that no URL has to be specified.

Parameters for the version check

In the default settings, the conditions for firmware, configuration and script in the Setup menu (under **Autoload** > **Network** > **…**) are set to **unconditionally**. As a result, the commands LoadFirmware, LoadConfig, or LoadScript load or start the corresponding firmware, configuration, or script file **without** carrying out a version check. However, by specifying the appropriate parameter, you can override this setting when uploading any particular file.

-Cd

Available for protocol: HTTP, HTTPS, TFTP

Available for command: LoadFirmware, LoadConfig, LoadScript

This parameter checks if the file is **different** to the firmware or configuration on the device, or newer than the last executed script. When the LoadScript command is used, this parameter updates the checksum stored in the device for the most recently executed script.

-Cn

Available for protocol: HTTP, HTTPS, TFTP

Available for command: LoadFirmware

This parameter checks if the file is **newer** than the firmware on the device.

-m

Available for protocol: HTTP, HTTPS, TFTP

Available for command: LoadFirmware

This value defines the minimum version of the firmware. The firmware referenced by the command must be at least of this version in order for the command to execute.

-u

Available for protocol: HTTP, HTTPS, TFTP

Available for command: LoadFirmware, LoadConfig, LoadScript

This parameter disables the version checking. The file referenced by the command is uploaded and executed unconditionally. When the LoadScript command is used, this parameter does not change the checksum stored in the device for the most recently executed script.



The parameter -u always has priority over other parameters entered in a command.

Parameters for the certificate check

When transferring files from an HTTPS server to a client device, the network components check the identity of the remote site by using certificates. For the automatic loading from HTTPS servers, additional parameters are available for downloading and subsequently checking the certificates. You download the certificate in question to the device as **SSL – root CA certificate (*.pem, *.crt *.cer [BASE64])**, for example using the file management features of LANconfig or WEBconfig.

-c <MainDir>/<File>

Available for protocol: HTTPS

Available for command: all

Use this parameter to specify the name of the certificate that the device uses to verify the identity of the server before loading the requested file.

-d <Passphrase>

Available for protocol: HTTPS

Available for command: LoadFile

The device uses this passphrase to encrypt an unencrypted PKCS#12 container.

-p <MainDir>/<File>

Available for protocol: HTTPS

Available for command: LoadFile

Use this parameter to specify the name of the PKCS#12 container when downloading a file. The PKCS#12 container can contain multiple CA certificates, and thus supports the identity checking of HTTPS servers with certificate chains. A PKCS#12 container can additionally contain a device certificate and the corresponding private key, so that it can confirm the identity of the device to the HTTPS server if this server requires authentication by certificate.

-n

Available for protocol: HTTPS

Available for command: LoadFile

Use this parameter to deactivate the server name check when loading a file. If you specify the server in the URL as a DNS name (and not as an IP address), then the device checks the certificate for the corresponding server name. If the HTTPS server is a virtual server, then this server can respond with the appropriate certificates

for the reported DNS name. Without this parameter, the device checks whether the DNS name in the relevant URL agrees with the 'common name' of the submitted certificates. The device downloads the file only if this check is successful.

-o <MainDir>/<File>

Available for protocol: HTTPS

Available for command: LoadFile

Use this parameter to specify the destination for downloading a file. For example, you can use this option to save a certificate on your device for future identity verification when accessing an HTTPS server.

Use one of the two following main directories as `<MainDir>`:

- If the destination is a file in the device's internal file system, use the main directory `/minifs/`. When combined with a parameter, an example would be `-c /minifs/sslroot.crt`. You can view the available file names under **File-System** > **Contents**. Alternatively, a general overview is also available in the section *File Names for SCP File Transfer* on page 102.
- If the destination is a file on an external USB data medium, use the main directory `/mountpoint/`. When combined with a parameter, an example would be `-o /mountpoint/Device-9.00.0244.upx`.

If the storage path you specify includes subdirectories, these must exist already. The device does not create new directories.

It is also possible to use variables in file names and paths to enable dynamic directory structures (see *Variables* on page 107.

2.9.3.3 Variables

You have the option of using dynamic paths in the load commands whenever you reference a file within a parameter or URL. The content of the individual variables are specified by the device and cannot be changed manually.

The following variables are available for your directory and file names:

%m

MAC address of the device in hexadecimal notation, with lowercase letters and without separators

%s

Serial number of the device

%n

Device name

%l

Location of the device as specified in the configuration

%d

Device type

In addition to these general variables, you can also use the following *environment variables* that relate to the device for more flexibility when executing the load commands.

2.9.3.4 Example applications

After logging in to the command line on the device, the following command loads...

- a firmware file named 'Device-8.80.0103.upx' from the directory 'LCOS/ 880' of the TFTP server with the IP address '192.168.2.200' into the device:

```
LoadFirmware -s 192.168.2.200 -f LCOS/880/Device-8.80.0103.upx
```

- a script intended for a certain MAC-address (named, for example, '00a0571735da.lcs') from the TFTP server with IP address '192.168.2.200' into the device:

```
LoadScript -s 192.168.2.200 -f %m.lcs
```

- a firmware file named 'Device-8.80.0103.upx' from the directory 'download' of the HTTPS server with the address 'www.myserver.com' into the device. This verifies the identity of the server with the certificate 'sslroot.crt' stored in the device's internal file system:

```
LoadFirmware -c /minifs/sslroot.crt https://www.myserver.com/download/Device-8.80.0103.upx
```

- a script matching the serial number and the current firmware version into the device. The device reads the values for serial number and firmware from the corresponding environment variables:

```
LoadScript $__SERIALNO-$__FWVERSION.lcs
```



This command works without specifiying a URL so long as one is entered under **Setup** > **Autoload** > **Network** > **Script** as the parameter **URL**. Without an entry here, a URL must be specified in the command:

```
LoadScript -s 192.168.2.200 $__SERIALNO-$__FWVERSION.lcs
```

Regularly updating configuration and firmware

This scenario describes how to use the CLI to configure the device to update the firmware and/or configuration at a specific time. The firmware and configuration are downloaded from an external server (see *File download from a TFTP or HTTP(S) server* on page 104) using the 'LoadFirmware' and 'LoadConfig' commands in combination with fixed file names. The scheduling is organized with cron jobs.

1. Specify the URL that the 'LoadFirmware' command uses to source the upload if no other parameters are available. For example, to upload the firmware from an HTTP server, the command would resemble the following:

```
set /Setup/Autoload/Network/Firmware/URL http://www.mycompany.de/firmware/LCOS.upx
```

2. Set the conditions for loading the firmware such that only firmware that is newer than that in the device is loaded:

```
set /Setup/Autoload/Network/Firmware/Condition if-newer
```

3. Specify the path that the 'LoadConfig' command uses to source the upload if no other parameters are available. For example, to upload the configuration from an HTTP server, the command would look similar to the following:

```
set /Setup/Autoload/Network/Firmware/URL http://www.mycompany.de/configuration/LCOS.lcf
```

4. Set the conditions for loading the configuration such that only a configuration that is different from that in the device is loaded:

```
set /Setup/Autoload/Network/Config/Condition if-different
```

5. Create a cron job that regularly runs the command 'LoadFirmware' at 23:55h:

```
cd /Setup/Config/Cron-Tabelle
set 1 * * * 55 23 * * * LoadFirmware
```

6. Create a cron job that regularly runs the command 'LoadConfig' at 23:59h:

```
set 2 * * * 59 23 * * * LoadConfig
```

That's it! The firmware and configuration will now be updated automatically.



The sequence (first the firmware, then the configuration) ensures that the configuration also contains any menu items that first appeared in the new firmware.

Update configuration after first updating firmware

This scenario describes how to use the CLI to configure the device to update the firmware and configuration at a specified interval. The firmware is updated **before** the configuration. The firmware and configuration are downloaded from an

external server (see *File download from a TFTP or HTTP(S) server* on page 104) using the 'LoadFirmware' and 'LoadConfig' commands in combination with dynamic file names. The scheduling is organized with cron jobs.

1. Specify the URL that the 'LoadFirmware' command uses to source the upload if no other parameters are available. For example, to upload the firmware from an HTTP server, the command would resemble the following:
   ```
   set /Setup/Autoload/Network/Firmware/URL http://www.mycompany.de/firmware/
   ```
   The file name is specified later by the cron job.

2. Set the conditions for loading the firmware such that only firmware that is newer than that in the device is loaded:
   ```
   set /Setup/Autoload/Network/Firmware/Condition if-newer
   ```

3. Specify the path that the 'LoadConfig' command uses to source the upload if no other parameters are available. For example, to upload the configuration from an HTTP server, the command would look similar to the following:
   ```
   set /Setup/Autoload/Network/Firmware/URL http://www.mycompany.de/configuration
   ```
   The file name is specified later by the cron job.

4. Set the conditions for loading the configuration such that only a configuration that is different from that in the device is loaded:
   ```
   set /Setup/Autoload/Network/Config/Condition if-different
   ```

5. Create a cron job that regularly runs the command 'LoadFIRMWARE' every 10 minutes:
   ```
   cd /Setup/Config/Cron-Tabelle
   set 1 * * * 10 * * * * LoadFirmware\ $__SERIALNO-Device.upx
   ```
   In the example above, the firmware on the HTTP server must be in the form `<SerialNumber>-Device.upx`, for example `000018100060-Device.upx`.

   In the cron command `LoadFirmware \ $__SERIALNO-Device.upx`, the space between the load command and the environment variables is protected with a backslash. Trying to use the alternative notation of enclosing the entire command in quotation marks will result in an error. LCOS treats environment variables in quotation marks as normal text, so that any variables would be ignored.

6. Create a cron job that regularly runs the command 'LoadConfig' every 10 minutes:
   ```
   set 2 * * * 10 * * * * LoadScript\ $__SERIALNO-$__FWVERSION.lcs
   ```
   In the example above, the configuration script on the HTTP server must be in the form `<SerialNumber>-<FirmwareVersion>.lcs`, for example `000018100060-8.84.lcs`.

That's it! With this configuration, the device always initially loads the latest firmware.

If the device executes the command 'LoadScript' after initially uploading the latest firmware and the latest configuration script (e.g. for version 8.84) from the HTTP server, then the environment variable '__FWVERSION' is, at this time, set with the value of the previous firmware, e.g. '8.80 '. The command `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` does not find a suitable configuration script at this time. The device then executes the command `LoadFirmware 000018100060-Device.upx` and after rebooting, the environment variable '__FWVERSION' is set to the value '8.84 '. The command `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` then finds a suitable script to update the configuration.

2.10 Automatic upload of firmware or configuration from USB

Devices with a USB connector can be commissioned very easily with the aid of an external data medium. Loaders, firmware files, and even full configurations or scripts can be uploaded into the device from a USB medium.

2.10.1 Automatic upload of loader and/or firmware files

With this function activated and a USB medium mounted, the device searches for a loader and/or firmware files in the directory 'Firmware'. All files in the directory with the file extension '*.upx' will be considered for automatic loading if they are for the correct device type. The device does this by reading the file headers and then using the files according to the following rules:

- If at least one *.upx file with a loader is found, then the loader with the highest version number is loaded, unless the device already contains a loader with a higher version number.
- If at least one firmware file is found, then the firmware with the highest version number is loaded into the device, assuming that its version number is not equal to that of active or inactive firmware versions already in the device.

During the automatic load procedure, the device's power LED and online LED blink alternately. If a loader is uploaded first, the device will restart after this and it will commence a second automatic upload if new firmware is found. During this second load procedure, too, the device's power LED and online LED blink alternately.

The automatic uploading of loaders and/or firmware may, if applicable, be followed by further uploads of configuration files and/or script files, see *Automatic upload of configuration and/or script files* on page 110.

Once the automatic upload procedure is complete, all LEDs on the device light up in green for 30 seconds. You can then remove the USB medium.

2.10.2 Automatic upload of configuration and/or script files

Configuration and/or script files are only automatically loaded into the device if the device is in its factory default settings. A configuration reset can be used to return the device to its factory settings at any time.

When mounting a USB medium, the device searches for a loader and/or firmware files in the directory "Config". All files in the directory with the file extension "*.lcf" (configurations) and "*.lcs" (scripts) will be considered for automatic loading if they are for the correct device type. The device does this by reading the file headers and then using the files according to the following rules:

- A full configuration is always loaded before a script. Full configurations will only be loaded if the device type matches the device doing the loading, and if the firmware version entered into the header is the same as the active firmware in the device. If several suitable full configurations are found, then selection follows these criteria:
  - The configuration header contains a device serial number that matches that of the device doing the upload.
  - The configuration header contains a MAC address that matches that of the device doing the upload.
  - If multiple configuration files are left over after applying these selection criteria, then the device takes the configuration with the most recent date.
- If no full configuration is available, the device will select a script file, if available. If several suitable scripts are found, then selection follows these criteria:
  - The script header contains a device serial number that matches that of the device doing the upload.
  - The script header contains a MAC address that matches that of the device doing the upload.
  - The script header contains a firmware version that matches that of the device doing the upload.

  If multiple scripts are left over after applying these selection criteria, then the device takes the script with the most recent version number or date.



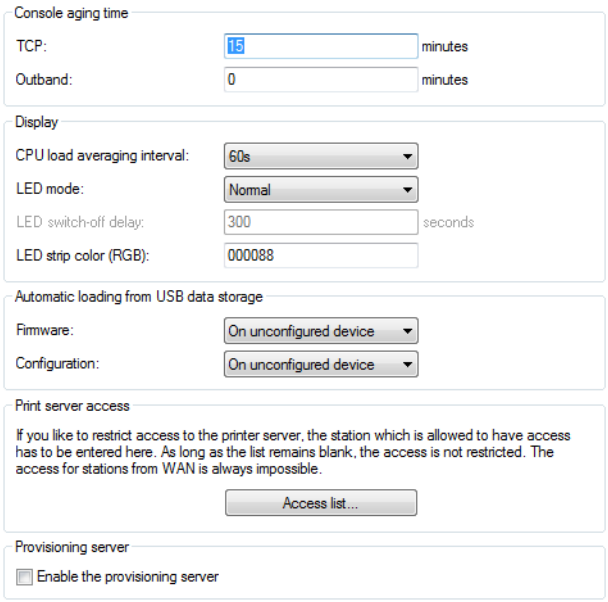
The meta data for the firmware version and the creation date are generated automatically when a configuration file or script file is saved. A MAC address and/or device serial number can be stored optionally. Learn more about under *Advanced meta data for configuration files* on page 193.

Once the automatic upload procedure is complete, all LEDs on the device light up in green for 30 seconds. You can then remove the USB medium.

2.10.3 Configuring automatic uploads via USB

The steps below will show you how to configure automatic uploading from a USB storage medium.

1. Start LANconfig and open the configuration dialog for the device.
2. Navigate to the dialog **Management** > **Advanced**.



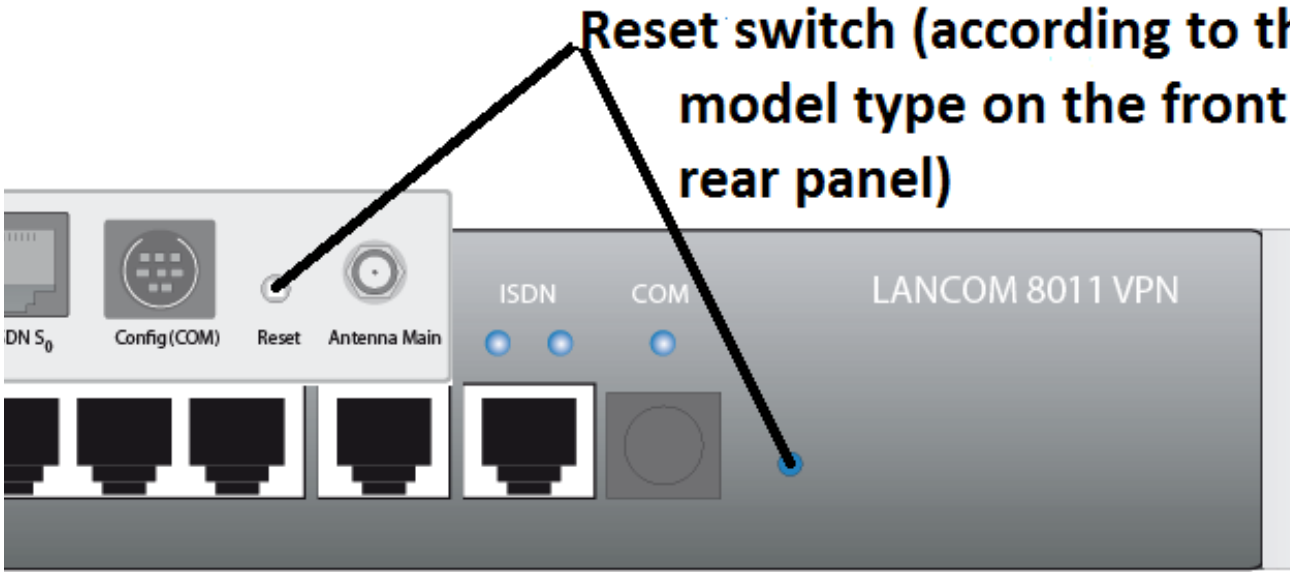
3. (De-)activate the automatic loading of loader and/or firmware files via the selection list **Firmware**. Select the appropriate option.
   - **Off**: Automatic loading of loader and/or firmware files is deactivated.
   - **On unconfigured device Device**: Automatic loading of loader and/or firmware files is only activated when the device has its factory settings. After successfully using the Wizards to configure the security settings and basic settings, set this option to **Off**.
   - **On**: Automatic loading of loader and/or firmware files is activated. When a USB medium is mounted, a suitable loader and/or firmware file is uploaded to the device. The USB medium is mounted when it is plugged into the USB port on the device, or when it is restarted.
4. (De-)activate the automatic loading of configuration and/or script files via the selection list **Configuration**. Select the appropriate option.
   - **Off**: Automatic loading of configuration and/or script files is deactivated.
   - **On unconfigured device Device**: Automatic loading of configuration and/or script files is only activated when the device has its factory settings. After successfully using the Wizards to configure the security settings and basic settings, set this option to **Off**.
   - **On**: Automatic loading of configuration and/or script files is activated. When a USB medium is mounted, a suitable configuration and/or script file is uploaded to the device. The USB medium is mounted when it is plugged into the USB port on the device, or when it is restarted.

That's it! This completes the configuration of automatic uploads from a USB medium.

A device can be fed with an undesirable configuration by resetting it to its factory settings and inserting a prepared USB data media. To prevent this you have to deactivated the reset switch.

2.11 Resetting the device

It is possible to reset the device to its factory settings if you need to reconfigure the device or if it is impossible to connect to the device even after restarting it. To do so, press the reset button **until all of the device LEDs light up** (after about 5 seconds).



After resetting, the device starts completely unconfigured and **all** settings are lost. If possible, backup the current device configuration **before** resetting.

After being reset, access points start in managed mode. In this mode, access to the device configuration is not possible via WLAN.

After a reset, the WLAN encryption settings in the device are reset to the default WPA key. The default WPA key consists of the MAC address of the physical WLAN interface preceded by an "L". Wireless configuration with the WLAN device only works after a reset if you have entered the standard WPA key under **Wireless LAN** > **Encryption** > **WLAN encryption settings**.

For outdoor access points, the way you reset the device depends on its design. The exact procedure for any specific device is explained in the corresponding Quick Reference Guide.

2.11.1 Configuring the reset button

The reset button offers two basic functions—boot (restart) and reset (to the factory settings)—which are called by pressing the button for different lengths of time.

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button is controlled with this setting.

For devices without serial interface, you cannot reconfigure the reset button, as otherwise it would no longer be possible to reset the configuration for these devices.

1. In the LCOS menu tree, navigate to the branch **/Setup/Config**.

2. Use the parameter **Reset button** to determine the behavior of the device when the reset button is pressed. The available settings are:
   - **Ignore**: Pressing the button does not trigger any action.
   - **Boot only**: Pressing the button triggers a reboot, regardless of how long it is pressed.
   - **Reset or boot**: With this setting, the reset button fulfills different functions depending upon how long the key remains pressed: Find more about the different key-press durations in the section *Special features of the rollout configuration* on page 90.

   The settings **Ignore** or **Boot only** makes it impossible to reset the configuration to the factory settings or to load the rollout configuration with a reset. If the password is lost for a device with this setting, there is no way to access the configuration! In this case the serial communications interface can be used to upload a new firmware version to the device—this resets the device to its factory settings, which results in the deletion of the former configuration.
3. Click the **Send** button to write the configuration back to the device.

2.12 Managing rights for different administrators

You have the option to configure your device with several administrators, each with different access rights and function rights.

Besides these administrators set up in the configuration, there is also the "root" administrator with the main password for the device. This administrator always has full rights and cannot be deleted, restricted or renamed. To log in as root administrator, use the user name `root` when logging in via LANconfig, WEBconfig or your terminal program, or leave the input field blank.

As soon as a main device password has been set in the device configuration, the login screen of WEBconfig is displayed in a web browser offering HTTP(S) access to the device. If other administrators are set up in addition to the root administrator, the mask contains the input fields **Login** and **Password**; otherwise it displays **Password** only. After entering the correct access credentials, users reach the main menu. This menu only displays the options corresponding to the access and function rights of the administrator who is currently logged in.

2.12.1 Rights for the administrators

The rights for administrators are divided into two areas:

- *Access rights*: Each administrator belongs to a certain group that has globally defined rights assigned to it.
- *Function rights*: Each administrator also has so-called "function rights" that determine personal access to certain functions such as the Setup Wizards.

2.12.1.1 Access rights

The following table is an overview of all of the rights that you can configure for administrator accounts. The following access rights and groups of administrator accounts are available:

Table 13: Access rights overview

Description under LANconfig	Description in the Setup menu	Rights description
All	Supervisor	Supervisor. Is a member of all groups and has full access to the configuration except for setting up and editing other administrators.
Restr. and trace	Admin-RW	Local administrator with read/write rights. Has full access to the configuration, although the following options are blocked:

Description under LANconfig	Description in the Setup menu	Rights description
		› Upload firmware onto the device › Upload configuration onto the device › Configuration by LANconfig › Cannot create or edit other administrators
Limited	Admin-RW-Limit	Local administrator with read and write access but without trace rights Has full access to the configuration, although the following options are blocked: › Upload firmware onto the device › Upload configuration onto the device › Configuration by LANconfig › Cannot create or edit other administrators › Trace output via the command line or LANmonitor
Read and trace	Admin-RO	Local administrator with read access but no write access. Can read the configuration from the command line, but cannot change any values.
Read only	Admin-RO-Limit	Local administrator with read access but no write access and no trace rights. Can read the configuration from the command line, but cannot change any values or request trace output.
None	None	Has no access to the configuration.

Local administrators cannot edit or view the Admin table. This is reserved for the root administrator.

2.12.1.2 Function rights

The following table is an overview of all function rights that are configurable for administrator accounts. The availability of individual function rights may vary, depending on the features of the device. If you wish to set the function rights at the CLI or with a script, you can optionally use the hexadecimal notation of the respective right instead of the plain text name. Learn more about this in section *Hexadecimal combination of privileges on the CLI* on page 116.

Table 14: Overview of function rights

Description: [1]LANconfig, [2]Setup menu	Hex notation on the CLI	Rights description
1. AP Assignment Wizard **2.** WTP Assignment Wizard	0x00000400	Wizard for assigning WLAN profiles
1. Content Filter Wizard **2.** CF Profile Wizard	0x00040000	Wizard for setting up the content filter
1. Dynamic DNS Wizard **2.** Dynamic DNS Wizard	0x00004000	Wizard for configuring dynamic DNS
1. Setting date and time **2.** Time setting	0x00000040	Setting the date and time (also applies for Telnet and TFTP)
1. Basic Wizard **2.** Basic Settings Wizard	0x00000001	Wizard for the Basic Settings
1. Internet Connection Wizard **2.** Internet Connection Wizard	0x00000004	Wizard for setting up the Internet connection
1. LAN-LAN Wizard **2.** LANLAN Wizard	0x00000020	Wizard for connecting two local area networks (VPN)
1. Public Spot Wizard (create account)	0x00000800	Wizard for creating Public Spot user accounts*

Description: [1]LANconfig, [2]Setup menu	Hex notation on the CLI	Rights description
2. Public Spot Wizard		
1. Public Spot Wizard (manage user) **2.** Public Spot user management Wizard	0x00100000	Wizard for managing Public Spot user accounts*
1. – **2.** Public Spot Configuration Wizard	0x00200000	Wizard for setting up a Public Spot
1. Public-Spot-XML-Interface **2.** Public Spot XML interface	0x00080000	Access to the XML interface of the Public Spot module A "normal" Public Spot administrator does not require this right. This right is intended for the implementation of complex authentication scenarios, such as when an external gateway (e.g. a machine or a program such as a Web server, script, etc.) needs to communicate with the module.
1. RAS Wizard **2.** RAS Wizard	0x00000010	Wizard for setting up dial-in access (RAS, VPN)
1. Rollout Wizard **2.** Rollout Wizard	0x00002000	Wizard for rollout scenarios*
1. Security Wizard **2.** Security Wizard	0x00000002	Wizard for adjusting the security settings
1. SMS-Transmit **2.** SMS transmission	0x400000	Sends SMS text messages via the 3G/4G WWAN module in the device.
1. SSH client **2.** SSH command	0x00020000	Establishes an SSH/Telnet connection from your device to other LCOS devices or SSH/Telnet servers
1. Search for other devices in the LAN **2.** Device search	0x00000080	Search for other devices in local and remote networks*
1. VoIP Provider Wizard **2.** Prepare VoIP provider access	0x800000	Wizard for setting up access to your VoIP provider
1. VoIP CallManager Wizard **2.** VoIP CallManager Wizard	0x8000	Assistant for setting up your VoIP CallManager
1. WLAN Wizard **2.** WLAN Wizard	0x00001000	Wizard for configuring the WLAN interface
1. WLAN link test **2.** WLAN link test	0x00000100	Runs the WLAN link tests* (also applies to Telnet)
1. WLC-Profile-Wizard **2.** WLC-Profile-Wizard	0x00010000	Wizard for setting up a WLC profile
1. CA-Web-Interface Wizard **2.** CA-Web-Interface	0x1000000	Creates profiles for the CA web interface

*) The permissions for and/or the execution of these Wizards or features relates exclusively to WEBconfig—unless otherwise stated. The Wizard or feature is either only available there (e.g. setting up and managing Public Spot users) or can only be constrained there (e.g. searching for devices).

Hexadecimal combination of privileges on the CLI

It can be a highly laborious process to configure multiple privileges by using plain text names in scripts. An alternative is to use the hex values instead of the names, to combine these values into a total, and to incorporate them into your script command.

The sum of several hex values results from the hexadecimal addition of the 1st, 2nd, 3rd ... nth position from the right. If, for example, the user should be able to execute features such as the **Security Wizard**, **Provider Selection**, **RAS Wizard**, **Time Setting** and the **WLAN link test,**, the sum of the individual hex values is calculated as follows:

- 1st position from the right: `2` (Security-Wizard) + `8` (Provider-Selection) = `a`
- 2nd position from the right: `1` (RAS-Wizard) + `4` (Time-Setting) = `5`
- 3rd position from the right: `1` (WLAN-Linktest) = `1`

For this example, the privileges have the value `0x0000015a`. Put differently, this is an OR operator with the following hexadecimal values:

Name on the CLI	Value
Security Wizard	`0x00000002`
Provider-Selection	`0x00000008`
RAS Wizard	`0x00000010`
Time setting	`0x00000040`
WLAN link test	`0x00000100`
OR operated	`0x0000015a`

As an alternative to the notation `0x0000015a` you can use the abbreviations `0000015a`, `0x15a` and `15a`.

Configuration example on the CLI

The following command (in the abbreviated form) sets up a new user in the Admins table (in the Setup menu under **Config** > **Admins**) who, as local administrator `NetAdmin` with the password `BW46zG29`, is able to select the Internet provider. The user will be activated immediately:

```
set NetAdmin BW46zG29 yes Admin-RW 8
```

Only the root administrator is allowed to execute this command because other administrators do not have access to the admin table.

The following command extends the privileges so that the user `NetAdmin` is able to execute the WLAN link test. The asterisks in the command stand for the values that remain unchanged:

```
set NetAdmin * * * 108
```

Only the root administrator is allowed to execute this command because other administrators do not have access to the admin table.

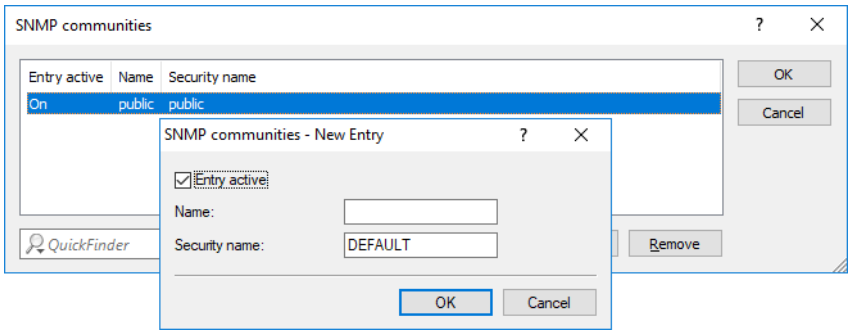
2.12.2 Configuring SNMP read-only access

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a “community”. Authentication is optionally handled

- by the `public` community (unlimited SNMP read access),
- by a master password (limited SNMP read access), or
- a combination of user name and password, separated by a colon (limited SNMP read access)

. By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community `public`. Because this represents a potential security risk, especially with external access,

LANconfig gives you the option define your own communities under **Management** > **Admin** and clicking **SNMP settings** and **SNMP communities**.



For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the `public` community in the list of the SNMP communities. This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community `public` has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

SNMP write access is reserved exclusively for administrators with the appropriate permissions.

For more information about SNMP, see the chapter *Simple Network Management Protocol (SNMP)*

2.13 Device-internal SSH/SSL keys

The device transmits fingerprints when establishing secure connections (e.g. via SSH or SSL) to the requesting remote site. On the basis of the fingerprint, the remote site can 1) uniquely identify the device and 2) verify that it has connected to the correct device, which is classified as trustworthy.

For example, if you use LANconfig to select the communication protocol SSH and you connect to a device for the first time, LANconfig produces a security query asking you whether the ssh-rsa key is known to you and whether you want LANconfig to accept this device as “known” in future.

2.13.1 Automatic generation of device-specific SSH/SSL keys

If you have not loaded an individual key into the device, then resetting the configuration will prompt the internal SSH server to try and compile its own device-specific SSH keys directly at the system startup. These include:

- an SSH-2-RSA key with 2048 bit length;
- an SSH-2-DSS key with 1024 bit length (as per FIPS 186-2);
- an SSH-2-ECDSA key with 256, 384 or 521 bit length;
- an SSL-RSA key with 2048 bit length;

which the device stores in its internal file system as `ssh_rsakey`, `ssh_dsakey`, `ssl_privkey` or `ssh_ecdsakey`.

If key generation is successful, the entry `SSH ... host key generated` is entered into the SYSLOG as a "notice"; If it fails, the entry `SSH: host key generation failed, try later again with '...'` is entered as an "alert". The failure to generate a key, for example if there is too little entropy, causes the system to revert to the factory implemented cryptographic key.

When you an update from an older LCOS version to 8.84 or higher without subsequently doing a configuration reset, the device does not generate a device-specific SSH/SSL key. This maintains compatibility with existing installations. However, you can trigger the key generation manually. Enter the following commands in the console:

```
sshkeygen -t rsa -b 3072 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
sshkeygen -t rsa -b 3072 -f ssl_privkey
```

2.13.2 Manually create custom SSH keys

You have the option to replace the automatically generated SSH/SSL keys with your own RSA, DSA or DSS keys, in order to achieve stronger encryption. A number of alternatives are available here:

- You can generate the individual keys on the console using LCOS.
- Using an external program, you can create an OpenSSH private key and then upload this key to the device as `SSH-DSA-key [...]` or `SSH-RSA key (*.key [BASE64 unencrypted])`.

The use of an external program is an option if your device has insufficient entropy, so causing key creation with LCOS to fail.

SSH key generation with LCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the console:

```
sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <Filename>]
```

-?, -h

Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa|ed25519|ed448)

This parameter specifies what type of key is generated. SSH supports the following types of keys:

- RSA keys are most widely used and have a length between 512 and 16384 bits. If possible you should work with keys of 3072 bits in length.
- DSA keys follow the Digital Signature Standard (DSS) set down by the National Institute of Standards and Technology (NIST) and are typically used in environments which are required to comply with the Federal Information Processing Standard (FIPS). DSA or DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.
- ECDSA keys are a variant of DSA keys, whereby the device uses elliptic curves for key generation (elliptic curve cryptography, ECC). ECC is an alternative to the conventional signature and key exchange techniques such as RSA and Diffie-Hellman. The main advantage of elliptic curves is that their mathematical properties offer the same key strength as RSA or Diffie-Hellman but with a significantly shorter key length. This provides for better hardware performance. ECC and its integration in SSL and TLS are described in RFCs *5656* and *4492*.
- Ed25519 is a method based on the Edwards-curve Digital Signature Algorithm (EdDSA) (*RFC 8709*) based on elliptic curves.
- Ed448 is also a method based on elliptical curves, which is specified in *RFC 8709*.

If no type is specified, the command generates an RSA key by default.

-b <bits>

This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.

-f <OutputFile>

These parameters specify the file name of the generated key file in the device file system. The choice of file name depends on what type key you are generating. The choices available to you are:

- `ssh_rsakey` for RSA keys
- `ssh_dsakey` for DSA keys
- `ssh_ecdsakey` for ECDSA keys
- `ssl_privkey` for SSL-RSA keys
- `ssh_ed25519key` for Ed25519 keys
- `ssh_ed448key` for Ed448 keys

-q

This parameter enables the 'quiet' mode for the key generation. If you set this parameter, LCOS overwrites any existing RSA or DSA keys without asking; there is no information about the progress of the operation. You can, for example, use this parameter in a script to suppress any security prompts for the users.

SSH key generation with Linux systems

Many Linux distributions already feature the OpenSSH package. All you have to do to generate the key file is to enter a simple command into the shell. The syntax corresponds to the LCOS command `sshkeygen`:

```
ssh-keygen [-t (dsa|rsa)] [-b <Bits>] [-f <OutputFile>]
```

The command `ssh-keygen -t rsa -b 4096 -f hostkey` creates an RSA key of 4096 bits in length, which consists of the private component 'hostkey' and the public component 'hostkey.pub'.

SSH key generation with Windows systems

Windows systems not are inherently capable of compiling SSH keys. You should instead use a suitable utility program such as the free software PuTTYgen.

A guide on how to create an individual key with PuTTYgen is available in the section *Generating an SSH keypair with PuTTY* on page 120. After following the various steps to generate the key, do **not** use the buttons **Save public key** and **Save private key**, but instead choose **Conversions** > **Export OpenSSH key**. The resulting OpenSSH private key can then be uploaded into the device without further processing.

2.14 SSH authentication using a public key

The SSH protocol and the LCOS-internal SSH server support two different authentication mechanisms:

1. Interactive by entering a user name and password at the keyboard;
2. Automated by submitting a public key

In the public key method, a key pair is used that is made up of a private and public key – a digital certificate. The private part of the key pair is saved on the client or with the user (frequently protected with a password, also known as a passphrase); the public part is loaded into the device. By definition, private keys cannot have predefined default values. For this reason, your device in its factory settings only supports interactive authentication by means of access credentials.

The following sections describe how to generate your own SSH key and implement authentication using a public key. For this example we are using LANconfig and the free SSH client PuTTY along with its associated utility PuTTYgen, which is used to generate the necessary key pair. Although PuTTY is available for the Windows and Linux operating systems the following description, like LANconfig, is limited to Windows.

Your device supports RSA, DSA, and DSS keys. RSA keys are somewhat smaller, thereby allowing somewhat faster operation. Further information about the keys mentioned here is available from VPN chapter of the Reference Manual in section *Working with digital certificates* on page 766.

2.14.1 Certificate check on SSH access

When establishing the SSH connection, the client first asks the device which authentication methods are permitted for this connection. If the public key method is allowed, the client searches for private keys that have been installed and transfers these with the user name to the device.

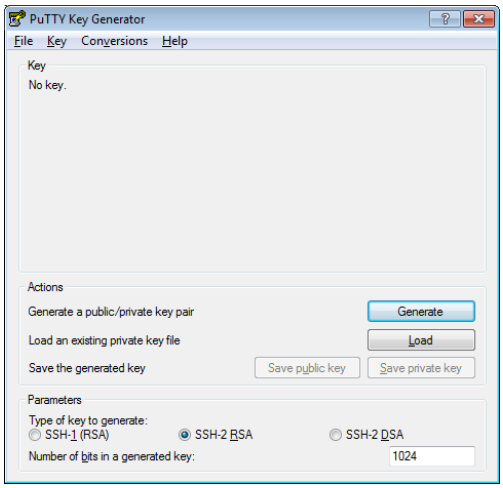
When the device finds an entry in the list that includes the user name that corresponds to its public SSH key, the SSH connection is permitted. If the client does not have a suitable private key installed or if the device does not have a corresponding entry with the user name or public key, the SSH client requests authentication by user name/password—as long as this authentication method is permitted—or it aborts the authentication process.

2.14.2 Generating an SSH keypair with PuTTY

The first thing you need for SSH authentication using a public key is a personal key pair. This tutorial describes how to use PuTTYgen to create an RSA key pair consisting of a public key and a private key.

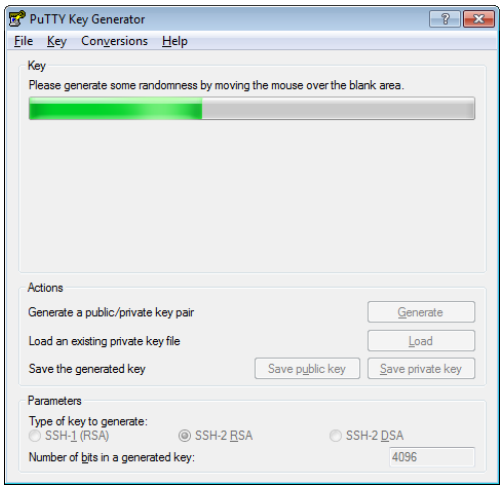
On Linux operating systems, the shell command `ssh-keygen` creates an RSA key pair consisting of the public part 'id_rsa.pub' and the private part 'id_rsa'.

1. Start the PuTTY utility **PuTTYgen**. The main window of the **PuTTY Key Generator** opens.

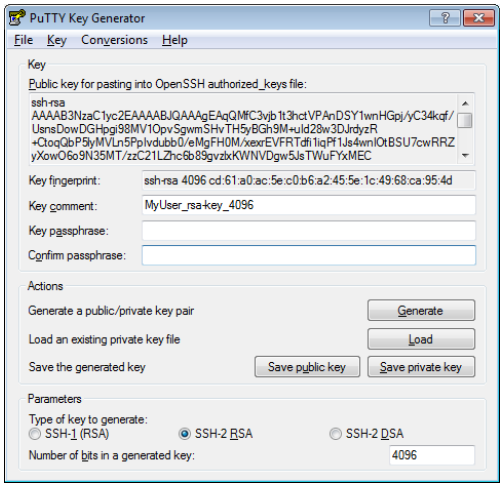


2. Select the type of key to be generated (in this case: **SSH-2-RSA**) and its bit-strength (e.g. `4096`). Then click on **Generate** to start the key generation.

3. Move the mouse around in the program window until the progress bar has reached the end. PuTTYgen uses the movements of the mouse cursor within the program window to generate the random numbers necessary for key generation. After generating the keys, the program displays the key data in the main window.



4. PuTTYgen uses the movements of the mouse cursor within the program window to generate the random numbers necessary for key generation. Move the mouse around in the program window until the progress bar has reached the end.



5. Optional: If you wish to additionally protect your private key with a passphrase, enter this in the **Key passphrase** field and confirm in the box below it.
   Please note that some SSH clients either do not store passphrases or they do it for the current session only (e.g. with PuTTY via Pageant only). For this reason you might want to avoid having to enter a passphrase where this is required manually during the process of connection establishment. LANconfig supports the persistent store of a passphrase.
6. You save your keys by clicking the buttons **Save public key** and **Save private key**.
   The public key is stored in the device, and the private key is used in combination with PuTTY for authentication.
7. At the same time you can save the key as an OpenSSH private key by clicking on **Conversions** > **Export OpenSSH key**.
   You can use the private key created in this way for authentication in combination with LANconfig.
8. Exit PuTTYgen. Now move to the next chapter of the installation.

2.14.3 Syntax and modifying public-key users

After creating a key pair, the public key has to be input to the device in a form that it understands. A LCOS device expects the public keys in the following syntax:

```
<EncryptionAlgorithm> <PublicKey> <Admin1> [<Admin2> … <AdminN>]
```

This makes it possible to assign multiple user accounts to a single public key. It is also possible to load several keys for different users into the device. Starting with a public-key file created with PuTTYgen, the following steps describe how you modify a public key.

1. Open the public-key file in a text editor. It shows you the following or similar content:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key_myuser"
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1wnHGpj/yC34kq
f/UsnsDowDGHpgi98MV1OpvSgwmSHvTH5yBGh9M+uId28w3DJrdyzR+CtoqQbP5l
…
0N8V3ydp+qbx+8FNbBQCVhxxiKZwXxmMh70pTWHxixOFte4HBxGHxcRaiSoMyNdv
wCkWlx8=
---- END SSH2 PUBLIC KEY ----
```

2. Delete the header and footer and the comment line so that all that remains is the actual key. Then remove any line breaks so that the public key is on a single line.

```
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8=
```

3. In front of the key, specify the encryption algorithm `ssh-rsa` and, after the key, add the name of the user account for which this key is valid (for example, `root`), separated with a space.

   You can assign multiple users to a key or place multiple keys in a single public-key file. **Examples**:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1j…wCkWlx8= root
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8= root admin user
ssh-rsa VLn5PpIvdubb0/eMgFH0M/xexrEVFRTdfi1iqPf1Js4wnIOtBSU…xKWNVDg/ backup
```

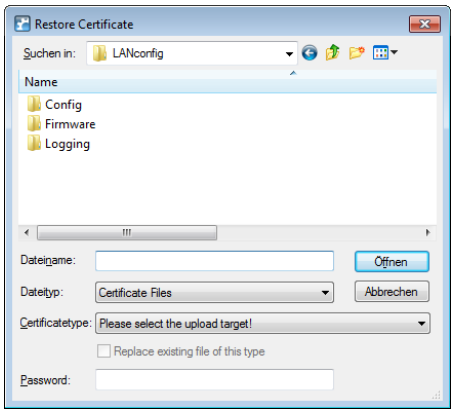
   Make sure that each each key (including the encryption algorithm and user [s]) is on a separate line. Line breaks invalidate the file and lead to an error in the subsequent authentication!

4. Save the file and close the text editor.

2.14.4 Setting up a device for public-key authentication

This tutorial describes how to load the key file into the device and prepare the device for SSH authentication.

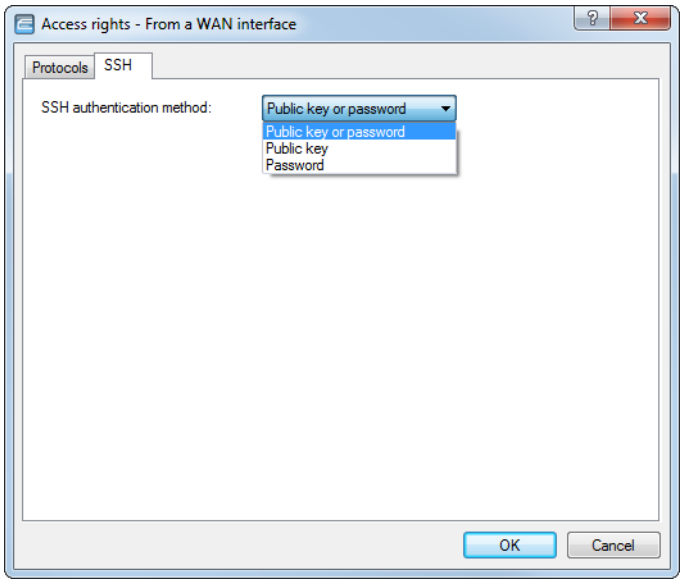
1. Start LANconfig and select the device on which you wish to set up SSH authentication.
2. Select **Device** > **Configuration management** > **Upload certificate or file**. In the window that opens, change the **File type** selection list to **All files** and the **Certificate type** selection list to **SSH – accepted public keys**.



3. Select the public-key file you created previously and click **Open**. LANconfig then starts uploading the public key to the device.

The uploaded file replaces the list of previously accepted keys. Alternatively, you can edit the keys directly in WEBconfig and attach individual keys to the existing list (see *Allowed SSH public keys* on page 40).

4. Open the configuration dialog for the device and navigate to **Management** > **Admin** > **Access settings**.
5. In the section **Configuration access ways**, click on **Access rights** > **...** > **SSH** and configure the **SSH authentication method** for each network.
   The authentication methods permitted for SSH access can be set separately for LAN, WAN and WLAN. The following options are available:
   - **Public key or password**: With this option, public-key authentication is attempted first. If this should fail, then a password query is issued.
   - **Public-Key**: With this option, only public-key authentication is attempted.
   - **Password**: Public-key authentication is switched off and a password query is issued.



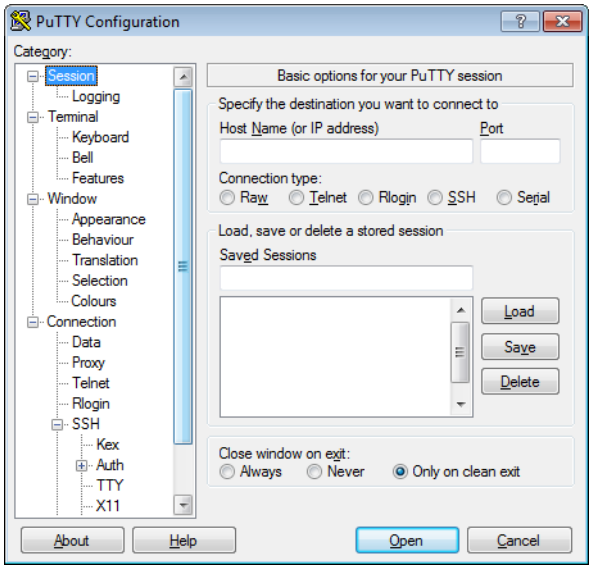
6. Close all of the configuration dialogs and write the configuration back to the device.

2.14.5 Public-key authentication with PuTTY

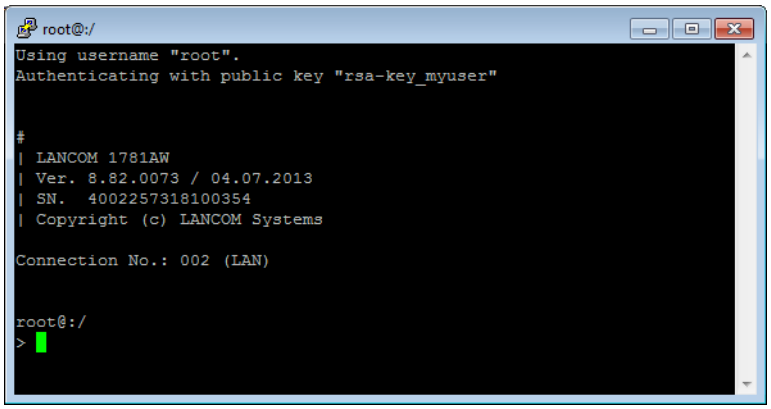
This tutorial describes how to use PuTTY to configure SSH authentication based on a public key and how to authenticate at the device.

1. Start PuTTY.

2. In the window that opens, enter the host name or the IP address of the device and set the **Connection type** to the option **SSH**. The default port for SSH connections is `22`.



3. Switch to the **Connection** > **Data** dialog and, in the input field **Auto-login username**, enter the user name for the public key you created previously (e.g. `root`).
4. Switch to the **Connection** > **SSH** > **Auth** dialog and, in the input field **Private key file for authentication**, enter the path and file name of the private-key file you created especially for PuTTY.
5. Then click on **Open**. PuTTY then attempts to establish a connection while using SSH authentication by public key.



If you have protected your private key file with an optional passphrase, PuTTY will ask you for this as part of the authentication process.

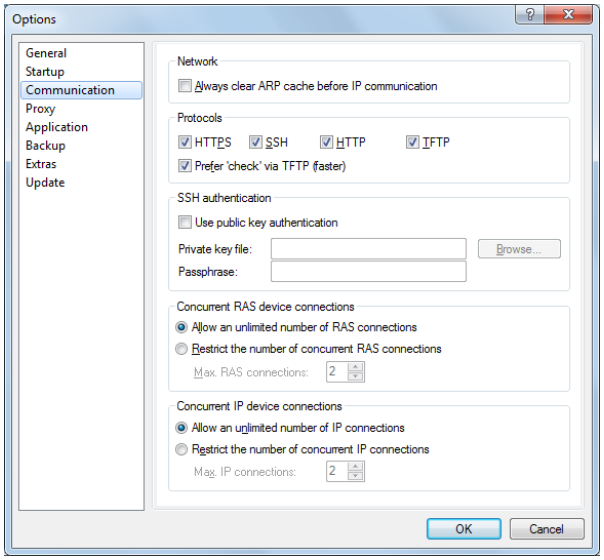
That's it!

2.14.6 Public-key authentication with LANconfig

This tutorial describes how to use LANconfig to configure public-key based SSH authentication.

1. Start LANconfig.

2. From the toolbar, open the dialog **Tools** > **Options** > **Communication**.



3. Under **Protocols**, disable all of the options except for **SSH** and **Prefer 'check' via TFTP**.
   This prevents LANconfig from favoring a different protocol for device communication (e.g. HTTPS) and falling back to another, possibly unencrypted protocol (such as HTTP) if authentication fails.
4. Activate the option **Use public-key authentication**.
5. Specify the path and file name of the OpenSSH private-key file as appropriate and, if required, enter the passphrase that secures your key.
6. Close the settings dialog with a click on **OK**.

That's it! Now if you open the configuration dialog or start the Setup Wizard for a device, LANconfig communicates using the SSH protocol and attempts to authenticate with the specified private key.

2.15 SSH and Telnet client in LCOS

2.15.1 Introduction

Along with an SSL server that provides secure and authenticated access to the device (see *SSH authentication using a public key* on page 119), the operating system of your device also features an SSH client. This SSH client enables SSH connections to be established from your device to a remote server, such as a further device or a Linux server. This function is also useful if it is not possible to connect directly to a remote device, but if there is an indirect connection via a further device that is accessible from both subnets.

The SSH client included with LCOS can be started with simple commands on the CLI, similar to the OpenSSH client on a Linux system.

2.15.2 Syntax of SSH clients

The SSH connection to a remote system using LCOS's own SSH client is initiated from the CLI with the following command:

```
ssh [-(?|h)] [-(b|a) <Loopback-Address>] [-p <Port>] [-C] [-j <keepalive-interval>] [-l login_name] [-o
"option=value"] [<User>@]<Host> <Command>
```

The individual parameters have the following meaning:

-?, -h

Displays a brief help text about the available parameters

-b, -a <Loopback-Address>

Allows a sender address (loopback address) to be specified. This option is especially important in connection with ARF: By entering an optional loopback address you change the source address and route used by the device to connect to the remote system. This can be useful, for example, when the system is available over different paths and it should use a specific path for its reply message.

-p <Port>

Specifies the port to be used. If you do not specify a port, the device reverts to the SSH standard TCP port 22.

-C

If you set this parameter, the SSH client uses the zlib algorithm to attempt to negotiate a method for data compression with the remote system. If the remote system does not support compression, then the data is transmitted uncompressed.

The use of compression is generally worthwhile only for very slow connections. With fast connections, the performance loss from the additional overhead due to compression tends to be greater than the gain from reduced data amounts.

-j <keepalive-Interval>

If the connection to the remote system is routed via a NAT router or a firewall, it may be worthwhile to leave the connection running permanently. With an interactive SSH session, data is not transferred at all at certain phases, which can lead to disconnection because of timeouts. In such cases the SSH client can regularly transmit keep-alive packets, which are irrelevant to the remote system but which inform the gateway that the connection is still being used.

Use this parameter to specify the interval in seconds in which your device sends the keep-alive packets. The keep-alive packets are only transmitted when the SSH client is not sending other data to the remote system.

-o <option=value>
Possible values:

- StrictHostKeyChecking=<yes|no|off|ask|accept-new>: enable/disable host key checking (default: ask)
- SignHostKeyAlgorithms=[+|-]<alg-list>: augment/reduce/set list of allowed signature algorithms
- VerifyHostKeyAlgorithms=[+|-]<alg-list>: augment/reduce/set list of accepted signature algorithms
- KeyAlgorithms=[+|-]<alg-list>: augment/reduce/set list of allowed key exchange algorithms
- Ciphers=[+|-]<alg-list>: augment/reduce/set list of allowed cipher algorithms
- MACs=[+|-]<alg-list>: augment/reduce/set list of allowed (H)MAC algorithms
- Password=<password>: set password (disables keyboard-interactive authentication method)

<User>

User name for logging in to the remote system. If you do not specify an explicit user name, LCOS uses your current username that you used to log in to the CLI.

<Host>

DNS name or IP address of the remote system.

<Command>

The LCOS SSH client either starts an interactive shell on the remote system or it executes a single command. If no command is entered, the interactive shell starts.

2.15.3 Syntax of the Telnet client

As an alternative to SSH you can use the internal LCOS Telnet client to connect to a remote system. Start the Telnet client in the terminal program with the following command:

```
telnet [-(?|h)] [-b <Loopback-Address>] <Host> [<Port>]
```

-?, -h

Displays a brief help text about the available parameters

-b <Loopback-Address>

Allows a sender address (loopback address) to be specified. This option is especially important in connection with ARF: By entering an optional loopback address you change the source address and route used by the device to connect to the remote system. This can be useful, for example, when the system is available over different paths and it should use a specific path for its reply message.

<Host>

DNS name or IP address of the remote system.

<Port>

Specifies the port to be used. If you do not specify a port, the device reverts to the SSH standard TCP port 23.

2.15.4 Public keys for authentication

Authentication with SSH works with public keys sent from the remote system. If an SSH client needs to connect to an SSH server, the server sends the public key to the client, which then looks for that key in its files. The following situations can occur here:

- The SSH client finds the key in its list of known server keys, and the key is allocated to the corresponding host name or IP address. The SSH connection can be established without further activity from the user.
- The SSH client does **not** find the key in its list of known server keys, and also no other key of the same type (RSA or DSA/DSS) for the corresponding host name or IP address. The SSH client assumes that this is the first connection to the server. It shows its public key and the associated fingerprint. The user can verify the key using a copy from another source, and can then decide whether the server should be stored in the list of known SSH servers. If the user declines this verification, the SSH connection is broken immediately.
- The SSH client finds a key for the corresponding host name or IP address, but this is different from the key currently in use. Both keys are displayed, but the SSH connection will be terminated because the SSH client suspects a man-in-the-middle attack. If the public key on the remote system was recently changed, then the administrator has to delete the outdated entry from the list of known servers (see *Manually deleting known SSH server keys* on page 128.

After successfully verifying the server key, the administrator can enter the password for accessing the remote system. The password cannot be entered directly at the command line.

SSH connections are usually closed at the server, e.g. by entering `exit` in the shell. Sometimes it may be necessary to close the SSH connection with the client, e.g. if the application on the server has problems. The SSH client in LCOS uses the same character string as OpenSSH to close the connection, i.e. 'tilde - dot'.

If the LCOS CLI session itself was opened with an OpenSSH client, you must use the string 'tilde – tilde – dot'; otherwise the wrong connection will be closed.

2.15.4.1 List of known SSH servers

The ssh client in LCOS automatically stores the known SSH keys of remote systems to its own key file. This key file is stored in the internal file system and named **ssh_known_hosts**. The contents of this file change each time you connect to an SSH server that is unknown to your device and you accept the remote-system key displayed to you as a security prompt.

Each key is stored to a line in this file and contains three fields:

- The name or IP address of the remote system as entered into the SSH command when establishing the connection.
- The key type, i.e. ssh-rsa or ssh-dss.
- The binary output of the key itself, coded as Base64.

Once an administrator has accepted the public key of an SSH server, this key applies to all of the administrators; there is no differentiation at user level.

The file(s) named here on the device are exclusively available to the root administrator via SCP (see *Loading a file via an SCP client* on page 101). Uploading and downloading via LANconfig or WEBconfig is not an option.

2.15.4.2 Manually deleting known SSH server keys

You have the option of specifically deleting SSH keys for external systems from your device. This may be required if, for example, if the SSH key of the external server has changed and your device refuses to connect to this system because of an outdated SSH key. To do this, use the `sshkeygen` command in combination with the parameter `-R`:

```
sshkeygen [-?|-h] [-t dsa|rsa|ecdsa|ed25519|ed448] -R <Host>
```

-?, -h

Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa|ed25519|ed448)

This optional parameter specifies the type of key that the device deletes. If no type is specified, the command deletes all SSH keys for the specified host.

-R <Host>

Use this parameter to specify the IP address or DNS name of the external system for which the outdated SSH key should be deleted from your device.

To delete the complete list of all known SSH server keys at once, delete the file **ssh_known_hosts** from the file system of your device.

2.15.5 Creating SSH keys in LCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the CLI of the device with the LCOS SSH client to be used:

```
sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b <bits>] [-f <Filename>]
```

A detailed description of the parameters in the `sshkeygen` command can be found in the section *SSH key generation with LCOS* on page 118. The device automatically creates the keys and saves them to its internal file system in the PEM format under the file name **ssh_rsakey** (for RSA keys), **ssh_dsakey** (for DSA or DSS keys) or **ssh_ecdsakey** (for ECDSA keys). The ID files have the following structure, which defines the use of a key for a certain LCOS administrator:

```
*** User <MyAdmin>
<SSH-Key>
*** End
```

Retrieving the public key

After the device has generated the key pair, you need to transfer the public part to the remote system. The public part of the key is retrieved with the following command:

```
show ssh idkeys
```

This command generates output similar to the following:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAQEA28BtnFFInAi8I5B1aOwq5g2Y…0nkuNQ== root@
```

- The first part shows the key type (ssh-rsa or ssh-dss).
- The second part is the binary output of the key itself, coded as Base64.
- The third part contains the host name and is intended for entering comments.

Transferring the public key to a remote system

Assuming that the remote system is a device equipped with LCOS, you load the relevant DSA or RSA key using either the device *file management* or by adding to the list of public keys in WEBconfig directly under **Extras** > **Edit list of allowed SSH public keys**. To do this, copy the first and second parts and replace the third part with a list of users to limit the use of this key to a selection of LCOS administrators.

For more information about the syntax required for public keys, how to use different keys, and how to link them to different administrators, see the section *Syntax and modifying public-key users* on page 122.

2.15.6 Priorities for SSH authentication

SSH authentication at a remote system follows a strict order of priorities:

1. Using the first method, the device always attempts to authenticate by means of a public key, unless the remote system does not support this method or the current administrator does not possess a public key.
2. With the second method, if public-key authentication is unavailable or if the remote system has rejected the public key of the authenticating administrator, the device offers interactive authentication by keyboard. Depending on the application, interactive authentication may consist of exchanging a number of messages between the SSH client and SSH server. In the simplest case, entering a valid password is sufficient.

2.15.7 Rights for operating the SSH/Telnet client

You have the option of explicitly assigning the right to use the SSH/Telnet client for each individual administrator. This is done by adding or modifying administrator accounts (in LANconfig under **Management** > **Admin** > **Further administrators**) and adding the right to use the **SSH client**. Without the right to use this feature, an administrator cannot connect to another SSH/Telnet device.

2.16 Importing files by copy & paste on the CLI

Your device supports the loading of files into file slots from the console and also by means of a script.

This offers the convenience of using a script to roll-out files together with the configuration or, for example, to import SSH keys and VPN certificates.

- The file format must be of type text or ASCII; binary formats are not supported.
- In the case of certificates, the file format must be PEM-encoded (ASCII/Base64). DER-encoded certificates are not supported.
- You will find a **list of possible files and formats** at the end of this chapter.

Syntax of the CLI command **importfile**:

importfile -a <application> [-p <passphrase>] [-n] [-h <hash> -f <fingerprint>] [-c] [-r]

Required parameters:

-a <application>

<application> specifies the storage location and thus the usage for the entered data. For a complete list of the storage locations on your device, enter **importfile -?**.

Optional parameters:

-n

-n starts the non-interactive mode. There are no prompts or other outputs on the CLI. The non-interactive mode is intended for use with scripts.

-p <passphrase>

<passphrase> is the password required to decrypt an entered private key.

-h <hash>

The hash algorithm used to determine the fingerprint of the root CA certificate.

-f <fingerprint>

The fingerprint of the root CA certificate, created with **–h**. The fingerprint can be entered either with or without colons.

-c

Only CA certificates are uploaded.

-r

Uploaded CA certificates replace any existing ones.

CTRL+Z cancels any active input.

Example:

In this example, user input is shown in **bold** and prompts for the user are shown in *italic*. Certificates and other long, multi-line outputs are abbreviated with **[...]** for legibility. At the end of the example you will find explanations for the individual steps.

```
root@test:/
    importfile -a VPN2 -p lancom -h SHA512 -f
4F:A7:5E:C9:D4:77:CE:D3:06:4C:79:93:D8:FA:3A:8E:7B:FE:19:61:B2:0C:37:4F:BB:7A:E6:46:36:04:46:EE:F6:DA:97:15:6B:BB:
2D:8F:B6:66:E6:7C:54:1E:B4:02:79:54:D6:DF:1E:9B:27:7C:9C:EA:B8:CB:1B:6D:90:1C

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device certificate, the end of the input will be detected automatically:
importfile>-----BEGIN CERTIFICATE-----
importfile>MIID9DCCAtwCCQDgaoWRCmWaLjANBgkqhkiG9w0BAQ0FADAkMQswCQYDVQQG[…]
importfile>[…]s7pM5l0L0d0=
importfile>-----END CERTIFICATE-----
Importing device certificate:
        Version: 1 (0x0)
        Serial Number:
            e0:6a:85:91:0a:65:9a:2e
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jul  4 12:34:07 2017 GMT
            Not After : Oct  5 12:34:07 2024 GMT
        Subject: CN=TEST,O=Internet Widgits Pty Ltd,ST=Some-State,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:93:f6:b9:9a:41:b2:3e:30:2b:09:7f:d1:f9:
                    49:54:5a:82:c9:17:10:1f:79:6d:ab:55:df:b8[…]
                […]2f:0c:8a:69:7b:a9:82:32:f3:ca:9c:02:20:14:
                    bd:8b:0d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha512WithRSAEncryption
         06:5b:a4:1a:a2:69:c1:bf:6f:b1:d2:6c:b0:21:e1:10:43:[…]
         […]50:e6:a3:1d:f3:15:b7:87:8c:65:2f:25:f6:b3:ba:4c:e6:
         5d:0b:d1:dd

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device private key, the end the input will be detected automatically:
importfile>-----BEGIN RSA PRIVATE KEY-----
importfile>Proc-Type: 4,ENCRYPTED
importfile>DEK-Info: AES-128-CBC,8FB95ED0568DA9AE17D7573BC294ACD8
```

```
importfile>[…]5Cuf2p798Obhw3isAe04XRwmdLno8ZcPDyB33ZKPjmhUzB0WsdzGdSSq5iYjD
importfile>-----END RSA PRIVATE KEY-----
The private key was read successfully.
The private key matches the device certificate.
The input can be aborted by pressing CTRL+Z.
Please enter the chain of PEM-encoded (Base64) CA certificates.
The input is closed with "endcachain":
importfile>-----BEGIN CERTIFICATE-----
importfile>MIIDGzCCAgOgAwIBAgIJAMlNxBFGQqpoMA0GCSqGSIb3DQEBDQUAMCQxCzAJB[…]
importfile>[…]EUDI9giYt9tnAT8hJfLkkyN/PHSiP+e+vopjSpKuyg==
importfile>-----END CERTIFICATE-----
importfile>endcachain
Importing CA certificate:
        Version: 3 (0x2)
        Serial Number:
            c9:4d:c4:11:46:42:aa:68
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jun  6 13:56:49 2017 GMT
            Not After : Jun 19 13:56:49 2045 GMT
        Subject: CN=OCSP-TEST-CA,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:ba:04:74:7d:78:5a:84:b3:63:cc:ad:4d:[…]
                    […]14:0e:27:c8:8c:5a:00:a3:4c:ed:4f:02:e8:0b:
                    fb:07
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30
            X509v3 Authority Key Identifier:
                keyid:57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha512WithRSAEncryption
         c8:cf:3b:97:1a:56:61:13:9c:61:ed:21:23:7a:37:b4:a8:[…]
        […]3f:21:25:f2:e4:93:23:7f:3c:74:a2:3f:e7:be:be:8a:63:
         4a:92:ae:ca

Content of the PKCS12 file: private key: 1, device certificate: 1, CA certificates: 1
root@test:/
```

1. The importfile command is called for the storage location VPN2, so we are dealing with a certificate for use in the VPN. The password for the private key is lancom and the root CA certificate can be checked with SHA512 and the specified fingerprint.
2. In the following, the user is prompted to enter the certificate.
3. After entering the certificate, it is then imported.
4. In the following, the user is prompted to enter the private key.
5. Following the input, the key is checked.
6. In the following, the user is prompted to enter the CA certificate chain. The end of the input is not detected automatically. After the last certificate, the end is determined by entering endcachain. Type this command on a new line, because all of the input on a line containing the string **endcachain** is discarded.
7. Following these entries, the CA certificates are imported and the process is completed.

Table 15: Possible Files and formats

File	Format	File	Format
CONFIG-SYNC	PEM	SCEP-TLS	PEM
CWMP	PEM	SIPS1	PEM
CWMP-ROOT-CA	PEM	SIPS2	PEM
DEFAULT	PEM	SIPS3	PEM
DEFAULT-ADD-CAS	PEM	SSH-AUTH-KEYS	TEXT

File	Format	File	Format
EAP-TLS	PEM	SSH-DSA	PEM
ISSUE	TEXT	SSH-ECDSA	PEM
LBS	PEM	SSH-ED25519	PEM
OCSP-SERVER	PEM	SSH-ED448	PEM
PBSPOT-TEMPLATE-AGB	TEXT	SSH-KNOWN-HOSTS	TEXT
PBSPOT-TEMPLATE-ERROR	TEXT	SSH-RSA	PEM
PBSPOT-TEMPLATE-HELP	TEXT	TLS	PEM
PBSPOT-TEMPLATE-LOGIN	TEXT	USER-WIZARD-1	TEXT
PBSPOT-TEMPLATE-LOGIN-EMAIL	TEXT	USER-WIZARD-2	TEXT
PBSPOT-TEMPLATE-LOGIN-SMS	TEXT	USER-WIZARD-3	TEXT
PBSPOT-TEMPLATE-LOGOFF	TEXT	USER-WIZARD-4	TEXT
PBSPOT-TEMPLATE-NOPROXY	TEXT	VCM-TLS	PEM
PBSPOT-TEMPLATE-REG-EMAIL	TEXT	VPN-ADD-CAS	PEM
PBSPOT-TEMPLATE-REG-SMS	TEXT	VPN1	PEM
PBSPOT-TEMPLATE-START	TEXT	VPN2	PEM
PBSPOT-TEMPLATE-STATUS	TEXT	VPN3	PEM
PBSPOT-TEMPLATE-VOUCHER	TEXT	VPN4	PEM
PBSPOT-TEMPLATE-WELCOME	TEXT	VPN5	PEM
PROVISIONING-SERVER	PEM	VPN6	PEM
RADIUS-ACCOUNT-TOTAL	TEXT	VPN7	PEM
RADSEC	PEM	VPN8	PEM
ROLLOUT-TEMPLATE	TEXT	VPN9	PEM
ROLLOUT-WIZARD	TEXT	WLC-SCRIPT1	TEXT
SCEP-CA	PEM	WLC-SCRIPT2	TEXT
SCEP-RA	PEM	WLC-SCRIPT3	TEXT
Wireless-ePaper	PEM		

2.17 Basic HTTP file server for external storage media

2.17.1 Introduction

The HTTP server integrated into the LCOS uses the HTTP protocol to connect to an external storage medium, so providing a basic data server.

This function is only supported by devices with a USB connector.

2.17.2 Preparing the USB storage medium

Accessing an external storage medium from your device requires some preparation. The following describes how to set up a USB medium to operate with the device.

1. Format the USB medium with a FAT16 or FAT32 file system.
2. Create the directory `public_html` on the USB medium.

   The LCOS HTTP server only accesses the files and subdirectories in this directory. All other files on the USB medium are ignored.

   You can also change the directory name in the Setup menu under **HTTP** > **File-Server** > **Public-Subdir**.

This concludes the configuration on the USB medium.

2.17.3 Determine the mount point of the USB medium in the LCOS

When a USB medium is connected to your device, a mount point is created automatically and used by LCOS to manage the medium internally. This mount point always remains the same for a certain USB medium, even after restarting. Different media are each allocated their own unique mount point.

The mount point must be known in order to access the files on the USB medium. The mount points for USB media are shown in the Status menu under **File system** > **Volumes**.



The Status table displays all of the volumes discovered by the device:

- `MiniFs` is the flash file system integrated into most devices.
- `BlkDev-n` are identifiers for the known USB media. If there is just one USB mass storage device connected, it is named `BlkDev-1` and is mounted under `/usb`.

2.17.4 Accessing the files on a USB medium

Use the following URL to access the files on the USB medium by using the HTTP server in the LCOS:

`http://<Device-IP-Address>/filesrv/<Mounting-Point>/<File>`

If, for example, the file is named `coupon.jpeg` and it is stored in the base directory `\public_html` of the only USB medium, then you can access it with the following link:

`http://<Device-IP-Address>/filesrv/usb/coupon.jpeg`

Files can be accessed with HTTPS as well as HTTP.

2.17.5 Rules for directory access

The directory `public_html` can contain sub-directories. You can access these directories without specifying any particular file. If a directory contains a file named `index.html` or `index.htm`, this file is transferred to the HTTP client. If not, the file server displays a list of all files and directories that exist in the requested directory.

2.17.6 Supported content type

The HTTP server in the LCOS uses the file extension to determine the MIME content type required to display the content correctly in a browser. The following extensions are currently recognized and will be translated into the correct MIME content type:

- .htm and .html for HTML files
- .gif, .jpg, .jpeg, .png, .bmp, .pcx for images in the corresponding format
- .ico for icon files
- .pdf for Adobe Acrobat PDF files
- .css for cascading style sheet files

2.18 Rollout Wizard

In large-scale networking projects, administrators often have to install many devices of the same or similar type at different locations. Administrators often perform rollouts to reduce or avoid the need to be personally present at the various locations. In the field of networking, a "rollout" refers to a largely automated process for the coordinated preconfiguration of devices for a specific application. There are two basic ways for administrators to do this:

1. The administrators prepare the devices at the central office for rollout. On location, an employee or a customer then runs a specifically customized Rollout Wizard that sets the site-related parts of the configuration and puts the device into operation.
2. The administrators located at their central office use the *Large Scale Rollout & Management (LSR)*. All configuration settings for a specific device are performed and managed through the management system. On location, an employee or a customer then runs the default Rollout Wizard on the device, which loads the configuration from the LSR server and brings the device into its desired operating state.

Unlike the custom Rollout Wizard, using the default Rollout Wizard in combination with the LSR means it is not necessary to configure a device in several stages; a current and complete configuration is uploaded directly after the device connects to the LSR.

However, where the LSR is not available for use, you as an administrator can still use the custom Rollout Wizard to conduct complex deployments that fulfill specialized applications.



It is not possible to operate both Wizards in parallel. The custom Rollout Wizard replaces the default Rollout Wizard, so excluding the use of remote configuration by an LSR system. To return to the default Rollout Wizard, you must delete the custom Rollout Wizard from the device's file system.

2.18.1 Default Rollout Wizard

Your device is supplied with a preconfigured Rollout Wizard, which allows you to retrieve a configuration from a *LANCOM Large Scale Rollout & Management (LSR)* server with just a few clicks. The **Default Rollout Wizard** runs if you have enabled the Rollout Wizard in LCOS but have not set up a customized Rollout Wizard.

The Default Rollout Wizard asks you for all the information that it needs to connect to the LSR. This includes:

- The protocol used for the connection (HTTP or HTTPS);
- The IP address or the DNS name of the LSR server;
- The user name and password for authentication against the LSR;
- The name or number of the rollout project;
- The device ID (optional); and
- The rollout TAN for the device.

This process can be partially or even fully automated if you enter the relevant information into the device permanently. The table for this is located in the Setup menu under **HTTP** > **Rollout-Wizard** > **Presets**. Standard presets are the port and the loopback address used by the Wizard.

If your device has a USB port, its automatic upload feature allows a USB stick to supply an unconfigured device with the basic information required by the Rollout Wizard. For more information about this function, see *Automatic upload of firmware or configuration from USB* on page 109.

Before the device starts processing the rollout, the wizard displays a summary of the connection data used. Also, the device uses an ICMP echo request (ping) to determine whether the specified server is available. If this test fails, you have the option to re-configure the wizard or to continue the rollout process anyway. The host is available, the device begins with the retrieval of a configuration from the LSR.

If the LSR server can be accessed via the Internet, but you are running the Rollout Wizard on a device without an Internet connection, you must first execute the Internet Setup Wizard.

2.18.2 Custom Rollout Wizard

The custom Rollout Wizard is a programmable setup wizard in WEBconfig, which allows administrators performing a rollout to implement a configuration wizard that customers or other (restricted) administrators can operate. To do this, you use a special description language that can be used to define very complex wizards.

Custom wizards support the following features:

- Definition of any internal variables
- Conditional branches
- Conditional goto instructions to any URL
- Conditional display of notices
- Runs all (non-interactive) actions that are available with the LCOS command line interface
- Read-out current values from the configuration in the device
- Write new values to the configuration in the device
- Status checks such as checking the time in the device
- Connection checks, e.g. the successful VPN connection to a specific remote site

Observing the rules of the description language, you create the new wizard in the form of a text file, which you then load into the device. The user on-site can run the custom wizard from WEBconfig by using the appropriate name.

You can restrict certain administrator accounts to be available specifically under the Rollout Wizard only, allowing even inexperienced users to configure certain functions without allowing access to the complete configuration.

2.18.2.1 Structure of the custom wizard

The instructions that describe a custom wizard consist of the following sections:

- String tables with the necessary texts in English and German.
- A definition of the wizard.
- Any number of sections describing the HTML pages that the wizard is to display.
- An initialization section, which defines the actions when you start the wizard.
- A concluding section, which defines the actions when you stop the wizard.

Note the following conventions for the instructions that describe the wizard:

- The elements of the instructions exactly follow the structure given above.
- The text file with the instructions is encoded in ISO 8859-1.
- Comments start with a semicolon and serve only to improve the readability of the instructions.
- Internal variables begin with the key word `wizard.` (Including the dot) and store information for the internal processing of the wizard.

- Configuration variables begin with the keyword `config.` (including the dot) and read out information from the current device configuration, or they write them to the current configuration. Enter the configuration variables in one of the following forms:
  - Dedicated parameters in the configuration are referenced via `config.1.<SNMP-ID>`, for example `config.1.2.1` to access the device name (to be found in the menu under **Setup** > **Name**).

    One way to find the SNMP-ID for a parameter in the configuration is to enter the command `ls -a` at the command line in the corresponding submenu.
  - You can reference the values in a table with:
    ```
    config.^.<SNMP-ID>.<Line>.ID:<Column>
    ```
    Example for finding the value in the first line and the column with ID '2' in the routing table '1.2.8.2':
    ```
    config.1.2.8.2.1.ID:2
    ```
  - If you do not know the ID of the column, an alternative for you to reference the values in a table is to enter:
    ```
    config.1.<SNMP-ID>.<Line>.<Column>
    ```
    Example for finding the value in the first line and second column:
    ```
    config.1.2.8.2.1.2
    ```
  - If you do not know which line in the table you need, you can reference the values in a table via a known value in the first column:
    ```
    config.<SNMP-ID>."<Known-Value>".ID:<Column>
    ```
    Example for finding the value in the column with ID '2' on the line with the value of the default route in its first column:
    ```
    config.1.2.8.2."255.255.255.0".ID:2
    ```
    If the table contains multiple rows with the same value in the first column, then the configuration variable references the first of these lines.
  - If the required line in the table is only defined after the user has entered input into the wizard, you can reference the value in the table by using a variable with:
    ```
    config.<SNMP-ID>.\"<Internal-Variable>\".ID:<Column>
    ```
    Example for finding the line whose first column contains a value that agrees with the current value of the internal variable wizard.target_network:
    ```
    config.1.2.8.2."\wizard.target_network"\.ID:2
    ```
- Device-property variables begin with the key word `device.` (including the dot) and are used to read-out specific properties from the device. For more information about the device variables, see the section *Using device properties as variables* on page 142.

String tables

The instructions for the custom wizard basically define the texts that are to be displayed in German and English.

The line `stringtable "English"` delivers the English text, the line `stringtable "Deutsch"` delivers the German texts. Each string definition consists of the keyword `string`, followed by the name of the string and the value enclosed by double inverted commas.

The following example shows the string tables with just one entry:

```
; -String tables start-------------------------------------------------
   stringtable "English"
   string title_test, "Test wizard"
   stringtable "Deutsch"
   string title_test, "Test-Assistent"
; -String tables end---------------------------------------------------
```

The interpreter of the instructions that describe the custom wizard in LCOS requires all texts to contain a German and an English definition. LCOS will not execute the wizard if an entry in the English string table is not accompanied by an entry of the same name in the German string table (or vice versa).

Definition of the wizard

The definition specifies the name of the wizard. The keyword `wizard` precedes the internal name in double inverted commas followed by the reference to an entry in the string table (*String tables*). The wizard displays the external name defined by this string when the HTML page is executed:

```
; -Wizard Definition Start---------------------------
   wizard "My_Test-Wizard", title_test
   ; -Wizard Definition End----------------------------
```

Sections

The sections represent the actual HTML pages that are displayed when the wizard is executed in the user's browser.

Each section begins with the keyword `section` and ends with the beginning of the next section. The last section ends at the beginning of the 'on-init' area, i.e. there is no explicit keyword for the end.

The sections include the following elements in any order and quantity:

- Conditions
- Optional freely definable name of the section, starting with the keyword `label`, followed by a string of upper- and lowercase letters and underscores '_':

  ```
  Label My_RolloutAssistent
  ```

  The instruction set for the wizard can use the freely definable name as a goto target.

- Static text starting with the keyword `static_text` followed by a reference to an entry in the string table *(String tables)*:

  ```
  static_text str.conf_general
  ```

- Fields for different data types such as text or IP address, check boxes, radio buttons, selection lists, etc.

  Information on the various fields can be found in the *Fields and attributes* on page 138 section.

- Actions performed by the wizard in different situations depending on the keyword at the beginning of the block:
  - `on_show`: The wizard performs the actions in this block before a section (HTML page) is displayed.
  - `on_skip`: The wizard performs the actions in this block if a section (HTML page) is not to be displayed due to conditions contained within it.
  - `on_next`: The wizard performs the actions in this block if the user clicks on 'Next' in the section (HTML page).
  - `on_back`: The wizard performs the actions in this block if the user clicks on 'Back' in the section (HTML page).

  Notes on the structure of the blocks with the actions and the elements in them are to be found in the *Actions* on page 143 section.

Conditions

The instructions for the wizard can add conditions to any element in a section. A condition can be used to change the output HTML page depending on the context by showing or hiding certain configuration options depending on the previous settings.

Conditions always refer to the previous element. They consist of a class specifier and one or more condition patterns. A pattern consists of two operands and one operator. The following applies here:

- If a condition contains multiple condition patterns in one line, the wizard evaluates this expression as an OR operator.
- If the instructions contains multiple conditions relating to a parent element on separate lines, the wizard assesses the expression to be an AND operation.

A class can contain any number of condition patterns and an element can contain any number of conditions. For example, the following conditions only display the section if the internal variable `wizard.test_select1` is equal to `1`, and `wizard.test_select4` or `wizard.test_select5` is equal to `0`:

```
section
only_if wizard.test_select1, "1", equal
only_if wizard.test_select4, "0", equal, wizard.test_select5, "0", equal
```

Classes

The instructions can include the following classes:

- `only-if`: The preceding element is only executed or displayed when at least one of the following condition patterns is fulfilled.
- `skip-if`: The preceding element is not executed or displayed when all of the following condition patterns are fulfilled.

Operands

The condition pattern can contain the following operands:

- Static text
- Internal variables of the wizard
- Variables for referencing values from the current configuration of the device (configuration variables)
- The character '*' as a wildcard

Operators

The condition pattern can contain the following operators:

- `equal`: Checks if the two operands are equal.
- `exists`: Checks if the specified configuration variable is set, i.e. that the value of the parameter in the configuration is not empty.
- `empty`: Checks if the first operand is empty. The second operand is specified as a wildcard '*'.
- `contains`: Checks if the first operand contains the second operand.
- `!`: Negates the condition.

Examples

The following condition only displays the section if the internal variable 'wizard.test_select' is equal to '0'.

```
section
only_if wizard.test_select, "0", equal
```

The following condition sets the internal variable 'wizard.intranet_name' to the value 'INTRANET' if this variable is empty.

```
set wizard.intranet_name, "INTRANET" only_if wizard.intranet_name, *, empty
```

The following condition sets the internal variable 'wizard.target_1' to the value 'TARGET_1' if the internal variable 'wizard.select_target' is set either to '1' or '5'.

```
set wizard.target_1, "TARGET_1" only_if wizard.select_target, "1", equal, wizard.select_target, "5", equal
```

Fields and attributes

The wizard uses fields in order to display information to the user and to give the user the option to enter information. Each field corresponds to an internal variable.

The wizard defines a field by specifying the appropriate key word, followed by an internal variable on the same line. Additional lines that follow can optionally contain the attributes for the field.

An example of a field definition in the wizard:

```
selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE
```

This field generates a group of radio buttons, only one of which can be activated by the user. The wizard places the text defined in the string table `str.inet_Selection` as a description next to the field. For the radio buttons themselves, the wizard displays the text under `str.inet_PPPoE` and `str.inet_IPoE`. After an option was selected by the user, the wizard writes the selected value to the internal variable `wizard.select_inet`.

You can use the following fields in the wizard:

`check_local_ip`

This field checks if the wizard previously changed the device's IP address and redirects the user to the corresponding HTML page. Possible attributes:

- `destination`: Target for forwarding as a FQDN or IPv4 address.
- `timeout`: Wait time before forwarding.

`check_time`

This field verifies if the device has valid time information. Possible attributes:

- `success_jump`: Label of the page that the wizard opens if the check is successful.
- `fail_jump`: Label of the page that the wizard opens if the check fails.
- `limit`: Maximum number of checks before the wizard considers the test to have failed. Set the limit to the value '0' to continue the checks without limit.
- `timeout`: Wait time between two checks.

`entryfield_hex`

This field is used for entering hexadecimal values, such as MAC addresses. Possible attributes:

- `description`: Field description in the HTML display
- `max_len`: Maximum number of characters that the user can enter into this field
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `add_to_charset`: Adds extra characters to the default input character set.
- `default_value`: Default value

`entryfield_ipaddress`

This field is used to enter IPv4 addresses. Possible attributes:

- `description`: Field description in the HTML display
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `never_zero`: A value of '1' for this attribute denotes a field that may not contain the value '0'.
- `add_to_charset`: Adds extra characters to the default input character set.
- `default_value`: Default value

`entryfield_numbers`

This field is used to enter telephone numbers. Possible attributes:

- `description`: Field description in the HTML display
- `max_len`: Maximum number of characters that the user can enter into this field
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `add_to_charset`: Adds extra characters to the default input character set.
- `default_value`: Default value

`entryfield_numeric`

This field is used to enter numbers. Possible attributes:

- `description`: Field description in the HTML display
- `range_min`: Minimum value that the user can enter in this field
- `range_max`: Maximum value that the user can enter in this field
- `signed_value`: Allows you to specify a numerical value with a sign
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `add_to_charset`: Adds extra characters to the default input character set.
- `default_value`: Default value
- `unit`: The unit of value shown after the input field in the wizard's HTML display.

`entryfield_text`

This field is used to enter text. The attribute `hidden` is for fields used to enter passwords. Possible attributes:

- `description`: Field description in the HTML display
- `hidden`: Identifies a field used by the user to enter a password.
- `add_to_charset`: Adds extra characters to the default input character set.
- `convert_to_upper`: Converts user input into uppercase letters
- `max_len`: Maximum number of characters that the user can enter into this field
- `min_len`: Minimum number of characters that the user can enter into this field
- `never_empty`: A value of '1' for this attribute denotes a field that the user must fill out.
- `unit`: The unit of value shown after the input field in the wizard's HTML display.

`entryfield_textwithlist`

This field is used to enter text. The user also has the option of selecting from a set of predefined values. Possible attributes:

- `description`: Field description in the HTML display
- `default_value`: Default value
- `max_len`: Maximum number of characters that the user can enter into this field
- `item_value`: List of predefined values that the user can select for this field

`onoff_switch`

This field creates a simple check box. Possible attributes:

- `description`: Field description in the HTML display
- `value_list`: List of the two values that the check box may take on

- `default_selection`: Default value

`page_switch`

This field creates a link with which the user can switch to one of the wizard's several other HTML pages. Possible attributes:

- `page_description`: Comma-separated list of text strings or references to strings that describe the possible link targets.
- `page_label`: Comma-separated list or page labels of the possible link targets.
- `description`: Field description in the HTML display

`ping_barrier`

This field stops the wizard from being executed until a ping to the target was answered successfully. Possible attributes:

- `destination`: Target address for the ping.
- `loopback`: Loopback address used by the ping instead of the default reply address
- `success_jump`: Label of the page that the wizard opens if the ping is successful.
- `fail_jump`: Label of the page that the wizard opens if the ping fails.
- `limit`: Maximum number of pings before the wizard considers the test to have failed. Set the limit to the value '0' to continue sending pings without limit.
- `timeout`: Wait time between two pings.

`popup`

This field opens the entered target address in a popup window. Possible attributes:

The target address can contain variables (see *Variables* on page 142).

`readonly_text`

This field creates a read-only field. The wizard can use these fields to display text. The wizard can use `hidden` attributes to define internal variables. Possible attributes:

- `description`: Field description in the HTML display
- `unit`: The unit of value shown after the input field in the wizard's HTML display
- `hidden`: Identifies a hidden field.

`selection_buttons`

This field generates a group of radio buttons, only one of which can be activated by the user. Possible attributes:

- `description`: Field description in the HTML display
- `button_text`: Comma-separated list of text strings or references to strings that describe the individual radio buttons.
- `button_value`: Comma-separated list of text strings with the values of the individual radio buttons.

`selection_list`

This field generates a drop-down selection list for the user to select a value. Possible attributes:

- `description`: Field description in the HTML display

- `item_text`: Comma-separated list of text strings or references to strings that describe the individual list entries.
- `item_value`: Comma-separated list of text strings with the values of the individual list entries.
- `default_selection`: Default value

`static_text`

This field creates static text on the HTML page following the field name as a reference to a text string.

Variables

In some attributes of the fields you can use variables to replace the value of the attribute with another string or supplement it with an additional string. You have a choice between the internal variables of the custom Wizard and the predefined environment variables of the CLI, which you insert using special placeholders.

Inserting Wizard variables

To insert an internal variable into the value of an attribute, use the syntax `$(VariableName)`. To insert the user name from the internal variable `wizard.username` into a URL, add the following attribute: `http://host/directory?param=$(username)`.

Inserting environment variables

To insert an environment variable into the value of an attribute, use the syntax `%VariableName`. The following environment variables can be used in the attributes:

- `%` inserts a percent sign.
- `f` inserts the version and the date of the firmware currently active in the device.
- `r` inserts the hardware release of the device.
- `v` inserts the version of the loader currently active in the device.
- `m` inserts the MAC address of the device.
- `s` inserts the serial number of the device.
- `n` inserts the name of the device.
- `l` inserts the location of the device.
- `d` inserts the type of the device.

Using device properties as variables

In some situations, a wizard has to make decisions based on the device properties. For instance, the wizard should only write certain values to the configuration if the device has a particular type of WAN interface. The wizard has access to certain variables of the device properties. These variables begin with the key word `device.` (including the dot), followed by the name of the relevant property. The wizard can use the following variables for read-access to the device properties:

`device.flags.dhcp_addr`

This variable indicates whether a DHCP server has assigned an IP address to the device (in which case the variable is set to '128 ') or not ('0').

`device.hasADSL`

This variable indicates whether the device has an ADSL interface ('1') or not ('0').

device.hasISDN

This variable indicates whether the device has an ISDN interface ('1') or not ('0').

device.hasUMTS

This variable indicates whether the device has an UMTS interface ('1') or not ('0').

device.hasDSL

This variable indicates whether the device has an DSL interface ('1') or not ('0').

device.FirmwareVersion

This variable indicates the current firmware version of the device.

device.HardwareRelease

This variable indicates the hardware release of the device.

device.LoaderVersion

This variable indicates the loader version of the device.

device.MacAddress

This variable indicates the MAC address of the device in hexadecimal notation without any separators.

device.SerialNumber

This variable indicates the serial number of the device.

device.Location

This variable indicates the location of the device as specified under **Setup** > **SNMP** > **Location**.

device.DeviceString

This variable indicates the type of the device.

device.Name

This variable indicates the name of the device as specified under **Setup** > **Name**.

Actions

The wizard uses actions to change values in the device configuration. One or more conditions can be defined for any action. If these conditions are met, the wizard performs the action.

set

This action replaces the content of the target variable with the specified source. The source contains a comma-separated list of variables or text strings.

```
set $target, $sourcelist
```

If the target variable is a single configuration parameter, specify only one value as the source. Other values are ignored.

If the target variable is a table, you should first specify the value in the source from the line that the wizard should change. The wizard searches the first index column for this value and it changes the first line in which it finds this value. If the wizard does not find a line with the matching value, it adds a new line to the table.

If the target variable is a numeric value, you can use the `add` or `sub` action to add or subtract the amount defined as `$number`.

```
set $target, $number, add
set $target, $number, sub
```

Examples

The following action sets the default route to the desired values:

```
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0", "on", "Yes", ""
```

The following action increases the value of the ARP aging minutes to '5':

```
set config.1.2.7.11, "5", add
```

The following action reduces the value of the ARP aging minutes by '5':

```
set config.1.2.7.11, "5", sub
```

del

This action clears the contents of the target variable. If this variable is a table, enter the value from the first index column in the line that is to be deleted.

Example

The following action deletes the default route from the routing table:

```
del config.1.2.8.2, "255.255.255.0"
```

cat

This action lists the content of the source variables after the target variable.

Example

The following action adds the content of the variables `wizard.user` and the variable `wizard.name`:

```
cat wizard.name, wizard.user
```

cut

This action removes a certain number of characters from the target variables. Enter as a parameter the position of the character to be deleted counting from the left and, optionally, the number of characters to be deleted.

Examples

The following action will delete all characters in the variable `wizard.name` after the 2nd character.

```
cut wizard.name, 2
```

The following action will delete all characters in the variable `wizard.name` exactly 4 characters after the 2nd character.

```
cut wizard.name, 2, 4
```

trigger_config_change

Depending on the part of the firmware that is affected, changes by the wizard to the configuration do not take immediate effect, as some modules use internal structures for the configuration.

The action `trigger_config_change` triggers an update to these internal structures. You should insert this action into a section if you want to make sure that the configuration has been updated when you change a page in the Rollout Wizard.



When you exit, the wizard automatically executes this action.

exec

The string that follows this is executed as a command on the console. In this case variables can be used in the string, for example to start a `LoadScript`.

2.18.2.2 Trace for rollout wizards

The HTML pages of the wizard only display the results of internal processing. While the wizard is being built, the trace can provide additional information to the administrator which could be used for further optimization, for example about the analysis of the various conditions.

Start trace from the command line using the command `trace + Rollout-Wizard`.

2.18.2.3 Using user-defined HTML templates

As an option, the appearance of the wizard can be adapted to your company's design guidelines by uploading a customized HTML template into the device. The template can specify the basic structure of HTML pages and the design of colors, fonts, etc. by means of CSS rules.

Two fixed tags in the HTML template are used to insert the contents from the wizard into the respective HTML pages:

- `<WIZARD_LOGO>`: The wizard inserts the logo (GIF, JPEG or PNG format) as saved to the device.
- `<WIZARD_CONTENT>`: This tag marks the point where the wizard inserts the contents of the sections in the form of a two-column table with the corresponding buttons.

A very simple example of an HTML template looks like this:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <title>Title of the wizard</title>
        <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
    </head>
    <body>
        <div>
            <WIZARD_LOGO>
        </div>
        <WIZARD_CONTENT>
    </body>
</html>
```

The wizard uses a selection of predefined CSS classes that you can easily customize by specifying appropriate values in your HTML template, including:

- `class="header"`: The CSS class for the header with the logo.
- `class="wizardName"`: The CSS class paragraph with the name of the wizard at the head of the page.
- `class="headerLogo"`: The CSS class for the area for the logo in the header.
- `class="wizardTable"`: The CSS class for tables with the displayed fields.
- `class="footer"`: The CSS class for the footer with the buttons.

2.18.2.4 Uploading files for the wizard

To make the wizard available, upload the following files to the device:

- **Rollout-Wizard (simple Text)**: The instructions for compiling the wizard (required). This ISO-8859-1 encoded text file is required for operating the wizard. There is no limit on its size.
- **Rollout-Wizard – Template (*.html, *.htm)**: An HTML template for the wizard (optional). This template controls the way that the sections appear in the HTML pages when the user's browser displays the wizard. The template allows you to use your own CSS information to define the layout. If you do not load a custom HTML template into the device, the wizard uses a predefined template. The template must not exceed a size of 64KB.
- **Rollout-Wizard – Logo (*.gif, *.png, *.jpeg)**: Your company logo (optional). The wizard places this image file at the location of the `<WIZARD_LOGO>` marker in the template. If you do not load a logo into the device, the wizard uses a predefined logo.

2.18.2.5 Deleting wizard files from the device

There are various ways to delete wizard files from the device: You either delete the relevant files from the file system of your device, or you use the `rollout` command with the appropriate parameters from the CLI.

Deletion via the rollout command

The delete function of the `rollout` command has the following syntax:

```
rollout (-r|-remove) <RelatedFile>
```

Possible files are:

- `wizard`: Deletes the wizard
- `template`: Deletes the template
- `logo`: Deletes the logo
- `all`: Deletes the wizard, the template and the logo

Deletion via the file system

In the file system, delete the Wizard's files via the correspondingly named file names:

- **rollout_wizard**
- **rollout_template**
- **rollout_logo**

2.18.2.6 Example of a Rollout Wizard:

This section presents an example of a Rollout Wizard. The wizard is used for setting up an Internet connection.

In the first section, the wizard defines the text that the device provides for display on the various HTML pages.

```
stringtable "German"
 string title_MyCompany, "MyCompany Rollout"
 string txt_Welcome, "Welcome to the MyCompany Rollout Wizard"
 string dev_serial_number, "Serial number"
 string dev_type, "Device type"
 ;---Page: What type of connection string inet_Selection, "Internet connection type" string inet_PPPoE, "PPPoE"
 string inet_IPoE, "IPoE" ;---Page: IPoE
 string inet_ipoe, "Please enter the details for the connection."
 string con_ipaddress,     "IP address"
 string con_subnet,        "Net mask"
 string con_gateway,       "Gateway"
 string con_dns,           "DNS"
 ;---Page: PPPoE
 string inet_pppoe, "Please enter your username and password."
 con_username string,      "username"
 string con_password,      "password"
 --- Page: End
 string end,              "The configuration is now complete."
```

The wizard starts the first line of the next section with the name 'MyCompany Rollout'. The device displays the text string `str.title_MyCompany` as the title of the HTML page.

The wizard then defines the sections, which correspond to the required HTML pages.

The 'Start' section first shows a static greeting text. Below that, the Wizard has two read-only fields that display the device type and serial number. The wizard reads out these two values from the device using the field `on_show` when it opens the page. The wizard offers the user a selection of options for the Internet connection, either 'PPPoE' or 'IPoE'. Since no values are defined for the option fields, the wizard sets the variable `select_inet` according to the user's selection, e.g. PPPoE to '0' and IPoE to '1'.

```
wizard "MyCompany Rollout", str.title_MyCompany

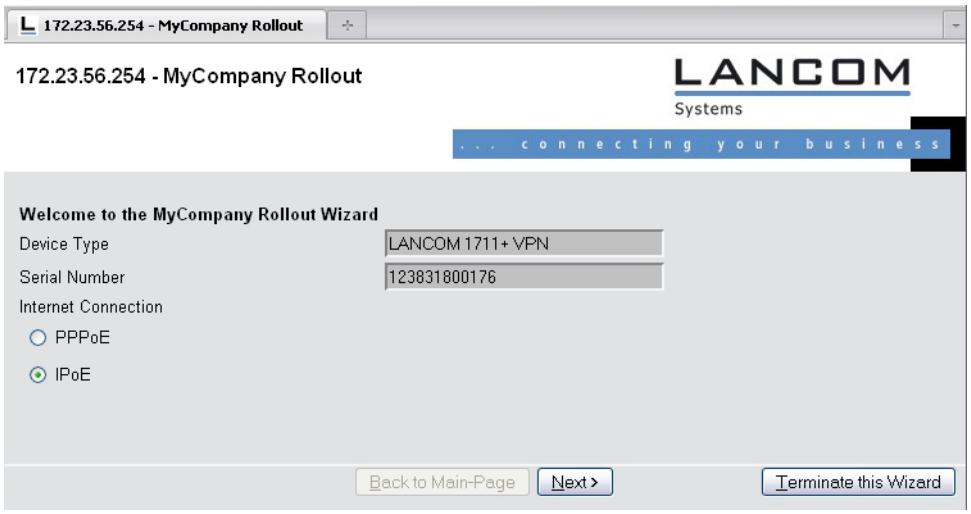
section ;---Start---
 static_text    str.txt_Welcome
```

```
readonly_text device_string
 description   str.dev_type
readonly_text device_serial_number
 description   str.dev_serial_number

selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE

on_show
 set wizard.device_string, device.DeviceString
 set wizard.device_serial_number, device.SerialNumber

on_next
```



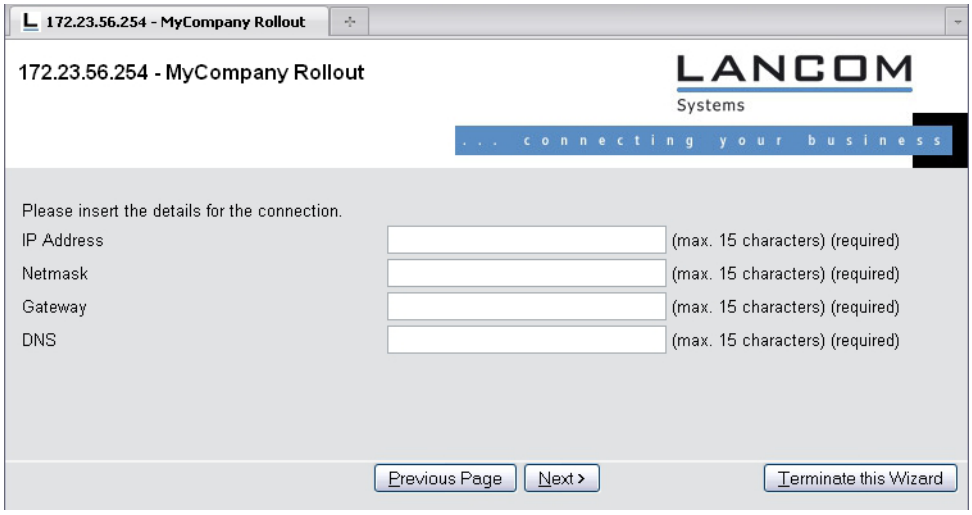
The wizard only displays the IPoE section if the variable select_inet is set to the value '1'.

On this page, the wizard asks the user to provide values for the IP address, netmask, gateway and DNS server. All fields are required to run the wizard.

```
section ;---IPoE---
 only_if wizard.select_inet, "1", equal

 static_text   str.inet_ipoe

 entryfield_ipaddress inet_ipaddress
  description  str.con_ipaddress
  never_empty  1
 entryfield_ipaddress inet_subnet
  description  str.con_subnet
  never_empty  1
 entryfield_ipaddress inet_gateway
  description  str.con_gateway
  never_empty  1
 entryfield_ipaddress inet_dns
  description  str.con_dns
  never_empty  1
```



The wizard only displays the PPPoE section if the variable select_inet is set to the value '0'.

On this page of the wizard prompts the user for the user name and password, each with a maximum length of 30 characters.

```
section ;---PPPoE---
 only_if wizard.select_inet, "0", equal

 static_text   str.inet_pppoe

 entryfield_text inet_username
  description  str.con_username
  max_len   30
 entryfield_text inet_password
  description  str.con_password
  max_len   30
```



The last page of the wizard initially displays a summary in static text. Follow-up actions are carried out when the wizard is finished:

- If the user has selected IPoE, the wizard creates a corresponding remote site and an entry in the list of IP parameters.
- If the user has selected PPPoE, the wizard creates a corresponding remote site and an entry in the PPP list.
- Whichever option is selected, the Wizard creates a default route 'INTERNET in the router.

```
section ;---ende---
 static_text   str.ende
```

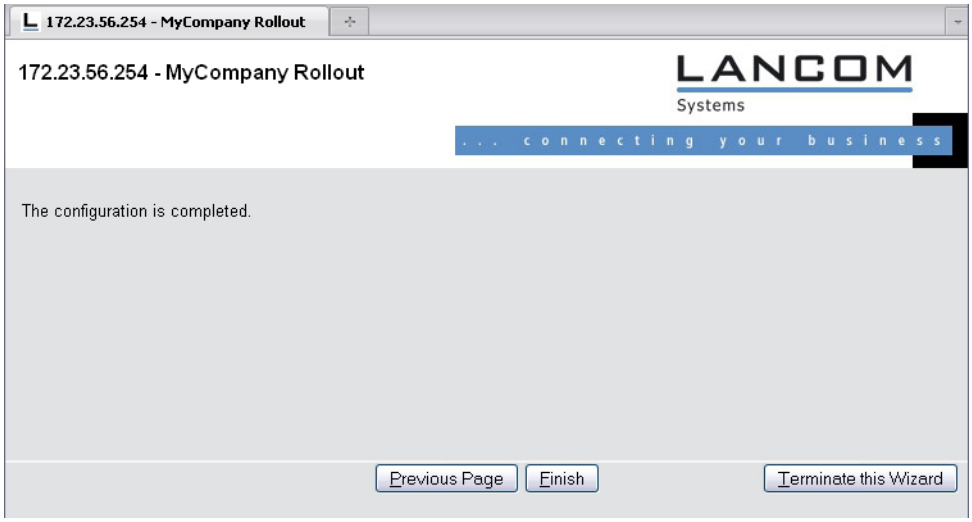
```
on_init  ;---Befehle, die bei der Initialisierung des Wizards durchgeführt werden.---

on_apply ;---Befehle, die bei der Fertigstellung des Wizards durchgeführt werden.---

 ;---Wenn IPoE ausgewählt wurde, werden die entsprechenden Daten nun eingetragen.
 ;---Remote site
 set config.1.2.2.19, "INTERNET", "9999", "", "", "IPOE", "0", "000000000000"
 only_if wizard.select_inet, "1", equal
 ;---IP-Parameter
 set config.1.2.2.20, "INTERNET", wizard.inet_ipaddress, wizard.inet_subnet, "0.0.0.0", wizard.inet_gateway,
wizard.inet_dns, "0.0.0.0", "0.0.0.0", "0.0.0.0"
 only_if wizard.select_inet, "1", equal

 ;---If PPPoE was selected, the corresponding data is entered.
 ;---Remote site
 set config.1.2.2.19, "INTERNET", "9999", "", "", "PPPOE", "0", "000000000000"
 only_if wizard.select_inet, "0", equal
 ;---PPP list
  set  config.1.2.2.5,  "INTERNET",  "none",  "60",  wizard.inet_password,  "5",  "5",  "10",  "5",  "2",
wizard.inet_username, "1"
  only_if wizard.select_inet, "0", equal

 ;---Set the default route.
 set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0", "on", "Yes", ""
```



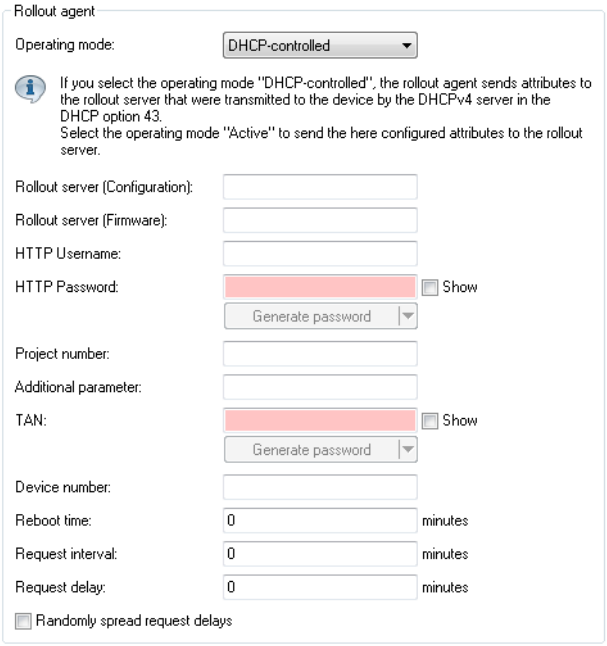
2.18.3 Activating the Rollout Wizard in WEBconfig

The Rollout Wizard is activated from the Setup menu by setting the parameter **HTTP** > **Rollout-Wizard** > **Operating** to **yes**. This initially activates the default Rollout Wizard. In WEBconfig, a new Wizard appears under **Setup-Wizards** with the name assigned under **HTTP** > **Rollout-Wizard** > **Title**.

You replace this with a custom Rollout Wizard by loading the description of the Wizard into the device (see *Uploading files for the wizard* on page 145).

2.18.4 Configuration with LANconfig

The rollout agent is configured in LANconfig under **Management** > **Rollout Agent**.



Operating mode

If you select the operating mode “DHCP-controlled”, the rollout agent sends the rollout server the attributes that the device received from the DHCP server by means of the vendor-specific DHCP option 43. In the “Active” setting, the device transfers the attributes configured in this dialog (for example, if no DHCP is available on the network). Setting the mode to “Off” disables the rollout agent.

The “DHCP-controlled” operating mode does not overwrite manually configured attributes. This makes it possible to perform a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

Rollout server (configuration)

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

Rollout server (firmware)

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

HTTP username

Set the user name used by the rollout agent to log on to the rollout server.

HTTP password

Set the user password used by the rollout agent to log on to the rollout server.

Project number

This entry specifies the rollout project number for the rollout agent.

Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

TAN

Use this entry to specify the rollout TAN.

Device number

Contains the device number of the device that is running the rollout agent.

Reboot time

Here you set the time after which the device reboots after a rollout.

Request interval

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.



If the value is "0", the renewed attempt starts in 1 minute.

Request delay

This entry contains the delay time in seconds for a rollout request.

Randomly spread request delays

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

2.18.5 Receiving LSR information via DHCP server (zero-touch rollout)

An unconfigured LANCOM device boots with an activated DHCP client and uses this to retrieve an IP address, netmask, DNS address, and gateway address from the network's DHCP server.

By means of the vendor-specific DHCP option 43, a suitably configured DHCP server sends information about how to reach an LSR (Large Scale Rollout) server, among other things. The rollout agent of the LANCOM device processes this information, contacts the LSR server and, according to the rollout strategy, it retrieves its configuration or updates its firmware.

This function simplifies the rollout process as the devices no longer have to be preconfigured.

The LSR server connects via HTTP, HTTPS or TFTP, in which case an SSL certificate needs to be stored on the LANCOM device to secure the connection.

It is also possible to configure (also partially) a rollout agent in advance. For example, the rollout server URL sent from the DHCP server can be adopted, although a project number in the device must be configured in advance.

2.18.5.1 Configuring the zero-touch rollout

Initial situation

In the case of a rollout to a number of branch sites, the large number of devices means that pre-configuring the LANCOM devices is not a viable option. Instead they should be commissioned after they have retrieved a configuration from a central LSR server, in a similar manner to the "zero-touch management" with a WLC.

Prerequisites

In order for the "zero-touch rollout" by means of the rollout agent in the device to work properly, a number of prerequisites need to be met first:

- A central rollout server must be available and the zero-touch devices must be able to contact it via HTTP/HTTPS.
- DHCP must be active in the network at the branch. That is,
  - a DHCP server is available on the branch network, or
  - a DHCP relay server on the branch network exchanges the DHCP data packets between the devices on the branch network and a DHCP server at the main office.
- The DHCP server has to be able to deliver the DHCP option 43.



The DHCP server transmits sensitive data such as the rollout password unsecured as a DHCP message. So take care to transport the data only over appropriately secured connections.

Process

The rollout of the configuration proceeds as follows:

1. The unconfigured device is connected to the branch network.
2. The device retrieves connection data (such as IP address, gateway, netmask, DNS address, and DHCP option 43) from the DHCP server.
3. The device uses the DHCP option 43 to decode various pieces of information including the URL of the rollout server and uses this to configure the rollout agent on the device.
4. The rollout agent then contacts the rollout server and performs the rollout in two steps:
   - Firmware-Update
   - Configuration update

The rollout agent contacts the rollout server at the configured firmware server URL and retrieves a firmware file in the `.upx` format, which it is then uses to update the device.

After the firmware update, the device restarts and contacts the rollout server again. The rollout agent checks whether the firmware provided by the rollout server is already installed. This test succeeds if the latest firmware was received by the device in the first step. The rollout agent continues with the configuration update and it downloads script files. It contacts the rollout server at the configured config-server URL and retrieves a script in the `.lcs` format, which it is then uploaded to the device.

DHCP option 43

DHCP option 43 is vendor-specific, i.e. each vendor is free to decide how to structure this option and what information is coded into it. The option can contain several sub-types, which are used for the detailed structuring of the data.

The following sub-types are specified for the device rollout agent:

Sub-type 1: Config-Server-URL

Server addresses are entered in the following available formats:

- HTTP, HTTPS, TFTP
- IP address, FQDN

Examples:

- https://rollout:443/
- tftp://10.1.1.1
- http://10.1.1.2/test

It is also possible to specify LCOS variables

The rollout agent expects that the rollout server available at this address will respond to its request by sending a configuration script with the extension `.lcs`.

If the rollout server is an LSR, the address requires the prefix `lsr:`, e.g. `lsr:https://rollout:443/`. The rollout agent then assembles the correct LSR-rollout URL from the sub-type 5 and the following. Accordingly, the sub-types 5 and up are only of importance when using this prefix.

If the rollout server is not an LSR, then specifying the URLs for the config-server and firmware server have to be done by hand with the use of variables.

Sub-type 2: Firmware-Server-URL

As with sub-type 1, the rollout agent expects the rollout server at this address to respond by sending a firmware file with the extension `.upx`.

Sub-type 3: HTTP-Username

Contains the user name for HTTP authentication in the URL (in the form `http://username:password@server`)

Sub-type 4: HTTP-Password

Contains the password for HTTP authentication in the URL (in the form `http://username:password@server`)

Sub-type 5: LSR project number

Contains the project number for the rollout project stored in the rollout server.

Sub-type 6: Additional URL parameters for LSR keyword

The rollout agent appends this content to the constructed LSR URL (e.g. `?approval=yes`).

Sub-type 7: Reboot-Time

Specifies the wait time in minutes before the device restarts after the update by the rollout server.

Sub-type 8: Request-Interval

Specifies the interval in minutes in which the rollout agent sends its requests to the rollout server.

Sub-type 9: TAN

This entry contains the rollout TAN.

Sub-type 10: Device number

Contains the device number of the device being updated.

Sub-type 11: Request-Delay

Contains the time in minutes that the rollout agent waits between request 1 and request 2.

Sub-type 12: Request-Random

This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time. The following entries are allowed:

0

Requests take place after set time delays.

1

With this entry, you specify that the request for a rollout takes place after a random delay.

Sub-type 13: Omit-Certificate-Check

This value determines whether the rollout agent skips the verification of rollout-server certificate.

If this subtype is missing or its content is empty, the rollout agent assumes the value is "0" and carries out a check of the server certificate.

Please note that the configuration received from the rollout server needs to switch off the rollout agent on completion **(`Operating: no`)**, otherwise the device will reboot after the specified reboot time.

Variables

URLs can contain any of the variables that are available at the LCOS console. These variables can be output by the console by using the command `printenv`.

The variables are specified in the URL with a leading "$" character (e.g. `$__SERIALNO`).

Generating DHCP option 43

The DHCP option 43 is generated on the basis of *RFC 2132, section 8.4*.

The following configuration section can be used to generate the option 43 with the use of an ISC DHCPd DHCP server:

Within the general configuration

```
option space Rollout;
option Rollout.config-server code 1 = text;
option Rollout.firmware-server code 2 = text;
option Rollout.HTTP-Username code 3 = text;
option Rollout.HTTP-Password code 4 = text;
option Rollout.Projectnumber code 5 = text;
option Rollout.AdditionalParams code 6 = text;
option Rollout.RebootTime code 7 = text;
option Rollout.RequestInterval code 8 = text;
option Rollout.Tan code 9 = text;
option Rollout.Devicenumber code 10 = text;
option Rollout.RequestDelay code 11 = text;
option Rollout.RequestRandom code 12 = text;
option Rollout.OmitCertCheck code 13 = text;
```

Within the subnet-specific configuration

```
vendor-option-space Rollout;
 option Rollout.config-server "LSR:https://10.200.50.1:443";
 option Rollout.firmware-server "LSR:https:// 10.200.50.1:443";
 option Rollout.HTTP-Username "RolloutUser";
 option Rollout.HTTP-Password "Secret";
 option Rollout.Projectnumber "1";
 option Rollout.RebootTime "300";
 option Rollout.RequestDelay "20";
 option Rollout.RequestRandom "0";
 option Rollout.OmitCertCheck "2";
```

Other DHCP servers (such as the Microsoft DHCP server) do not permit the definition of option 43 in the configuration. In this case, the byte sequence that the server is to deliver as option 43 needs to be prefabricated and inserted into the configuration.

2.19 TCP port tunnel

In some cases it can be useful to enable temporary HTTP access to a station within a network, e.g. via HTTP (TCP port 80) or TELNET (TCP port 23). For example, if questions come up concerning network devices, the Support department is best able to assist when they have direct access to the device in the customer's network. The standard method for accessing networked devices via inverse masquerading (port forwarding) sometimes requires a special configuration of the firewall—changes are made which, if they are not deleted again afterwards, can represent a security risk.

As an alternative to permanent access which is based on port forwarding, a temporary remote-maintenance access can be set up that automatically closes again after certain periods of inactivity. This is done by creating a **TCP/HTTP tunnel** for the Support staff, which gives them temporary access to the relevant device.



This access only applies to the IP address that was the source of the tunnel. Network access to devices released in this way is not transferable!

2.19.1 Configuring the TCP/HTTP tunnel

A TCP/HTTP tunnel is configured from the Setup menu.

1. In the Setup menu of the device, go to the directory **HTTP**.
2. Set the parameter **Max Tunnel Connections** to the maximum number of simultaneously active TCP/HTTP tunnels you wish to allow.
3. Set the parameter **Tunnel Idle Timeout** to the lifetime for an inactive tunnel (in seconds). After expiry of this time period the tunnel closes automatically unless data transfer is actively taking place.

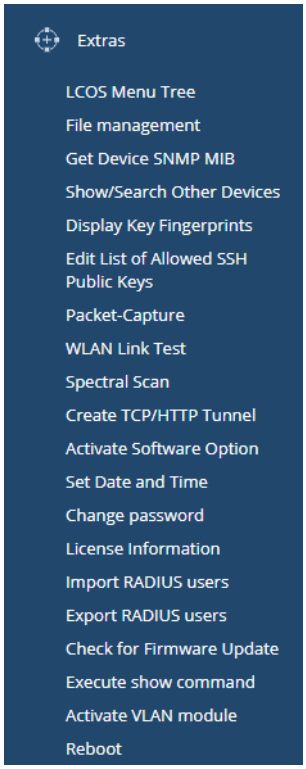
That's it! You have now completed the configuration of the TCP/HTTP tunnel.

2.19.2 Create the TCP/HTTP tunnel

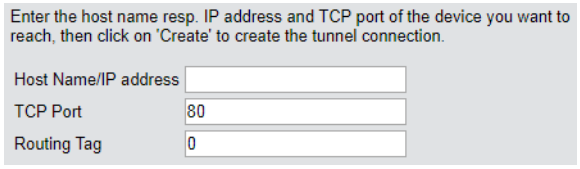
Use the WEBconfig interface of your device to set up a TCP/HTTP tunnel.

1. In WEBconfig, log on to the device which is to provide access to the device behind it.

2. In the area **Extras**, select the entry **Create TCP/HTTP tunnel**.



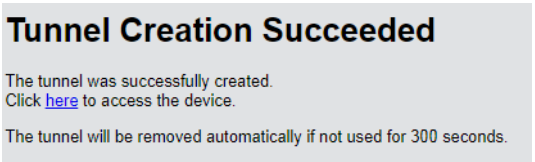
3. Enter the DNS name or IP address of the device to be accessed temporarily via HTTP and select the port to be used for the HTTP tunnel.



Apart from HTTP or HTTPS-based access, remote maintenance can also be based on any other TCP service such as telnet connections (TCP port 23) or SSH (TCP port 22).

4. If applicable, specify the routing tag of the IP network that contains the device to be accessed.
5. Accept your entries with **Create**.

The dialog that follows displays a confirmation of the newly created tunnel and provides a link to the device.



2.19.3 Create a TCP-/HTTP Tunnel via CLI

You can set up a TCP-/HTTP tunnel via the CLI of your device.

1. For example, log in to the device via SSH, behind which the device to be accessed is reachable.
2. Navigate to this directory using `cd /setup/http`

3. Execute the command `do Start-TCP-HTTP-Tunnel -r <Routing Tag> -h <IP Address> -p <Local Port> [-a <Remote Address>]`.

   -r

   Routing tag.

   -h

   Host address to be accessed via the tunnel.

   -p

   Local port.

   -a

   Optional remote address.

The TCP-/HTTP tunnel has been created.

2.19.4 Deleting the TCP/HTTP tunnel before it expires

The newly created HTTP tunnel is deleted automatically if the tunnel remains inactive for the duration of the tunnel idle timeout (see *Configuring the TCP/HTTP tunnel* on page 155. To delete the tunnel earlier, click on the Status menu under **TCP-IP** > **HTTP** > **Active-Tunnels** to access the list of active tunnels and delete the one you no longer require. However, the tunnel is only removed as soon as there are no more active TCP connections.

Although active TCP connections in this tunnel are **not** terminated immediately, no new connections can be established.

2.20 The LANCOM High Availability Clustering Option

The LANCOM High Availability Clustering Option offers you greatly simplified administration and significant time savings. You only have to configure one device in a set group of devices (cluster). The changes are automatically transferred to the other devices in the cluster.

If a device should fail or undergo maintenance (e.g. a firmware update), the APs automatically connect to another WLC or the established VPNs automatically connect to the backup central-site VPN gateway, as applicable. The automatic configuration synchronization mean that these devices already share an identical configuration. The result is a convenient way to high availability.

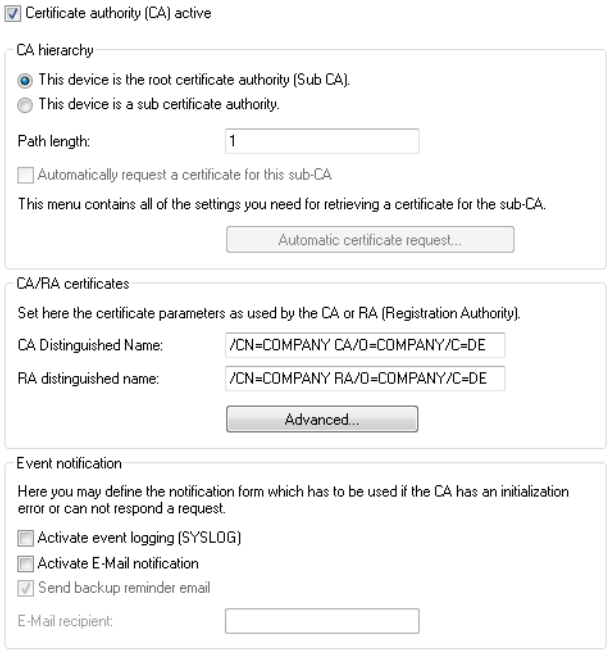
The prerequisites for a device to be a valid member of a cluster are:

- The LANCOM WLC High Availability Clustering XL Option (as of LCOS version 9.10).
- All cluster members must be able to establish IP communications via LAN, WAN or VPN.
- It must be in the list of group members that is stored in each device.
- It must have a valid certificate.
- It must be able to authenticate itself as a member of the cluster by certificate.

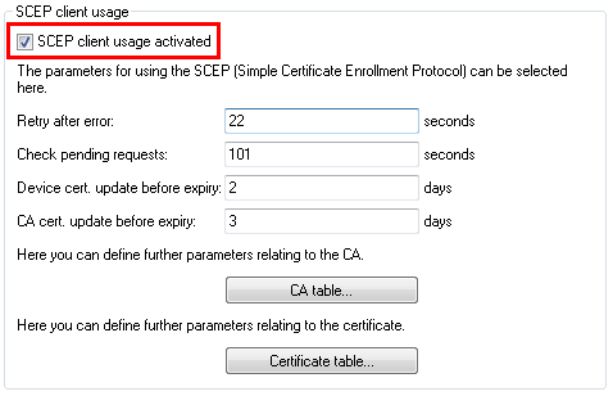
2.20.1 Setting up configuration synchronization

In order for configuration synchronization to function, all of the devices to be configured need to have valid certificates. In the interests of easy certificate distribution, you first need to configure a SCEP-CA on one of the devices.

1. To do this it is necessary to enable the SCEP server under **Certificates** > **SCEP CA**. If you set up the configuration synchronization on a WLC, it is most likely that the SCEP server is already active.



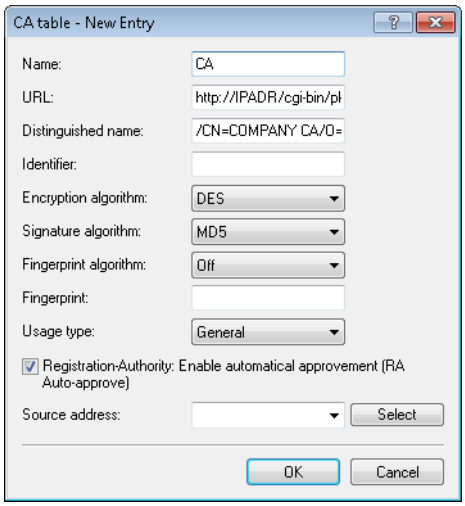
2. Then you enable the SCEP client on any device that is to work with configuration synchronization (including the SCEP CA device) under **Certificates** > **SCEP client**. If you set up the configuration synchronization on a WLC, it is most likely that the SCEP client is already active.



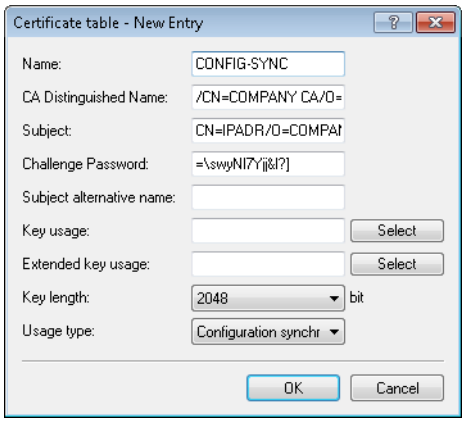
3. Add a new entry for the SCEP server to the **CA table**.

   The values for the CA table match the settings of the SCEP server from step 1 and are thus the same for all stations. For the URL you enter `http://IPADR/cgi-bin/pkiclient.exe`, replacing `IPADR` with the IP address of the device configured as SCEP-CA.

If you set up the configuration synchronization on a WLC, a corresponding entry for the WLC operation will already be available. This entry can also be used to obtain a certificate for configuration synchronization, and in this case there is no need to make any changes to the CA table.



4. The **Certificate table** in the SCEP client needs a new entry for the retrieval of a configuration synchronization certificate. The **CA distinguished name** is the one you used when you created the CA table entry.

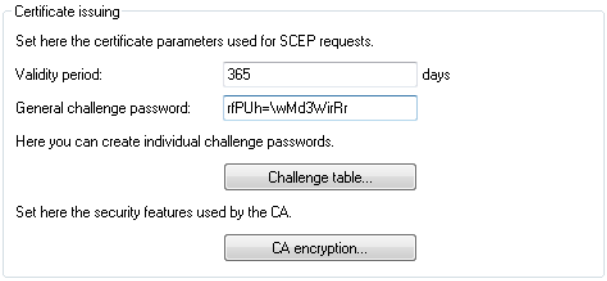


As the subject, enter each device's own IP address (e.g. `/CN=IPADR /O=COMPANY/C=DE`), replacing `IPADR` with the IP address of the device configured as SCEP-CA.

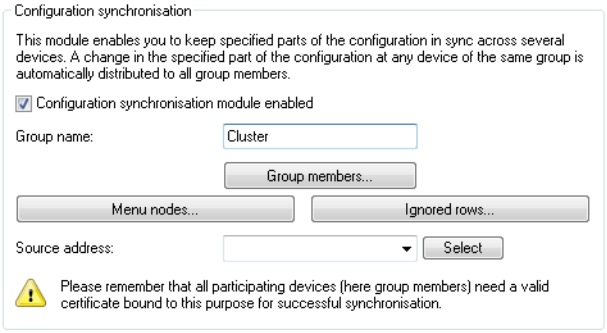
In order for the configuration synchronization to function, it is absolutely necessary for the IP address of the device to be included in the certificate's subject.

Set the **Usage type** to "Configuration synchronization". Also, adjust the **Key length** to "2048 bits". Set a **Name** of your choice for the table entry.

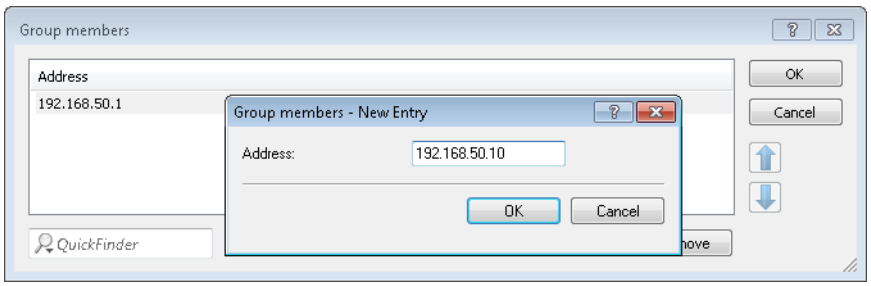
The challenge password of the device configured as SCEP CA is located in its configuration under **Certificates** > **Certificate handling** > **General challenge password**.



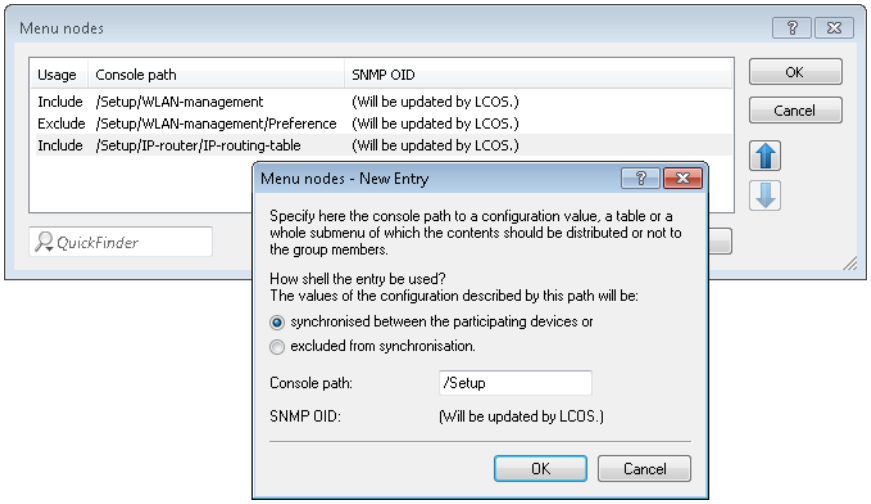
5. This concludes the set up of the SCEP CA and the SCEP client for the retrieval of configuration synchronization certificates. At this time you can write the configuration back to the device in order to retrieve the certificates.
6. Now activate the configuration synchronization under **Management** > **Synchronization** with the option **Configuration synchronization module enabled**. Under **Cluster name** you can also set a name that appears in the LANconfig device list.



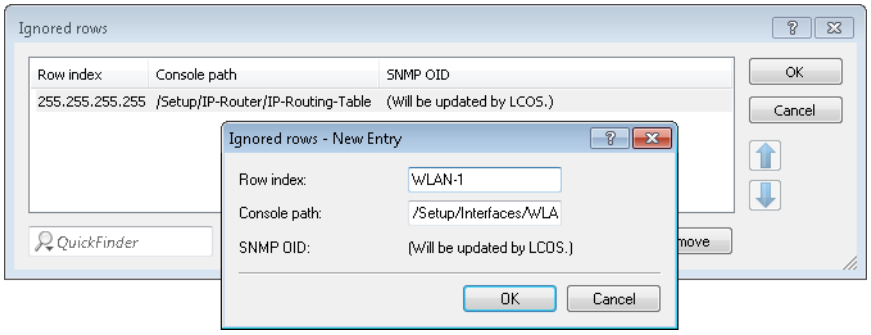
7. Under **Cluster members**, enter the IP addresses of **all** of the devices that are to be members of the cluster.



8. Under **Menu nodes** you specify the menus you want to synchronize. If you wish to explicitly exclude menu nodes from the synchronization, set the **Usage** to "excluded from synchronization".



Under "Ignored rows" you can optionally specify the rows of a table that should be excluded from synchronization. Example: The default route on VPN gateways, which should be different for each gateway. The rest of the routing table can be synchronized by making an entry in the **Menu nodes**.



9. The set up of configuration synchronization is now concluded for this device. You can write the configuration back to the device.
10. Perform steps 2 through 9 on the other devices that belong to the cluster. When configuring each SCEP client, point to the SCEP CA of the first device, as indicated above.
11. Now start the cluster on the device that should initially distribute its configuration to the other cluster members. To do this in LANconfig, select the appropriate entry from the device list and, in the context menu, click **[Start cluster...]**.
12. The cluster is now in operation. You can check the state of the cluster in WEBconfig under **Status** > **Config** > **Sync** > **Status**. Now, configuration changes made on any cluster member are synchronized to the other members.

Please note the following requirements:

- The correct time must be set on all of the involved devices (certificate checks).
- The IP address of each device must appear in the subject of its own certificate.
- To menu trees for synchronization must be the same on both devices (which is not always the case with different firmware versions or device options).
- If any changes are made to the configuration of the configuration synchronization (menu nodes, etc.) after the cluster was started already, then the cluster must be restarted.

2.20.2 1-Click WLC High Availability Clustering Wizard

With the 1-Click WLC High Availability Clustering Wizard, you can use LANconfig to simultaneously configure multiple WLCs under the following conditions:

- All of the WLCs have the WLC High Availability Clustering XL option enabled.
- At least one WLC is fully configured. This is the case if it is already managing APs.
- At least one WLC has a basic configuration (at least the name and IP address are set).

In case of doubt, you should start the Basic Settings Wizard on the corresponding WLC.

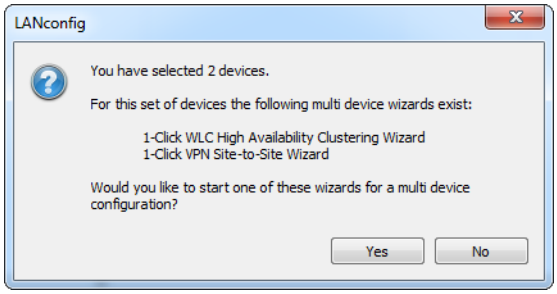
All WLCs in the cluster have the same rights.

1. In the device list, select the two WLCs that you want to configure together.

   There are two ways to start the WLC Clustering Wizard:

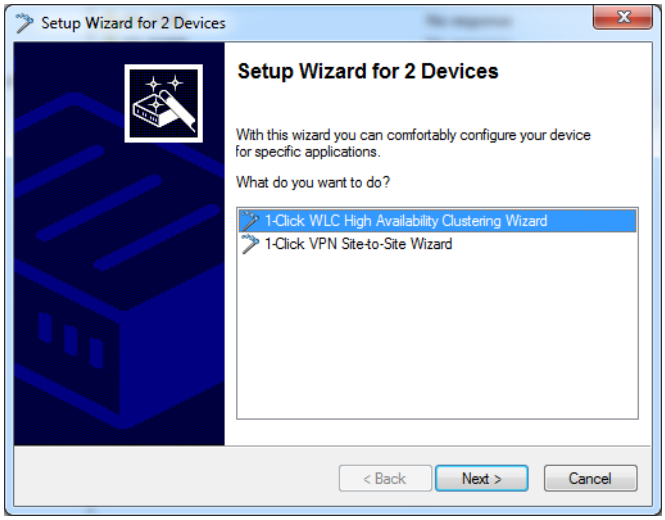
   - In the device list, drag & drop the unconfigured WLC onto the configured WLC.
   - Select the two WLCs in the device list and, after a right-click, select the item **Setup Wizard** from the context menu.

   LANconfig then displays the following message:

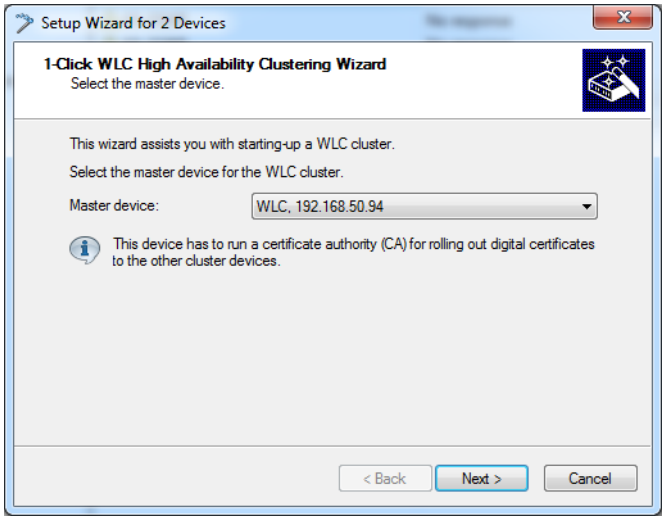


   Start the Setup Wizard by clicking on **Yes** The Setup Wizard starts with the selection dialog for the multiple-devices Wizard.

2. Select the "1-Click WLC High Availability Clustering Wizard" and then click **Next**.



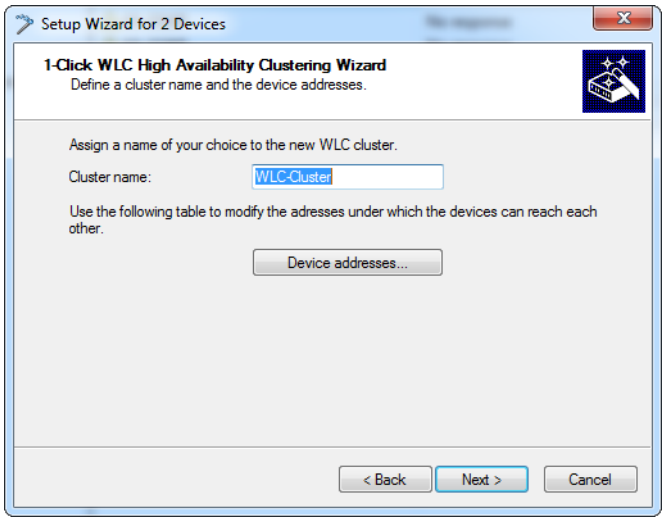
3. Select the master device, and then click **Next**



The master device is the preconfigured WLC. After you finish, the Setup Wizard transfers its configuration to all of the other selected WLCs.

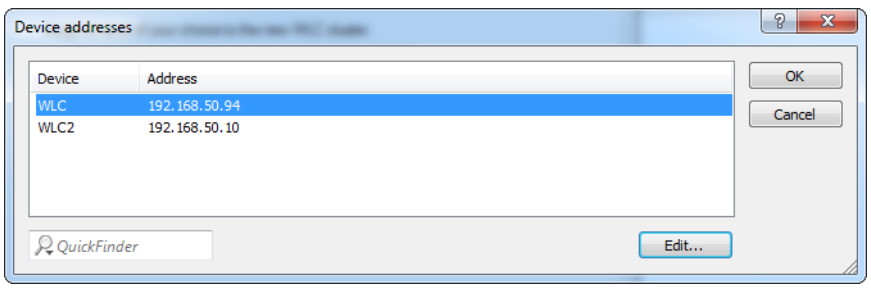
This query does not appear if you transfer the configuration to another WLC via drag & drop. In this case, the Setup Wizard automatically takes the "dragged" WLC to be the master device.

4. Assign a cluster name and click **Device addresses**.



The Setup Wizard suggests a cluster name, although you can change this if you so wish.

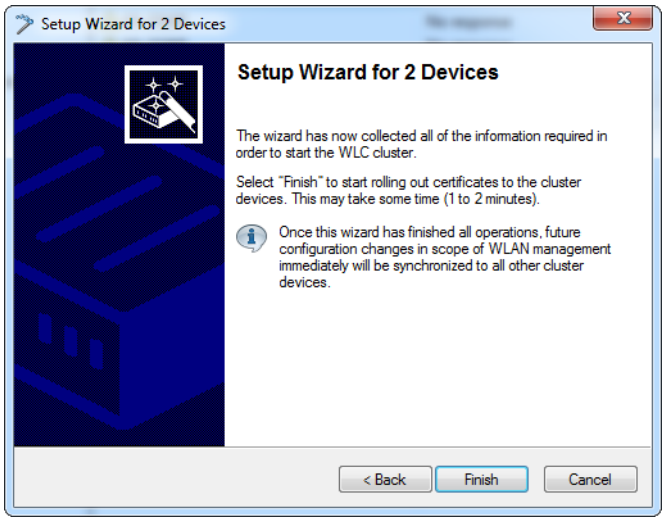
5. Enter the device addresses of all of the WLCs in the cluster.



By default, the Setup Wizard enters the devices that LANconfig is able to reach. Make any necessary changes, for example by entering devices that are accessible via VPN.

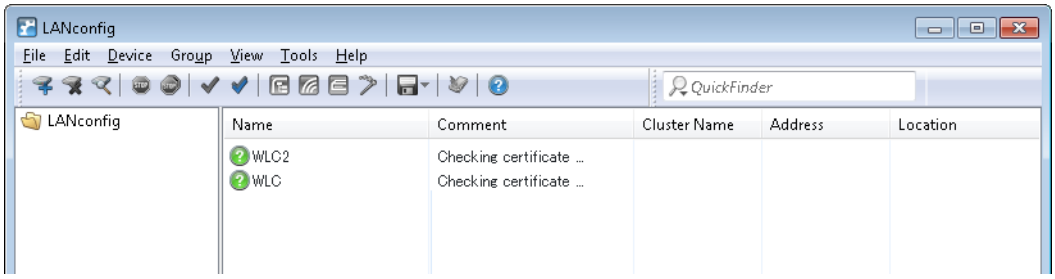
Click **OK**, and then click **Next**.

6. Click **Finish** to complete the Setup Wizard.



The Setup Wizard now loads the configuration of the master device to the selected WLCs.

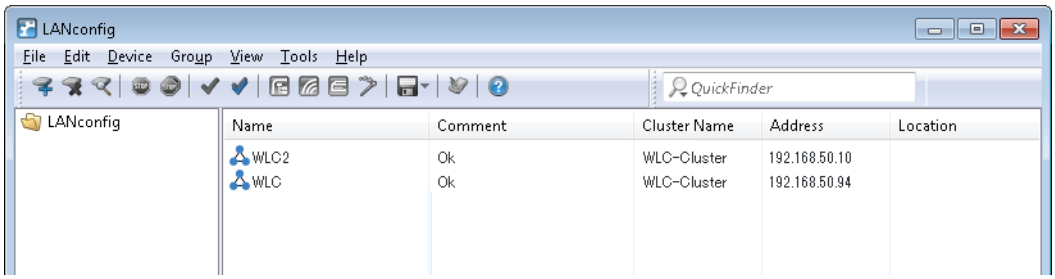
7. The device list displays the WLCs as follows:



The Setup Wizard has configured the SCEP client on all WLCs so that they can fetch a Config Sync. LANconfig now waits until the certificates are available for all of the WLCs.

Creation of the certificates may take up to one minute.

8. Once the certificates are available for all of the WLCs, LANconfig displays the status "OK" for these WLCs along with the cluster icon and the configured name of the cluster.



From now on, Config Sync configures the complete path **Setup** > **WLAN management** between all of the participating cluster members. Config Sync immediately synchronizes any configuration changes on any of the WLCs to all of the other WLCs in the cluster.

The master unit operates a master-CA, while all of the other WLCs operate a sub-CA of this master-CA. APs which connect to a WLC other than the master WLC will receive a valid certificate from it, if required.

2.21 CPE WAN Management Protocol (CWMP)

The CPE WAN Management Protocol (CWMP) enables devices to be remotely configured via a WAN link. Communication between the device (customer premises equipment, CPE) and the configuration server (auto configuration server, ACS) is conducted via SOAP/HTTP(S) in the form of remote procedure calls (RPC). A large number of RPCs are specified for the CWMP, the following of which are implemented in LCOS:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- GetParameterNames
- FactoryReset
- Reboot
- Download
  - Firmware-Update
  - Script download (*.lcs files)

LCOS additionally supports the manufacturer-specific RPCs:

- X_LANCOM_DE_Command
- X_LANCOM_DE_CommandResponse



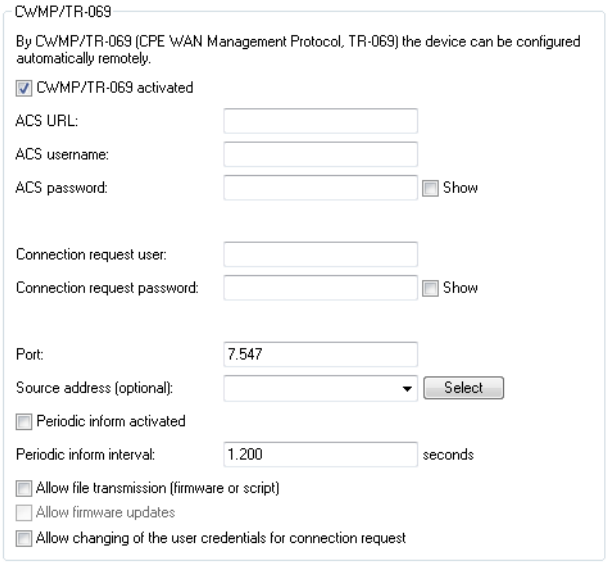
To find more information about the parameters of the RPC, visit the *Broadband Forum*.

The CPE supports the following types of authentication at an ACS:

- HTTP Basic
- HTTP Digest
- HTTPS by client certificate

2.21.1 Setting up CWMP with LANconfig

In LANconfig, the CPE WAN Management Protocol is configured under **Management** > **CWMP/TR-069**.



CWMP activated

Enables or disables CWMP.

ACS URL

Here you enter the address of the ACS (auto configuration server) which the CPE (customer premises equipment) connects to. The address is entered in the IPv4, IPv6, or FQDN format.

HTTP and HTTPS are permitted, although the use of HTTPS is preferred. Otherwise the devices transmit device-specific parameters, such as passwords or access data, unencrypted. Before you can use HTTPS, the trusted root certificate for verifying the server identity needs to be uploaded to the device.

ACS username

Enter a user name for the device to use when connecting with the ACS (auto configuration server).

ACS password

Enter a password for the device to use when connecting with the ACS (auto configuration server).

Connection request user

Select a user to be used by the ACS (auto configuration server) when connecting to this device.

Connection request password

Assign a password that the ACS (auto configuration server) uses for connection requests.

Port

Specify the local port used by the ACS (auto configuration server) when connecting to this device.

If you use IPv6, you additionally need to set the IPv6 firewall to allow access to the corresponding port under **Firewall/QoS** > **IPv6 rules** > **IPv6 inbound rules**.

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, you can specify them here as source address.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

Periodic inform activated

Enables or disables the sending of periodic inform messages from the device to the ACS (auto configuration server).

Periodic inform interval

This is the interval in seconds between two periodic inform messages sent by the device to the ACS (auto configuration server). The ACS then requests further information from the device.

The default value is 1200 seconds (20 minutes). Do not set a value that is too small, as inform messages increase network load. The interval does not commence before the device and server have exchanged all of the necessary information.

Allow file transmission (firmware or script)

This switch allows you to transfer a firmware or a script file from the ACS (auto configuration server) to this device.

Allow firmware updates

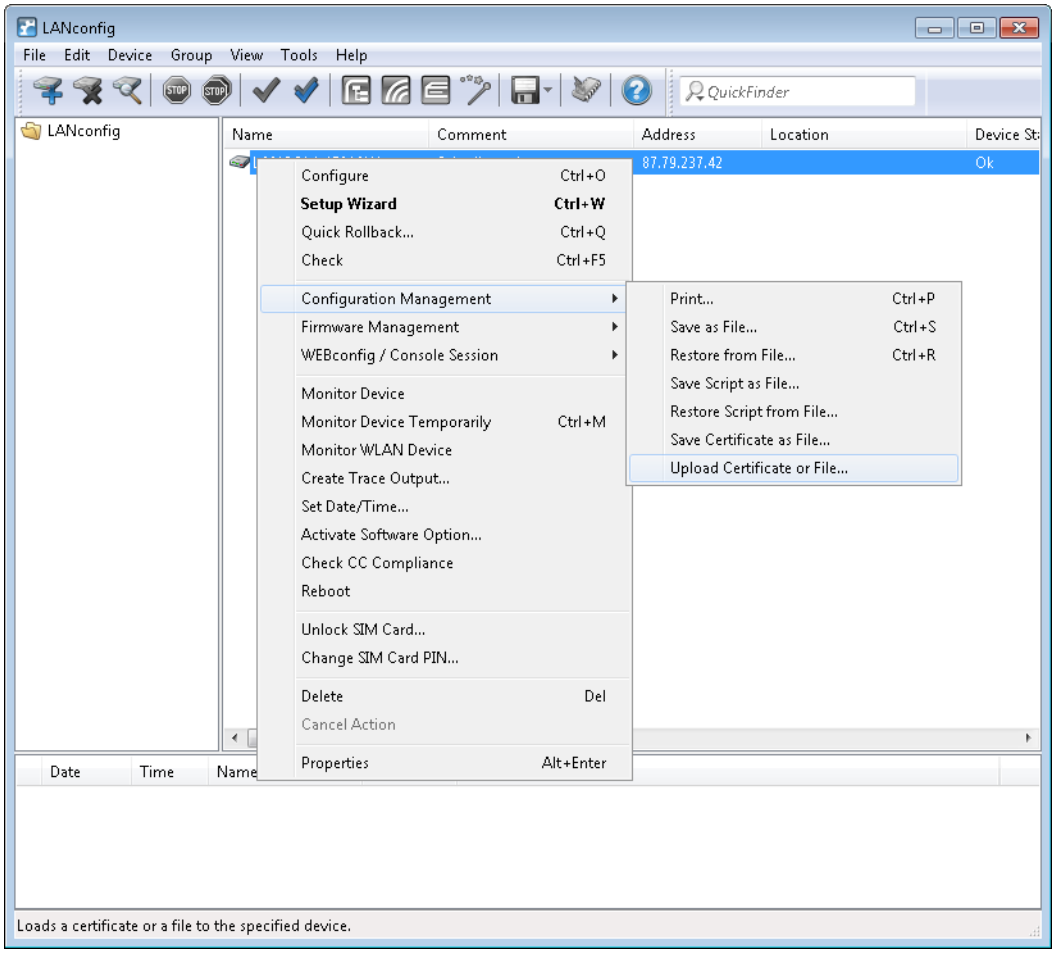
This switch allows the ACS (auto configuration server) to make firmware modifications to the device.

Allow changing of the user credentials for connection request

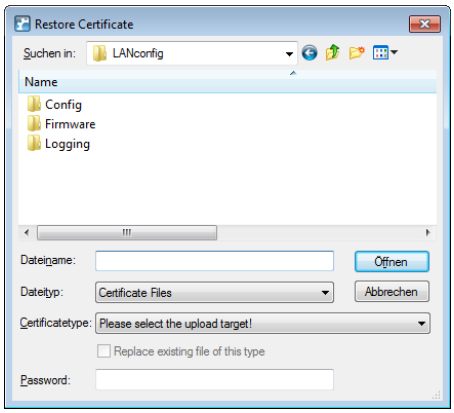
This switch allows the ACS (auto configuration server) to change the device administrator or to change the name and password of the device administrator used to connect to the device.

If HTTPS is used in the ACS URL, the CPE validates the ACS certificate. To this end, you first have to save the CWMP root CA certificate on the CPE. If the CPE is unable to validate the server certificate against the existing root CA certificate, it rejects the connection. The certificate is uploaded either by LANconfig or WEBconfig. In LANconfig you do this as follows:

1. In the device view section, right-click on the corresponding device and, under **Configuration management**, select the item **Upload certificate or file**.



2. In the dialog that follows, set the certificate type to “CWMP root CA certificate” and click **Open**.



When using SSL/TLS for authentication at the CPE, you upload the client certificate and the private key by means of PKCS#12 file (CWMP container as PKCS#12 file) onto the CPE.

2.21.2 Device configuration via CWMP

All CWMP parameters are configured on the command line either by a script file or by the manufacturer-specific RPC `X_LANCOM_DE_Command`.

Configuration via script

The CWMP download command `<cwmp:download>` is used to configure the device by means of a script file (`*.lcs`). The file type is `3 Vendor Configuration File`. The URL is the address of the server where the configuration script is stored.

LANconfig files of the *.lcf format are not supported.

Configuration by means of manufacturer-specific RPC `X_LANCOM_DE_Command`

The `X_LANCOM_DE_Command` function is defined as follows:

Request

```
<cwmp:X_LANCOM_DE_Command>
<Command> CLI-Kommando </Command>
</cwmp:X_LANCOM_DE_Command>
```

Response

```
<cwmp:X_LANCOM_DE_CommandResponse>
<Status>1</Status>
<Result>1</Result>
</cwmp:X_LANCOM_DE_CommandResponse>
```

The following example sets the IPv4 address of the device to the “INTRANET”:

```
<cwmp:X_LANCOM_DE_Command>
<Command>set /Setup/TCP-IP/Network-list/INTRANET {IP-address} 192.168.80.1</Command>
</cwmp:X_LANCOM_DE_Command>
```

Due to the asynchronous execution of the console commands, the `X_LANCOM_DE_Command` always reports a successful execution of the command, regardless of whether the command was executed correctly or not. A successful execution requires the config status to be read out under **Status** > **Config**.

To check the configuration status, you can read out the following CWMP parameters before or after using the script or `X_LANCOM_DE_Command`:

- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_ConfigVersion
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptComment
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptErrorLine
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptSuccessful

The values correspond to the status values under **Status** > **Config**.

Configuration by means of manufacturer-specific RPC `X_LANCOM_DE_CommandResponse`

The function `X_LANCOM_DE_CommandResponse` is executed synchronous and has a return value. The function is defined as follows:

Request

```
<cwmp:X_LANCOM_DE_Command_Response>
  <Command>ls /Status/Current-Time</Command>
</cwmp:X_LANCOM_DE_Command_Response>
```

Response

```
<cwmp:X_LANCOM_DE_Command_ResponseResponse>
  <Status xsi:type="xsi:unsignedInt">1</Status>
  <Result xsi:type="xsi:string">Current-Time  INFO:    11/30/2017 09:54:49</Result>
</cwmp:X_LANCOM_DE_Command_ResponseResponse>
```

The function returns the following return values:

1. Parameter: `<Status type="xsd:unsignedInt">[1/0]</Status>`

   1 = no errors, 0 = Error during execution

2. Parameter: `<Result type="xsd:string">[Output]</Result>`

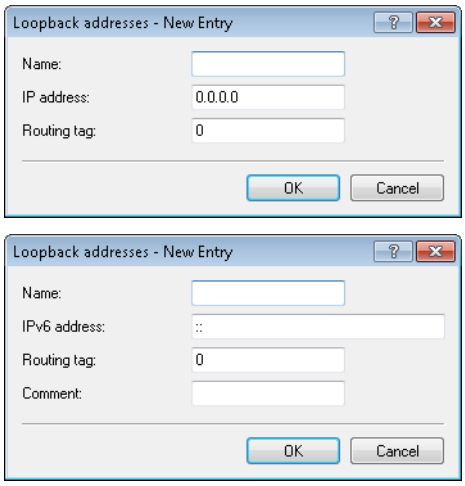
   Output = Output according to console (max. 2048 characters, more characters are cut off)

2.22 Setting known loopback addresses

Your device can be assigned up to 16 IPv4 and 8 IPv6 loopback addresses where the device can be reached (e.g. for managing larger network structures). To use the loopback addresses for particular networks (e.g. in the context of "Advanced Routing and Forwarding"), you can assign routing tags to these addresses. To simplify the identification in other configuration units, the loopback addresses can be given freely definable names.

The following steps show you how to set a loopback address.

1. Start LANconfig and open the configuration dialog for the device.
2. Navigate to the dialog **IPv4** > **General** > **Loopback addresses** or **IPv6** > **General** > **Loopback addresses** and click on **Add**.



3. Use the input field **Name** for a name of your choice for the loopback address, e.g. `LOOPBACK_1`.
4. Enter the loopback address for this device into the input field **IP address** or **IPv6 address**, e.g. `10.0.0.99` for an IPv4 address or `::1` for an IPv6 address.

   The device considers each of these addresses to be its own address and behaves as if it has received the packet from the (W)LAN. This applies in particular to masked connections. Responses to packets sent to a loopback address are **not** masked.
5. Use the input field **Routing tag** to enter an optional routing tag for the loopback address.
   Loopback addresses with the routing tag '0' (untagged) are visible to all networks. Loopback addresses with a different routing tag are only visible to networks with the same routing tag.
6. For IPv6 loopback addresses, the **Comment** field allows you to enter an additional comment.

2.23 Configuration option for IPv4/IPv6 resolution with DNS resolutions

Parameters that can be used to configure DNS host names can be transmitted with a switch that specifies how to prioritize IPv4 or IPv6 when a connection is established.

Specific use cases are, for example, the use of DNS names in VPN connections or SIP registrars, where you need to control whether the connection is established via IPv4 or IPv6.

Example 1: If the host name `vpn.example.org` is resolved to an IPv4 and an IPv6 address, a host usually prefers IPv6 over IPv4. However, if IPv4 is to be used, this can be controlled by appending `?4` to the host name, i.e. in this case: `vpn.example.org?4`.

Example 2: If IPv4 is to be preferred for a CLI ping of an IPv4/IPv6 DNS host name, the following syntax can be used: `ping www.example.org?4`.

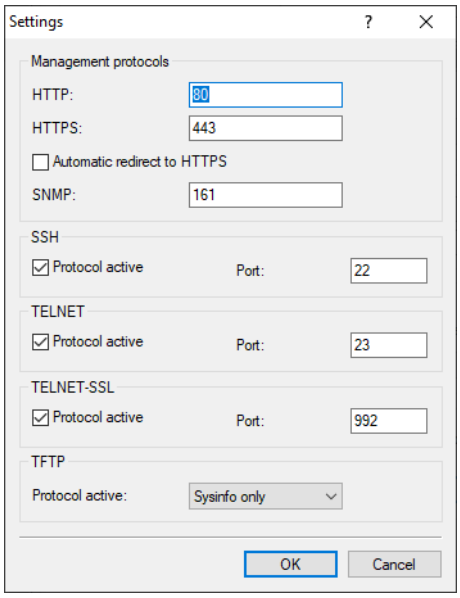
The following suffixes are allowed:

- `?4`: Resolve only over IPv4
- `?6`: Resolve only over IPv6
- `?46`: Prefer IPv4 over IPv6, i.e. if IPv4 cannot be resolved, IPv6 is used.
- `?64`: Prefer IPv6 over IPv4, i.e. if IPv6 cannot be resolved, IPv4 is used.

2.24 Customize the management ports for device access

LANconfig features the option to change the port numbers for the management protocols.

1. Start LANconfig and open the configuration dialog for the device.
2. Switch to the dialog **Management** > **Admin** and click **Ports**.
3. Enter the port numbers for the required management protocols.



4. Close all open dialog windows by clicking on **OK**.

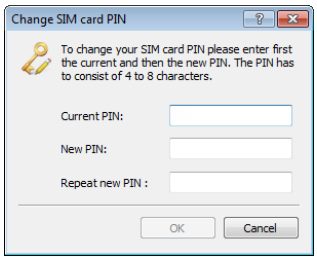
LANconfig writes the configuration back to the device.

2.25 Changing the SIM card PIN

For devices with a cellular modem, LANconfig gives you the option to change the PIN of the SIM card. You make the change simply by entering the old PIN and then the new PIN. In the interests of security, LANconfig requires an additional confirmation of the new PIN. Alternatively you can make the change from the command line by executing the action **PIN-change**.

The following steps describe the procedure in LANconfig.

1. In the LANconfig device overview, select the device requiring the PIN change.
2. From the menu bar, choose **Device** > **Change SIM card PIN**. A new dialog box opens.



3. Enter the old PIN and then your new PIN. Confirm the new PIN by entering it again.
4. Click **OK** to accept the change.

3 LANtools

The device supports different ways (i.e. interfaces) and means (i.e. software) of configuration. There is no end of different situations in which configurations have to be carried out, or ways in which operators prefer to work. This is why the device offers a wide range of ways to set up the configuration.

One option is to carry out the configuration with **LANconfig**, the menu-based, clearly structured software that allows you to adjust almost all of the relevant parameters.

The program **LANmonitor** provides an overview of the status of the device, its connections, and status values. With WLAN devices, further information about the wireless networks and the clients connected to them are available from the **WLANmonitor**.

LANtracer allows you to perform advanced trace functions for specific information (e.g. status values and function messages), either once only or for monitoring over a longer period. The trace data it produces can be used for logging or diagnostics.

The following sections discuss in detail the operation of the applications mentioned above.

To work with the various LANtools applications you will need a configuration computer with a Windows operating system.

3.1 LANconfig – configuring devices

From the easy commissioning of a single workplace device with convenient Installation Wizards to the overall management of large scale installations—the spectrum of applications for LANconfig is wide:

Basic functions

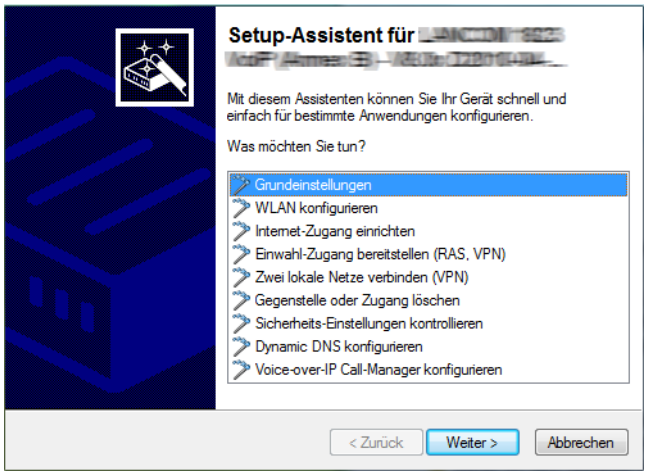
- Automatic detection of new, unconfigured devices
- (Remote) configuration of devices via IP address, URL, or via the serial interface
- Integration of Telnet, SSH, HTTPS and TFTP configuration
- Context-based help on the configuration parameters
- The Wizards provide customized input masks at every stage of installation
- Backup connection setup

Management of large installations

- Grouping
- Central firmware distribution (multitasking, also in parallel with multiple dial-in connections)
- Simultaneous configuration of multiple devices
- Configuration script distribution
- WLAN group configuration
- Logging of all actions
- Creation of new "offline" configurations for all devices and versions of LCOS

3.1.1 Start LANconfig

Start LANconfig, for example with a double click on the desktop icon. LANconfig now automatically searches the local network for devices. If LANconfig detects a device in the LAN which is not yet configured, then the program automatically starts the Setup Wizard.



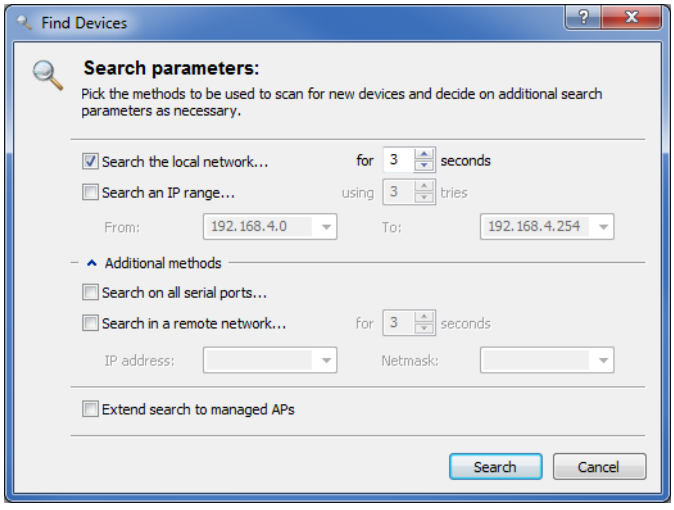
LANconfig may be unable to detect devices in the LAN if the "Internet connection firewall" or any other personal firewall is activated on the configuration computer. If your unconfigured device cannot be found, deactivate the firewall for the time during which you carry out the configuration.

Your device is equipped with a powerful integrated firewall. This provides protection for your computer even if no other firewall, such as the "Internet connection firewall", is activated.

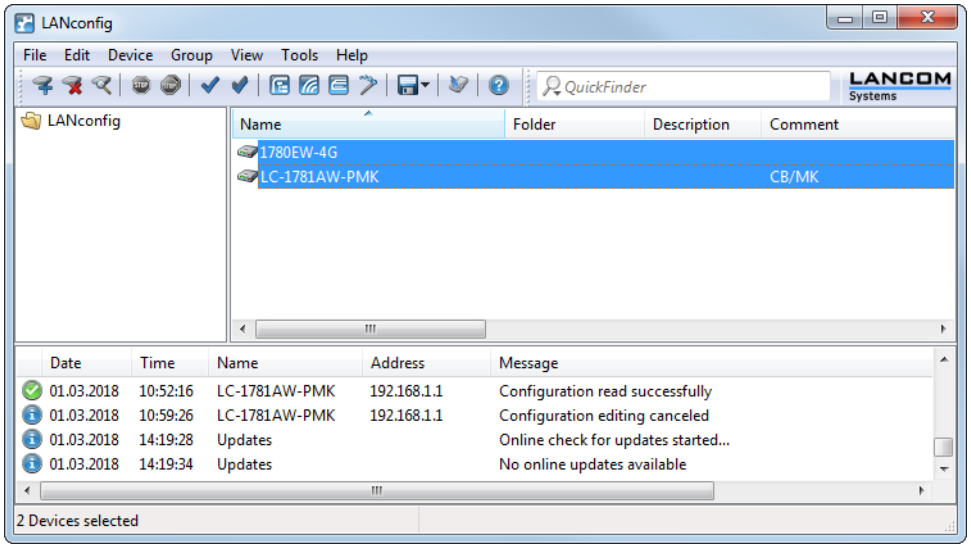
LANconfig can be automatically started when the operating system starts. Learn more about this in chapter *Application* on page 235.

Finding new devices

You can manually initiate the search for a new device by clicking on the **Find devices** ( ) button or by calling the menu command **File** > **Find devices**. LANconfig then asks where it should search. To make further adjustments to the search, click on **Tools** > **Options** and then select the menu item **Startup**.



As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.



A click on the **Configure** button or the menu item **Device** > **Configure** reads the current settings from the device and displays general information on the device. Double-clicking on the device entry optionally opens the Configuration Wizard or the device's configuration directly.

The integrated Help function

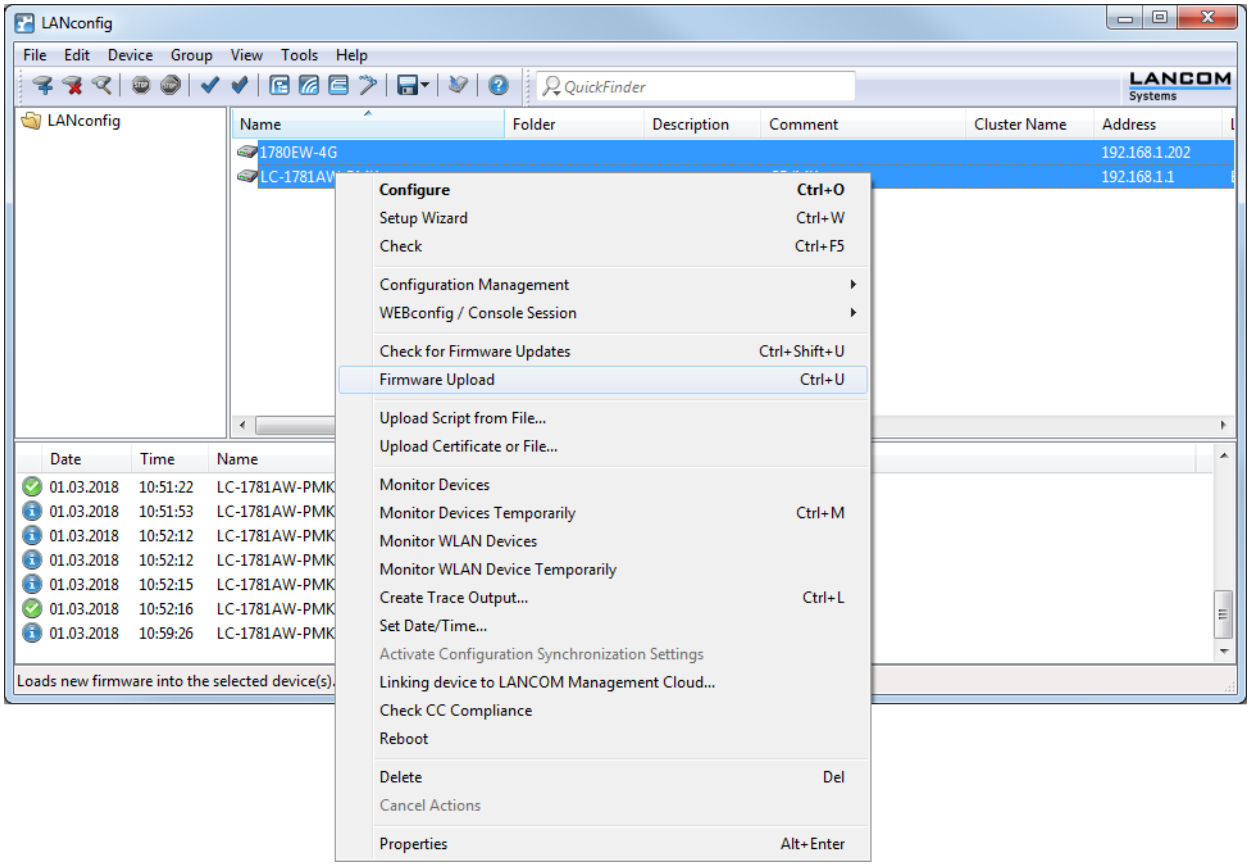
Operating the program is mostly self-explanatory or explained with the aid of the Online Help. If you click the question mark icon in the top right-hand corner of a dialog box ( ) and then click a section of the dialog, the context sensitive Help is invoked with more information about the setting. Alternatively you can also right-click on the section of the dialog to be clarified.

Selecting multiple devices

LANconfig offers a convenient way of (remote) servicing multiple devices simultaneously. There are various ways of selecting multiple devices at once:

- Press the mouse key and drag a selection frame over multiple devices.
- You can select multiple devices which are listed in sequence by pressing the Shift key and clicking on the first and the last device.
- Select any device while holding down the Ctrl key and clicking on the desired devices.
- Select the option **View** > **Display check boxes** and select the devices by activating their check boxes.

LANconfig will then carry out the actions for all of the selected devices, one after the other. For example, you can upload new firmware simultaneously for multiple devices in this way.



Administration is made easier by collecting devices into groups. The **Folder tree** view must be activated for this. The folder tree allows new directories to be created with the context menu, or by selecting **File** > **New folder**. You then group the devices simply by dragging and dropping them into the appropriate folder.

When carrying out a multiple-device configuration, LANconfig only displays the entry fields that are relevant to multiple-device configuration, e.g. for access points this includes the MAC access control list.

3.1.2 Working with LANconfig

LANconfig offers many features for you to customize your working environment to suit your needs. The QuickFinder takes you to the setting you are looking for in an instant, and the LANtools software update will keep your application up to date automatically, if you so wish.

3.1.2.1 User-specific settings for LANconfig

The program settings for LANconfig are saved to the file 'lanconf.ini' located in the program directory when the program is ended. This includes, among others, the displayed devices, directory structure, selected language, etc. When the program is started, LANconfig reads this ini file and restores the previous state of the software. To save the ini file, the user needs a write authorization to the program directory.

As an alternative to the program directory, LANconfig can load the ini file with its program settings from another directory. This can be, for example, the current user's user directory, or any other storage location:

- By selecting the user directory, users can save their personal settings even if they don't have a write authorization for the program directory.

› Selecting an alternative storage location allows you, for example, to transfer program settings to any other LANconfig installation, or to save the settings to a central location in the network for use by multiple users.

You configure the location of the program settings in the dialog **Tools** > **Options** > **Application**. Also see the chapter *Application* on page 235.

3.1.2.2 Switching the language of the graphical user interface

The language of the graphical user interface can be set to **German**, **English** or **Spanish** under **Tools** > **Options** > **Application**.

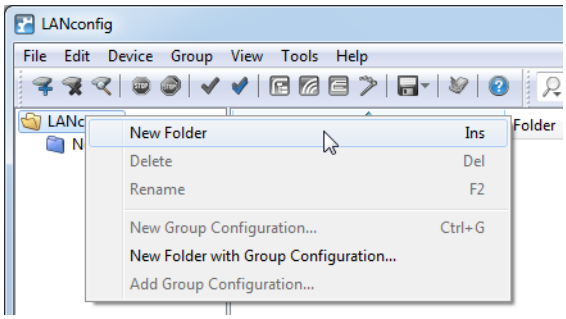
3.1.2.3 Using directory trees to get organized

LANconfig uses a directory structure for a clear overview when managing multiple devices. You can create a separate folder for each project or each customer and organize the corresponding devices here:

› Create a new folder by clicking on the parent directory with the right mouse key and selecting **New Folder** from the context menu. Alternatively you can also click **File** > **New Folder** in the application menu.

› Just 'drag and drop' with the mouse to move the individual devices from the list and into the corresponding folder. Devices can also be moved from one folder to another in this way.

The arrangement of devices in folders effects only the display of the devices within LANconfig. The organization of the folders has no influence on the configuration of the devices.

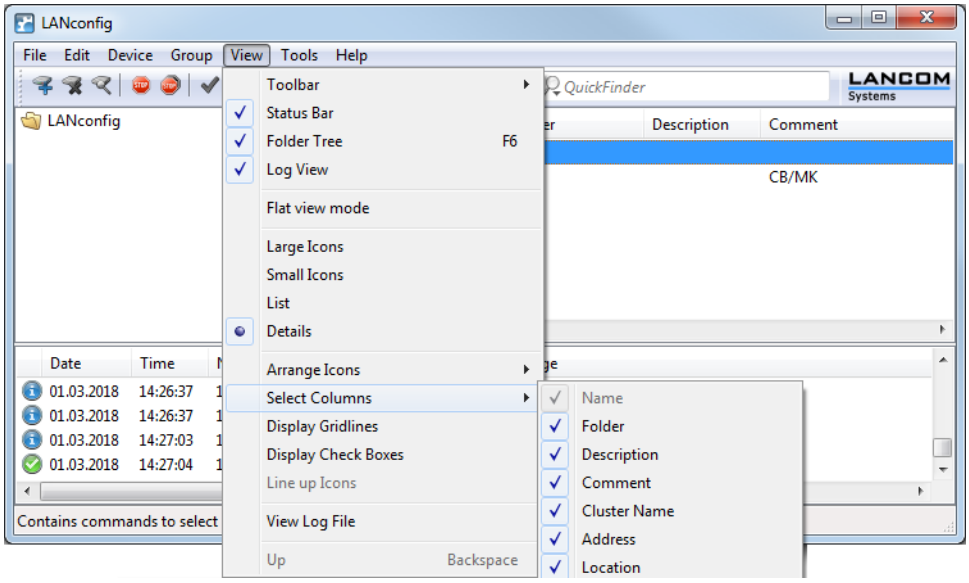


The directory structure in the left margin of the window can be switched on and off with the function key F6 or by using the menu **View** > **Folder Tree**.

3.1.2.4 Better overview in LANconfig with more columns

As a help for large-scale projects, LANconfig provides a better overview and quicker orientation with its columns featuring device-related details that can be shown or hidden according to your needs. Choose the columns to be displayed from **View** > **Select columns**. The menu item **View** > **Arrange icons** allows you to sort the items as you prefer.

Sort the view by clicking with the left mouse button in the appropriate column heading. Each new click reverses the sorting.

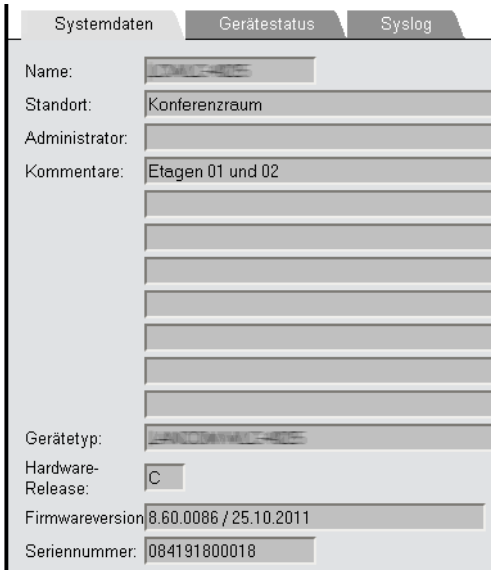


The following details can be displayed in the various columns:

- Name
- Folder
- Description
- Comment
- Address
- Location
- Device status
- Progress
- Device type
- Product code
- Hardware release
- Serial number
- MAC address
- Firmware-Version
- Firmsafe
- 1st Image version
- 2nd Image version

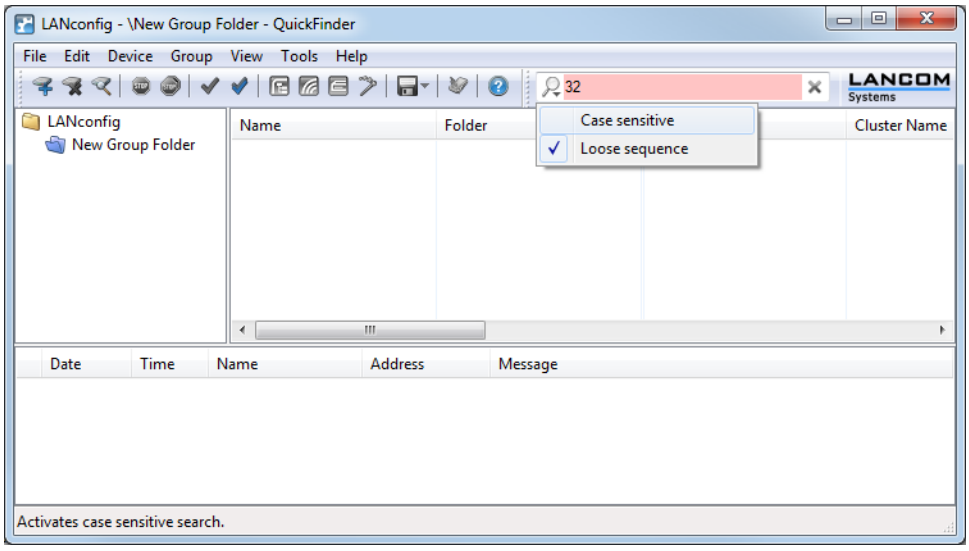
With **Select all** or **Hide all** you can show or hide all columns with just one click.

The column **Comment** contains the information in comment field 1 for the device.



3.1.2.5 QuickFinder in LANconfig

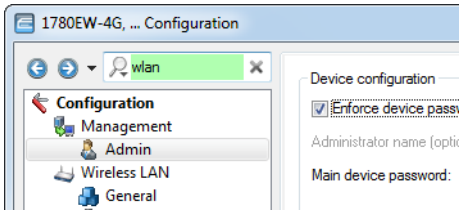
In the main view of LANconfig, the QuickFinder is located in the toolbar. Entering a search term in the search window reduces the number of available devices in the list. LANconfig searches through all the values available in the columns in the device list, including any hidden columns. Click on the icon next to the magnifying glass to make the search case sensitive.



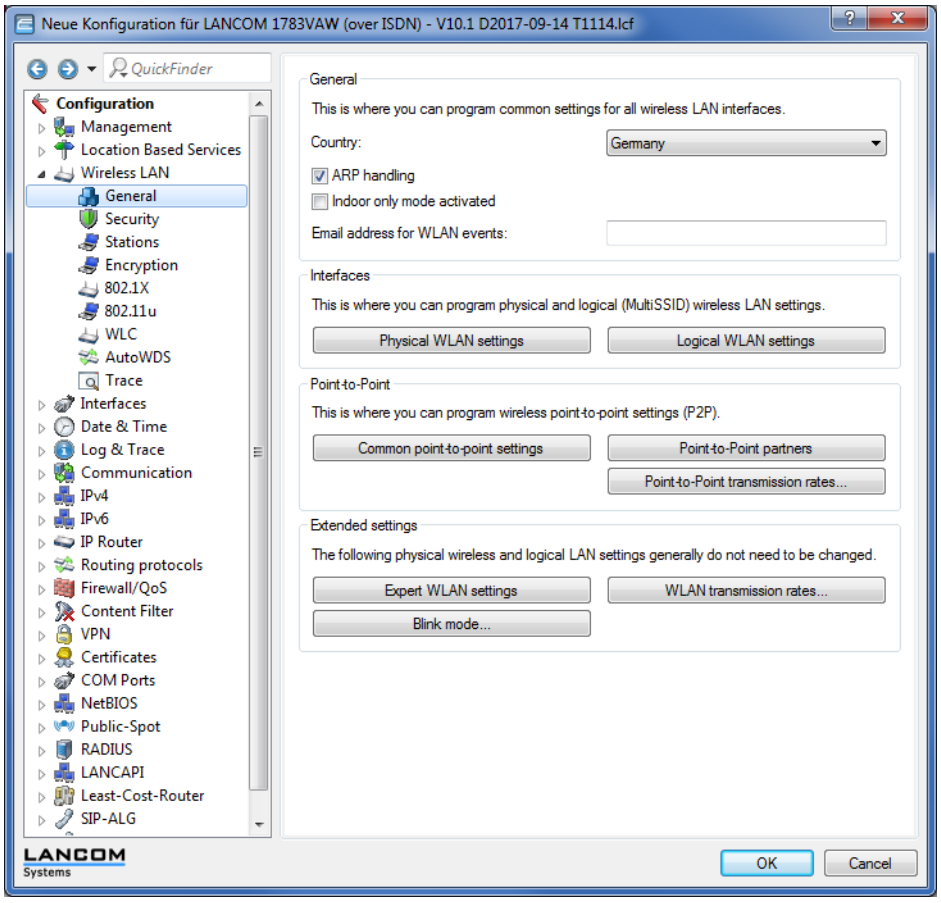
If you are looking for a particular value or term in LANconfig or in the configuration, QuickFinder quickly displays all of the locations where the string occurs in the LANconfig dialogs.

1. Start LANconfig.
2. Open the device configuration that you want to search through.
3. In the search box, type the phrase that you are looking for e.g. `wlan`. Searching is not case-sensitive. You can enter parts of words or numbers, as well as complete strings. If there are spaces in the search string, then only strings containing the matching spaces will be searched for. The search function does not support wildcards.

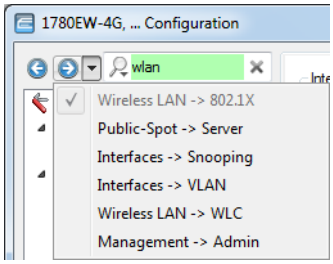
The configuration tree in the left pane of LANconfig is now reduced to just those sections that feature the search string:



Select an area in the configuration (e.g. **Wireless LAN** > **General**) to view the relevant search results framed in color in the configuration dialog:

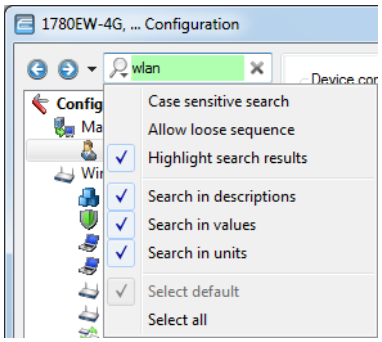


Use the navigation buttons 'back' and 'forwards' to move between the most recently visited dialogs: For quick access to the last 10 visited dialogs, click on the arrow to the right of the 'forwards' button:



Click on the 'x' to the right of the search box to clear the search and display all entries in the configuration again.

An option to reduce the number of search results is to select the sections where LANconfig should limit the search to. Click on the magnifying glass to the left of the search box and select or deselect the required categories. Here you can also specify whether the search should highlight the results in color, or whether the configuration tree is to be reduced to the relevant dialogs only:



LANconfig resets the search settings and the list of recent dialogs when the configuration is closed.

For example, your configuration may contain settings for your Internet provider. To find these you just have to enter the name to find all of the places in the configuration that refer to this provider.

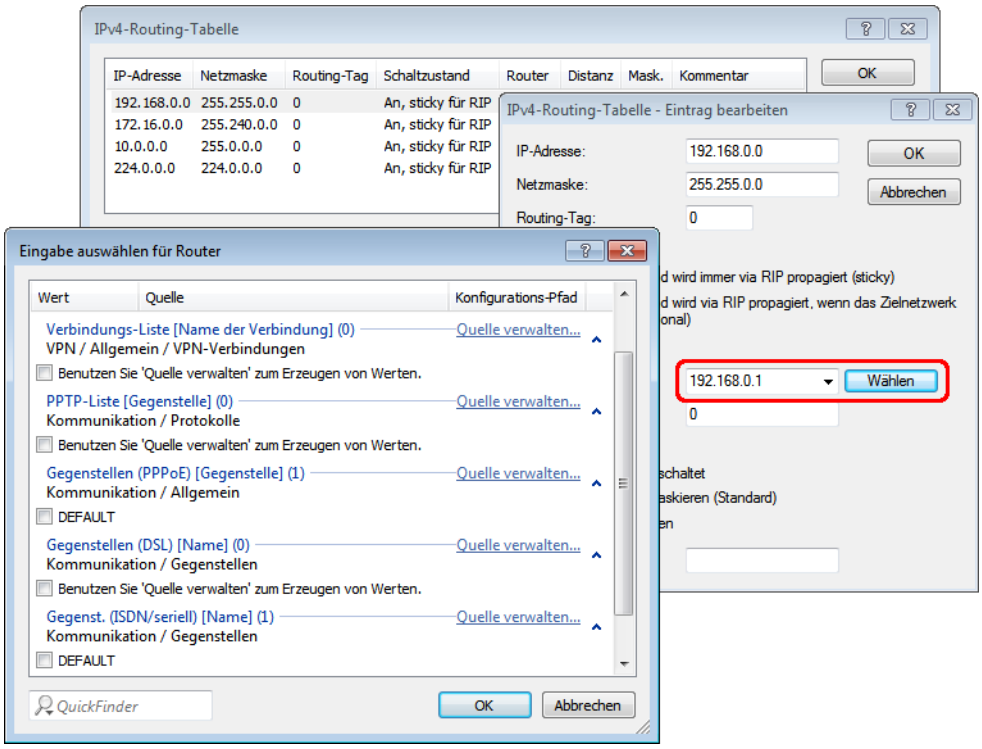
You can search for text from the following areas:

- Entries in the configuration tree
- Names of the sections in each configuration dialog
- Parameter
- Values of the parameters
- Explanatory texts in the dialogs
- Table names
- Column names in tables

3.1.2.6 Quick links for managing source tables

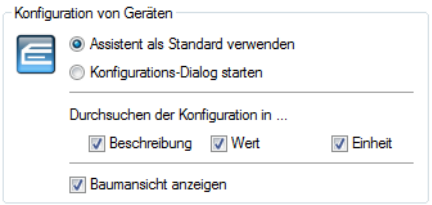
Values can be selected from an input field after they have previously been specified in one or more tables. So-called Quicklinks offer you a direct way to manage these source tables. This allows you to bypass the default configuration order. Instead of creating new elements after first exiting the current selection, you can create these items directly if necessary. These new elements are immediately available for selection.

To clarify the structure of the configuration, LANconfig shows the configuration path apart along with the individual sources. If the configuration parameters can be chosen from multiple source tables, LANconfig groups the entries accordingly. For each group, LANconfig additionally specifies the number of entries contained.



3.1.2.7 Choice of Wizard or configuration dialog

You can define how LANconfig reacts when an entry in the list of devices is double-clicked, i.e. whether a Setup Wizard or the dialog for manually editing the configuration appears. The default behavior of LANconfig can be set in the dialog **Tools** > **Options** on the **General** page.

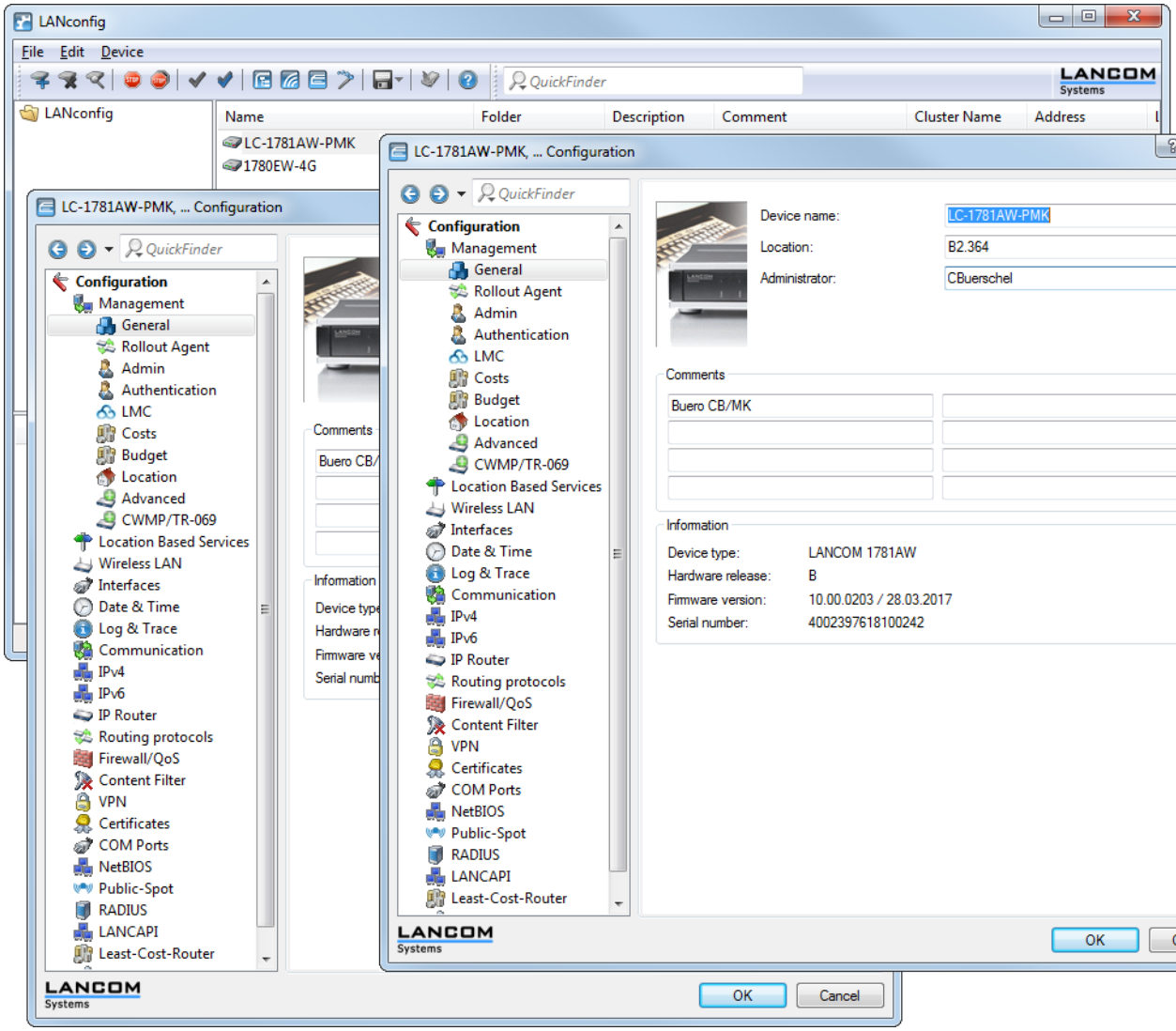


- **Use Wizard as standard:** Double-clicking on a device entry in LANconfig will open up a dialog offering a choice of Wizards.
- **Start the configuration dialog:** Double-clicking on a device entry in LANconfig will open up the Configuration dialog.

3.1.2.8 Multithreading

The management of projects can be aided by simultaneously opening up configuration windows for multiple devices to compare similarities and differences. LANconfig allows multiple configuration dialogs to be opened at the same time

("multithreading"). After opening the configuration for a device, simply open up further configurations from the device list in LANconfig. All of the configurations can be processed in parallel.

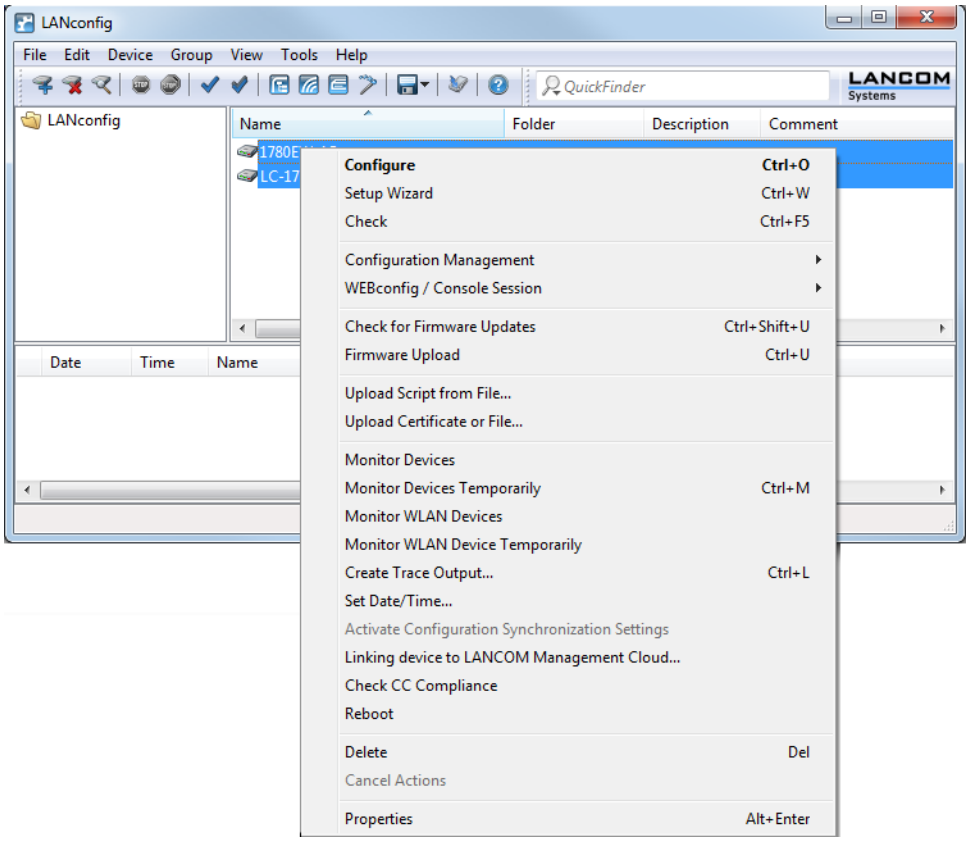


"Copy and paste" can be used to transfer content between the configuration windows via the Windows clipboard.

Multithreading allows changes to both the internal configurations of the available devices and to the configuration files. Each configuration is written separately to the file and to the device when the dialog is closed.

3.1.2.9 Project management with LANconfig

LANconfig facilitates the configuration of various devices within a project with a range of functions that can be run on several devices at once. If the list in LANconfig contains multiple devices, just click on the device of your choice with the right mouse key to open a context menu offering the following actions:



- **Configure**

  Opens up the LANconfig configuration dialog for the selected device.

- **Check**

  Checks if the selected device can be contacted.

- **Configuration management**

  Back up the current device configuration as a configuration script or as an *.lcf file.

- **Check for firmware updates**

  Searches for available firmware updates in the **Firmware archive** folder specified under **Tools** > **Options** > **Update**.

- **Upload new firmware**

  Uploads firmware simultaneously to all selected devices.

- **Restore configuration script from file**

  Executes a configuration script for all selected devices.

- **Open Telnet sessions**, **Open SSH sessions**

  Opens up multiple command-line consoles and sets up a Telnet or SSH connection to each device. LANconfig uses the external client programs configured in the settings. If no client programs are installed and specified, LANconfig cancels this action with an error message.

- **Upload certificate or file**

Opens the upload dialog for the internal file management of the device.

- **Monitor devices**, **Monitor devices temporarily**

  Starts LANmonitor for monitoring of the selected devices.

- **Monitor WLAN devices**

  Starts WLANmonitor and monitors the selected devices.

- **Create trace output**

  Opens up multiple LANtracer windows and creates a separate trace output for each device.

- **Set date/time**

  Sets the same time on all selected devices.

  When setting the time, please observe the functions of the device as NTP client and NTP server.

- **Check CC compliance**

  Checks whether the configuration of the selected devices is CC compliant. This action is useful only for CC devices.

- **Reboot**

  Restarts the selected devices.

- **Delete**

  Deletes the selected devices from the LANconfig list.

- **Cancel action**

  Forces the cancellation of any running LANconfig action (such as a file upload).

- **Properties**

  Opens a dialog of shared properties. Here you can adjust any identical general and backup-related settings for multiple devices at the same time. Please be aware that this collective dialog does not present you all of the settings available with the device-specific properties dialog.

3.1.2.10 Flexible group configuration with LANconfig

Flexible group configuration helps you to manage multiple devices: You apply a carefully selected range of configuration parameters to a group of devices, in one go. This is far more convenient than manually setting the parameters in each individual device, e.g. identical SSID settings in WLAN access points. This helps you to avoid transferring complete configuration files from other devices, in which case device-specific parameters such as the IP address are also included. Group configuration with LANconfig enables the simultaneous setting of shared group-configuration parameters, thus facilitating the simultaneous administration of multiple devices.

By collecting multiple devices into a group configuration, these devices can be a co-managed as a group. The group configuration files with the common parameters for a group of devices are, just like the full configuration files, stored on hard disk or on a server. To aid the configuration of entire groups of devices, links to the group configuration files are created under LANconfig. These links provide a convenient connection between these group-configuration files and the device entries in LANconfig.

LANconfig provides generalized group templates as an aid to creating group configurations. You define which parameters are to be used for a group according to your individual needs. Use this feature to add additional configuration parameters to the group parameters, or to remove the suggested group parameters. You can store the configurations you created either as group configurations or as a customized template for the generation of further group configurations.

Subsequently you can edit your own group configuration templates, but not the LANconfig basic templates.

The following templates for group configurations are available in LANconfig:

- **Group Template WLAN:** Includes the parameters that are co-managed on WLAN devices.

- **Group Template WLC:** Useful when operating WLCs in a cluster, this template includes the full range of parameters that minimize the need for individual device configuration.
- **Group Template Empty:** Contains no pre-selected group parameters, and so serves as a basis for creating your own group templates which exceed the scope of the WLAN and WLC group templates. Here, the total amount of all available configuration parameters in all device types is available for you to choose those which you want to use for your group configuration.

If you enable the option **Use alternative basic settings** instead, LANconfig offers a list of group templates for devices of a specific type. The Group Templates give you the option of including the common parameters for different device types into the group template. However, some parameters overlap between different device types (e.g. DSL and DSLoL). Thus the group templates are always a compromise in which some parameters may be missing. For homogeneous groups containing just one type of device, it makes sense to select a specific device configuration with a specific firmware version as a template for the group. These basic settings thus allow you to chose from precisely those configuration parameters that are required for this type of device.

Creating a new group configuration file

To work with group configurations, the devices are collected into folders. These LANconfig folders contain the devices that benefit from the co-management of shared group-configuration parameters as well as a link to the group configuration. The following steps describe how you create a new group configuration.

A group configuration allows you to manage all device parameters that are shared by the devices in the group. An individual device configuration refers to the parameters that are specific to a single device.

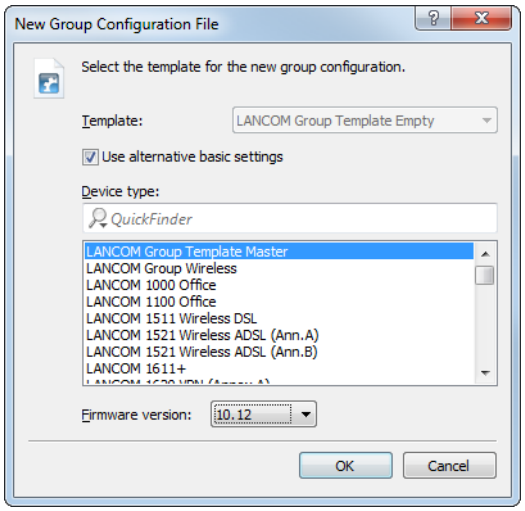
1. Create a new folder for the devices to be grouped.

   You have two ways to create this folder:

   - Click the right mouse button on an existing folder in the folder view. Select **New folder with group configuration**. The configuration dialog initially creates a new folder as a sub-directory and then continues with the selection of the template to be used for creating a new group configuration.
   - In the folder view, click the right mouse button to the directory where you wish to create the new folder. Select the context dialog **New folder** and enter a name. Use the mouse to move the devices for grouping into the new folder. Then click on the folder with the right-hand mouse key and select the context-menu entry **New group configuration**. This opens the template selection for the creation of a new group configuration.

2. Select a **template** and the appropriate **firmware version**. If you have saved your own group templates previously, these will be also displayed in the list of templates.

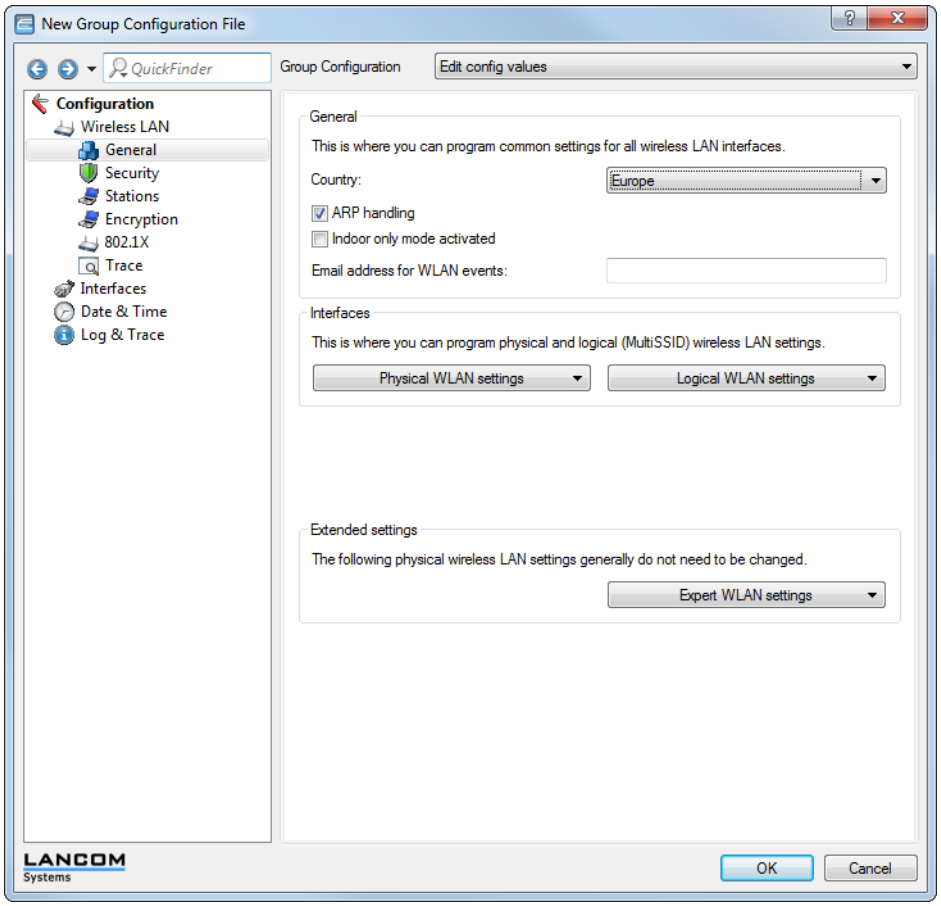
An alternative option is available by enabling the item **Use alternative basic settings**, which takes the basic settings for a particular type of device as the basis for the new group configuration. In this case, the new group configuration is created with the default values for the selected device type.



In order to avoid inconsistent sets of configuration parameters, the alternative basic settings are based on a blank template corresponding to the **Group Template Empty**.

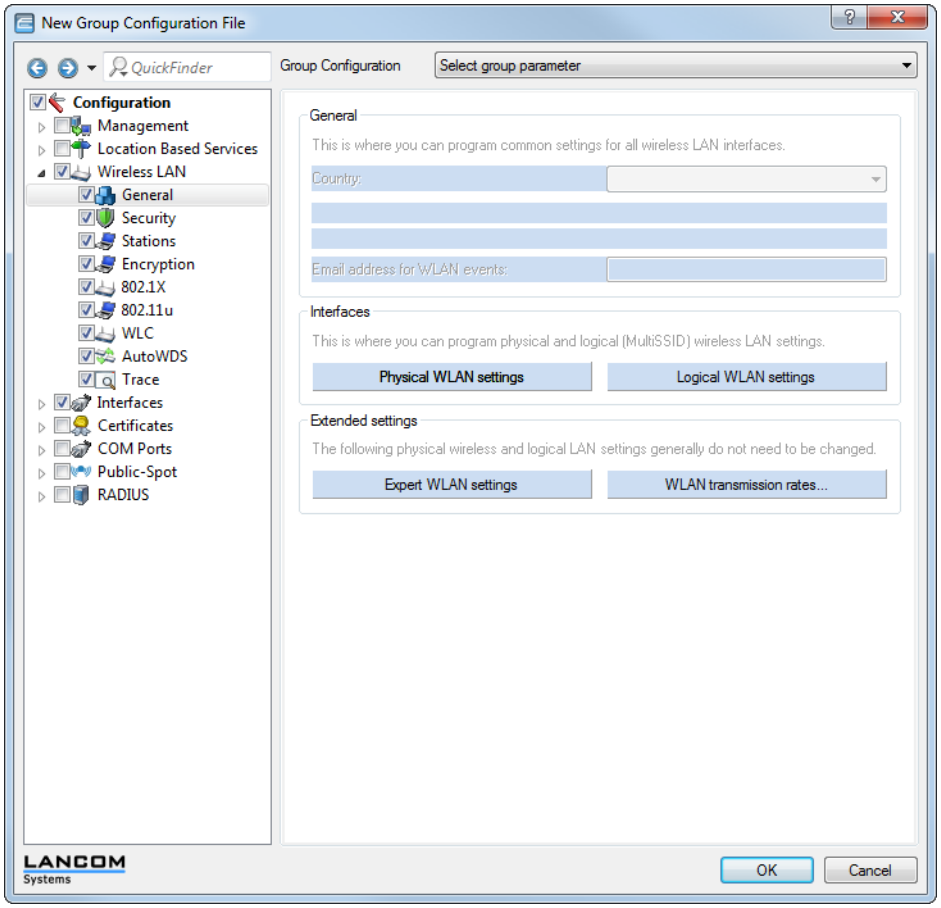
3. Click on **OK**. This opens the configuration dialog for the device parameters.
   At the top of the **Groups configuration** selection list you see two editing modes:
   - **Edit config. values** mode.
   - **Select group parameters** mode.

The configuration dialog opens in the **Edit config. values** mode. In this view, you see only the common parameters which are to be co-managed for the group. You can define the required values and content here. Parameters that apply to individual devices are hidden.



If you have selected an empty group template, the displayed dialog is empty. The first step is to select the group parameters for editing in the mode chosen above.

In the **Select group parameters** mode you can select or de-select all of the parameters that you require for a customized group configuration.



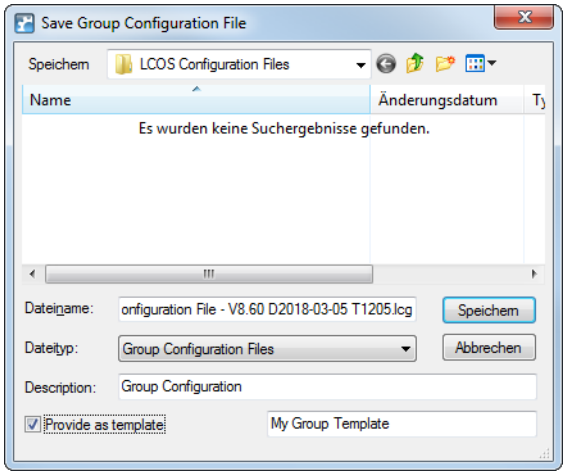
Light-blue colored items are selected for use in the group configuration. Click once with the left mouse button on an item to change its selection status.

Please note the following:

- For tables with statically specified rows (such as interface-related tables and **Logical WLAN settings**) you additionally have the option of transferring individual parameters into the group configuration. In LANconfig you can often recognize these tables in that a pull down menu appears when you click on the corresponding button.
- For tables with dynamically generated rows (such as the **Routing table**, for example) you can only select or de-select the entire table for the group configuration.
- Similarly, it is only possible to select or de-select the entire firewall for the group configuration.

4. Now modify the configuration values according to the explanations given for the previous step, and if necessary add additional groups parameters to the configuration. Then click on **OK**.
5. Enter a descriptive **file name** for the new group configuration and set the path for it to be saved.

You also have the option to include this group configuration into the list of templates for creating further group configurations in future. Enable the option **Provide as template** and give the file a descriptive name.



It is also possible to use an existing group configuration to create a template at a later time. Do this by right-clicking on the group configuration in the appropriate group folder. Then select the context-menu option **Provide as template** and give the file a descriptive name.

6. Click **Save** to conclude.

That's it! The associated configuration file now appears in the device list with the specified name. To customize these names, click on the group configuration with the right-hand mouse button and under **Properties** > **General**, change the text for the **Description.**

The group configuration saves all parameters in a group configuration file, including parameters with preset default values. Use the scripting function to read out only the non-default settings from a device and, if applicable, transfer them to other devices.

Using an existing group configuration file

In some cases it may be useful to use a different structure of devices managed with LANconfig than required by the group configuration. For example, devices in different site-specific folders may belong to the same groups. In order to avoid redundant group configuration files for every folder, you may want to create links to a shared file in multiple folders.

To use an existing group configuration file for a group of devices, use the mouse and right-click on the appropriate folder. In the context menu select **Add group configuration**.

In the subsequent dialog, select the existing group configuration file to create a link to this file in the folder.

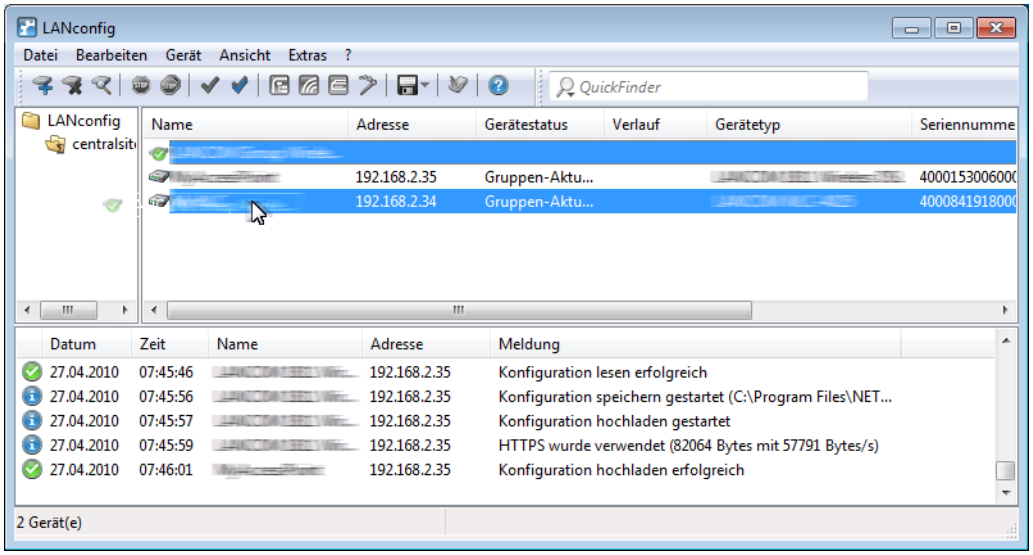
Please note that changes to the group configuration file will lead to changes in that group configuration in various folders.

If you create additional devices in a group folder, or if you modify an existing group configuration, LANconfig informs you that an update to the appropriate devices is available. This update can be carried out either directly afterwards or at any later time by using the context menu.

Updating device configurations with group configurations

By selecting or updating a folder, LANconfig checks the configuration of the devices in this folder for agreement with the settings in the active group configuration. In case of discrepancy from the group configuration, the device status informs that **Group update recommended**.

To load the group configuration into the WLAN device, drag the group configuration entry onto the appropriate device entry. After successfully transferring the parameters, the device status will change to **OK**.



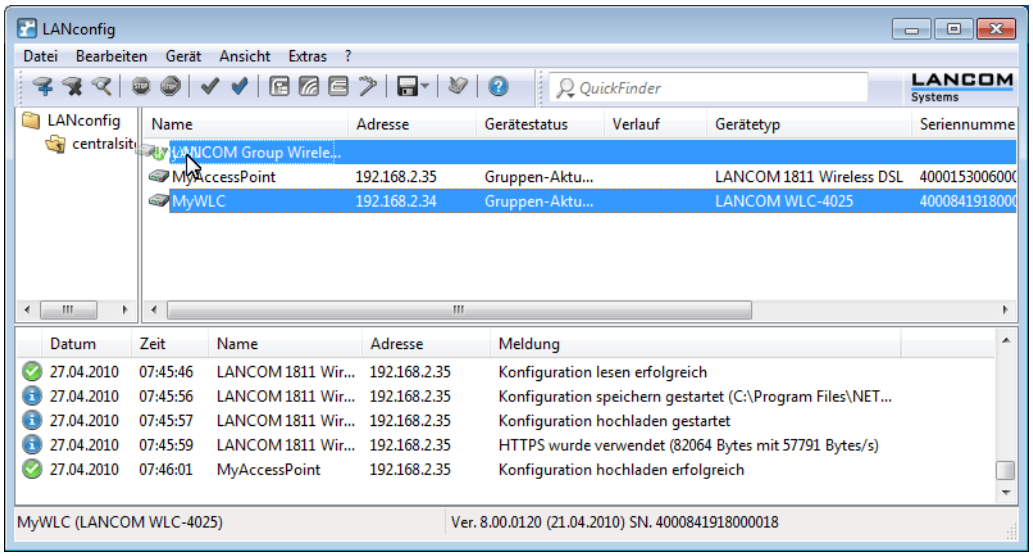
It is also possible to use the partial configuration for a WLAN device as a group configuration. Simply drag the device entry onto the group configuration entry.

Updating group configurations by means of a master device

Apart from manually changing the parameters in a group configuration (see chapter *Updating device configurations with group configurations* on page 190), the current configuration of a device can be used as the basis for a group configuration. One device is thus declared as "Master" for all other devices in the same folder.

To take over the values from a current device configuration for a group configuration, simply drag the entry for this device onto the desired group configuration. All of the parameters defined in the group configuration are then overwritten by the values in the device configuration.

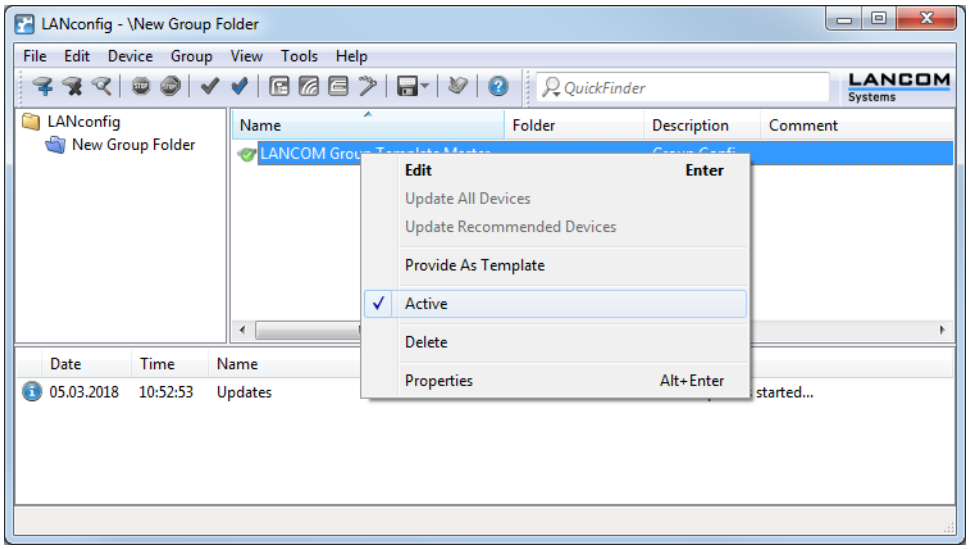
The next time that LANconfig checks the devices, it will find that the configurations in the other devices no longer agree with the new group configuration; this will be indicated by the device status.



Using multiple group configurations

Multiple group configurations can be created within a single folder. Only one of these group configurations may be active at a time since the device status can only relate to one single group configuration. Active group configurations are marked with a blue tick, inactive group configurations with a red cross. To activate a group configuration, click on the entry with the right-hand mouse key and select 'Active' from the context menu. All other group configurations are then deactivated automatically.

Different group configurations in one folder may not be linked to the same partial configuration file.



Transferring device configurations to similar models

When changing to a different device type, it is often necessary to adopt aspects of the configuration of the previous model. To do this, LANconfig enables you to load the configuration file (*.lcf) of a source device onto a similar target device. All of the configuration parameters available on both source and target devices assume the previously used values where possible:

- If the target device has the appropriate parameter, and the value lies within the possible range, the value of the source device is taken.
- If the value of a parameter available on the target device is not supported, the default value is used. Example:
  - The source device has four Ethernet interfaces.
  - The target device only has two Ethernet interfaces.
  - The interface for an IP network is set to LAN-4 on the source device.
  - This value is not supported on the target device. The value is therefore set to default value 'LAN-1' on loading the configuration file.
- All destination-device parameters that were not available on the source device retain their respective values.

Necessary steps

Proceed as follows to transfer the configuration onto a new device:

1. The firmware levels of the source and target devices should be matched as closely as possible. Every new LCOS firmware version features new parameters. Using the same firmware on the two devices allows the greatest possible matching of available parameters.
2. Save the configuration of the source device with LANconfig, e.g. via **Device** > **Configuration Management** > **Save as File**.
3. Disconnect the source device from the network to avoid address conflicts.

4. Upload the configuration onto the target device using **Device** > **Configuration Management** > **Restore from File**. Messages on the conversion of the configuration are displayed in an information window.

Please note that this function is intended primarily for replacement devices and not for the configuration of new devices to be operated in parallel with the source device in the same network. Because key communication settings, such as the IP address of the device and DHCP settings, are transferred to the target device, parallel operation of the source and target devices in one network may result in conflicts. The configuration of several devices in one network is facilitated by group configuration and configuration via scripts.

3.1.2.11 Automatic backup of the device configuration

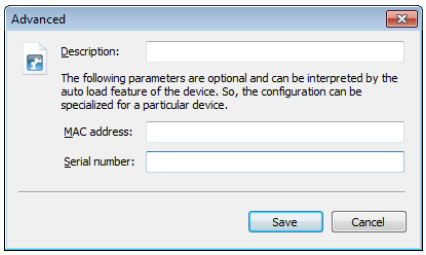
LANconfig can automatically save backups of the current configuration prior to changes in firmware or configuration. Global settings to be used for all of the devices are available under **Tools** > **Options** on the page **Backup** (see *Backup* on page 236).

Additionally, special backup settings can be defined for individual devices. To access them, right-click the appropriate device and select entry **Properties** > **Backup** from the context menu (see *Backup* on page 209).

3.1.2.12 Advanced meta data for configuration files

If a device configuration is stored manually, LANconfig provides the option to save extra meta data in addition to the usual MAC address and/or device serial number in the configuration file (*.lcf). This extended meta-data can be taken into account, for example when performing a quick config rollback or when loading a device configuration via USB.

To include the additional meta data into a configuration file, click the **Advanced** button in the LANconfig save-file dialog and enter the data—if not entered already—into the respective fields.



Alternatively you can open a lcf/lcs file in a text editor and enter the advanced meta data by hand. Add to the line `(<Firmware>) (<Feature-Mask>;<Feature-IDs>;<Hardware-Mask>)` the following text with the brackets `(MAC:<MAC-Address>;SERIAL:<Serialnumber>)`.

Example:

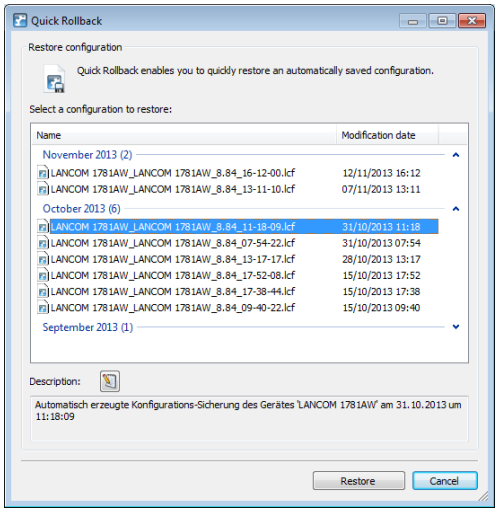
```
(Configuration of 'DEVICE-01' from 8/12/2014)
(9.00.0212) (0x0000c010,IDs:4,e,f,2b;0x0c000002) (MAC:00a0571d12fc;SERIAL:4002578718100036)
```

3.1.2.13 Quick Rollback

As the counterpart to the automatic backup of device configurations, you can restore configuration backups with a single click. Just highlight the device and select **Device** > **Quick rollback**. LANconfig lists all of the device configurations that have been saved under the path for the automatic device-configuration backups. If LANconfig cannot find a backup file for the selected device, it cancels this action with a warning message.

LANconfig allocates the configuration backup to the device by using the serial number stored in the meta data of the backup. As of LCOS8.84 the serial number is automatically written to the backup; for older configuration backups without the serial number, you need to add these manually in order for Quick Rollback to recognize the files. Please also refer to *Advanced meta data for configuration files* on page 193.

To restore a configuration backup, select an entry and click on **Restore**.



You also have the option to add comments to the configuration backups, or edit existing comments: The **Edit description** button ( ) enables you to edit the field below it containing the comment text. Click on **Save description** ( ) to write the text in the comment box back to the backup file.

Quick Rollback is not available for switches.

3.1.2.14 CSV export

You can export the list of devices found on the network and later import them into LANconfig in one go. LANconfig stores the list of managed devices in a CSV file.

To export the data, proceed as follows:

1. Select the menu item **File** > **Export device list**.
2. Set the location to save the file.
3. Enter a file name.
4. Specify the column separator, which separates the various device parameters.
5. Start saving by clicking on **Save.**
6. A dialog confirms the number of data sets stored.
7. Close the dialog by clicking **OK**.

The resulting CSV file contains the following data (one record per line):

```
DEVICE_PATH;DEVICE_INTERFACE;DEVICE_TIMEOUT;DEVICE_ADDRESS;
DEVICE_ADMIN;DEVICE_PASSWORD;DEVICE_SNMPCOMMUNITY;DEVICE_NAME;
DEVICE_STARTUP;DEVICE_PROTOCOLS;DEVICE_PORTS;DEVICE_DESCRIPTION;
DEVICE_COMMENT;DEVICE_LOCATION;DEVICE_TYPE;DEVICE_EXTENDED_NAME;
DEVICE_PRODUCTCODE;DEVICE_SERNO;DEVICE_HWADDR;DEVICE_HWREL;
DEVICE_BACKUP;DEVICE_VPN;DEVICE_SSH_FINGERPRINT;DEVICE_CREDENTIALS
MyGroup;IP;3;192.168.2.101;;;;LANCOM WLC-4025;1;263;;;;;
LANCOM WLC-4025;LANCOM WLC-4025;;4000841918000018;00a0571218bb;C;"31;
C:\Users\MyUser\AppData\Roaming\LANCOM\LANconfig\Config\;
\%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s;12|";;
02:5a:e5:42:ea:d2:da:f0:93:b5:d0:3d:0c:08:70:b8;
```

The first line contains the name of the device parameters. The following lines itemizes the various devices line by line, and their parameters are separated by semicolons. If 2 semicolons appear in direct succession, then the enclosed parameter value is blank.

The variable names in the first row correspond to the following LANconfig entries:

› **DEVICE_PATH**: Path name in the folder view

- **DEVICE_INTERFACE**: Connection type
- **DEVICE_TIMEOUT**: Maximum response time of the device
- **DEVICE_ADDRESS**: IP address or domain name and COM port or telephone number respectively
- **DEVICE_ADMIN**: Administrator name
- **DEVICE_PASSWORD**: Administrator password
- **DEVICE_SNMPCOMMUNITY**: The SNMP community of the device
- **DEVICE_NAME**: Device name
- **DEVICE_STARTUP**: Checking of the device at startup
- **DEVICE_PROTOCOLS**: Communication protocols
- **DEVICE_PORTS**: Ports
- **DEVICE_DESCRIPTION**: Description
- **DEVICE_COMMENT**: Comment
- **DEVICE_LOCATION**: Location of device
- **DEVICE_TYPE**: Device type
- **DEVICE_EXTENDED_NAME**: Device name with any supplements
- **DEVICE_PRODUCTCODE**: Product code
- **DEVICE_SERNO**: Serial number
- **DEVICE_HWADDR**: MAC address
- **DEVICE_HWREL**: Hardware release
- **DEVICE_BACKUP**: Storage location for the configuration backup created by LANconfig
- **DEVICE_VPN**: Parameter set for 1-Click-VPN
- **DEVICE_SSH_FINGERPRINT**: Cached fingerprint of the imported SSH key, also see *Exporting key fingerprints when commissioning CC devices* on page 206
- **DEVICE_CREDENTIALS**: Cached fingerprint of the device's internal ssh-rsa key



Use a text editor or spreadsheet to manage the list of exported devices.



If a device password is stored in LANconfig, the password is saved in cleartext in the CSV file. Remember to delete these access credentials before you pass this file on or save it to a freely accessible server.

3.1.2.15 Importing from a data source (CSV)

In LANconfig you can import a large number of devices from a script file in one go by processing the device files with an Import Wizard. You also have the option of using this device file together with a configuration template file to create a custom configuration file for each device. The template file contains variables for the values in the device file.



The device file is saved in CSV format.

Example application: Importing from a single data source

The scenario which is the subject of the following sections describes how to use a script file and a simple CSV-format device file to generate your own data source for importing data.

Content of the CSV file

The CSV file contains device-related data records, which LANconfig can import. This provides you with a convenient method of managing this data on the network.

The following is an example of a simple CSV file:

```
CONFIG_FILENAME;DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_LOCATION;DEVICE_NAME;KEY;USER
Fil52146.lcs;Filialen/NRW;IP;192.168.1.1;Wuerselen;Fil52146;secret1;user1@internet
Fil80637.lcs;Filialen/BAY;IP;192.168.2.1;Muenchen;Fil80637;secret2;user2@internet
```

The first line contains the name of the device parameters. The following lines itemizes the various devices line by line, and their parameters are separated by semicolons. If 2 semicolons appear in direct succession, then the enclosed parameter value is blank.

The parameter names on the first line can be freely defined. If you decide to use the default variable names, LANconfig automatically allocates the device parameters during the import. Information about the default variables is available in the chapter *CSV export* on page 194.

If you choose not to use the default variable names, you may need to manually assign the values to the appropriate device properties in LANconfig during the import.

Content of the configuration template file

The template file contains Telnet commands that Telnet executes sequentially. This is why this template file is also referred to as a script file.



For an overview of available telnet commands, see the Reference Manual section *Commands for the CLI* on page 51.

A configuration template file can appear as follows:

```
lang English
flash No
set /Setup/Name "$DEVICE_NAME$"
set /Setup/SNMP/Location "$DEVICE_LOCATION$"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type Rtg-tag Comment
add "INTRANET" $DEVICE_ADDRESS$ 255.255.255.0 0 any loose Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username Rights
add "INTERNET" none PAP "$KEY$" 6 5 10 5 2 "$USER$" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

The variables begin and end with a character or a string (here: '$').

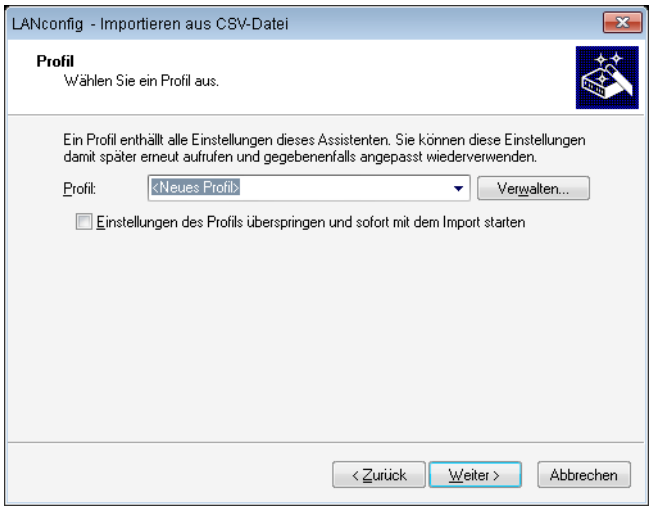
In this template file, the variables represent certain device parameters. During the import process, you associate these variables with the corresponding entries in the device file. The Configuration Wizard then replaces the variables with the associated device data from the CSV file.

Creating the configuration files

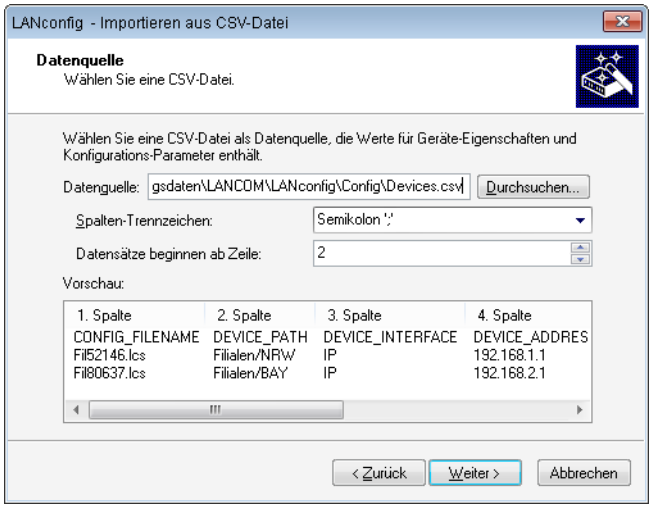
Proceed as follows to create device-specific configuration files:

1. Open the Import Wizard in the menu **File** > **Devices/Configurations from CSV file...**.
2. If necessary, confirm the Welcome dialog with **Next**. The option to **Skip this page on next call** will suppress the appearance of the welcome screen when the Wizard is run in future.

3. If applicable, select the profile used for a previous data import. The option **Skip profile settings and start the import immediately** uses the settings in the selected profile without modification. Select **<New profile>** to use a new profile instead of an existing one. Click on **Next**.

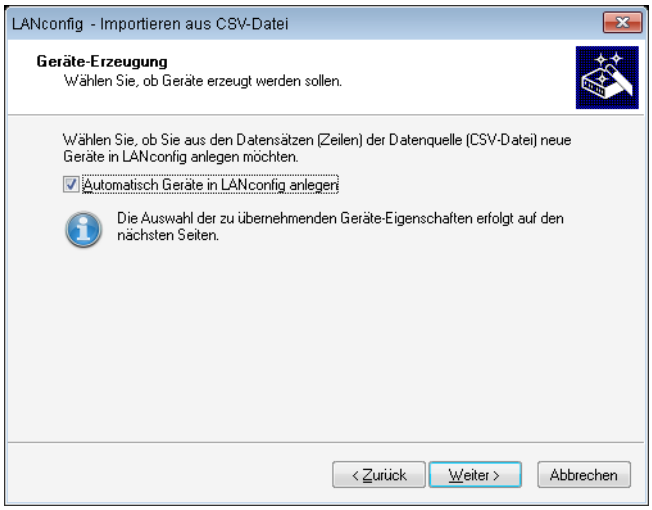


4. In the **Data source** field enter the path to the CSV file. With **Browse ...** you select the file from your local file system.



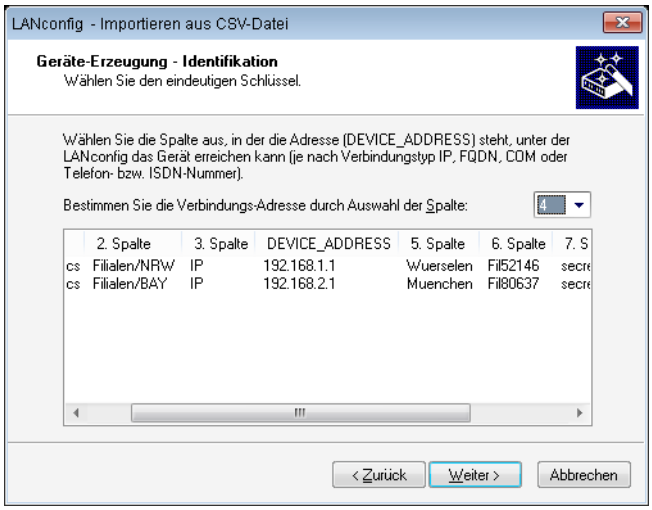
5. You can select the column separator for the CSV file. The default is the semicolon.
6. Set the row number where the data records start. This allows you to avoid importing any existing column headings and additional information. If a line in the CSV file contains only default variable names (see section *Exporting CSV data sets*), then this line is used to assign the variables automatically. This ensures that exporting and importing the same file will function without any manual assignment. However, if a configuration is generated with additional variables, the auto-detect will not function.
7. The **Preview** field instantly shows the parameters you have selected for import. Confirm your entries with **Next**.

8. To use the data records to create new devices in LANconfig, select the option **Automatically create devices in LANconfig.** After clicking **Next**, the following pages are used to select the device properties to be carried over to LANconfig.

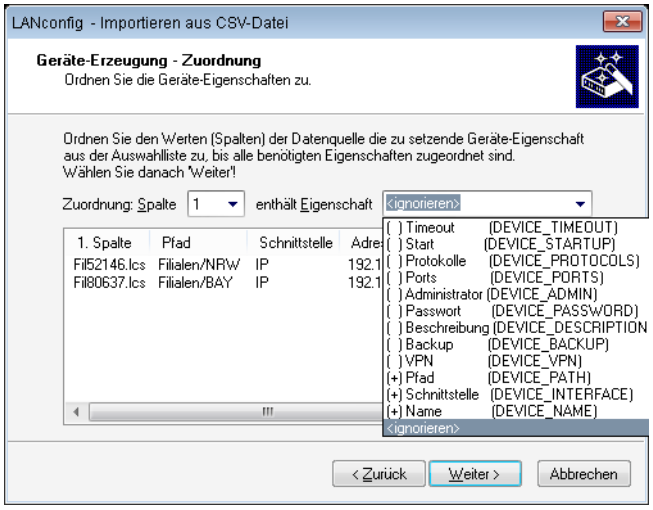


If this option is disabled, the Wizard will skip the subsequent 2 steps.

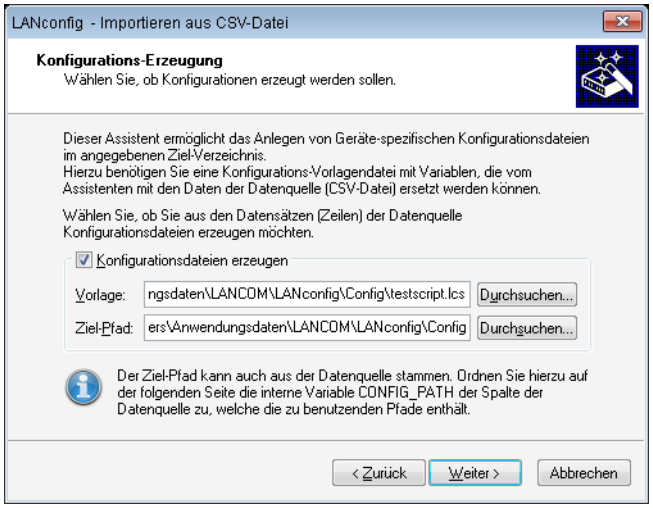
9. The devices are identified using their connection address. Use the drop-down list to select the column in the data set that contains the connection address and click on **Next.** If you use default variable names, assignment takes place automatically.



10. Align the columns according to the relevant device properties. Properties that have been aligned are marked in the list with a preceding "+". Then click on **Next**. If you use default variable names, assignment takes place automatically.

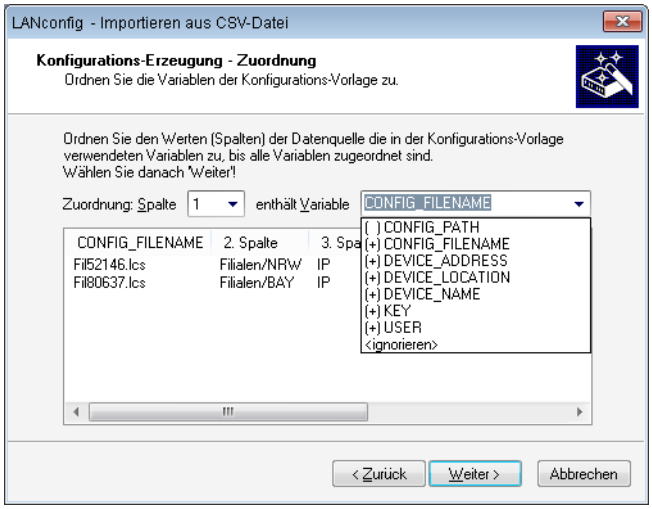


11. You have the option to create individual configuration files from the data sets. Simply activate the option **Generate configuration files**.



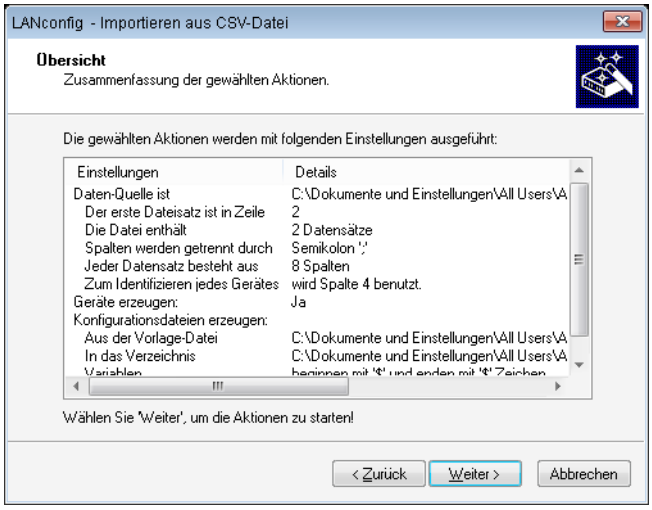
12. Use the **Template** field to set the path to the template file to be used as the basis for these configuration files. By clicking on **Browse** you open the dialog for loading a configuration script template. In the fields **Variable start** and **Variable end** you define which characters (or strings) are to mark the start and end of the variables in the template file. This enables the Wizard to identify the variables in the template file.
13. You specify the storage path in the field **Target path**. This is where LANconfig stores the new configuration files. Click on **Browse** to specify a target path on your local file system. Click on **Next**.
14. Assign the columns in the data source to the variables used in the template file. Do this by selecting the column number from the list of columns and assigning this number to a variable from the properties list. Variables are also assigned automatically if the column headings contain the same variable names as those between the start and end

characters in the script file. The column headings in the view below updates immediately with every change. To continue, click on **Next**.



If your entries are incomplete, the Wizard alerts you about potential import problems and suggests corrections.

15. The summary informs you about the actions that are executed in the next step. If you need to make any changes, click on **Back**. This returns you to the appropriate input mask. By clicking on **Next** you start the data import.



If the data import would overwrite a device that already exists in LANconfig, the Wizard gives you the following options:

- Overwrite the device.
- Create a configuration file, nevertheless.
- Use this decision for all other existing devices.

16. The status dialog that follows indicates the actions performed. Click on **Copy to clipboard** to save the status message to the clipboard. Click on **Next**.
17. Finally, you have the option to save the current import settings to a profile for future actions.
18. Complete the import by clicking on **Finish**.

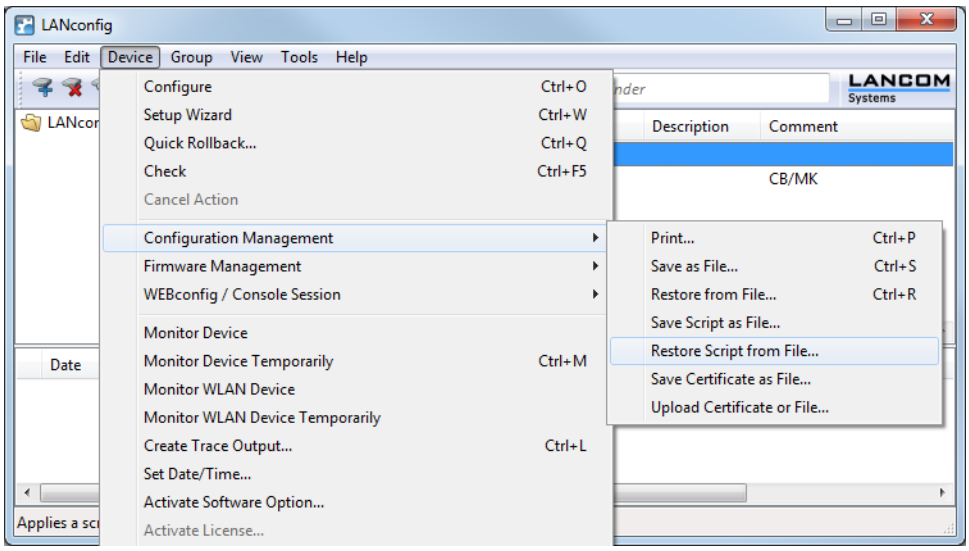
If you have opted to generate a custom configuration file, the Wizard saves a separate configuration file for each device in the specified folder. These configuration files are named according to the file name "<CONFIG_FILENAME>.lcs", which defines the CSV file:

```
lang English
flash No
set /Setup/Name "Fil52146"
set /Setup/SNMP/Location "Wuerselen"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type Rtg-tag Comment
add "INTRANET" 192.168.1.1 255.255.255.0 0 any loose Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username Rights
add "INTERNET" none PAP "secret1" 6 5 10 5 2 "user1@internet" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

The Wizard has replaced all variables with the appropriate device parameters.

This configuration file gives you the option to use LANconfig to transfer the device settings as defined in the template file to other devices. Highlight the appropriate device and click on **Device** > **Configuration management** > **Restore script from script file**.



3.1.2.16 LANCOM Software Update for LANtools

The software update for the LANtools allows you to automatically download new versions of the LANtools and your device firmware.

New versions for the LANtools (LANconfig, LANmonitor and WLANmonitor) are downloaded directly from the freely accessible download section of the LANCOM web server.

Manually starting LANCOM Software Update

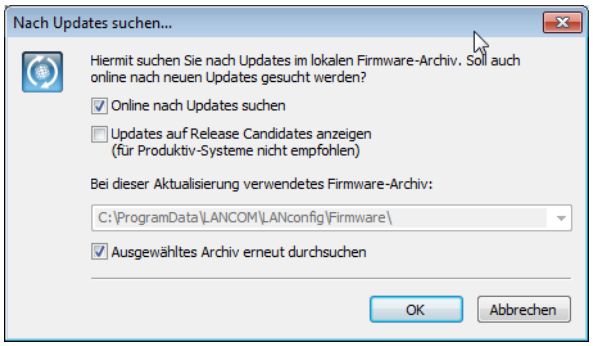
To start the software update manually in LANconfig proceed as follows:

1. Start LANconfig.
2. Click on the **Tools** menu and select **Check for updates...**.

LANconfig searches the local firmware archive for updates. Optionally, you can extend the search with the following items:

- Find more updates online in the download area of the LANCOM web server.
- Include Release Candidates in the search. If you enable this option, the Software Update will not only offer to download the released software versions for use in productive environments, but also any available release candidates.

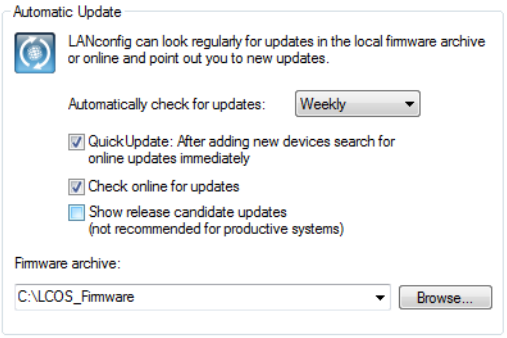
Release candidates include the new features of upcoming software versions and have been thoroughly tested. Until the final release of version, the software may be further optimized—partly due to user feedback.



Settings for the automatic search for new updates

Proceed as follows to start the software update automatically in LANconfig each time the application starts:

1. Start LANconfig.
2. Click on the **Tools** menu and select **Options**.
3. Go to the **Update** page.



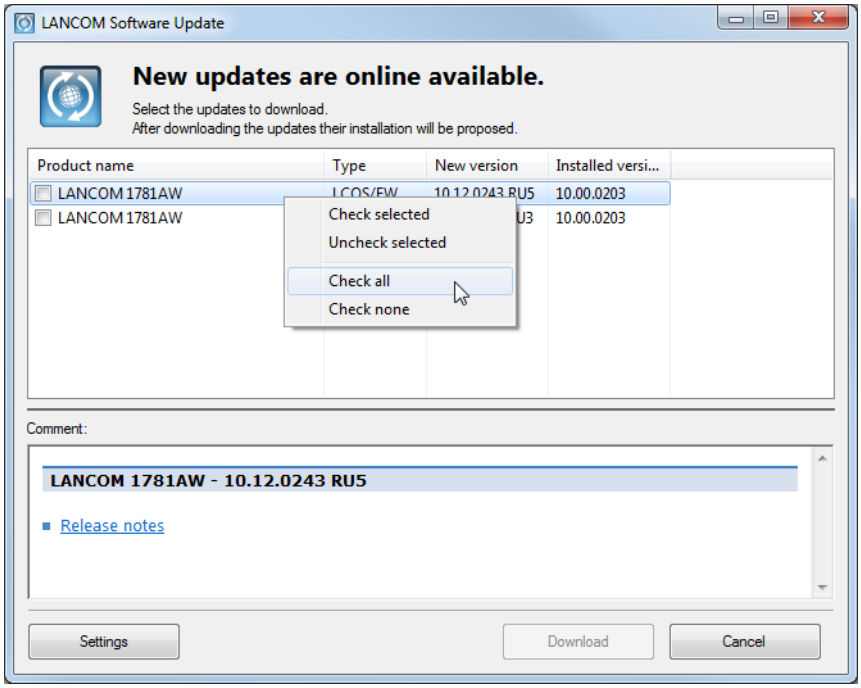
4. Select the time interval for the automatic check for updates (**Daily**, **Weekly** or **Monthly**).

For the remaining settings for software updates, refer to the chapter *Update* on page 239.

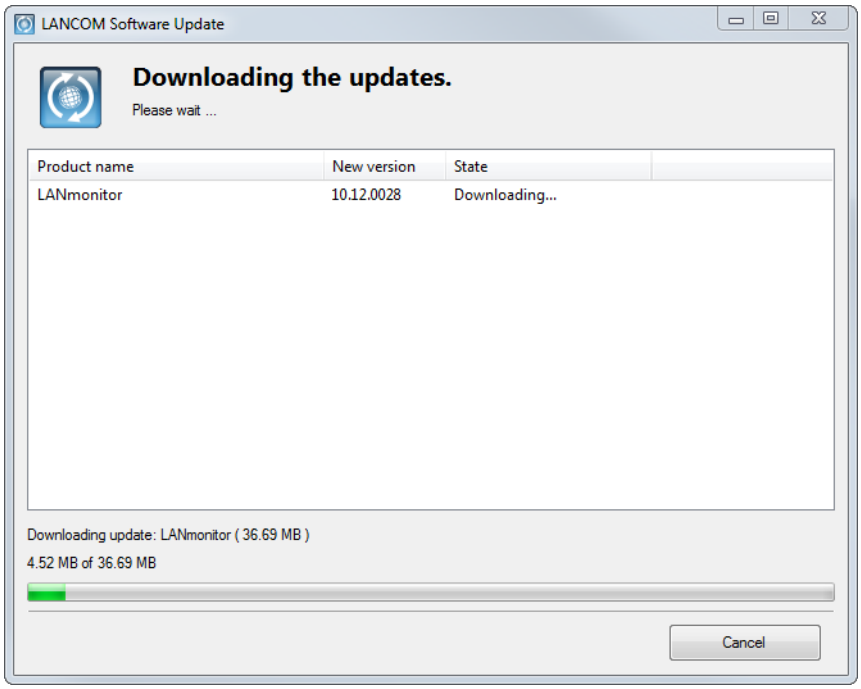
Selecting and installing the available updates

After successful connection to the update server, LANconfig displays the available updates.

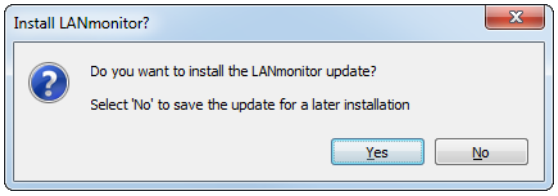
Select the appropriate versions and click **Download**. As an alternative, you can click on the entries with the right-hand mouse key and select the entry **Select all** or **Select none** from the context menu.



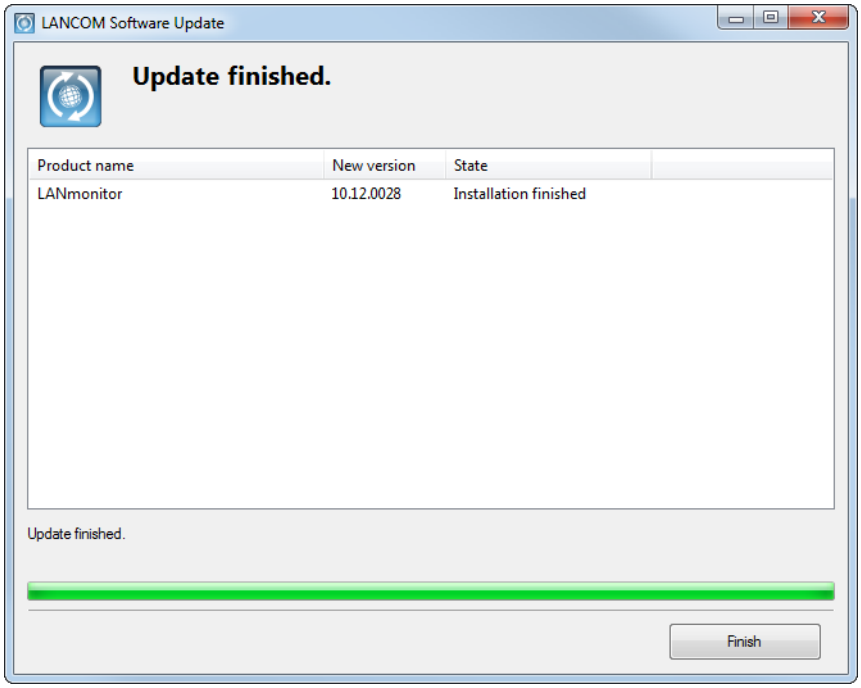
Software Update now downloads the selected software one after other and stores the files in the firmware archive.



After successfully downloading the software, Software Update offers to install the downloaded software (LANconfig and LANmonitor only):



After installation, the Software Update displays the results of the update procedure:

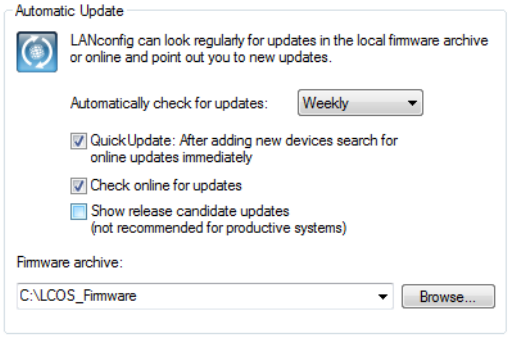


3.1.2.17 Searching for firmware updates in the archive

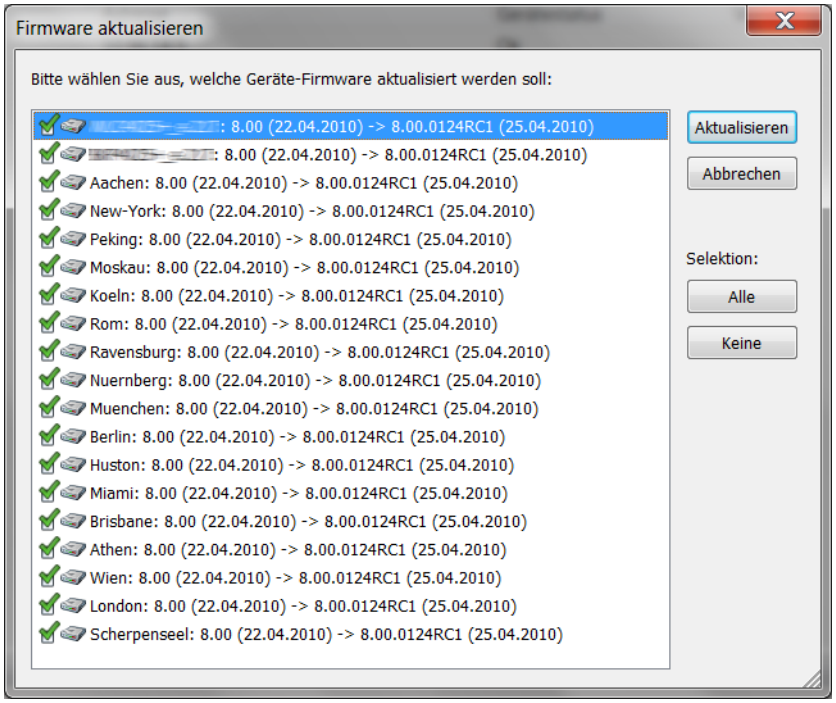
To make the update of devices with new firmware as convenient as possible, the firmware files for the various models and LCOS versions are, ideally, saved to a central archive directory. The search for new firmware versions in this directory can either be initiated manually or automatically after starting LANconfig.

Automatic search for firmware updates

The directory where LANconfig looks for updates is configured under **Tools** > **Options** > **Update** > **Firmware archive**.

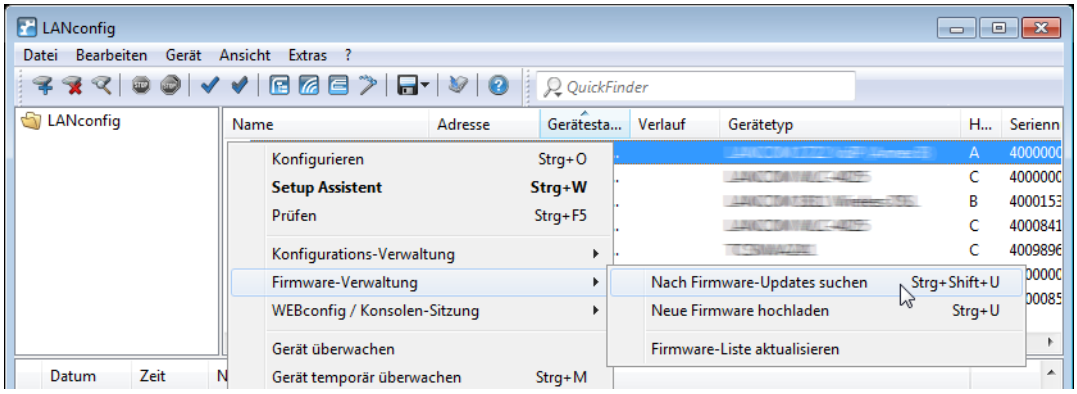


If you set an interval for the automatic search, starting LANconfig automatically displays all of the devices for which new updates are available.



Manual search for firmware updates

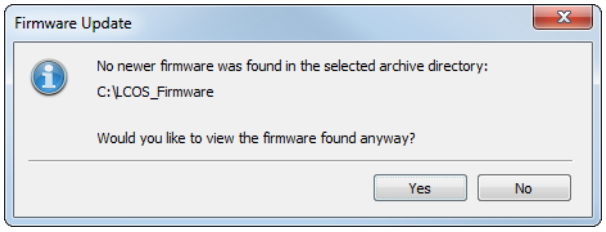
To seach manually for firmware updates, click with the right-hand mouse key on a device marked in the list and select the following point from the context menu: **Firmware management** > **Check for firmware updates**. If you highlight several devices, the item **Check for firmware updates** is displayed directly in the context menu.

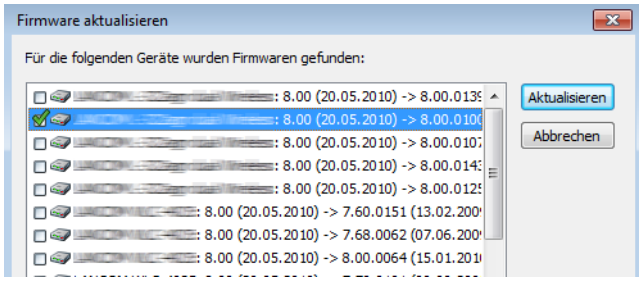


View a full list of all firmware versions

If your search in the archive did not reveal a new firmware version, you can alternatively view a full list of all of the firmware files that have been found. You can, for example, switch back to an older version. LANconfig displays all versions

found for the marked devices, including the version currently active in each device. For each device, you can select precisely one firmware version that will then be uploaded onto the device.





3.1.2.18 Exporting key fingerprints when commissioning CC devices

As of LCOS8.84, LANconfig offers a convenient way to export the SSH key fingerprints when you commission CC devices. While running the CC Start-up Wizard, LANconfig creates the file **CCWizSummary.csv**, which contains the IP address of the device, the device name, and its (SSH) key fingerprint. This generates a list which is useful, for example, for a system administrator who needs to be certain of connecting to the correct device when conducting remote maintenance or when logging in after a rollout.

By default, LANconfig saves the CSV file under `C:\Program Files (x86)\LANCOM\LANconfig\Logging\`.

You have also the option to change this path in the input field under **Tools** > **Start CC Start-up Wizard** > **Settings** > **Path**.

3.1.3 LANconfig menu structure

Using the menu bar, you can manage devices and their configurations, and you can customize the appearance and functioning of LANconfig.

3.1.3.1 File

This menu item is used to manage devices in general, and to exit LANconfig if required.

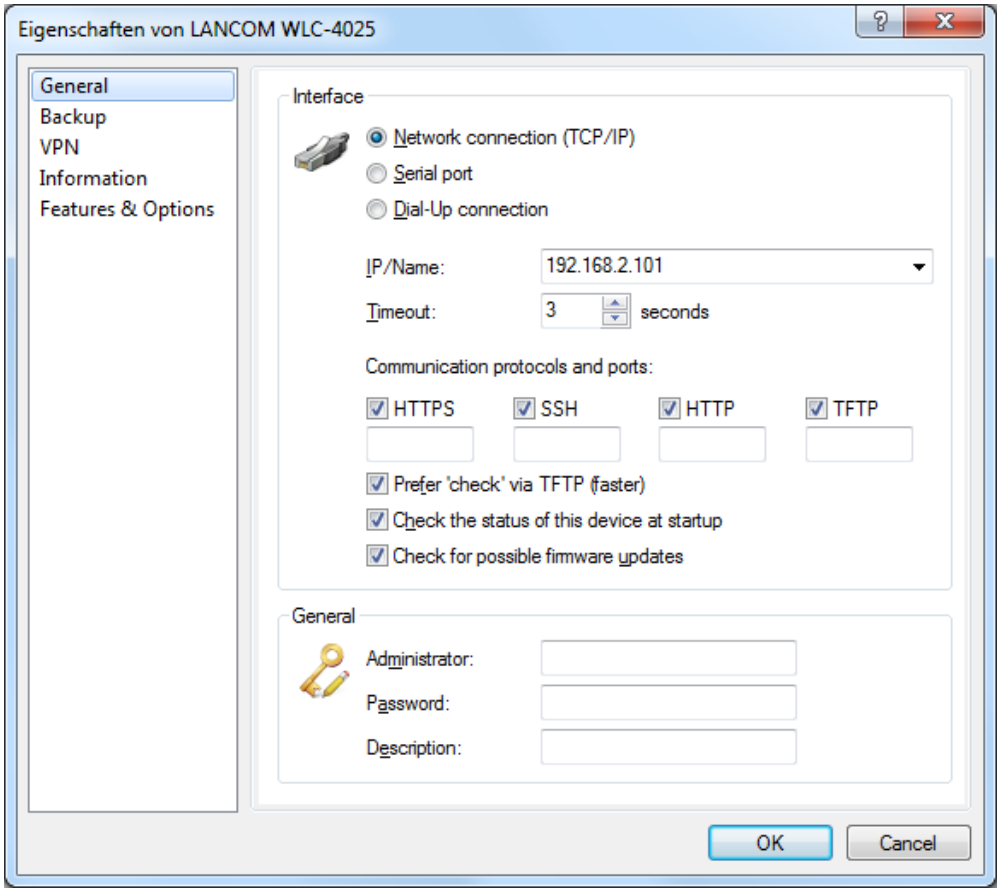
Add device

A new device is added under **File** > **Add device**. It opens a dialog where you can make the settings for the connection to the device and for the backup.

General

On this page, you can define how LANconfig connects to a device. It is also possible to permanently store the access credentials in the program, saving you from having to manually enter them when you connect to the device for the first time after restarting LANconfig.

If you save the username and password permanently, any user who is permitted to run LANmonitor also has access to the device.



Interface

In the **Interface** section you can configure the connection settings for a device.

Please select how the device is to be reached:

- **Network connection (TCP/IP)**: Select this option if the device can be reached over an IP network.
- **Serial port**: Select this option if the device is connected directly via your computer's serial port.
- **Dial-up connection**: Select this option if the device can be reached via Dial-Up Networking.

  Please note that some devices do not support remote configuration via a dial-up connection.

- **IP/Name**: Enter the IP address of the device. You can also enter a domain name (DN or FQDN). This name is checked at every access. LANconfig stores and uses the resolved IP address. If this check is not possible, then LANconfig takes the last IP address that was last used successfully.
- **Timeout**: Here you enter how many seconds the program should wait for a response from this device.
- **HTTPS**, **SSH**, **HTTP**, **TFTP**: When this is selected, you enable the individual protocols for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, SSH, HTTP and TFTP. If the transfer fails when using one of the selected protocols, LANconfig automatically tries the next protocol.
- **Prefer 'check' via TFTP**: This option causes LANconfig to perform checks with TFTP, irrespective of other protocols that are selected. This is advantageous for devices located in the LAN. The checks are faster and place less load on the computer, which makes an appreciable difference when processing a large number of devices. The fact that HTTPS is not used should not be a problem in the LAN.

- **Check the status of this device at startup**: Check this box if LANconfig should check the status of the device every time it is started.
- **Check for possible firmware updates**: Select this option if LANconfig should check for possible firmware updates.

As described in the section *Communication protocols and ports* on page 208, LANconfig tests other protocols and executes them if TFTP is not available. Here, too, global settings take priority over the device-specific settings.

After you have made the settings, the program tries to access the device and retrieve its name and version. If this fails, LANconfig shows a short error message in the **Device status** column.

General

In this section you can enter a description of the device.

- **Administrator**: Enter the username for an administrator.
- **Password** Enter the associated password here.
- **Description**: Enter the description of the device that you want LANconfig to display in the main window.

Communication protocols and ports

LANconfig uses the communication protocols selected here to check the availability of the device, and to execute firmware uploads as well as the uploading and downloading of scripts/configurations.

LANconfig attempts to carry out the device actions outlined above in the order HTTPS, SSH, HTTP, and TFTP. If an action fails because of the protocol, then LANconfig repeats them with the next selected protocol.

At least one protocol must be selected in order for the action to function.

When using HTTP(S) and a proxy server, it may be necessary to circumvent this proxy server so that LANconfig can reach the device. You can bypass the proxy server for local addresses by using a setting in the Window's Control Panel, Internet options. In the Internet options' advanced settings, you can also define further addresses which should not be contacted via the proxy server.

Protocols can be set globally or by means of device-specific settings. The global settings in the options menu take priority over the device-specific settings. A benefit of this is that a single global switch can be used to disable a protocol for all devices.

Tips

- When shipped, the device does not yet have an IP address. In this case, enter the IP address of your computer and replace the last part of the number sequence by 254: If your computer's IP address is 192.168.1.1, then assign the IP address 192.168.1.254 to the device.
- Also, if you do not know the device's IP address, you additionally have the option of searching for it with **File** > **Devices**.

Potential problems when connecting with a new device

If LANconfig cannot reach a device at all, then one of the following error messages is displayed under status. To check a device again, mark it in the list and click on **Device** > **Check** in the menu bar.

- **Serial error**: LANconfig could not open the serial interface. Close any program that may be accessing the port.
- **IP error**: Check that the IP address of the device is correct and that your computer is properly connected to the network. You can also check that the TCP/IP protocol is installed properly and correctly configured.
- **No response**: Check if the IP address of the device is correct. Another possibility is that the network connection between your computer and the device is too slow or unreliable.
- **Status unknown**: LANconfig reached the device via the specified IP address, but was unable to request any additional information. LANconfig may not support this device.

- **Access denied:** Access to this device from your computer is blocked.

Backup

On this page you enable and configure the device-specific backup settings. The setting options are identical to the global settings (see *Backup* on page 236).

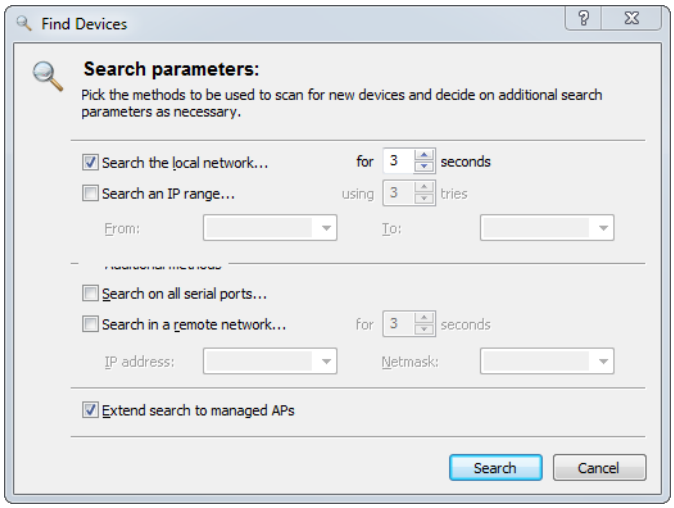
Delete device

You can delete a device that has been marked under **File** > **Delete device**. You can also use the 'Del' key to delete a device.

Deleting a device only removes it from the current view. You can add it to the display again using **File** > **Add device** or **File** > **Find devices**.

Find devices

This menu item triggers an automatic search for new devices for adding to the device view section.



Select where you wish to search for devices:

- Search on all serial ports
- Search in the local network
- Search in a remote network

  If you wish to search in a remote network you must specify its address and the relevant network mask.

- If necessary, you can extend the search to managed access points (APs).

Click on **Search** to start the search. Any devices found will be added to the list automatically.

If a device is found that is already in the list, it will not be included in the list a second time. For this reason fewer devices may be added to the list than were reported during the search operation.

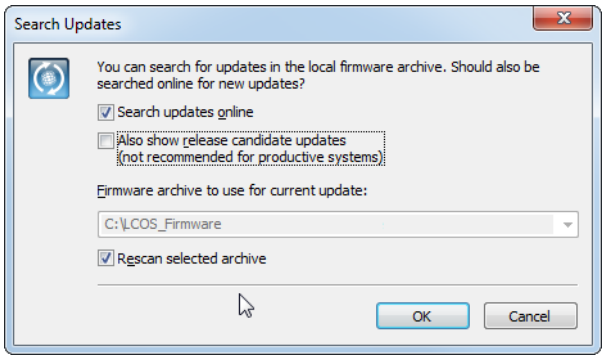
Check devices in this view

You can check the status of all devices under **File** > **Check devices in this view**. The device status indicates, for example, that new firmware is being uploaded or that a device cannot be reached.

A device can only be configured if the status of the device is **OK**.

Check all devices for firmware updates

Manually starts the automatic search for firmware updates. Here, the online LANCOM database and your local firmware archives are searched for firmware versions that are more recent than those currently installed on the devices. Also see the chapter *Searching for firmware updates in the archive* on page 204.



Cancel all actions

Use this menu item to cancel all ongoing actions for all devices shown in the view. You can use this function to cancel the upload of a script or firmware, for example. This function is particularly suited to canceling processes that were initiated through multiple selection or the execution of actions.

Devices/configurations from CSV file

In LANconfig you can import a large number of devices from a script file in one go by processing the device files with an Import Wizard. You also have the option of using this device file together with a configuration template file to create a custom configuration file for each device. The template file contains variables for the values in the device file.

Please refer to section *Importing from a data source (CSV)* on page 195 for further information.

Export device list

You can export the list of devices found on the network and later import them into LANconfig in one go. LANconfig stores the list of managed devices as a CSV file.

Please refer to section *Importing from a data source (CSV)* on page 195 for further information.

New folder

This menu item creates a new folder in the directory tree. Also see *Using directory trees to get organized* on page 177.

Exit

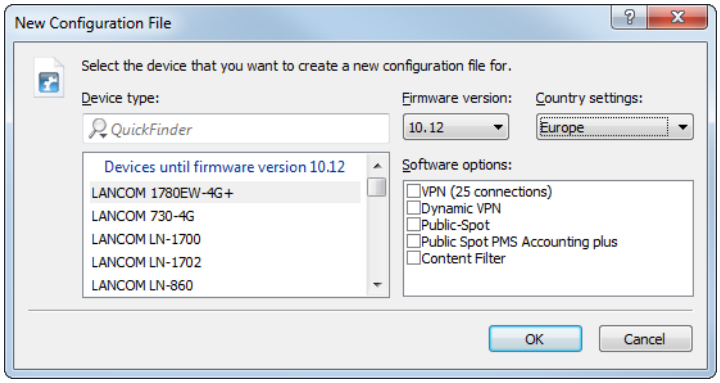
This menu item terminates and closes LANconfig.

3.1.3.2 Edit

This menu item allows you to organize the configuration files for all of the devices in a device list.

New configuration file

This function allows a configuration and a device entry to be created without a connection to an actual device.



Device type

If you wish to create a configuration file you must specify the type of device this configuration is intended for so that the program can display the correct parameters for it. Choose the desired device from the list.

Use the QuickFinder to filter the list of available devices. Simply enter a part of the name of the required device type into the QuickFinder field and the dialog automatically reduces the selection to the appropriate devices.

Firmware-Version

Since different firmware versions often provide options that differ from each other, the program needs to know the version that this configuration is intended for. Please specify the firmware version number in the desired device. The program will inform you if the version number is incorrect or not supported.

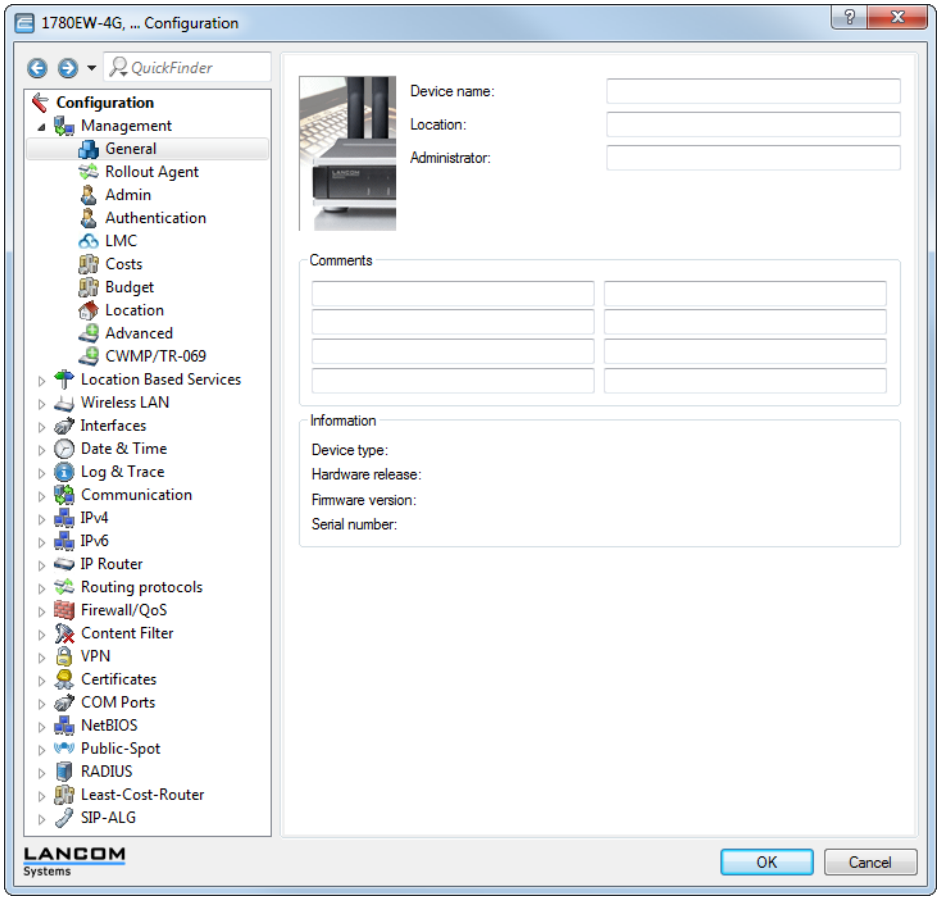
Country setting

Choose the country/region where the configuration file is to apply. In this case the configuration file only offers those parameters, which are permitted in the selected country or region.

Software options

Choose the relevant software option that should be displayed.

Clicking on **OK** opens the configuration dialog.

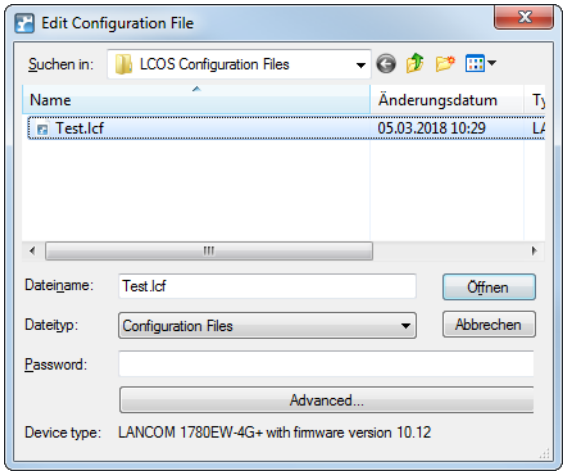


You can also create a new configuration file by right-clicking on your desktop to open the context menu and clicking on **New** > **LANconfig configuration**.

You will find information on the individual configuration parameters in the LCOS documentation.

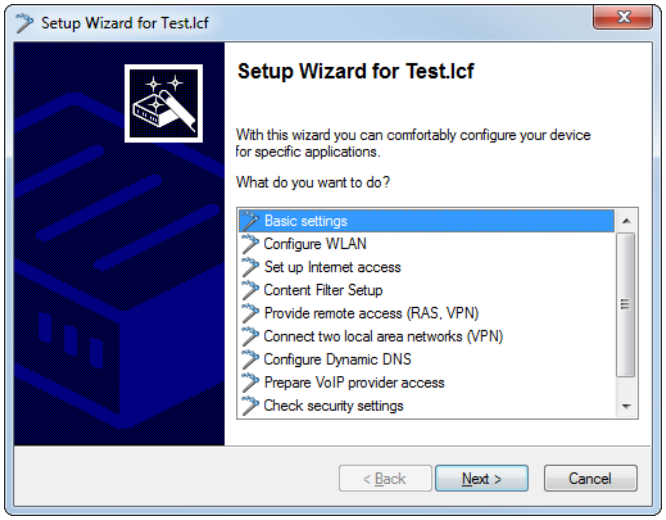
Edit configuration file

This menu item is used to open a stored configuration file for editing in the configuration dialog.



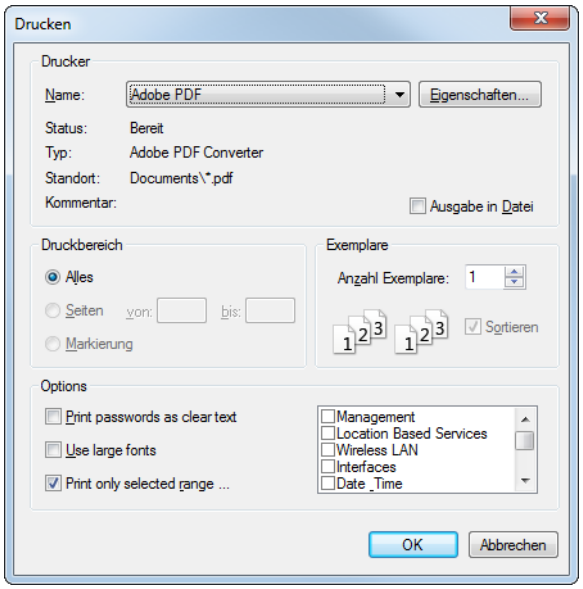
Wizard configuration file

This menu item is used to open a stored configuration file for modification in the Setup Wizard.



Print configuration file

This menu option allows you to print out a stored configuration file.



The normal print dialog features an additional **Options** section, with options as follows:

Print passwords as cleartext

Activating this option will print your passwords in cleartext. The main device password is printed on the first page.

Use large fonts

A large font will be used for printing.

Print only selected range

Only specific areas of the configuration are printed, e.g. only WLAN controllers.

Select all devices in this view

This menu item allows you to highlight all of the devices in the current view.

Invert selection

This menu item inverts the current selection of highlighted devices. The result is that all entries that were previously marked become unmarked, and all entries that were previously unmarked become marked.

3.1.3.3 Device

Under this menu item you can edit the configurations of devices connected to the network, organize firmware updates and monitor device connections.

These functions are only offered for selection if at least one device has been chosen from the list of devices. The menu can also be called by clicking on a device with the right mouse button when it is marked.

Configure

Loads the configuration of the selected device using the connection settings as defined in the properties, assuming that a connection can be established in this way. The configuration is then displayed in the configuration-settings window, and changes can be made.

Setup Wizard

Loads the configuration of the selected device using the connection settings as defined in the properties, assuming that a connection can be established in this way. The configuration is opened in the Setup Wizard, and this supports you with the configuration of various application scenarios.

With WLCs equipped with the "WLC High Availability Clustering XL option" you are able to select all of the listed WLCs and configure them all in one go using the WLC Clustering Wizard (see *1-Click WLC High Availability Clustering Wizard*).

Quick Rollback

This menu item provides the option to restore automatically created configuration backups for the selected device with just one click. This returns the device to a previous configuration state. Learn more about this feature under *Quick Rollback* on page 193.

Check

Checks the devices or the selected devices by reading out device information via the chosen connection. The status is generated on the basis of this operation. The device status indicates, for example, that new firmware is being uploaded or that a device cannot be reached.

A device can only be configured if the status of the device is **OK**.

Cancel action

This menu item cancels any action running on the selected device. You can use this function to cancel the upload of a script or firmware, for example. However, actions for other devices that have not yet completed will continue to run.

Configuration management

The functions provided by configuration management enable you, among other things, to backup and restore configurations and to transfer a configuration from one device to another. If the firmware versions of the two devices are different the program will display the difference in the configurations, warning you that parameters will be lost. This menu item is also used for file management, as used to upload special files such as templates or certificates directly into the device.

The following configuration-specific actions are available:

Print

Loads the configuration of the selected device using the connection settings as defined in the properties, assuming that a connection can be established in this way. In the subsequent print dialog you can select the same output options as you can under **Edit** > **Print configuration file**. The configuration is printed out after confirmation.

Save as file

Saves the configuration of the chosen device as a configuration file to a location that you select. Enter a name for the configuration file in the file selection dialog. Then click on **Save**.

Restore from file

Loads a configuration file into the specified device (e.g. from an automatic backup). In the file-selection dialog, select the configuration file that you wish to upload, and click on **OK**.

Save script as file

Saves the configuration of the chosen device as a script file to a location that you select. When doing this you can select the same options as you can when saving a file.

Restore script from file

Loads a script file into the specified device (e.g. from an automatic backup).

Save certificate as file

In the file dialog that opens, you specify which certificate should be saved to a file from the chosen device. The file type depends on the certificate selected.

Upload certificate or file

This menu item is used to upload certificates and special files to the device. Certificates are required, for example, when using VPN encryption or for operating a WLAN controller. Special files, on the other hand, are files with which you can replace device-specific templates (e.g. custom templates for the Rollout Wizard) or which are required for certain features by the device (e.g. the Terms and Conditions for the Public Spot module).



You can enter a description for any configuration that you save. This is a convenient way of maintaining various configurations for different devices.

Firmware management

This menu item is used to update the device firmware or switch the device to a different firmware version. The following firmware-specific actions are available:

Check for firmware updates

Manually starts the automatic search for firmware updates. Here, the online LANCOM database and your local firmware archives are searched for firmware versions that are more recent than those currently installed on the selected device. Also see the chapter *Searching for firmware updates in the archive* on page 204.

Upload new firmware

Opens a file selection dialog with which you can upload a specific firmware file to the selected device.



The firmware already on a device is overwritten when the new firmware is uploaded. For this reason, the upload should not be interrupted under any circumstances as the device may no longer function properly.

Activate firmware running in test mode ([memory space number])

If you have performed a firmware update for a device and this is running in the (time-limited) test mode, you can use this menu item to permanently activate this firmware. Learn more about this in section *FirmSafe* on page 93.

1, 2 [firmware version] of [date]

Devices with FirmSafe are able to manage two firmware versions. This allows the system to return to the previous firmware in the event of a failed update or in case of problems, for example. The memory space numbers 1 and 2 enable you to select another firmware version and restart the device.

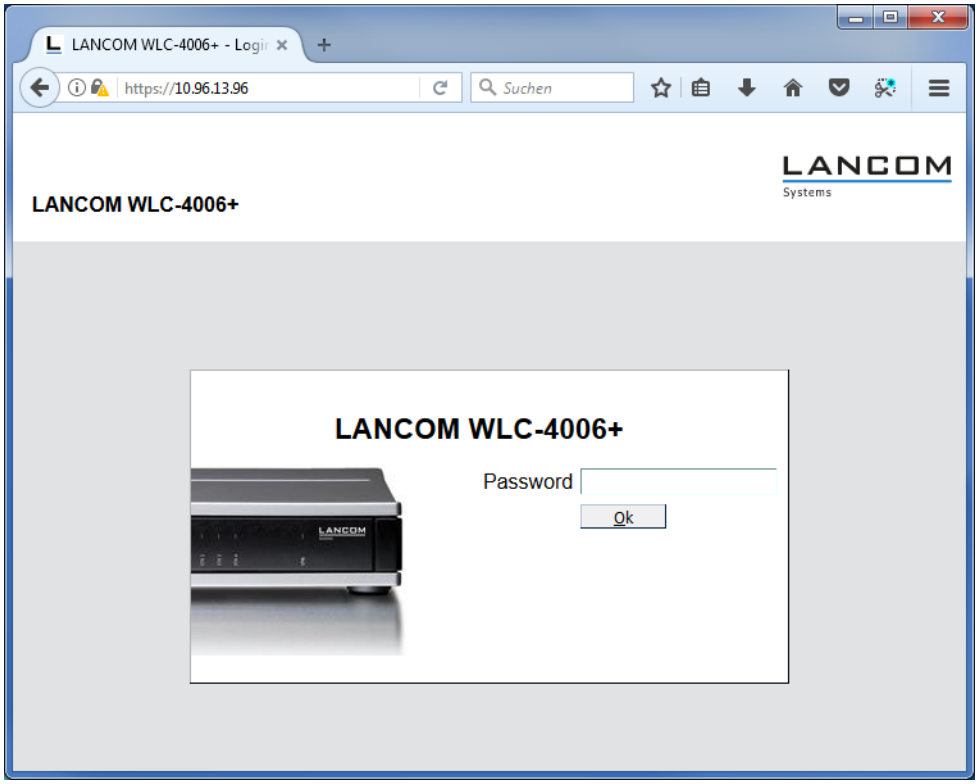
Note that switching the firmware terminates any existing connections and deletes all statistics and charging information.

WEBconfig / console session

This menu item allows you to open a new configuration session by means of an alternative configuration path. The following configuration paths are available:

Start the web browser

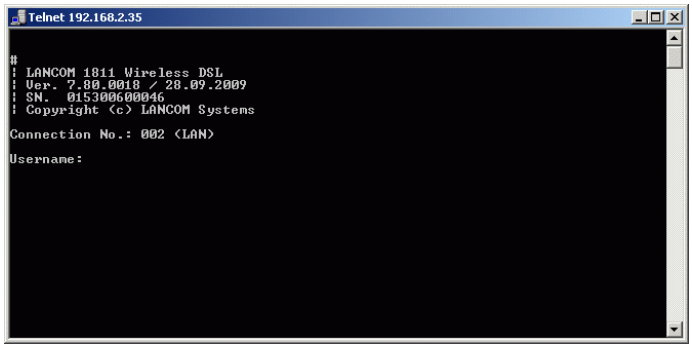
Opens the WEBconfig user interface for the highlighted device.



Under **Tools** > **Options** > **Extras** > **Browser used to display WEBconfig**, you choose whether LANconfig should use the system default browser or its own internal browser.

Open Telnet session

Opens a connection to the device with the Telnet client that is configured in the settings.



Open SSH session

Opens a connection to the device with the SSH client that is configured in the settings.

Monitor device

This menu item enables the basic monitoring of the device in LANmonitor.

The device is then added to LANmonitor's list of monitored devices, and will remain in the list even after exiting and starting LANmonitor.

Monitor device temporarily

This menu item enables the temporary monitoring of the device in LANmonitor.

Information for the device is contained in a separate window from LANmonitor. The setting is not stored, meaning that LANmonitor will not automatically display the device the next time that the program is started. Please also refer to *LANmonitor – monitoring devices on the LAN* on page 247.

Monitor WLAN device

This menu item enables the monitoring of a WLAN device in WLANmonitor. Please also refer to *WLANmonitor – monitoring wireless devices* on page 273

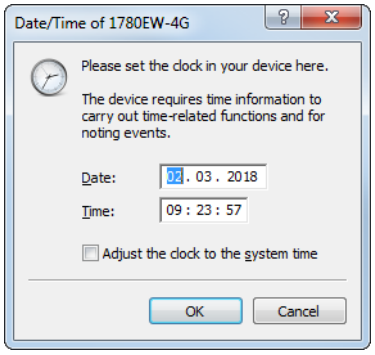
Create trace output

This option starts the trace output in LANtracer.

Please also refer to *LANtracer – tracing with LANconfig and LANmonitor* on page 289.

Set date/time

This menu item is used to set the date and the time for the device. This action is vital for a number of functions (e.g. accounting) and steps in the Setup Wizard (e.g. setting up a Public Spot).



If you check the option **Adjust the clock to the system time**, the time is taken from your computer's operating system.

Activate software option

If you have purchased additional software options, you activate these under **Device** > **Activate software options** by entering the activation key.

You can test an option on any device by activating a demo license that is valid for 30 days. To do so click on the link below the license key input fields. You will automatically be connected to the website for the LANCOM registration server. Simply select the required demo license and you can register your device.

Previously activated options are displayed in the dialog **Device** > **Properties** > **Features & options**. Please also refer to *Features & options* on page 222.

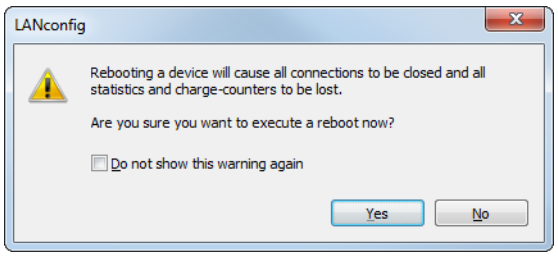
Check CC compliance

This menu item starts a test of whether the configuration of the selected device is CC compliant.

This action is useful only for CC devices. With non-CC devices, this action produces an error message.

Reboot

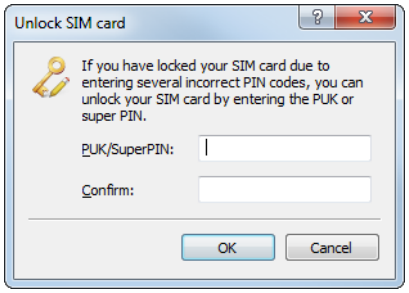
This menu item reboots the device.



After restarting the credentials for the admin account are requested, assuming that these where not already stored on the device.

Unlocking the SIM card

Your SIM card will be locked if you enter an incorrect PIN three times. You can unlock your SIM card again by entering the PUK or super PIN under this menu item.



Applies only to devices with WWAN.

Properties

This menu item opens the Properties dialog for the selected device. A number of pages here allow you to inspect or adjust various device-specific settings.

General

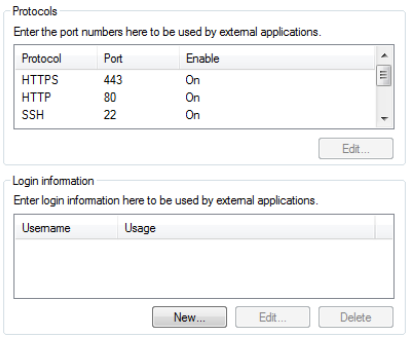
On this page you can adjust the device-specific connection settings. The corresponding setting options are identical to those under **File** > **Add device** > **General** (see *General* on page 206).

Protocols & logins

On this page, you can configure and manage the protocols, ports, and access credentials used by the other components of the LANtools when they call programs from within LANconfig. Configurable programs include:

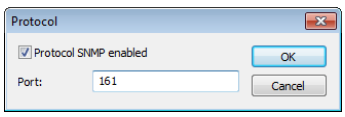
- LANmonitor
- LANtracer
- LANtools-internal and also external Web browsers

If program is invoked with certain protocols already deactivated or configured differently, for example, only the matches are applied.



Protocols

Select a Protocol and click **Edit** to enable/disable the selected protocol for use in external programs, and to change the default port if necessary.



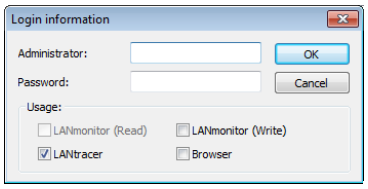
Login information

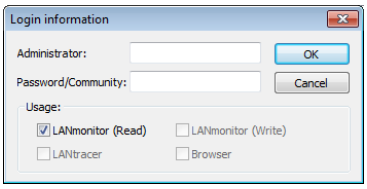
Enter the access credentials for the external programs in this field. Click **New** to select one or more application(s) and enter the corresponding access credentials. Depending on your selection, the dialog window requests different access credentials. If you invoke the program from LANconfig, you have the option of authenticating yourself with the username and password of your administrator login.

In the case of LANmonitor, you have the option to specify an individual SNMP community for read-only access. By default, when LANconfig opens a device configuration it checks whether and to what extent you have stored access credentials for external programs. If you do not have access credentials or if these credentials have been configured in the form of an SNMP community only, then invoking LANmonitor prompts LANconfig to take the SNMP community from the loaded device configuration. If you edit a configuration in LANconfig and you have set an SNMP community here, LANconfig automatically saves the SNMP community for the corresponding device. This convenient behavior reduces the scope of authentication for LANmonitor, so no separate configuration of the read-only access is required.

LANconfig evaluates the setup parameter *2.9.15 Read-Only-Community* for the convenient behavior described above. Any additional read-only SNMP communities configured in the device are ignored.

For more information about the SNMP access through single or multiple SNMP communities, see the section *Configuring SNMP read-only access* on page 116.





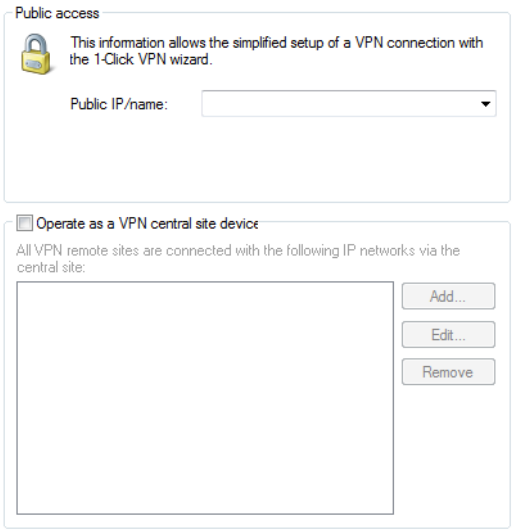
Backup

On this page you enable and configure the device-specific backup settings. The setting options are identical to the global settings (see *Backup* on page 236).

VPN

This page contains the settings for VPN access.

This dialog page is only displayed if the device supports VPN.



Public access

An easy way to set up VPN connections is to enter a public IP number or a name and telephone number here. You can decide whether the telephone number is to be used as the preferred way of establishing a VPN connection.

A telephone number can only be used if both devices are connected to the public telephone network and both have their own unique telephone number (MSN). Devices can simultaneously be configured to connect via IP number or telephone number. Connecting via telephone number is the more reliable method, but this is not always possible and the connection may be subject to a charge.

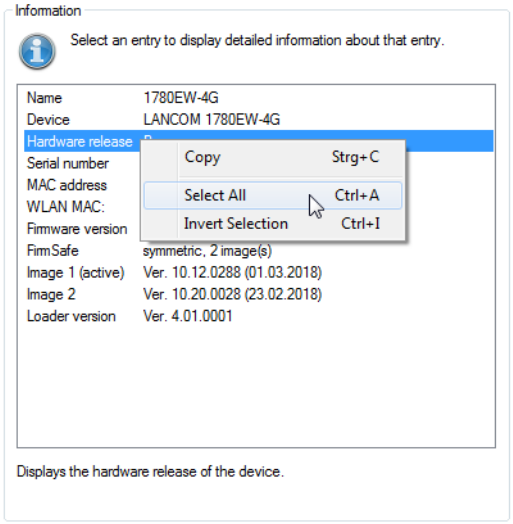
Use as VPN central-site device:

Here you set the IP networks that the VPN remotes are to connect to.

Information

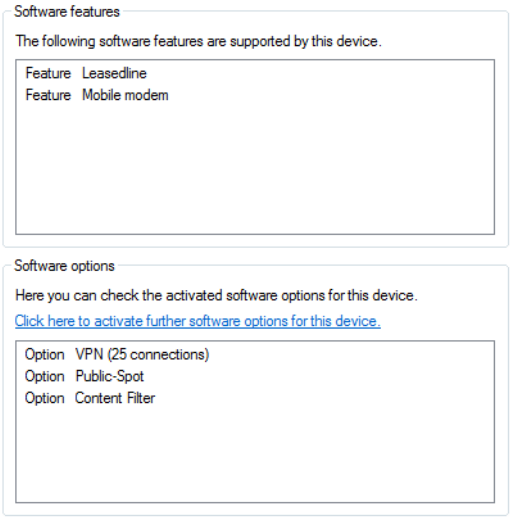
This page provides hardware- and system-specific information about the device.

By using the mouse to right-click on the name of the entry in the left-hand column, a context menu will be displayed. You can use this to copy the values into the Windows clipboard.



Features & options

This page contains details about the features supported by the device and options activated on it.



3.1.3.4 Group

This menu item is used to manage the Group configurations.

Please refer to section *Flexible group configuration with LANconfig* on page 185 for further information.

New group configuration

Under **Group** > **New group configuration** you create a new group configuration in the current folder.

For further information please refer to section *Flexible group configuration with LANconfig*.

New folder with group configuration

Under **Group** > **New folder with group configuration** you create a new sub-folder with a new group configuration in the current folder.

For further information please refer to section *Flexible group configuration with LANconfig*.

Add group configuration

Under **Group** > **Add group configuration** you can save an existing group configuration to the active folder. Select the relevant file to do this.

For further information please refer to section *Flexible group configuration with LANconfig*.

Edit group configuration

Under **Group** > **Edit group configuration** you have the option to edit the highlighted group configuration.

The parameters set here must be valid for the entire group. When the configuration dialog is closed, LANconfig will request that you save the group configuration file to a location of your choice.

For further information please refer to section *Flexible group configuration with LANconfig*.

Refresh all devices

Under **Group** > **Update all devices** you have the option to use the selected and activated group to update all of the devices in the current folder.

For further information please refer to section *Flexible group configuration with LANconfig*.

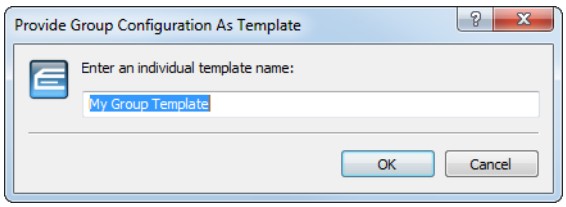
Update recommended devices

Under **Group** > **Update recommended devices** you have the option to use the selected and activated group to update the recommended devices in the current folder.

For further information please refer to section *Flexible group configuration with LANconfig*.

Provide as template

Under **Group** > **Provide as template** you have the option to set the highlighted group configuration as a template for future group configurations.



For further information please refer to section *Flexible group configuration with LANconfig*.

Active

Enable or disable the selected group configuration with the menu item **Group** > **Active**.

For further information please refer to section *Flexible group configuration with LANconfig*.

Delete

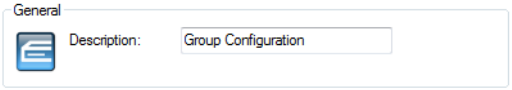
With **Group** > **Delete** you can delete the highlighted group configuration.

For further information please refer to section *Flexible group configuration with LANconfig*.

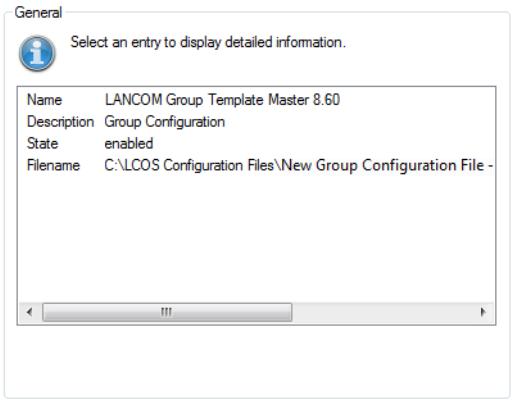
Properties

Under **Group** > **Properties** you can view information about an existing group configuration. Select the relevant file to do this.

The **General** page displays the description of the group configuration.



The **Information** page shows the name, status, and the file name of the group configuration.



For further information please refer to section *Flexible group configuration with LANconfig*.

3.1.3.5 View

This menu item is used to customize the behavior of the LANconfig graphical user interface.

Toolbar

To customize the toolbar, select the following options in LANconfig:

Standard buttons

Shows/hides the buttons.

QuickFinder

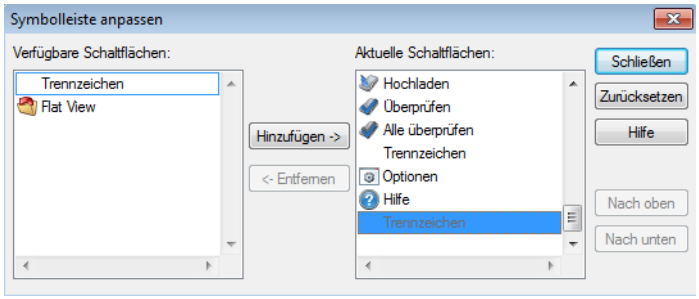
Shows/hides the QuickFinder.

Large icons

Shows a larger view of the icons.

Customize

Opens up a dialog enabling the displayed icons to be selected. A separator can be inserted between groups of icons. The order of the icons can also be changed.



Reset

Resets the settings for the toolbar to the default values.

Information about the icons is available in the chapter *Toolbar icons* on page 240.

Status bar

This menu item allows you to show or hide the status bar.

Folder tree

The directory structure in the left margin of the LANconfig window can be shown or hidden with this menu item (or alternatively with the function key F6). Also see the chapter *Using directory trees to get organized* on page 177.

Log view

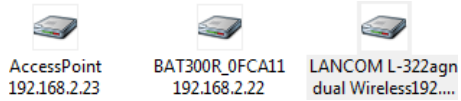
This menu option is used to show or hide the log view (including the date, time, name, address, and message) in the lower part of the LANconfig window.

Flat view mode

Here you can activate the flat view mode in LANconfig.

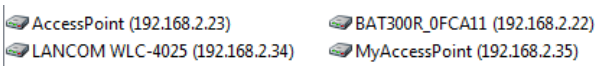
Large icons

In the display mode 'Large icons', the device icons are displayed in an enlarged view; useful for high-resolution displays.



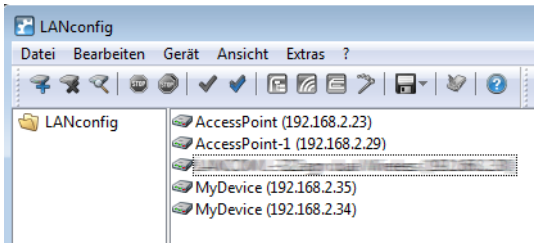
Small icons

The display mode 'Small Icons' reduces the size of the device icons.



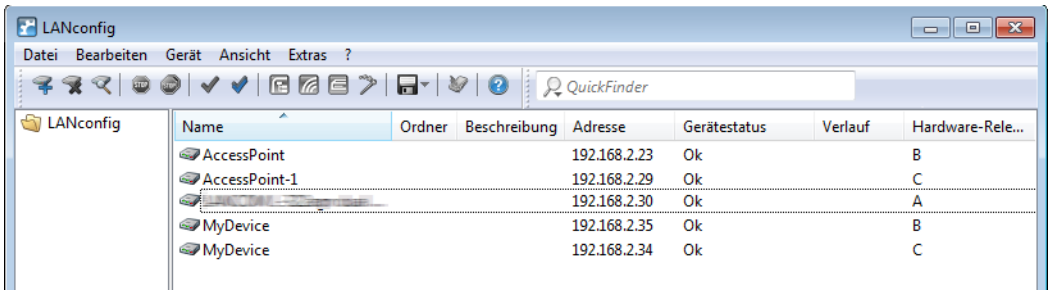
List

In display mode 'list', the devices are shown in a list.



Details

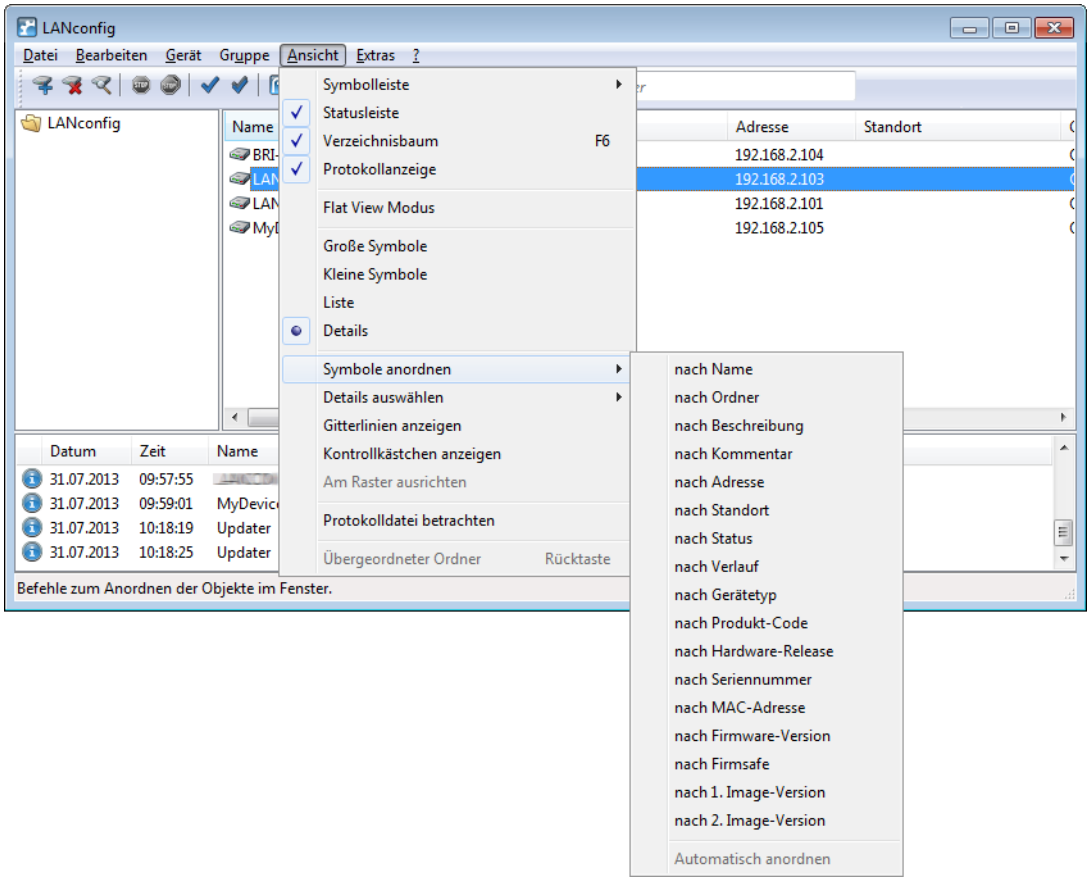
The 'Details' display mode shows details for each device.



Arrange icons

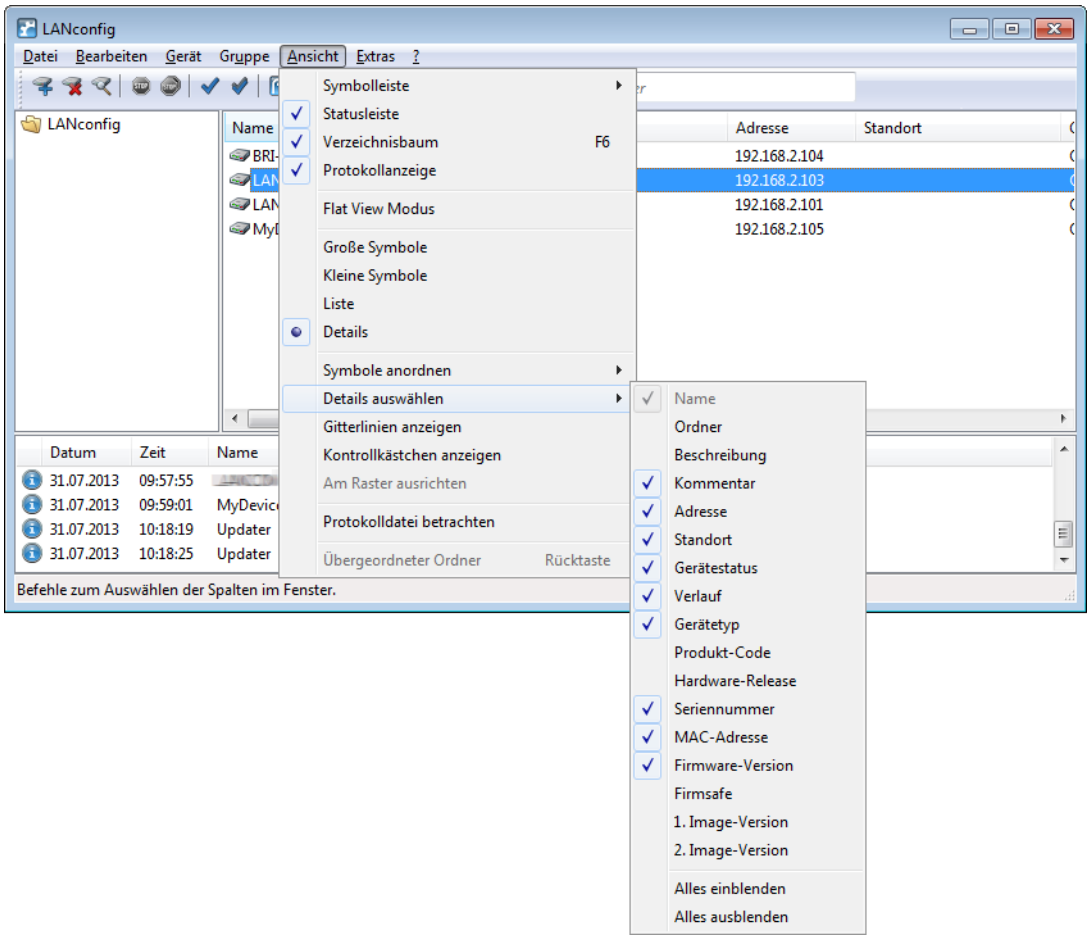
Even for large-scale projects, a better overview and quicker orientation are facilitated in LANconfig by the columns which feature device-related details that can be displayed or concealed according to your needs. Simply click on the column header with the right-hand mouse button and use **View** > **Details** to select the columns to be displayed. The menu item

Arrange icons allows you to sort the items as you prefer. If you select the option **Auto arrange** the icons in the configuration area are sorted automatically.



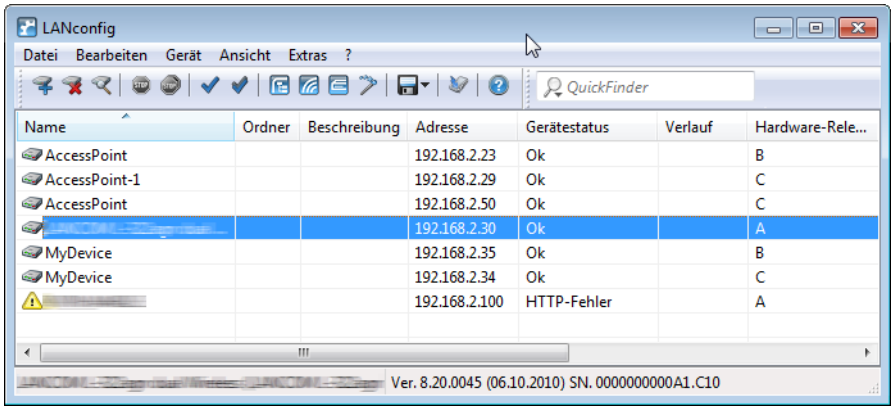
Select columns

Even for large-scale projects, a better overview and quicker orientation are facilitated in LANconfig by the columns which feature device-related details that can be displayed or concealed according to your needs. Alternatively, you can right-click the column headings and, in the context menu that opens, select the menu item **View** > **Details**.



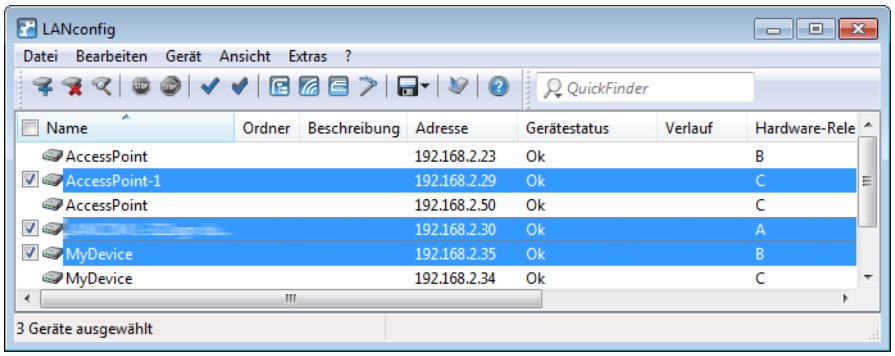
Display gridlines

This menu item allows you to show or hide gridlines in the devices view.



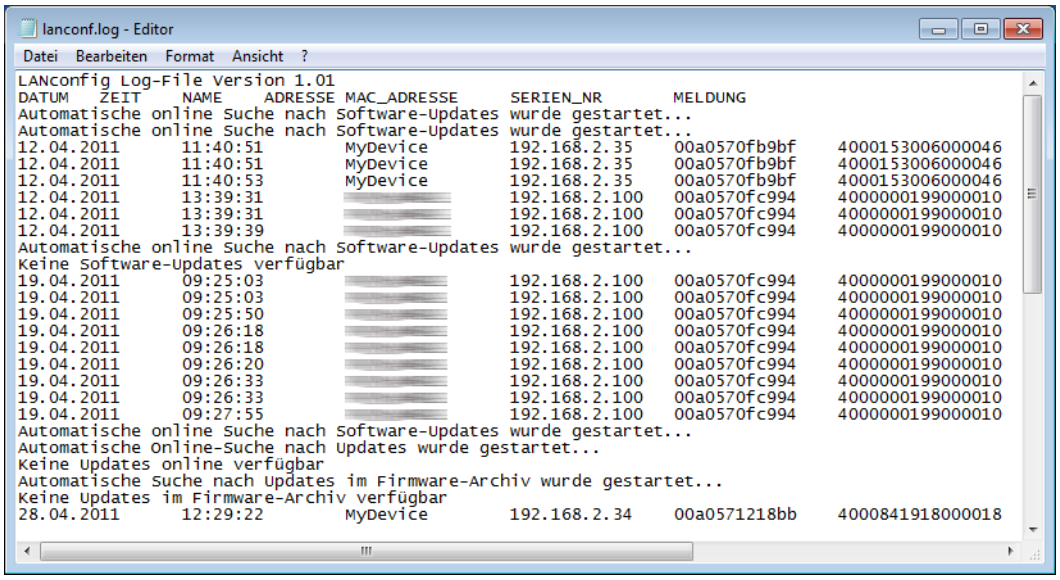
Display check boxes

This menu item is used to enable the display of check boxes. A check box is then displayed next to each device entry, which enables you to select the device. This gives you the option of selecting multiple devices for carrying out targeted actions (e.g. uploading new firmware) without the need of keyboard shortcuts.



View log file

This menu item enables you to view and edit the LANconfig log file.



Up

Use this menu item to switch to the parent folder.

3.1.3.6 Tools

See this menu item for further options in LANconfig. You can also reach this dialog box by pressing F7.

Options

Under the menu item **Options** you can invoke additional functions, for example to communicate with connected devices, invoke external applications, or carry out automatic searches for firmware updates.

Further information is available in the following sections:

General

This dialog box is used to set the General program settings.

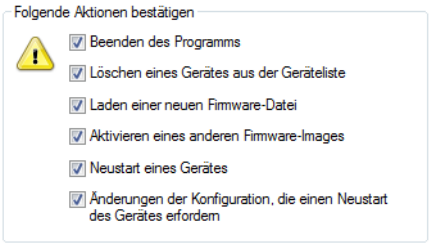
Configuration of devices



You can decide that the Setup Wizard should be used by default when carrying out a configuration or that the manual configuration dialog should be opened when you double-click on a device. In the default setting the Setup Wizard starts when a device is double-clicked.

- **Search the configuration in...**
  - **Description**: Searches through the description in the configuration
  - **Value:** Searches through the values in the configuration
  - **Unit**: Searches through the units in the configuration

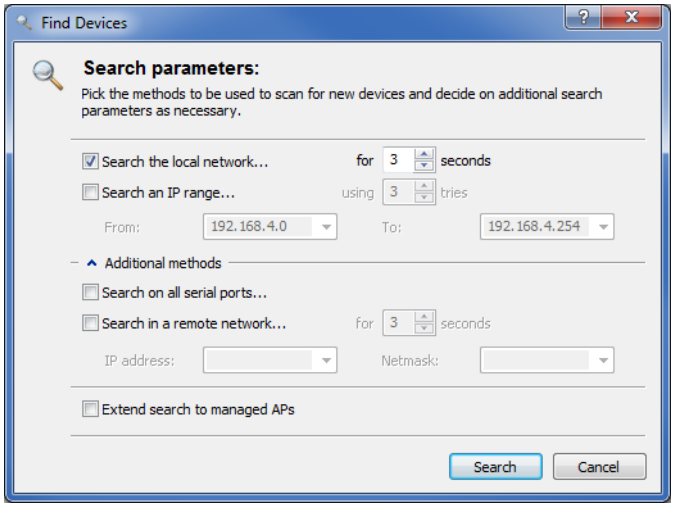
Confirm the following actions



- **Closing the program**: Activates or deactivates the message of confirmation when you exit the program.
- **Deleting a device from the list:** Deactivate this option if you do not wish to be warned when you delete a device from the list.
- **Loading new firmware onto the device:** If you activate this option, you will see a warning when you try to upload new firmware to the device.
- **Activating a new firmware image** If you activate this option, you will be warned each time you try to activate another firmware image.
- **Device reboot:** With this option activated, you will receive a warning before the device is rebooted.
- **Making changes to the configuration which cause the device to reboot:** If you activate this option, you will be warned each time you try to edit the device configuration.

Home

In this dialog box, you specify how LANconfig behaves and acts when started.



- Search for new devices at startup: With this option activated, the program searches predefined networks for new devices each time the program is started.

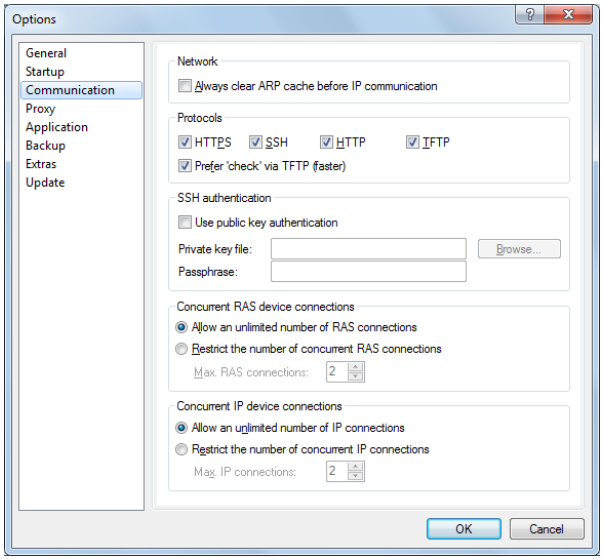
This procedure may take some time in major installations with a large number of devices, or it may undesirable for the program to try to establish contact to the devices.

- **In the local network:** If this option is activated, the program searches the local network for devices each time it is started. It waits for a response for the time set here.
- **In the following remote networks:** With this option activated, the program searches the remote networks for devices each time the program is started. The networks to be searched through are defined in the list that follows.
- **Extend search to managed APs:** Fully managed access points (APs) are normally excluded from the search as their configurations are completely managed by a WLAN controller. Select this option if you wish to find fully managed APs regardless of this.

This option is meaningless if your network does not contain WLAN controllers or managed APs.

Communication

This dialog sets the global settings for the connections between LANconfig and the devices:



Network

If a number of frequently changing devices share the same IP address in your network, then you should activate the option **Always clear ARP cache before IP communication** to ensure that your computer can communicate with these devices.

Protocols

The transfer of configuration data when working with LANconfig can be handled by various protocols: HTTPS, SSH, HTTP or TFTP.

Widely available protocols are defined globally. In addition, it is possible to disable protocols for specific devices. However, it is not possible to re-enable a globally disabled protocol for individual devices as the global communication settings take precedence over the device-specific settings.

The configuration of the communication protocols differentiates between the protocol strictly for testing the device and the protocols for other operations, such as firmware uploads, etc.:

- **HTTPS**, **SSH**, **HTTP**, **TFTP**

  When this is selected, you enable the individual protocols for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, SSH, HTTP and TFTP. If the transfer fails when using one of the selected protocols, LANconfig automatically tries the next protocol.

- **Prefer checks via TFTP**

  The device evaluation only transfers small amounts of data with the system information. As such, it makes sense to perform device checks in the LAN by TFTP protocol. When this option is activated, LANconfig first uses the TFTP protocol to check the device, regardless of the communication protocols set previously. If the check via TFTP fails, then LANconfig attempts the protocols HTTPS, SSH, and HTTP.

SSH authentication

If you have selected the SSH protocol, you can alternatively perform the authentication via a private key. In this case, the authentication dialog for password entry is not invoked. If you select **Use public key authentication**, enter the path to your private key file into the field, and, if necessary, the passphrase that you used to encrypt the file. Load the corresponding public key with LANconfig or WEBconfig onto each device.

For detailed instructions about configuring the public-key authentication for your devices, see chapter *SSH authentication using a public key* on page 119.

Concurrent RAS device connections

The number of concurrent RAS connections can be restricted. This makes sense where a limited number of physical RAS channels is available, or where extreme loads on the system or network should be avoided.

If an action causes the number of RAS connections to exceed this limit, then the surplus actions are placed in a queue and are only started when a RAS channel becomes available.

If you do not place a limit on the number, or you allow a higher number of connections than those physically available, then the surplus actions are placed in a queue as mentioned above.

This option can minimize the effects that a large number of concurrent actions can have on the system or network load.

If you do not limit the number and sufficient resources are available, then there is no limit on the system load or network load generated!

Concurrent IP device connections

The number of concurrent IP connections can be restricted. This makes sense where a limited number of physical channels is available, or where extreme loads on the system or network should be avoided.

If an action causes the number of IP connections to exceed this limit, then the surplus actions are place in a queue and are only started when a logical IP channel becomes available.

If you do not place a limit on the number, or you allow a higher number of connections than those physically available, then the surplus actions are interrupted with an error

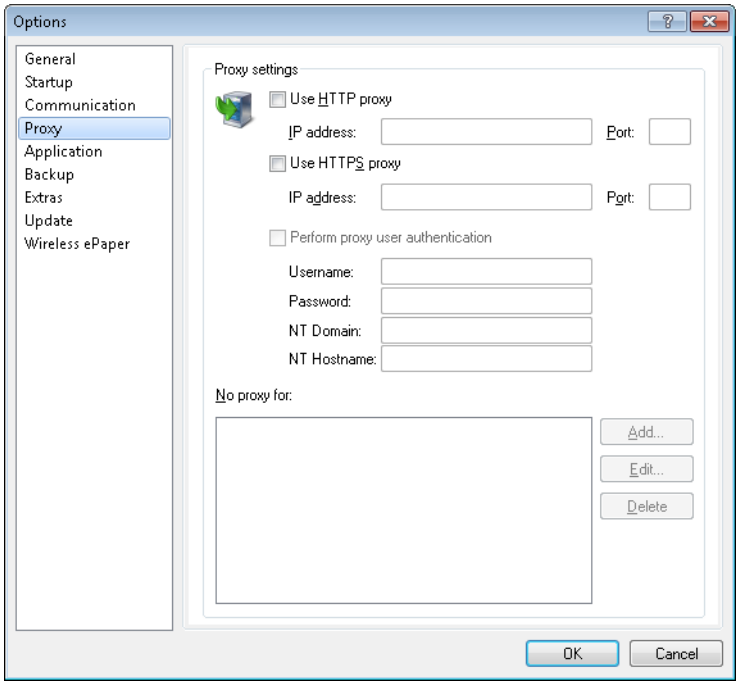
This option can minimize the effects that a large number of concurrent actions can have on the system or network load.

If you do not limit the number and sufficient resources are available, then there is no limit on the system load or network load generated!

Proxy

If you wish to use a proxy server for access to your device, you can configure this here. Activate the required protocol and enter the address and port for accessing the proxy server.

Depending on the protocol, it may be possible to specify a list of networks or individual hosts for which the proxy settings do not apply.



Use HTTP proxy

Enables the use of an HTTP proxy.

- **Address**: Enter the IP address of the the HTTP proxy server.
- **Port**: Enter the port used by the HTTP proxy server.

Use HTTPS proxy

Enables the use of an HTTPS proxy.

- **Address**: Enter the IP address of the the HTTPS proxy server.
- **Port**: Enter the port used by the HTTPS proxy server.

Perform proxy user authentication

If the proxy server requires authentication, enter the user name and password here. If the NT LAN Manager (NTLM) is to carry out the authentication, you additionally enter the NT domain and computer name.

This option is available only if the proxy setting is enabled.

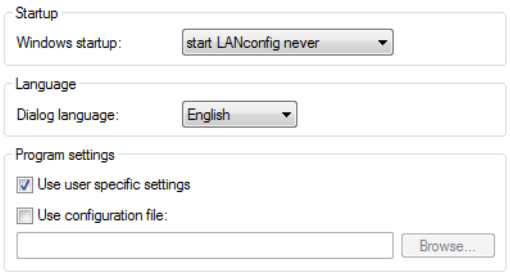
No proxy for

Enter the IP addresses and the corresponding netmask to which the proxy settings do not apply.

This option is available only if the proxy setting is enabled.

Application

This dialog contains the settings for the user interface.



Startup behavior

LANconfig can be automatically started when the operating system starts. The following **Windows startup** types are available:

- **Start LANconfig never**

  The application does not start automatically with the operating system, and it has to be started manually.

- **Start LANconfig always**

  The application always starts automatically after Windows starts successfully.

- **Start LANconfig like last time**

  The application starts in the same status as when Windows was shut down the last time. If the application was active then it will be started again; if inactive, it will not be automatically restarted.

When changing to a setting that enables the application to be started automatically, a change is made to the operating system's registry. Firewalls applications on the computer or the operating system itself may interpret this change as an attack and may issue a warning or even prevent the entry from being made. In order to allow the desired startup behavior, you can ignore these warnings and allow the changes to be made.

Language

This item changes the language of the user interface (GUI). The language is usually selected based on the language of the operating system.

The application must be restarted in order for the language setting to take effect.

Program settings

Here it is possible to define that user-specific LANconfig settings are to be used. Also see the chapter *User-specific settings for LANconfig* on page 176.

- **Use user-specific settings**

  Activates the use of the lanconf.ini file in the current user's directory `...\Application Files\LANCOM\LANconfig`.

  With this option activated, changes to the program settings are saved to this ini file.

- **Use configuration file**

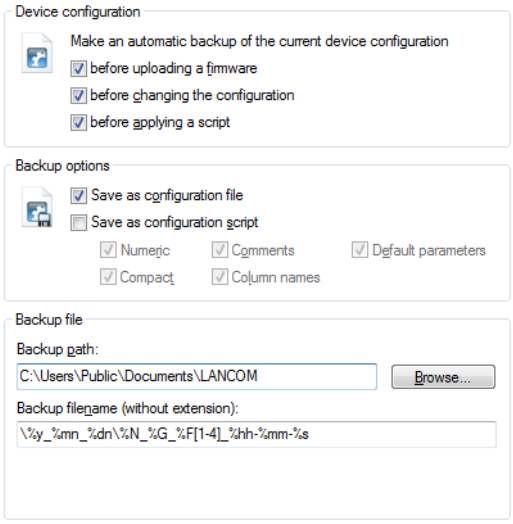
  The activates the usage of the lanconf.ini from the given directory. With this option activated, changes to the program settings are saved to the ini file selected in the input field.

The file you select must be a valid LANconfig settings file.

If neither of the two options is activated, the ini file from the program directory will be used instead.

Backup

This page contains the global backup settings.



Device configuration

You can select what type of action is to be preceded by an automatic backup of the current device configuration. To activate the automatic backup, you have to have selected at least one of the following settings:

- **Before uploading the firmware** The device configuration is automatically backed up before new firmware is uploaded to the device.
- **Before changing the configuration:** The device configuration is automatically backed up before uploading or when editing the device configuration.
- **Before applying a script:** The device configuration is automatically backed up before before a script is applied to the device.

Backup options

This section allows you to select the type of backup. At least one of the following options must be selected for the automatic backup of the current device configuration:

- **Save as configuration file:** The automatic backup saves the current device configuration to a configuration file.
- **Save as configuration script:** The automatic backup saves the current device configuration to a configuration script.
  - **Numeric**: This option means that the sections in the script are shown numerically.
  - **Comments**: This option adds additional comments.
  - **Default parameters**: Normally the only settings to be stored are those that deviate from the default values. This option causes the default values to be stored as well.
  - **Compact**: This option produces output in a compact format. This suppresses spaces and tabs.
  - **Column names**: Normally tables are filled first by describing the columns with the TAB command and then by filling out each line with a SET command containing only those values which are to be

set. If this option is activated, the columns of the table are not described by the TAB command, but instead each table SET command contains the column descriptors.

Backup file

- **Backup path:** Here you can set the path to the storage folder on your computer or in the network. The **Browse** option lets you navigate to the folder of your choice. In the default setting, backups are saved to the 'Config' folder in the program directory on the local computer.
- **Backup filename (without extension):** Here you can set the filename (without the file extension). The file extension is set according to the backup type. The file name can contain the variables outlined in the following table. These variables are used to produce the filename when an action is carried out. It is also possible to suffix the backup filename with folders, which are created at the time of backup.

Table 16: Device information

Name	%N
MAC address	%M
Device type	%G
Hardware release	%W
Firmware-Version	%F
IP address	%I
Firmware date	%D
Address	%H
Serial number	%S

The following regular expressions can be used to display information about the device itself. Numbers in square brackets following the variables generate partial information, such as %N[5]. The n-th character in the variable will be expanded. A hyphen defines a character string, e.g. %H[2-5].

Table 17: Examples of the variables

[]	Expands all characters
[1]	Expands the first character only
[12], [12-12]	Expands the twelfth character only
[1-5]	Expands from the beginning to the fifth character
[2-5]	Expands from the second to the fifth character
[6-]	Expands everything as of the sixth character

Table 18: Date and time

%y	Year
%hh	Hour
%mn	Month of the year (1-12)
%mm	Minute
%ma	Month of the year (January - December)
%s	Second
%dn	Day of the month (1-31)

%ms	Milliseconds
%da	Day of the week (Sunday - Saturday)
%dw	Weekday (Sunday is 0, 0-6)
%%	% (single percent sign)

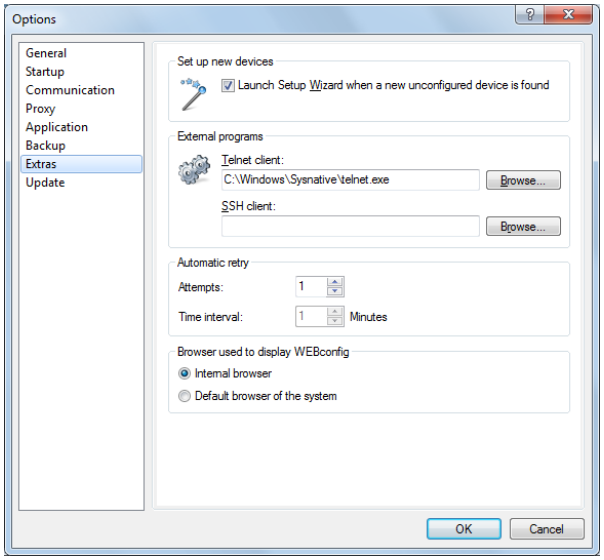
If a file of the same name already exists in the target directory, then the name of the backup file is automatically suffixed with an ascending number.

Table 19: Examples

Backup filename: MyBackup_%N_%S_%I	Result: MyBackup_MyDevice_12481632_10.10.1.1
Backup filename: %d_%mn_%y\Folder_2\%N	Result: 25_08_2008\Folder_2\MyDevice

Extras

This dialog window allows you to make additional settings.



Set up new devices

If this option is checked, LANconfig launches the Setup Wizard whenever it finds an unconfigured device.

External programs

This item specifies the executable files for the Telnet client and the SSH client to be used by LANconfig for connections to the devices.

Automatic retry

Attempts

Specify the number of attempts for a firmware or configuration upload. You can set a number between 1 and 9999. LANconfig always attempts to make a connection. If this fails a retry is attempted after the defined interval. The operation is retried until LANconfig reaches the number of defined attempts or until the operation

succeeds. LANconfig may terminate the retries if a situation arises in which completion is unlikely without external intervention. This may be when the device cannot open a file, for example.

Time interval

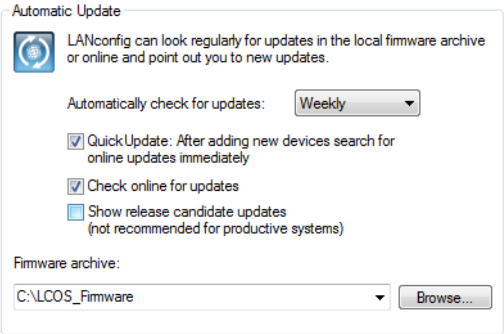
Enter the time interval in minutes between two attempts to upload the firmware or configuration. You can set an interval between 1 and 9999.

Browser used to display WEBconfig

This item sets the default browser used by LANconfig to display WEBconfig. You can choose between your operating system's default browser and LANconfig's internal browser, LCCEF (LANCOM Chromium Embedded Framework).

Update

This dialog contains the settings for the automatic updating.



To make the update of devices with new firmware as convenient as possible, the firmware files for the various models and LCOS versions are, ideally, saved to a central archive directory. The search for new firmware versions in this directory can either be initiated manually or automatically after starting LANconfig.

- **Automatically check for updates:**

  Select the time interval for the automatic check for updates (**Daily**, **Weekly** or **Monthly**). Alternatively, disable the automatic search with the setting **Never**.

- **Check online for updates**

  Enable this option and LANconfig will check online for updates in the download area of the LANCOM web server.

- **Show release-candidate updates**

  If you enable this option, the Software Update will not only offer to download the released software versions for use in productive environments, but also any available release candidates.

  Release candidates include the new features of upcoming software versions and have been thoroughly tested. Until the final release of version, the software may be further optimized—partly due to user feedback.

- Select a suitable local folder for the **Firmware archive**. When carrying out the automatic search for updates, LANconfig searches this location for new versions of the LANtools and the firmware. This is the location where LANCOM Software Update stores the updates from the download section of the LANCOM web server.

Start LANmonitor

This starts LANmonitor. Refer to chapter *LANmonitor – monitoring devices on the LAN* on page 247 for more information on this.

Start WLANmonitor

This starts WLANmonitor. Refer to chapter *WLANmonitor – monitoring wireless devices* on page 273 for more information on this.

Analyze trace output

This starts LANtracer. Refer to chapter *LANtracer – tracing with LANconfig and LANmonitor* on page 289 for more information on this.

Start CC Startup Wizard

This menu item invokes the CC Start-up Wizard, which helps you to configure your LANCOM CC products to run in the certified CC operating mode as per CC EAL 4+.

Further information about using the Wizard and the configuration of CC devices is available separately in the "LANCOM CC Installation Guide". You can find this together with the "LANCOM CC Start-up Kit" on *www.lancom-systems.com*.

This Wizard is irrelevant for non-CC devices.

Check for updates

Manually starts the automatic search for online updates. Also see the chapter *LANCOM Software Update for LANtools* on page 201.

3.1.3.7 Help

This menu item offers help about the program and displays information about the software.

Help topics

This menu item gives you access to the help topics. Alternatively you can press F1.

Support

This menu item invokes the Support web page.

Info

This menu item shows you which software version you are operating and its build date.

3.1.4 Toolbar icons

Table 20: Icon meanings

	Add		Upload
	Delete		Check
	Find		Check all
	Cancel action		Help
	Cancel all actions		Upwards
	Check		Flat view
	Check all		Restore

	Monitor		Folder
	Monitor WLAN		Log view
	Configure		Options
	Setup Wizard		View
	Backup		Properties

For information about the toolbar setup options, see the chapter *Toolbar* on page 224.

3.1.5 LANconfig context menu

The context menu in the device view contains the same functions as the **Device** menu.

3.1.6 LANconfig keyboard shortcuts

Ins	Add device
Del	Delete device
F3	Find devices
F5	Check all devices
Alt+F4	Exit
Ctrl+N	New configuration file
Ctrl+E	Edit configuration file
Ctrl+Shift+W	Wizard configuration file
Ctrl+Shift+P	Print configuration file
Ctrl+A	Select all
Ctrl+O	Device > Configure
Ctrl+W	Device > Setup Wizard
Ctrl+F5	Device > Check
Ctrl+P	Print
Ctrl+S	Save as file
Ctrl+R	Restore from file
Ctrl+Shift+U	Check for firmware update
Ctrl+U	Upload new firmware
Ctrl+B	Open secure web browser
Ctrl+T	Open Telnet session
Ctrl+Shift+S	Open SSH session
Ctrl+M	Monitor device temporarily
Alt+Enter	Properties
F6	Folder tree
Backspace	Parent directory

Spacebar, ENTER	Edit the selected table entry
+	Jump one table entry upwards (dynamic tables only)
-	Jump one table entry downwards (dynamic tables only)
Ins	Add new table entry (dynamic tables only)
Del	Delete highlighted table entry (dynamic tables only)
F7	Tools > Options
F1	Help topics

3.1.7 LANconfig command line parameters

With the help of the Windows command line, you can optionally launch LANconfig with specialized options and commands. The input is carried out according to the syntax outlined below. Forward slash and hyphen are supported as parameter prefixes. The use of upper or lower case is irrelevant when entering parameters.

The syntax is as follows:

```
lanconf.exe [(-|/)<Option>[:<Value>]] [(-|/)<Command>[:<Value>]]
```

- Square brackets indicate optional parameters.
- Parentheses indicate mandatory parameters.
- A vertical bar is used to indicate alternatives.
- Angle brackets indicate objects that are described under *Options* on page 242 and *Commands* on page 243.

For example, to start LANconfig with an English user interface, enter `lanconf.exe /language:English`. To additionally open the Configuration Wizard with a specific configuration file, you add the Wizard command to the entry like so: `lanconf.exe / language:English /wizard:MyConfig.lcf`.

3.1.7.1 Options

This section describes the options available when using the command-line interface:

Restart

Checks the LANconfig start options in the .ini file. Use this parameter to influence the behavior of LANconfig when starting Windows. LANconfig will only start automatically if under **Tools** > **Options** > **Application** the startup type is set to **start LANconfig always** or **start LANconfig as before** (i.e. the program was running when Windows was shut down).

WizStyle

Influences the appearance of the Configuration Wizard. Possible values for `<Value>` are:

- `0`: Old Wizard style: The headers (title and subtitle) on the dialog pages are separated from the other contents of the dialog by a horizontal line.
- `1`: Current Wizard style (since Windows 98). The headers (title and subtitle) on the dialog pages are separated from the other contents of the dialog by a horizontal line and a different color background.

Language

Changes the language for the user interface temporarily. By default LANconfig uses the system language, if available. Otherwise the language is English. Possible values for `<Value>` are:

- `English`
- `German`
- `Spanish`

3.1.7.2 Commands

This section describes the options available when using the command-line interface: Commands that relate to specific configuration files require a file name to be specified as `<Value>`, e.g. `lanconf.exe /printto:MyConfig.lcf`.

Close

Closes the program after executing any pending commands. After executing the commands, LANconfig starts normally unless another setting was made.

Owner

Handle to the owner of the window [hwndParent] . This can optionally be used with the commands `Print`, `PrintTo` and `AutoUpdate`.

Edit

Used for editing a configuration file if it is not being edited already. If a configuration file is being edited, it will be brought into focus.

Wizard

Starts the Wizard for the configuration file. If this has been opened already, it appears in the foreground.

Print

Prints the configuration file, unless a print job has already been dispatched.

PrintTo

Prints out the configuration file on a specified printer.

ShellNew

Creates a new configuration file.

AutoUpdate

This is how you start a firmware auto-update:

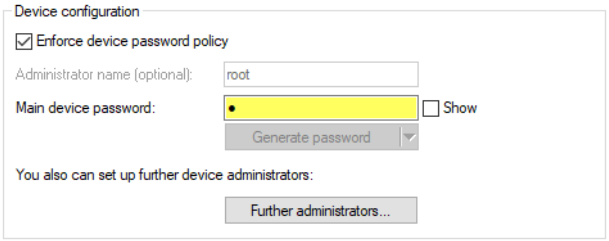
1. Search for the devices.
2. Search for the firmware files.
3. Select the new firmware.
4. Set which device the firmware update is intended for.

3.1.8 LANconfig application concepts

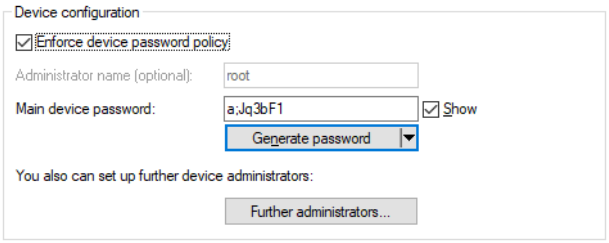
This section describes various applications of LANconfig.

3.1.8.1 Creating a password in LANconfig

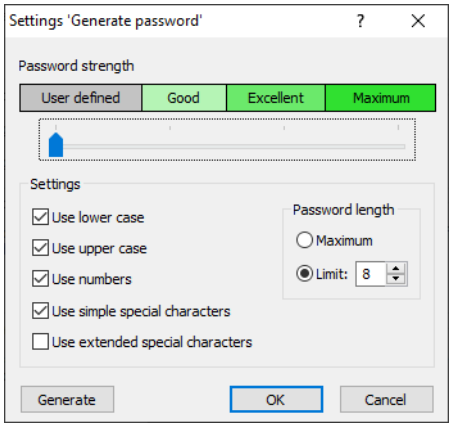
At all points in the configuration that require the input of a password or a passphrase, LANconfig provides the option to generate a password automatically.



Enable the option **Show** next to the box for entering the password. Then click on the button **Generate password** to create a password suggestion.



Optionally click the arrow next to the **Generate password** button to open the dialog box for the password policy settings.



Use the slider to set the desired password strength. With the **User defined** setting, you can define the maximum password length and the required character types. The settings **Good**, **Very good**and **Maximum** are predefined settings with reasonable, non-modifiable values.

After making your changes, click on the **Generate password** button again to create a new password proposal in line with your password guidelines.

LANconfig stores the current settings in this dialog box for the current user.

3.1.8.2 Different notations for MAC addresses

To make it easier to enter MAC addresses by using copy and paste from other applications into LANconfig, the following formats can be used when entering MAC addresses:

- 000000000000
- 00:00:00:00:00:00
- 00-00-00-00-00-00
- 000000-000000

The input is then automatically converted into the form `00:00:00:00:00:00`.

3.1.9 Pairing devices with the LANCOM Management Cloud

3.1.9.1 Basics of the LANCOM Management Cloud

The LANCOM Management Cloud is capable of managing any size of “software-defined” networks. The LMC handles the configuration of all of the network components to minimize the amount of work involved in monitoring and configuration.

Further information about the LANCOM Management Cloud is available from *www.lancom-systems.com/cloud*.

If you wish to use the LANCOM Management Cloud for the configuration and monitoring of your device, the device needs to be paired with the LMC.

3.1.9.2 Pairing devices with the LANCOM Management Cloud

This chapter describes the different ways of pairing LANCOM devices with the LMC. Existing devices are paired in a different way than Cloud-ready devices.

Cloud-ready devices are LANCOM devices that the manufacturer has already equipped with LCOS version 10.0 or higher (LANCOM switches: Switch OS 3.30) and that have a PIN for pairing with the LMC. You will find the PIN on the enclosed product information.

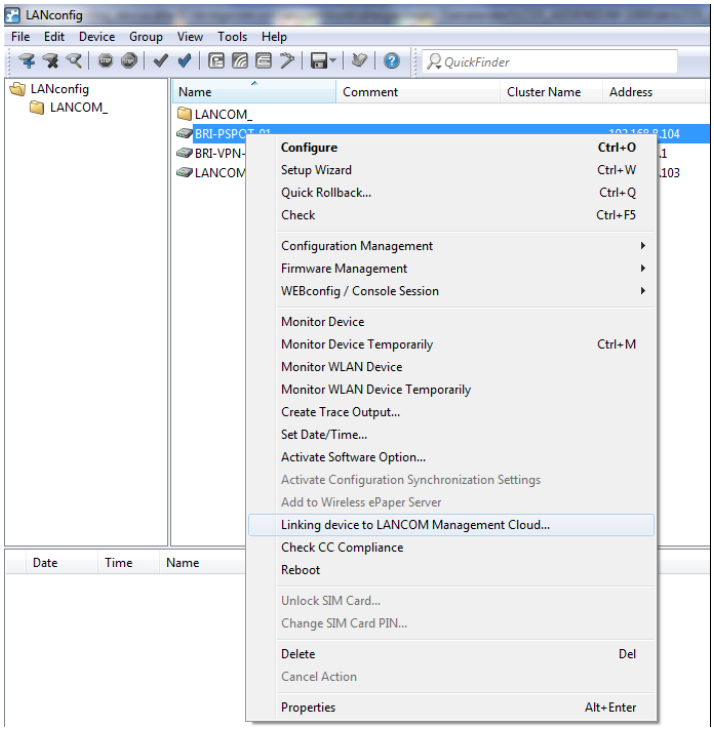
Existing devices are LANCOM devices that have been updated from an older LCOS version to version 10.0 (LANCOM switches: Switch OS 3.30) or higher, which readies them for management by the LMC.

If you have a Cloud-ready device, no pairing is required. All you have to do in this case is to add your device to your account in the LANCOM Management Cloud and enter the serial number and PIN. If you wish, you can alternatively perform a pairing for Cloud-ready devices as well.

Some pairing possibilities are described below.

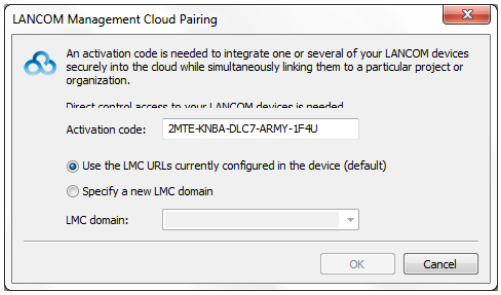
Pairing existing devices via LANconfig

1. In the first step, you need to generate an activation code in the LANCOM Management Cloud.
2. Click on the corresponding LANCOM device with the right-hand mouse button.
3. In the context menu, select the entry **Link device to the LANCOM Management Cloud**.



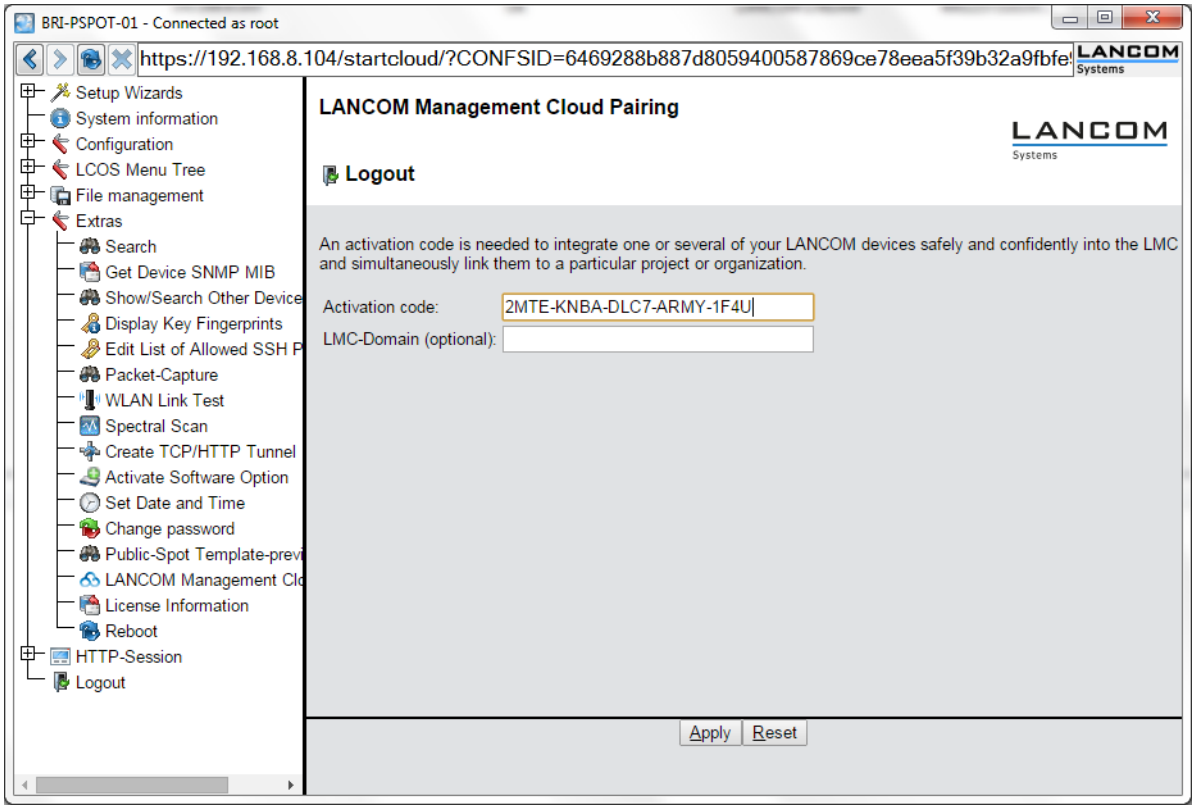
4. Follow the Wizard's instructions to enter the activation code.
   Three options are available:
   - Public Cloud (default): You use the LANCOM Management Cloud.
   - Private Cloud: You use your own Cloud.

› Use the settings currently stored in the device: A public or private cloud is used depending on the existing configuration in the device.



Pairing existing devices via WEBconfig

1. Start WEBconfig.
2. Under **Extras** > **LANCOM Management Cloud Pairing** you enter your activation code.



3. Click on the **Send** button.

Pairing existing devices via the command line

To conduct pairing from the command line, enter the command `startlmc`.

1. Launch a command line utility.
2. Enter the pairing command using the activation code as a parameter, e.g. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

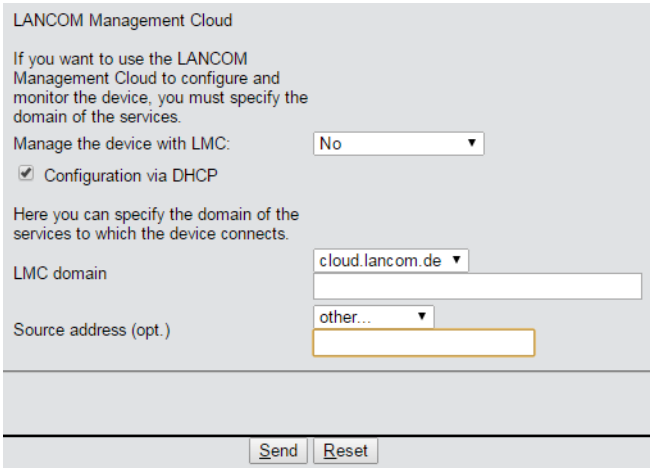
An on-screen message will inform you if the pairing process has started successfully, or you will see an error message.

3.1.9.3 Manual upfront configuration of your device for management by the LANCOM Management Cloud

This section informs you about the steps necessary in order for your device to be configured and monitored by the LANCOM Management Cloud.You specify:

- Whether your device is to be managed by the LMC.
- Whether the LMC domain is to be retrieved from a DHCP server.
- Which domain your device connects to.
- The source address (optional).

1. Navigate to **Management** > **LMC**.



2. Select one of the three options under **Manage the device with LMC:**
   - **No**: The device does not connect to the LMC.
   - **Yes:** The LMC manages the device. (Default for devices without a WLAN interface)
   - **Only without WLC**: Devices within a network managed by a WLC do not connect to the LANCOM Management Cloud. (Default for devices with a WLAN interface)
3. To obtain the LMC domain from a DHCP server, place a check mark in **Configuration via DHCP**.

   In order for the DHCP server to provide the LMC domain, the DHCP server requires sub-option 18 of the DHCP option 43 to be set to the LMC domain. For more information about the configuration of LMC parameters, see the section *Delivery of the LMC domain by the LCOS DHCP server* on page 48.
4. Under **LMC domain** you set the domain of the LANCOM Management Cloud that the device should connect to.
5. Enter an optional **Source address (opt.)** to be used instead of the one otherwise automatically selected for the source address. If you have configured a loopback address, you can specify it here as the source address.

3.2 LANmonitor – monitoring devices on the LAN

LANmonitor is a monitoring tool for Windows that provides a convenient and structured on-screen display of key information about the LANCOM devices.

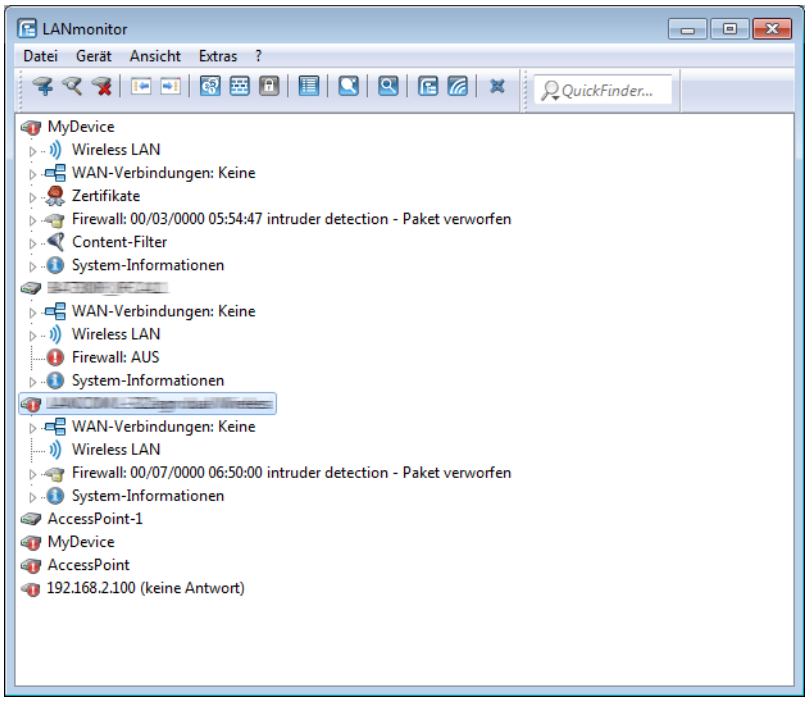
- Display of connections and interface activities
- Interface states
- Transfer rates, protocols and IP addresses
- Error statuses
- Display of device information, SW version, CPU load and memory usage

- Display of accounting information (online times, charges and transfer volume)
- Display and logging of device activities
- Establishment and termination of WAN, VPN and WLAN connections
- Firewall action log(s)

Many of the internal messages from the devices are translated into cleartext to display the current state of the device and to help you with troubleshooting.

You can also use LANmonitor to observe the data traffic at the various router interfaces, which can be a significant help in optimizing the settings for data traffic.

In addition to reading-out device statistics which are also available from telnet or terminal sessions or by using WEBconfig, LANmonitor provides useful functions such as increasing a charge limit.



LANmonitor can only be used to monitor devices that can be access by IP (local or remote). This program does not communicate with devices via serial interface.

If you are unable to find a device in LANmonitor, it may be that the readout of device information via the access path you have chosen (e.g. remotely via VPN) is not permitted. LANmonitor uses the SNMP protocol to read-out device information, and this can be individually configured and restricted by the administrator.

3.2.1 Start LANmonitor

Start LANmonitor, for example with a double click on the desktop icon.

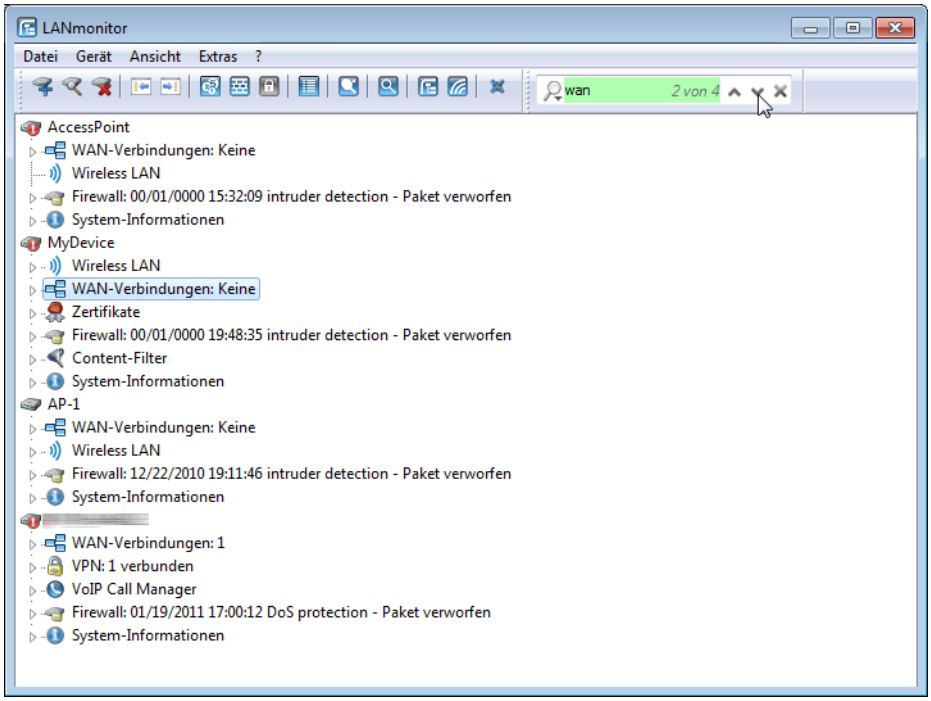
You can influence the startup behavior of LANmonitor under **Tools** > **Options**. Please also refer to *Options* on page 268.

You can also launch LANmonitor for a specific device via the context menu in LANconfig or with the keyboard shortcut 'Ctrl+M'.

3.2.2 QuickFinder in LANmonitor

Depending on the application, LANmonitor can display multiple devices with entries containing the searched term. After starting the search LANmonitor initially highlights the first finding. You can move between the search results either by

using the arrow keys to the right of the search window, or by pressing 'Ctrl+F3' for the next occurrence and 'Ctrl+Shift+F3' to the previous occurrence.



3.2.3 Display functions in LANmonitor

LANmonitor supports the administration of the applications by offering a range of functions that simplify the surveillance of devices at widely dispersed locations. The overview of devices monitored by LANmonitor already shows the most important information about the status of the devices: The information that can be taken from the overview includes, among others, details about active WAN connections, the five most recent firewall messages, the current VPN connections and system information about charges and online times.

Right-clicking with the mouse on a device in LANmonitor opens up a context menu with further information, including among others:

- *Activity log*
- *DHCP assignments*
- *VPN connections*
- Firewall event logs for *IPv4* and *IPv6*
- *Syslog*
- *Accounting information*

3.2.4 The menu structure in LANmonitor

LANmonitor supports the administration of the applications by offering a range of functions that simplify the surveillance of devices at widely dispersed locations. From the menu bar you can retrieve status information from the devices, reset them, or carry out further analyses (e.g. spectral scan, trace output). Numerous menu items are also available in the context menus in the device overview for each of the devices.

The overview of devices monitored by LANmonitor already shows the most important information about the status of the devices: The information that can be taken from the overview includes, among others, details about active WAN connections, the five most recent firewall messages, the current VPN connections and system information about charges and online times.

3.2.4.1 File

This menu item is used to manage devices in general, and to exit LANmonitor if required.

Add device

A new device is added under **File** > **Add device**. It opens a dialog where you can make the settings for the connection to the device and for the protocol.

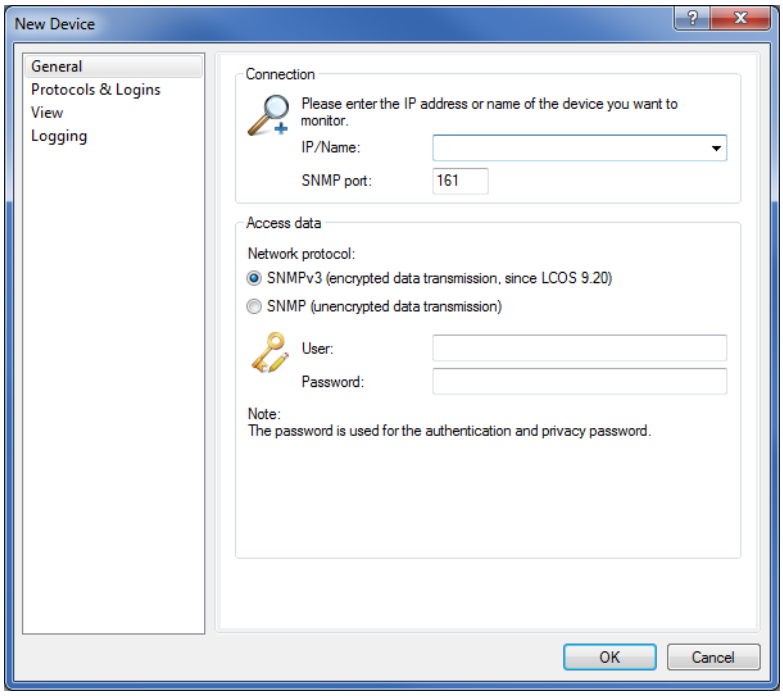
You also have the option of configuring new devices by entering IP addresses and the SNMP port when executing the program. To do this, start the LANmonitor with the syntax `lanmon /add:[<IPv6-Address>]:<Port>`, for example, `lanmon /add:[fe80::2a0:57ff:fe1b:3302]:161`.

General

On this page you specify the IP address and the SNMP port of the new device for monitoring by LANmonitor. If authentication is required to read-out the device data or perform actions on the device, these access credentials must also be stored in LANmonitor.

You must permanently store the credentials for read-only access as a minimum; otherwise the program cannot connect to the device. Permanently storing write-access credentials is optional. This saves you having to enter the credentials manually each time you send an action to LANmonitor for the first time.

If you save the username and password permanently, any user who is permitted to run LANmonitor also has access to the device.



Interface

- **IP/Name**: Enter the IP address of the device. You can also enter a domain name (DN or FQDN). This name is checked at every access. LANmonitor stores and uses the resolved IP address. If this check is not possible, then LANmonitor takes the last IP address that was last used successfully.
- **SNMP port:** Specify the port under which the SNMP service on the device is accessed. The default is this `161`. Depending on the setting in the device (see Setup parameter 2.9.21) or ARF context, a different port may be required.

Authentication

In this section, choose how and with what credentials you authenticate yourself to the device. The setting you need depends on whether you have restricted the SNMP read-access to the device and have defined a community of your own. Learn more about this in the Section *Configuring SNMP read-only access* on page 116.

Network protocol

Select whether the LANmonitor accesses the device via SNMPv3 (encrypted), or via SNMPv2 (unencrypted, not recommended). Access via SNMPv3 is supported as of LCOS 9.20.

SNMPv3

- **User**: Specify the user for SNMPv3 access.
- **Password**: Specify the password for SNMPv3 access. This is usually the master device password.

SNMPv2

- **SNMP read-only community**: Use this setting if authentication at the device is handled by
  - the public community `public` or
  - your own community in the form of a master password or username:password pair

  . You then enter these into the **Community** field.
- **Administrator/Password**: Use this setting if authentication at the device is handled by
  - your own community in the form of a username:password pair or
  - the credentials of an administrator account

  . You then specify the user name in the **Administrator** field and the password in the **Password** field.

Pay attention to the correct spelling/capitalization, because SNMP access to the device is blocked if the wrong data is entered.

You also have the option of saving the **access credentials for device actions (SNMP write community)** either for the current session or permanently in LANmonitor. This data is required for all device actions (such as deleting or resetting status values). If you do not store any credentials, the program prompts you for them the next time you attempt to execute an action.

For read-only access, you should preferably specify a read-only community instead of an administrator account, as SNMP packets are transmitted in cleartext with SNMPv2.

Protocols & logins

On this page, you can configure and manage the protocols, ports, and access credentials used by the other components of the LANtools when they call programs from within LANmonitor. Configurable programs include:

- LANconfig
- LANtracer
- LANtools-internal and also external Web browsers

If program is invoked with certain protocols already deactivated or configured differently, for example, only the matches are applied.

The setting options are equivalent to those of LANconfig. Please refer to the section *Protocols & logins* on page 219 for more on the configuration.

View

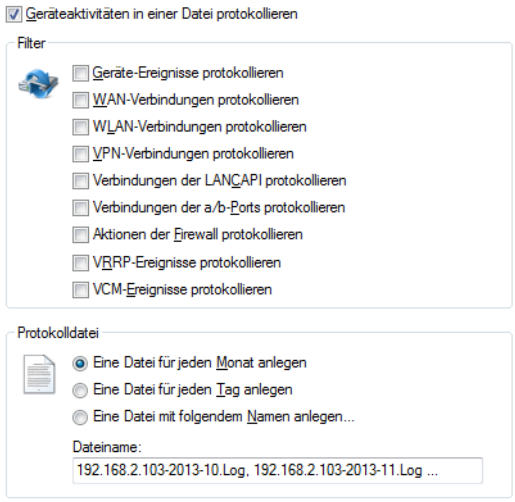
On this page you can adjust the display-related connection settings.



If you select the option **Disable tooltips in systray for this device**, LANmonitor displays no tooltips for this device in the system tray.

Logging

This page gives you control over how LANmonitor logs the device activities. Your selections under **Filter** determine which activities LANmonitor records and which log file to write.



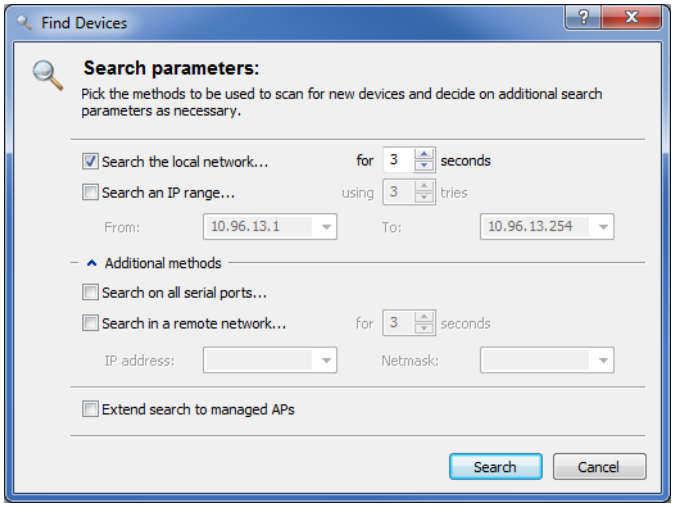
Delete device

You can delete a device that has been marked under **File** > **Delete device**. You can also use the 'Del' key to delete a device.

Deleting a device only removes it from the current view. You can add it to the display again using **File** > **Add device** or **File** > **Find devices**.

Find devices

This menu item triggers an automatic search for new devices for adding to the device view section.



Select where you wish to search for devices:

- Search in the local network
- Search in a remote network

  If you wish to search in a remote network you must specify its address and the relevant network mask.

- If necessary, you can extend the search to managed access points (APs).

Click on **Search** to start the search. Any devices found will be added to the list automatically.

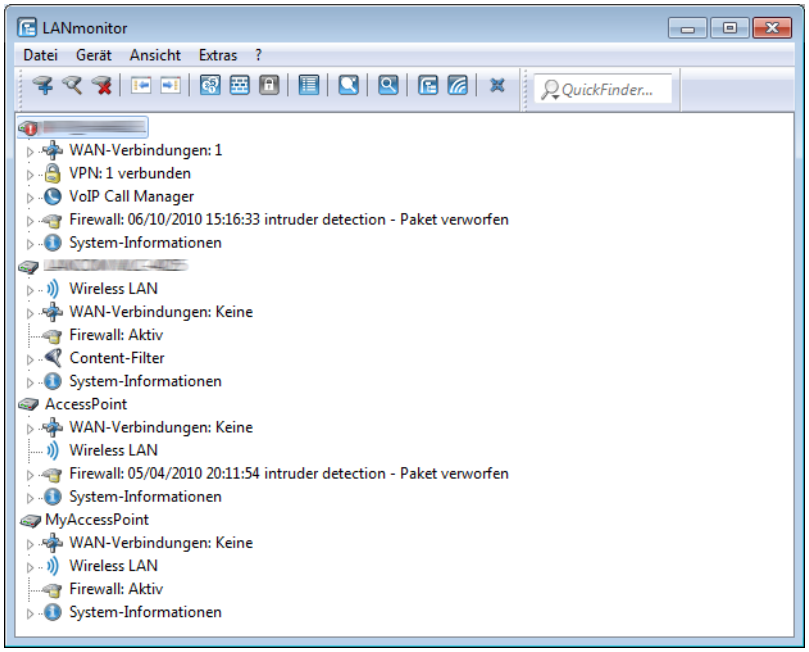
If a device is found that is already in the list, it will not be included in the list a second time. For this reason fewer devices may be added to the list than were reported during the search operation.

Refresh all devices

Refreshes the connection to all devices.

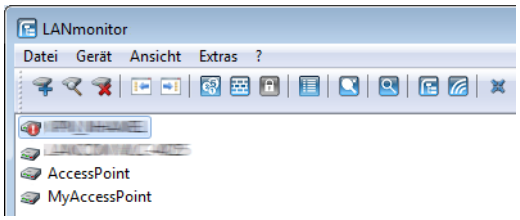
Expand devices

Expands the display of devices in the list. The opposite is the *Collapse devices* view. The expanded display look as follows:



Collapse devices

Reduces the display of devices in the list. The opposite is the *Expand devices* view. The reduced view appears as follows:



Exit

Closes and terminates LANmonitor.

3.2.4.2 Device

This menu item is used to manage and monitor a selected device in the network.

Refresh display

Updates the information displayed for the selected device.

View VPN connections

You can view the VPN connections for a certain device. The list of VPN connections is a log of the 100 most recent VPN connections. Detailed information is recorded:

Name

Name of the remote station

Status

Status of the connection (for example, **Connected** or **Not connected**)

Last error

Last error to occur

Short hold time

The short hold time set for this connection. The short hold time specifies the number of seconds that pass before the device disconnects from the remote site if no data is transferred. Special values are:

- '0': The device does not disconnect by itself. In the case of a disconnect, the connection must be manually established by the user.
- '9999': The device does not disconnect by itself. In the event of a disconnect from the remote station, the router automatically attempts to reconnect immediately.

Connection

Name of the network used for the physical connection to the remote site

Gateway

IP address of the remote VPN gateway or remote site

Nat detection

Indicates whether NAT is active

Encryption algorithm

The encryption algorithm used

Hash algorithm

The hash algorithm being used and the length of the hash code (in bits)

Hmac algorithm

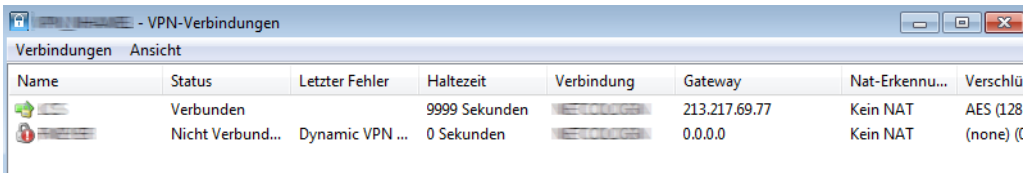
The HMAC algorithm being used and the length of the HMAC code (in bits)

Compression algorithm

IPCOMP algorithm used

SSL encapsulation

Indicates whether SSL encapsulation is used



You will find the following functions in the **Connections** menu:

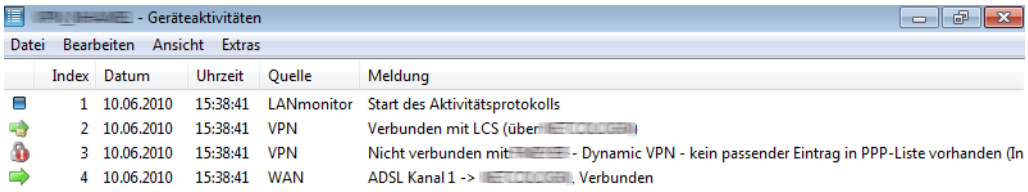
- **Refresh**: Updates the displayed information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

View device activities

You can view the device activities for a certain device. The activity log is a detailed list of the connections via WAN, WLAN, VPN and a/b port, and a list of firewall activities. Detailed information is recorded: **Index**, **Date**, **Time**, **Source** and **Message**. The activity log is continually being updated.



You will find the following functions in the **Connections** menu:

- **Save device activities**: Stores the displayed device activities to a location of your choice in a suitable file format (*.log).
- **Close**: Close the information window.

You will find the following functions in the **Edit** menu:

- **Save selection**: Stores the highlighted entries to a location of your choice in a suitable file format (*.log).
- **Delete buffer**: Deletes the marked entries.

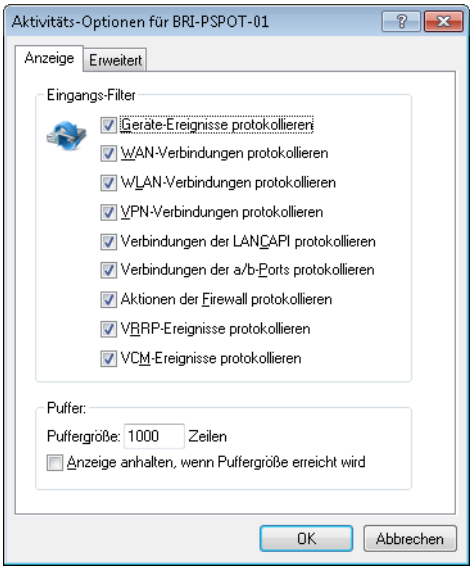
You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

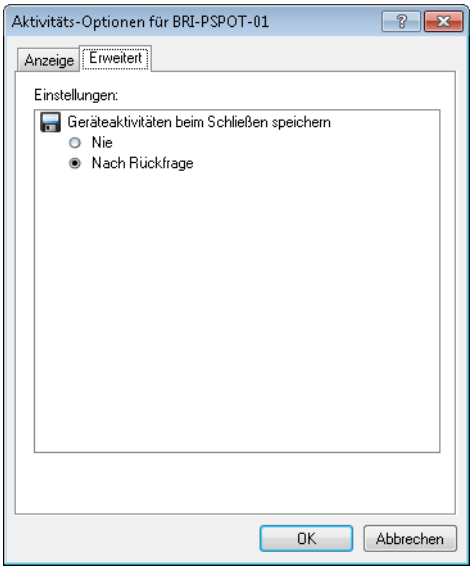
You will find the following functions in the **Tools** menu:

- **Options**:

  This menu item gives you control over how LANmonitor logs device-specific activities. For this purpose, select the **Inbound filter** on the tab **Display** to specify which activities and to what extent (**buffer**) LANmonitor records the activities.



On the **Advanced** tab, you specify whether LANmonitor saves the recorded data to a file.



To specify the file, go to **Device** > **Properties** > **Logging**.

View syslog

You can view the syslog for a certain device. Detailed information is recorded:

Time

Date, time of the syslog entry

Source

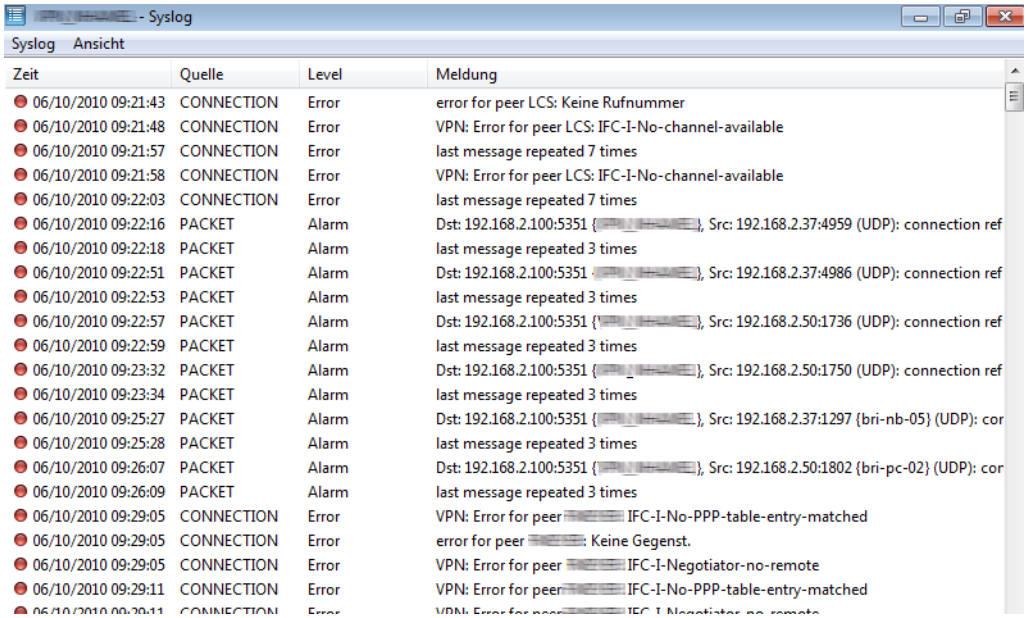
Source of the syslog message

Level

Level of the syslog message, e.g. alarm or error

Message

Details of the syslog message



You will find the following functions in the **Syslog** menu:

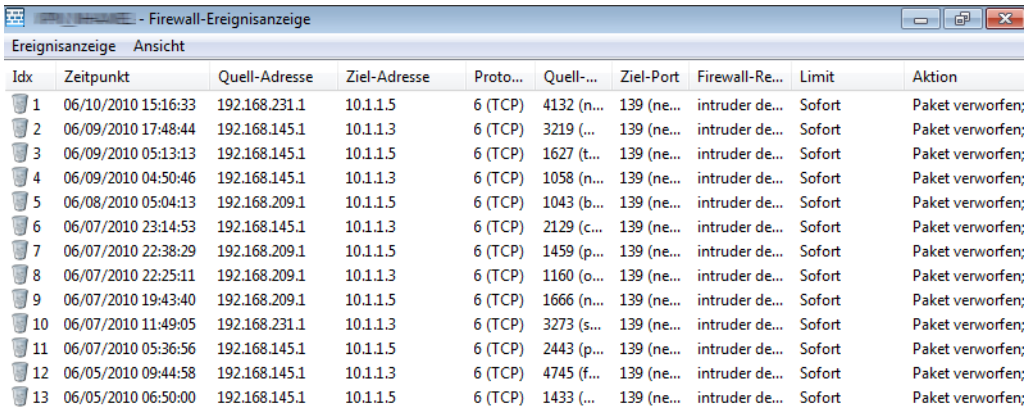
- **Refresh**: Updates the displayed information.
- **Save syslog**: Stores the displayed syslog output to a location of your choice in a suitable file format (*.lsl).
- **Load syslog**: Loads a saved syslog file.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

View IPv6 firewall event log

In LANmonitor you can view the firewall events for a selected device under **Device** > **View firewall event log**. The firewall events show the last 100 actions of the firewall. The information displayed and the explanations are identical to those of the *IPv4 firewall*.



You will find the following functions in the **Event log** menu:

- **Refresh**: Updates the displayed information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

View IPv4 firewall event log

You can view the firewall events for a certain device. The firewall event log lists the last 100 actions taken by the firewall. Detailed information is recorded:

Idx

Sequential index entry of events

System time

Time when the event was logged

Source address

Source address of the filtered packet

Destination address

Destination address of the filtered packet

Protocol

Protocol (TCP, UDP, etc.) of the filtered packet

Source port

Source port of the filtered packet (only for port related protocols).

Destination port

Destination port of the filtered packet (only for port related protocols)

Firewall rule

Name of the rule that created the entry

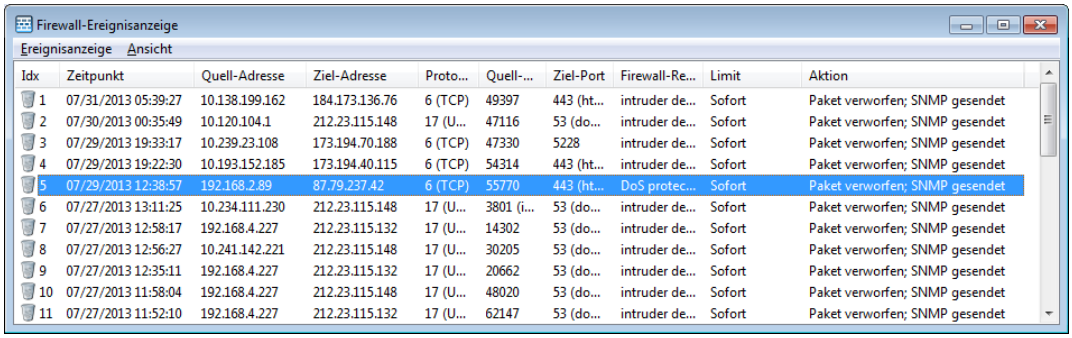
Limit

Limit associated with the relevant firewall action. If a firewall action is not associated with a limit, this implies a packet limit that is immediately exceeded with the first packet. In this case, the column shows the value **immediate**.

For more information on limits, see the Menu Reference Guide under "2.8.10.4 Action table" in the section "Limits".

Action

Short description of the performed action



Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Proto...	Quell-...	Ziel-Port	Firewall-Re...	Limit	Aktion
1	07/31/2013 05:39:27	10.138.199.162	184.173.136.76	6 (TCP)	49397	443 (ht...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
2	07/30/2013 00:35:49	10.120.104.1	212.23.115.148	17 (U...	47116	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
3	07/29/2013 19:33:17	10.239.23.108	173.194.70.188	6 (TCP)	47330	5228	intruder de...	Sofort	Paket verworfen; SNMP gesendet
4	07/29/2013 19:22:30	10.193.152.185	173.194.40.115	6 (TCP)	54314	443 (ht...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
5	07/29/2013 12:38:57	192.168.2.89	87.79.237.42	6 (TCP)	55770	443 (ht...	DoS protec...	Sofort	Paket verworfen; SNMP gesendet
6	07/27/2013 13:11:25	10.234.111.230	212.23.115.148	17 (U...	3801 (i...	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
7	07/27/2013 12:58:17	192.168.4.227	212.23.115.132	17 (U...	14302	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
8	07/27/2013 12:56:27	10.241.142.221	212.23.115.148	17 (U...	30205	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
9	07/27/2013 12:35:11	192.168.4.227	212.23.115.132	17 (U...	20662	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
10	07/27/2013 11:58:04	192.168.4.227	212.23.115.148	17 (U...	48020	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet
11	07/27/2013 11:52:10	192.168.4.227	212.23.115.132	17 (U...	62147	53 (do...	intruder de...	Sofort	Paket verworfen; SNMP gesendet

You will find the following functions in the **Event log** menu:

- **Refresh**: Updates the displayed information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

View DHCP table

You can view the DHCP table for a certain device. Detailed information is recorded:

IP address

IP address of the local network device

MAC address

MAC address of the local network device

Timeout

Lease for the address assignment in minutes.

Host name

Names of the local devices on your network (if known)

Type

Type of assignment

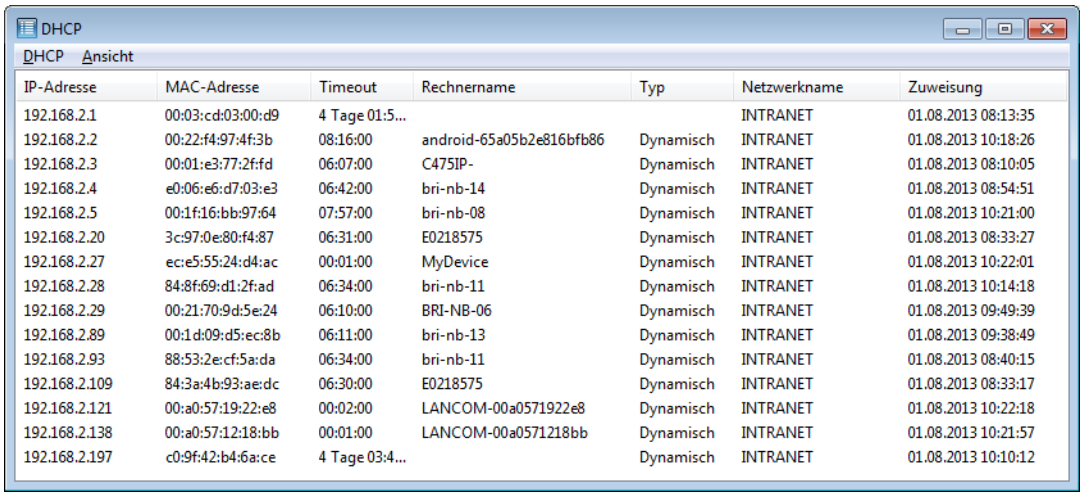
- **New**: The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.
- **Unknown:** When the server checked if the address was unique, it was found that the address had already been assigned to another client. Unfortunately, the DHCP server does not have any way of obtaining further information about this client.
- **Static**: A client has informed the DHCP server that it has a fixed IP address. This address may not be used for any other clients in the network.
- **Dynamic**: The DHCP server has assigned an address to the client.

Network name

Displays the name of the network that the local network device is connected to

Assignment

Date and time of the address assignment.



You will find the following functions in the **Accounting** menu:

- **Refresh**: Updates the displayed information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

Show accounting information

You can view the accounting information for a certain device. The accounting information is a protocol of the connections from each station in the LAN to remote sites in the WAN. Detailed information is recorded:

User

The connection name, usually the name of the network device that has established a connection via the selected device.

Remote site

Name of the remote site to which the selected device has established a connection.

Type

Type of connection

Connections

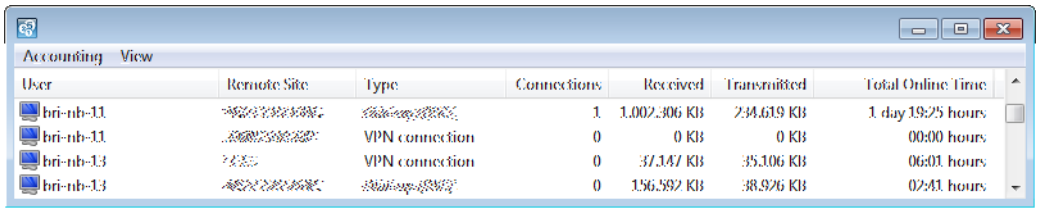
Number of connections of a certain type that are currently open to the listed remote site.

Received, transmitted

The amount of data that the user has received/transmitted within the connection time.

Total online time

Total online time in hours, minutes, and seconds.



You will find the following functions in the **Accounting** menu:

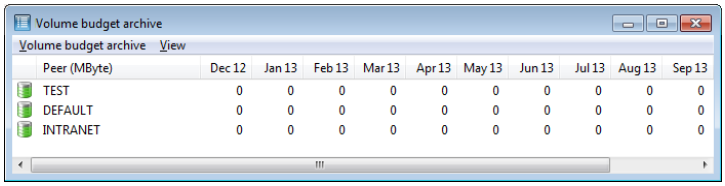
- **Reset**: Clears all accounting information and resets all counters to '0'.
- **Refresh**: Updates the displayed information.
- **Save accounting information**: Stores the displayed accounting information to a location of your choice in a suitable file format (*.acc).
- **Load accounting information**: Loads a saved file with accounting information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.
- **Accounting list (current)**: Displays the current accounting list.
- **Accounting list (last billing period)**: Shows the accounting list for the last accounting period.

View volume budget archive

Displays the volume budget archive of all WAN interfaces.



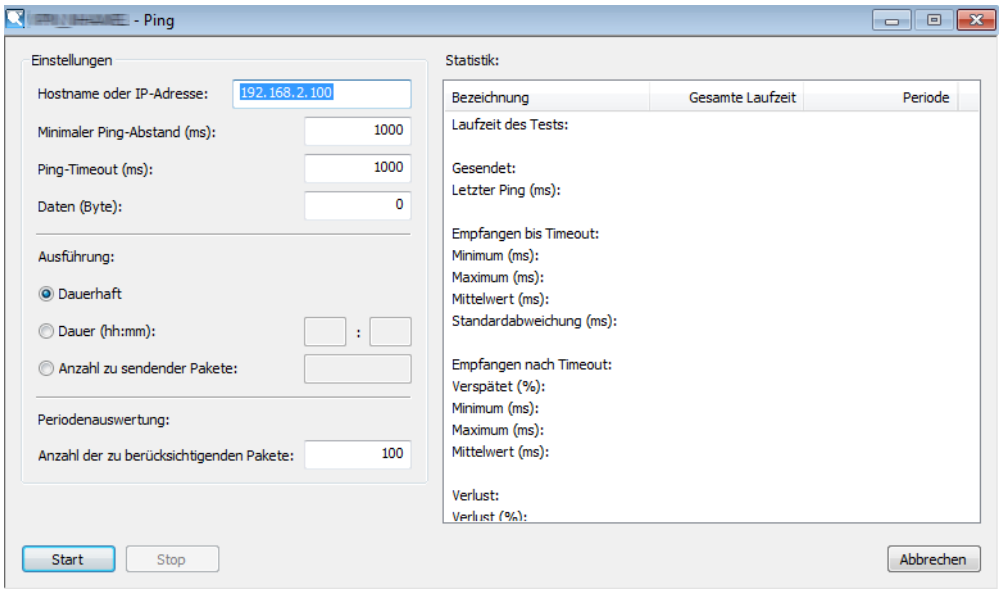
Reset time and charge limit

This is where you can reset the time and charge limit of the marked device to zero. The time and charge counter restart from zero even if the period for the limit has not been reached.

Ping

You can use LANmonitor to check the connection quality between stations in the LAN, WAN or WLAN. LANmonitor sends ping command from the computer on which it is installed to the remote site at regular intervals. The responses it receives are the basis for a compiled report.

To enter the parameters and display the results of the ping test, LANmonitor has a dedicated dialog.



Configuring ping

- **Host name or IP address**: The remote site which is to be queried by Ping is entered here. The following information can be entered for all of the different network devices (servers, clients, routers, printers, etc.) which can be reached via LAN, WAN or WLAN.

If a device is selected when the Ping dialog is opened with Device > Ping or via the context menu in LANmonitor, then the IP address of this device is assumed to be the remote site.

- **Minimum ping interval**: The time interval between two consecutive pings in [ms].

The interval between two pings cannot be less than the packet transmission time, i.e. before sending a ping, the previous ping must have been answered or the ping timeout must have expired.

- **Ping timeout**: The time waited for the response to a ping to arrive [ms]. If this time expires and no response was received then the ping is assumed to be lost.
- **Data**: The size of a ping packet [bytes]. A "ping" is an ICMP packet which is generally transmitted without any content, i.e. it is just a header. To increase the load of the packets used for testing a connection, a payload can be created artificially. The overall packet size then consists of an IP header (20 bytes), an ICMP header (8 bytes) and the payload.

The packets will be fragmented if the payload of the ICMP packets exceeds the maximum IP packet size.

- **Execution**: Repeat mode for the ping command. You have the option to stop the ping transmission manually, after a certain period, or after a specified number of sent data packets.
- **Period evaluation**: The right-hand portion of the Ping dialog displays the results of the ping test. The first column shows the sum values over the entire test; the second column shows only the values collected over the evaluation period, i.e. the sum of the most recent packets. Unanswered pings are not included in the evaluation.

The period evaluation considers only the pings sent during the defined period.

Statistics

The following information is displayed for evaluation:

- Test run time: The total run time [hr./ min./ sec.]
- Transmitted: Total number of pings sent
- Run time of the last ping [ms]
- Received until timeout: The number of pings answered in the timeout period
- Minimum runtime
- Maximum runtime
- Average
- Standard deviation from the mean run time
- Received after timeout: The number of pings answered after the timeout period
- Late packets as a proportion of the total number
- Minimum runtime
- Maximum runtime
- Average
- Lost
- Last error

Create trace output

This option starts the trace output in LANtracer.

Please also refer to *LANtracer – tracing with LANconfig and LANmonitor* on page 289.

Show spectral scan

This menu item starts the spectral scanning module in the selected device. The results are displayed by LANmonitor's internal Web browser. More information about its configuration is available under *Functions of the software module* on page 983.

Setting up point-to-point WLAN antennas

If the selected device is equipped for WLAN, you can align the point-to-point WLAN antennas.

This menu item is only visible in LANmonitor if the monitored device has at least one base station defined as a remote station for a P2P connection (in LANconfig under **Wireless LAN** > **General** > **Physical WLAN settings** > **Point-to-Point**).

Antenna alignment for P2P operations

The precise alignment of the antennas is of critical importance for establishing P2P connections. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better is the actual power and the effective bandwidth. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result.

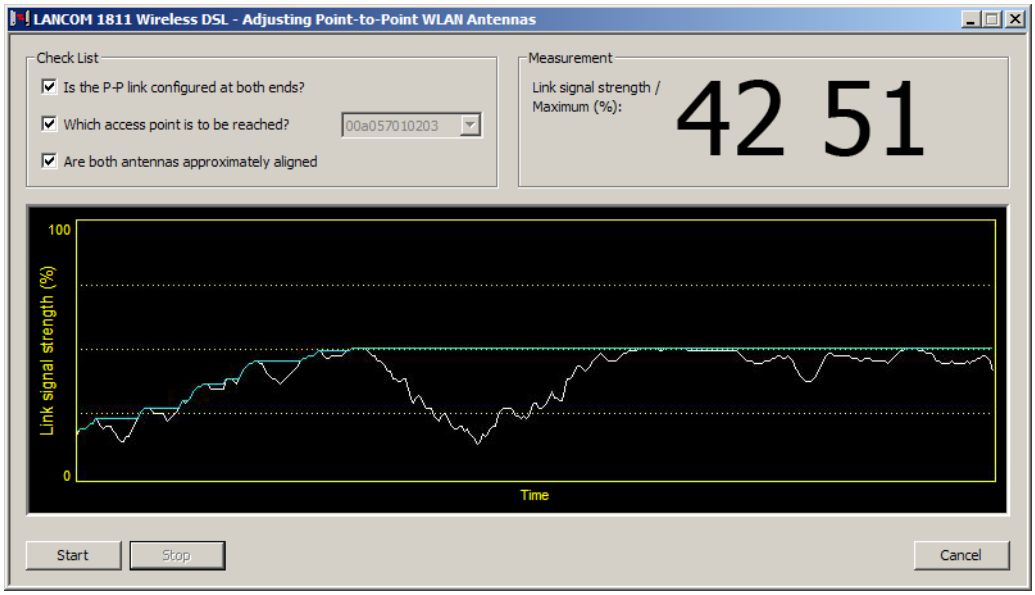
The current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor in order to help find the best possible alignment for the antennas.

The display of signal quality with the LEDs must be activated for the physical wireless LAN interface. The faster the LED blinks the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double the frequency indicates that the signal strength is twice as high).

In the dialog for setting up point-to-point connections, LANmonitor prompts for the information required to establish the P2P connection:

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Which access point is to be monitored? All of the base stations defined as P2P remote sites in the device concerned can be selected here.
- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The trend of the signal strength over time and the maximum value are also displayed in a diagram.



Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

Configure

Start LANconfig to configure the selected device.

Start the web browser

Starts the default web browser to configure the selected device via WEBconfig.

Show content filter categories

If your device is equipped with an activated content filter module, you use this menu item to access the content filter categories.



You will find the following functions in the **Content filter categories** menu:

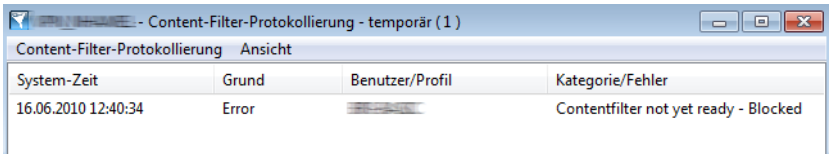
- **Reset**: Clears all displayed information and resets all counters to '0'.
- **Refresh**: Updates the displayed information.
- **Save category information**: Stores the displayed category information to a location of your choice in a suitable file format (*.acc).
- **Load category information**: Loads saved categories information from a file.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.
- **Show content filter categories (current)**: Displays the current status of the content filter categories.
- **Show content filter categories (last snapshot)**: Displays the status of the content filter categories at the last snapshot.

Show content filter log

If your device is equipped with an activated content filter module, you use this menu item to view the content filter log.



You will find the following functions in the **Content filter logging** menu:

- **Reset**: Deletes the displayed information.
- **Refresh**: Updates the displayed information.
- **Close**: Close the information window.

You will find the following functions in the **View** menu:

- **Always on top**: The window always stays in the foreground.

Properties

This menu item opens the Properties dialog for the selected device. A number of pages here allow you to inspect or adjust various global and device-specific settings.

The dialogs are largely identical to those under **File** > **Add device**. For this reason, this section covers only those pages that appear in the Properties dialog. For all other pages, see

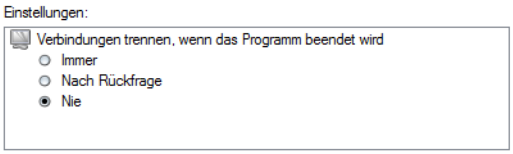
- *General* on page 250
- *Protocols & logins* on page 251
- *View* on page 252
- *Logging* on page 252

Information

This page contains more information about the manufacturer and device.

Advanced

On this page you will find advanced settings.



Under **Disconnect all lines when the program shuts down**, you set whether LANmonitor disconnects active connections between the device and remote sites when you exit the program.

- **Always**: LANmonitor always disconnects without asking.
- **Prompt**: LANmonitor disconnects only after prior confirmation by the user.
- **Never**: LANmonitor does not disconnect. The connections remain active.

3.2.4.3 View

This menu item is used to customize the behavior of the LANmonitor graphical user interface.

Always on top

If you enable this setting, the window always appears in the foreground.

Show status in systray

If you enable this option, LANmonitor displays the device status (error) in the systray.

Minimize LANmonitor to systray

If you enable this setting, LANmonitor is moved to the systray instead of the taskbar when minimized.

Toolbar

Hides or displays the toolbar. Please also refer to *The toolbar in LANmonitor* on page 268.

Show

This menu item is used to enable or disable the display of the following information:

- Error messages
- Diagnostic messages
- System information

Many important details on the status of a device are only shown if the display of system information is activated. This includes, among others, the interfaces and charge management. For this reason we recommend that interested users should activate the display of system information.

3.2.4.4 Tools

This menu item is used to open the information stored by selected information windows (e.g. syslog or accounting logs) and to start the other program components of the LANtools.

Start LANmonitor (temporary)

Opens a new LANmonitor window to temporarily monitor devces. When LANmonitor is closed the settings of the temporary LANmonitor window will be lost.

Start WLANmonitor

This starts WLANmonitor. Refer to chapter *WLANmonitor – monitoring wireless devices* on page 273 for more information on this.

Start LANconfig

This starts LANconfig. Refer to chapter *LANconfig – configuring devices* on page 173 for more information on this.

Open device logging file

Opens the backup of an activity log log file for viewing. Please also refer to *View device activities* on page 256.

Open accounting file

This is where you can load an accounting file. Please also refer to *Show accounting information* on page 261.

Open SYSLOG file

This is where you can load a system log file. Please also refer to *View syslog* on page 257.

Analyze trace output

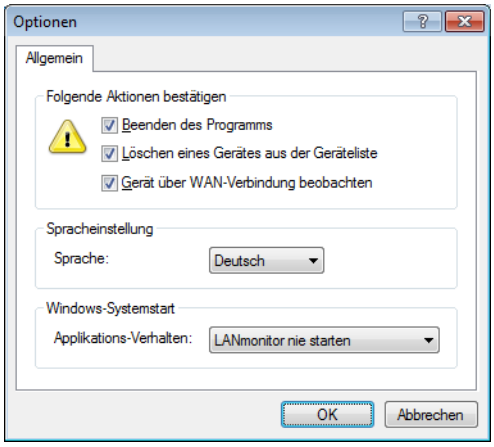
This starts LANtracer. Refer to chapter *LANtracer – tracing with LANconfig and LANmonitor* on page 289 for more information on this.

Ping

Click on this item to start a ping test. Please also refer to *Ping* on page 262.

Options

This item is for editing the settings for the confirmation of actions, the language setting and the behavior of the application at Windows startup.



- **Confirm the following actions**: Specify which actions need to be confirmed by the user.
- **Application language**: Select the language for the graphical user interface (English, German or Spanish).
- **Windows system startup**: Choose how LANmonitor should behave when you start Windows.

3.2.4.5 Help

This menu item offers help about the program and displays information about the software.

Help topics

This menu item gives you access to the help topics. Alternatively you can press F1.

Info

This menu item shows you which software version you are operating and its build date.

3.2.5 The toolbar in LANmonitor



The toolbar in WLANmonitor provides the following functions:

- Add device
- Find devices
- Delete device
- Collapse devices
- Expand devices
- Show accounting information
- View IPv4 firewall event log
- View VPN connections
- View device activities
- Ping
- Create trace output
- Show spectral scan
- Start LANmonitor (temporary)

- Start WLANmonitor
- Minimize all windows to systray
- QuickFinder

You can show or hide the toolbar with the menu item **View** > **Toolbar**.

3.2.6 LANmonitor context menu

The context menu for each device added to the LANmonitor contains the same functions as the **Device** menu in the menu bar. It also contains the **Delete** function allowing a device to be removed from the LANmonitor view.

3.2.7 LANmonitor keyboard shortcuts

Ins	Add device
Del	Delete device
F3	Find devices
F5	Refresh all devices
Alt+F4	Exit
Arrow up	Move up one entry in the list of devices
Arrow down	Move down one entry in the list of devices
Arrow left, ENTER	Collapse menu tree in the device list
Arrow right, ENTER	Expand menu tree in the device list
Ctrl+F5	Refresh display
Space	Device > Options
F7	Tools > Options
F1	Help topics

3.2.8 LANmonitor application concepts

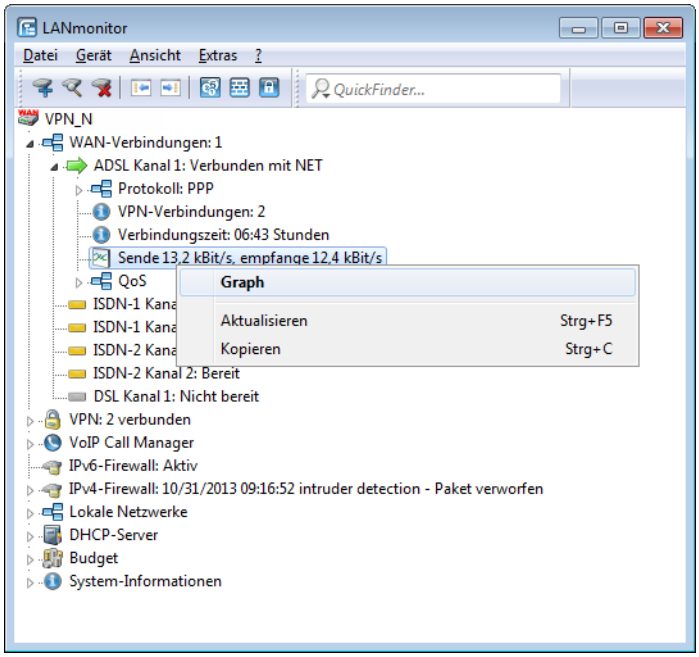
This section describes various applications of LANmonitor.

3.2.8.1 Performance monitoring with LANmonitor

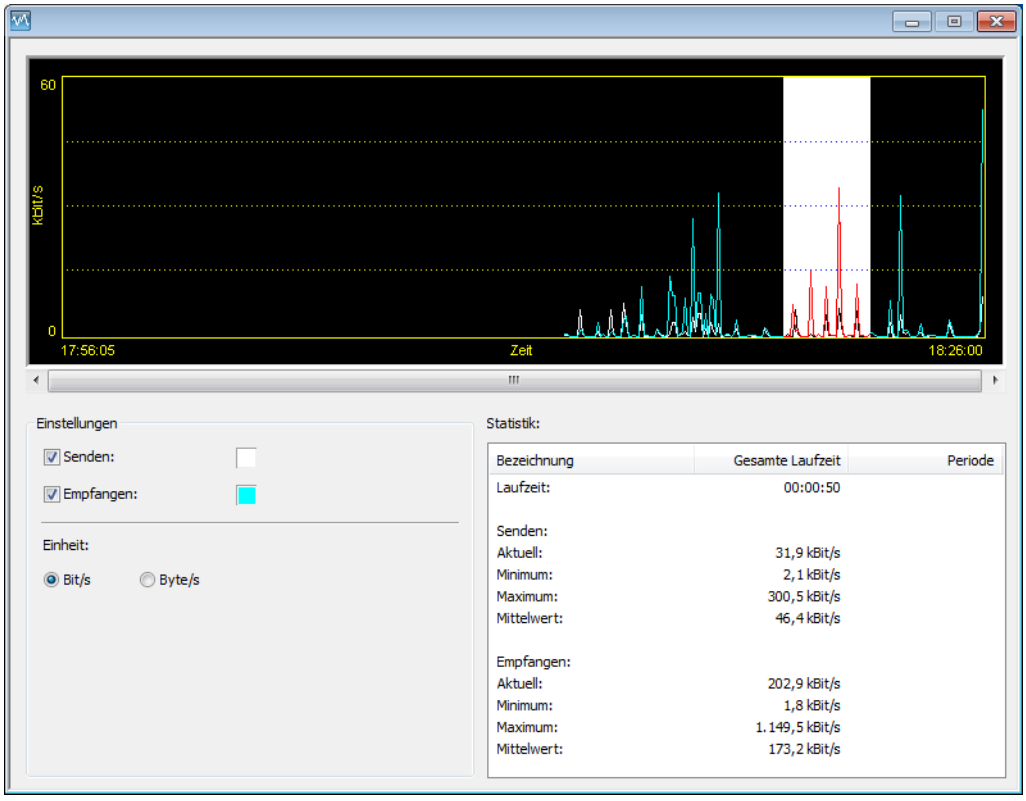
LANmonitor is able to record various parameters of a device and to represent them graphically in the form of a curve. These include among others:

- Transmit and receive rates for WAN connections
- Transmit and receive rates for point-to-point connections
- Signal reception strength for point-to-point connections
- Link signal strength for point-to-point connections
- Throughput for point-to-point connections
- CPU load
- Free memory
- Temperature (not available on all models)

LANmonitor displays the current values of a parameter in the device overview directly in the corresponding group branch. To start the graphical display, open the context menu for a parameter and select **Graph**.



An additional window is opened, which shows variation of of the parameter over time.



By using the left mouse button to mark a time period on the current graph, the statistics for these values are displayed separately.

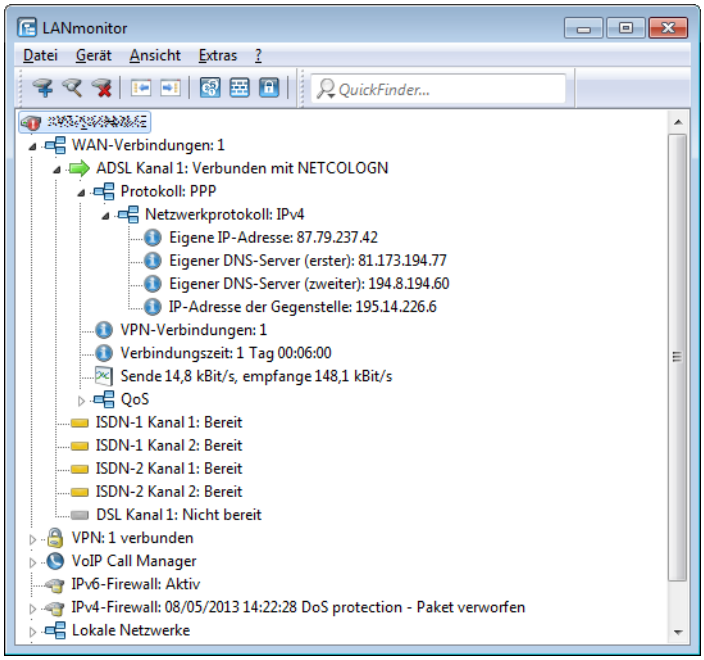
Please note that the values on display are deleted when the dialog is closed. For monitoring over a longer period, leave the window open. The dialog displays at most the values over the last 24 hours.

3.2.8.2 Check Internet connection

This section provides an example of how LANmonitor works by demonstrating the kind of information that it can supply about your Internet provider.

1. Start LANmonitor, for example with a double click on the desktop icon.
2. Add a new device with **File** > **Add device** and, in the window that opens, enter the IP address for the device that is to be monitored. If the configuration of the device is password protected, you can enter the password here. LANmonitor automatically creates a new entry in its list of devices and it initially shows the status of the connection channels.
3. Start your web browser and enter any web address.
4. Return to LANmonitor and open the branch **WAN connections** for the device. Under **ADSL channel x:** Under **Connected with...**, LANmonitor shows you which channel is used to make the connection and also the remote site that is contacted.

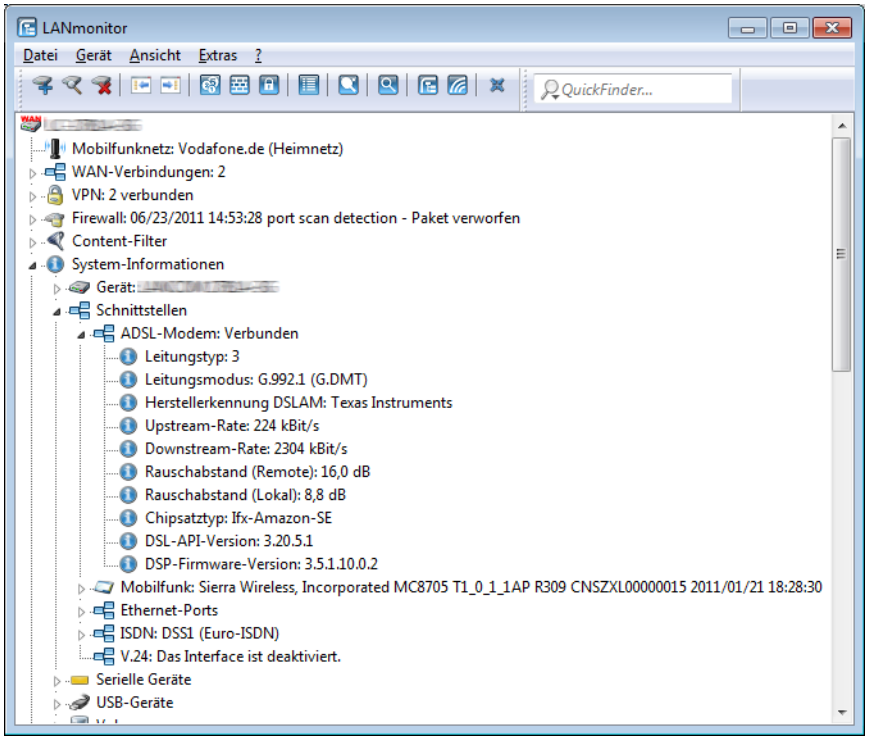
As soon as the connection is established, the communication channel is displayed with a plus sign in front of it, indicating that information is available for this channel. By clicking on the plus sign or double-clicking on an entry, you open a tree-like structure that displays various information.



- This example illustrates how the protocol information on PPP shows the IP address the provider has allocated to your router and the addresses of the DNS servers.
- Under the general information you can observe the data transfer rates of the current Internet connection.
- Right-click with the mouse on the active channel and you can manually terminate the connection. You may require the configuration password for this.
- If you wish to log the LANmonitor output to a file, you can start the activity log (also see *View device activities* on page 256).

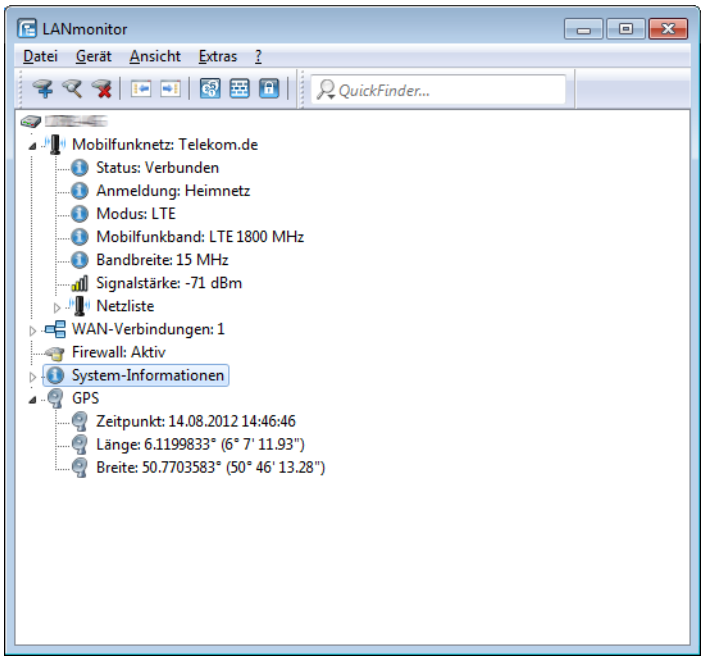
3.2.8.3 Show the current protocol for the ADSL/VDSL interface

For devices with an integrated ADSL/VDSL modem, LANmonitor's **System information** displays the ADSL standard currently being used. Switch to the **Interfaces** branch and select **ADSL/VDSL modem**.



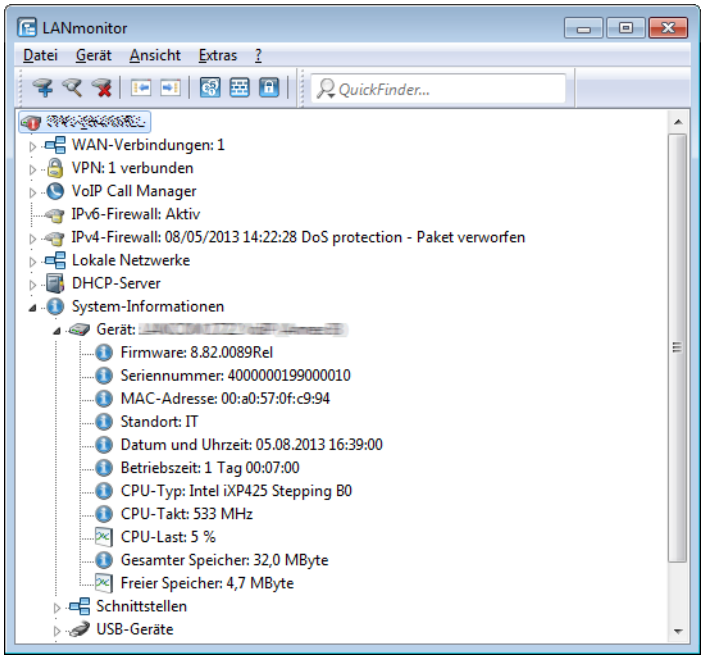
3.2.8.4 Display of the GPS time

As of LCOS version 8.80, LANmonitor gives you the option to display the time received from the GPS network. Navigate to the **GPS** section for the device in LANmonitor. The current GPS time is displayed under **Timestamp**.



3.2.8.5 Querying CPU and memory utilization via SNMP

LANmonitor uses SNMP to query and display CPU load and memory utilization of a device. Open the menu tree of a device, switch to **System information** and open the branch **Device: …**.



3.2.8.6 Password protection for SNMP read-only access.

Read-only access to a device via SNMP – for example with LANmonitor – can be password protected. This uses the same user data as that used to access LANconfig. Password protection of SNMP access means that the user data must be entered before information about the device status, etc. can be accessed over SNMP.

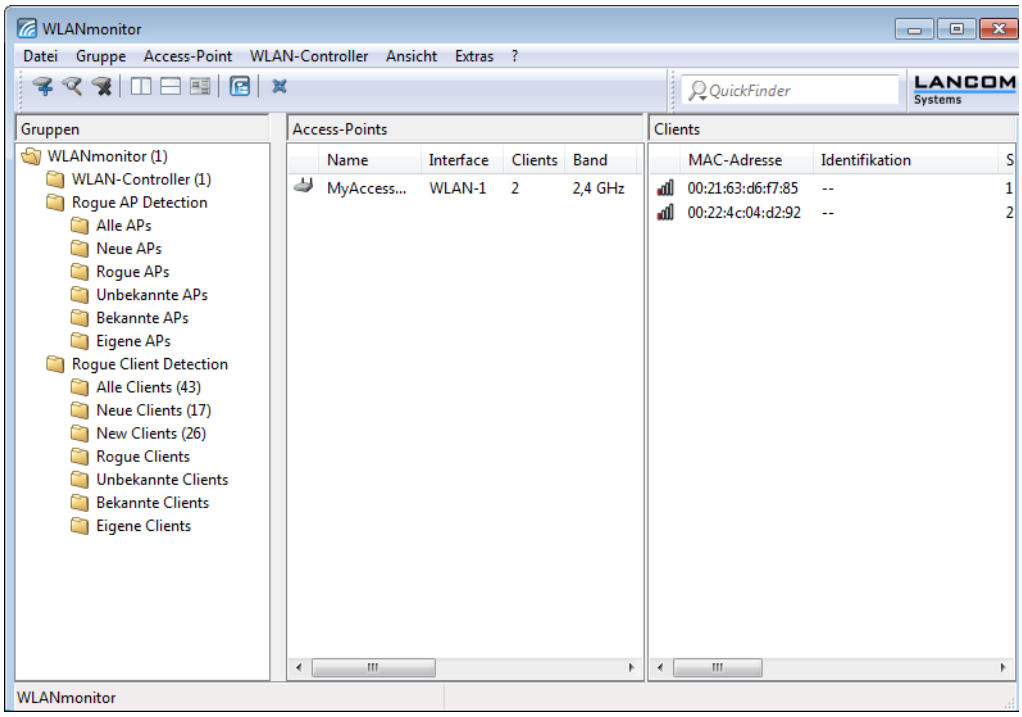
User information can be entered in LANmonitor separately for each device. To do this, click with the right-hand mouse key on the required device, select the **Options** item from the context menu and enter your user data.

Access rights in LANmonitor depend on the rights possessed by the user.

3.3 WLANmonitor – monitoring wireless devices

WLANmonitor is a separate component of LANmonitor. This program is for the central monitoring of the status of a wireless network (WLAN). It provides access to information about the entire network in general and detailed information about individual WLAN controllers, access points, and associated clients. This program also helps you to detect third-party access points (*Rogue AP detection*).

WLANmonitor also provides the option to collect access points into groups. These groups may consist of access points gathered in buildings, departments, or at particular locations. In particular with large WLAN infrastructures, this helps to keep an overview of the entire network.



The program interface of WLANmonitor is divided into three columns:

The left column (**Groups**) contains a number of predefined group folders, which WLANmonitor uses to automatically categorize the different types of devices. You can rename these groups as you like, or create additional groups.

The middle column (**Access points**) lists the access points found by the WLANmonitor. Also display is key information about each access point.

- Name of the access point
- Active physical interface(s)

  Devices with multiple WLAN modules appear multiple times in the list. Each WLAN module has its own separate entry.
- Number of clients associated with it
- The frequency band used
- The channel in use
- The transmission power measured by the device
- The noise level measured by the device
- The current channel load
- IP address of the access point
- The activation status of the *Background scan*

The right-hand column (**Clients**) lists the clients that are logged in to the selected access point. The following information is shown for each client:

- Connection quality as a bar chart
- MAC address of the WLAN client
- Identification or name of the logged-in clients, if these are entered into the access list or a RADIUS server.
- Connection signal strength
- Name of the access point that the client is logged on to

- Name of the WLAN network (SSID)
- Encryption method used for radio communication
- WPA version (WPA-1 or WPA-2)
- Transmit rate (TX)
- Receive rate (RX)
- Last error that occurred with the client
- IP address of the WLAN client

If no access point has been selected or if the respective access point has no clients, LANmonitor instead displays all existing clients.

3.3.1 Start WLANmonitor

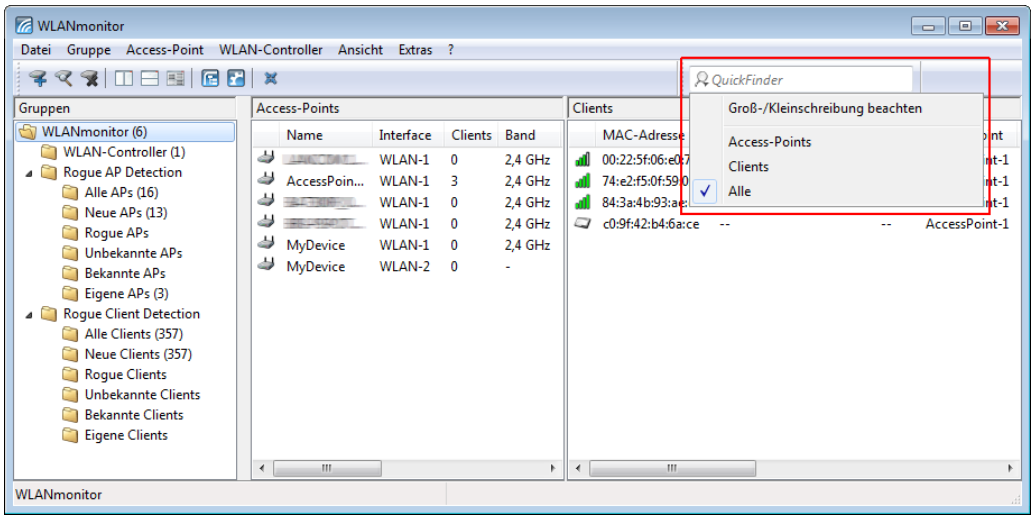
WLANmonitor is a component of LANmonitor. Start the WLANmonitor from LANmonitor using the **Tools** > **Start WLANmonitor** menu item; you can do this via the corresponding button in the LANmonitor toolbar or directly from the desktop icon.

Alternatively, WLANmonitor can be started from the console with the following command: `[installation path]lanmon -wlan`

If you are running LANconfig, you can also start WLANmonitor by right-clicking with the mouse on a WLAN device and selecting **Monitor WLAN device**.

3.3.2 QuickFinder in WLANmonitor

WLANmonitor includes access points and WLAN clients. Clicking on the magnifying glass on the left side of the search window opens a context menu to select the type of search. Depending on the application you can search for access points only, clients only, or all entries.



3.3.3 Rogue detection

WLANmonitor enables you to detect so-called "rogue access points (APs)" and "rogue clients" in your network. WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues.

- **Rogue clients** are computers equipped with WLAN adapters that are located within the range of a WLAN and attempt to log on to one of the access points in order, for example, to use the Internet connection or gain access to secured areas on the network.
- **Rogue APs** are access points that, for example, a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to

potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least they are a disturbance, and so they need to be identified to decide whether further measures in securing the local network need to be introduced. Information about the clients within range of your network is automatically stored to an internal table in the access point. Once activated, **background scans** record neighboring access points and list them to the scan table. Also see the chapter *Enabling background scans for access points* on page 288.

WLANmonitor conveniently processes this information by dividing the access points and clients into categories such as 'Known', 'Unknown' or 'Rogue'.

3.3.3.1 The group "Rogue AP detection"

WLANmonitor organizes any rogue access points into the following pre-defined (sub) groups:

- **All APs**: Contains the overview of the APs in all of the scanned WLANs and thus represents the superset of all subsequent groups. The APs are colored according to their grouping.
- **New APs**: Contains new unknown and unconfigured WLANs. The relevant APs are yellow in color.
- **Rogue APs**: Contains WLANs that are identified as rogue and require immediate observation. The relevant APs are red in color.
- **Unknown APs**: Contains WLANs that require further investigation. The relevant APs are gray in color.
- **Known APs**: Contains WLANs that pose no risk. The relevant APs are gray in color.
- **Own APs**: Contains new affiliated WLANs from APs monitored by WLAN monitor. The relevant APs are green in color.

If a parameter is changed on an AP, e.g. the security settings, then it is displayed again as a newly discovered AP.

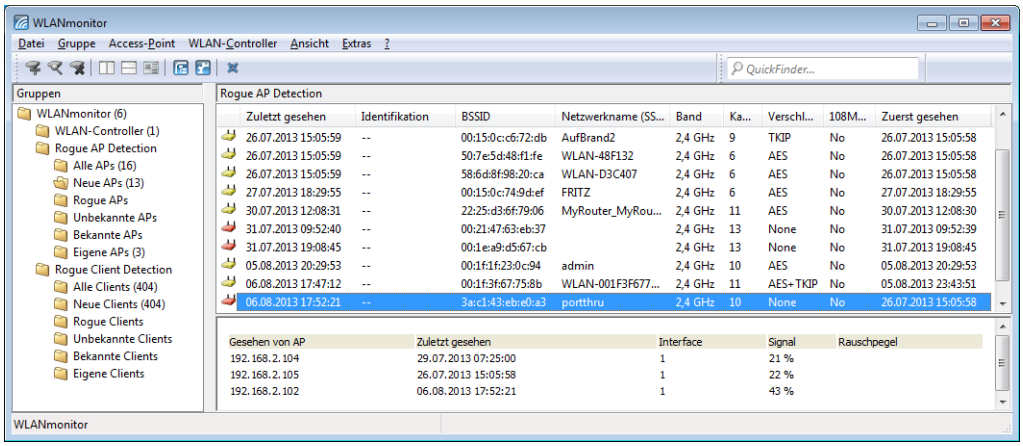
Within each group, WLANmonitor displays the following information about the rogue APs:

- Time of first and last detection
- Name of the AP (identification)
- MAC address of the AP for this WLAN (BSSID)
- Name of the WLAN (SSID)
- The frequency band used
- The channel in use
- Encryption method used for radio communication
- Use of the 108 Mbps mode

When you click a list entry, WLANmonitor displays the following details:

- IP addresses of the APs scanned by the WLAN in question
- The time when last seen or of the last scan
- WLAN interface used to perform the scan
- Signal strength of WLAN reception by the APs
- Noise level

You have the option to move the found WLANs into an appropriate group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button), with the exception of the group **All APs**.



3.3.3.2 The group "Rogue client detection"

WLANmonitor organizes any rogue clients into the following pre-defined (sub) groups:

- **All clients**: Contains the overview of all discovered clients and thus represents the superset of all subsequent groups. The clients are colored according to their grouping.
- **New clients**: Contains new unknown clients. The relevant clients are yellow in color.
- **Rogue clients**: Contains clients that are identified as rogue and require immediate observation. The relevant clients are red in color.
- **Unknown clients**: Contains clients that require further investigation. The relevant clients are gray in color.
- **Known clients**: Contains clients that pose no risk. The relevant clients are gray in color.
- **Own clients**: Contains new own clients associated with access points being observed by the WLANmonitor. The relevant clients are green in color.

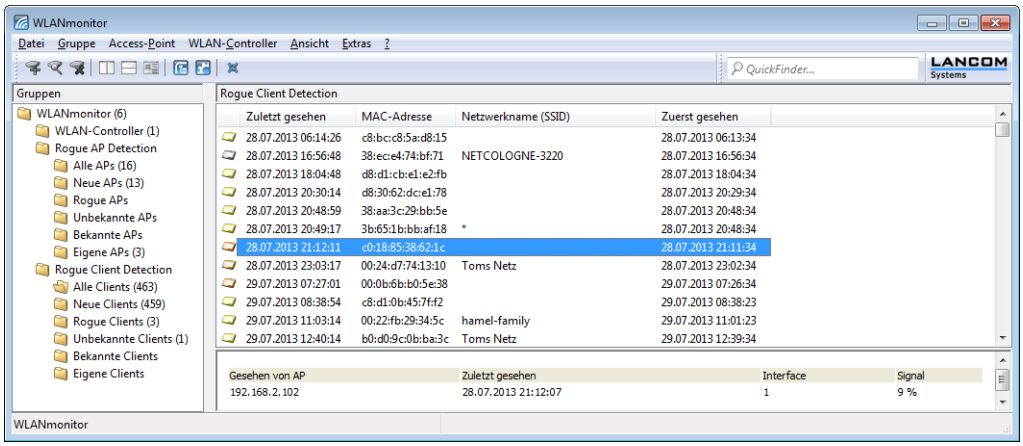
Within each group, WLANmonitor displays the following information about the rogue clients:

- Time of first and last detection
- MAC address of the client
- Name of the WLAN network (SSID)

When you click a list entry, WLANmonitor displays the following details:

- IP address of the access point that saw the client
- Time when last seen
- WLAN interface used to discover the client
- Signal strength with which the APs received the WLAN network

You have the option to move the found clients into an appropriate group depending on their status. You can set up your own network groups within the individual groups by using the context menu (right mouse button), with the exception of the group **All clients**.



3.3.4 The menu structure in WLANmonitor

The menu bar helps you to manage WLAN devices and their configurations, and you can customize the appearance and functioning of LANconfig.

3.3.4.1 File

This menu item stops LANmonitor.

Exit

Closes and terminates WLANmonitor.

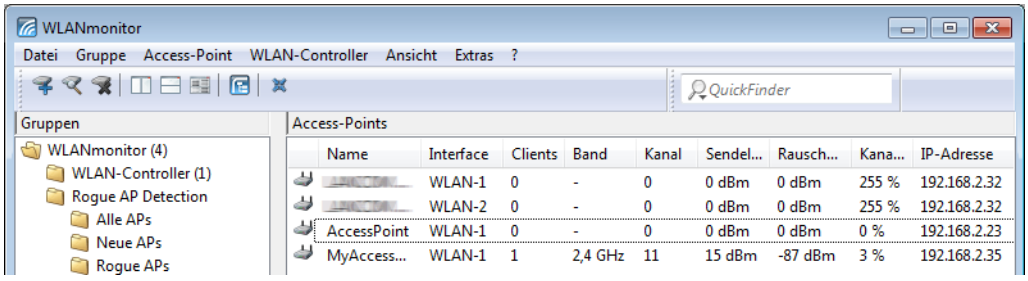
3.3.4.2 Group

Groups are edited with the following functions:

- Add group
- Delete group
- Rename group

WLANmonitor lets you organize all of the available access points in a manner that is independent of their physical location. This helps to maintain an overview of the network and is particularly useful when localizing problems. Further, WLAN information can be called up according to the groups. You can group your access points according to their departments, locations or applications (e.g. public hotspot), for example.

The groups are shown in the left column in WLANmonitor. Starting from the top group 'WLANmonitor', you can use the menu item **File** > **Add group** to create new sub-groups and so build up a structure. Access points found during a search are assigned to the currently selected group in the group tree.



Access points that have been recognized already can be moved to the another group with drag and drop.

The allocation of access points and clients is made easier by marking a device with the mouse. The counterpart(s) will then be marked in the linked list as well:

- If an access point is marked in the access point list, all of the clients logged in to this device will also be marked in the client list.
- If a client is marked in the client list, the access point that it is registered with will be marked in the access point list.

Add group

Adds a group.

Delete group

Deletes a group.

Rename group

This option allows you to change the name of a group.

3.3.4.3 Access point

This menu item is used to manage the access points.

Add access point

Use this menu item to add an access point to the list if WLANmonitor does not automatically detect it. The corresponding setting options are identical to those under LANmonitor, i.e. **File** > **Add device** > **General** (see *General* on page 206).

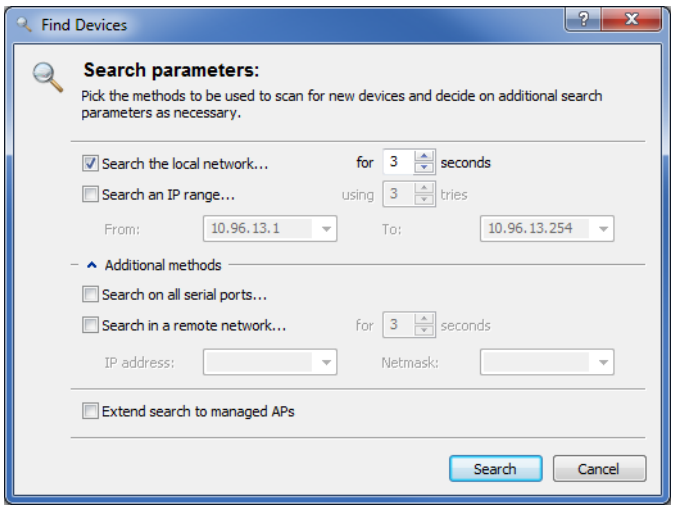
If you save the username and password permanently, any user who is permitted to run WLANmonitor also has access to the device.

Delete access point

Removes the selected access point from the list.

Find access points

This menu item triggers an automatic search for available access points in the network.



Select where you wish to search for devices:

- Search in the local network
- Search in a remote network

  If you wish to search in a remote network you must specify its address and the relevant network mask.
- If necessary, you can extend the search to managed access points (APs).

Click on **Search** to start the search. Any devices found will be added to the list automatically.

If a device is found that is already in the list, it will not be included in the list a second time. For this reason fewer devices may be added to the list than were reported during the search operation.

Refresh all access points

Refreshes the list of all access points.

Refresh display

Updates the information displayed for the selected access point.

Properties

Use this item to display the properties of the selected access point. The corresponding setting options are identical to those under LANmonitor, i.e. **File** > **Add device** > **General** (see *General* on page 206). This page also contains further information about the manufacturer and device.

If you save the username and password permanently, any user who is permitted to run WLANmonitor also has access to the device.

3.3.4.4 WLAN controller

This menu item is used to manage the WLAN controllers in your network.

Add WLAN controller

Under **Groups**, click the **WLAN controller** folder and then select the menu item in the menu bar **Add WLAN controller** in order to add a WLAN controller that WLANmonitor did not automatically detect. The corresponding setting options are identical to those under LANmonitor, i.e. **File** > **Add device** > **General** (see *General* on page 206).

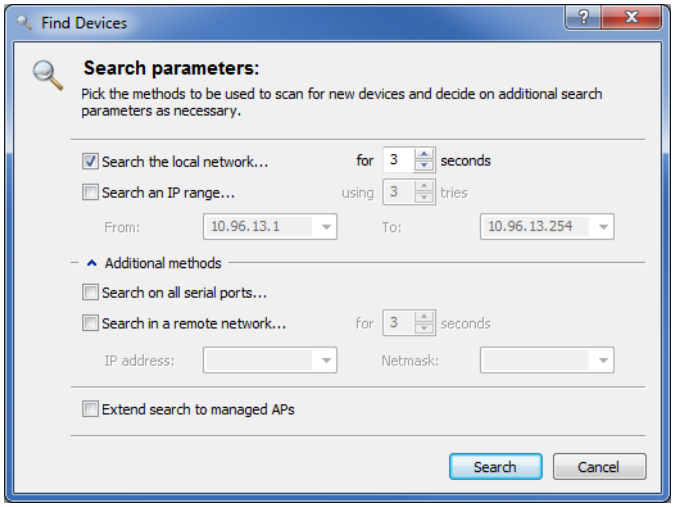
If you save the username and password permanently, any user who is permitted to run WLANmonitor also has access to the device.

Delete WLAN controller

Deletes the selected WLAN controller.

Find WLAN controller

This menu item triggers an automatic search for available WLAN controllers in the network.



Select where you wish to search for devices:

- Search in the local network
- Search in a remote network

  If you wish to search in a remote network you must specify its address and the relevant network mask.
- If necessary, you can extend the search to managed access points (APs).

Click on **Search** to start the search. Any devices found will be added to the list automatically.

If a device is found that is already in the list, it will not be included in the list a second time. For this reason fewer devices may be added to the list than were reported during the search operation.

Refresh all WLAN controllers

Refreshes the list of all WLAN controllers.

Refresh display

Updates the information displayed for the selected WLAN controller.

Properties

Use this item to display the properties of the selected WLAN controller. The corresponding setting options are identical to those under LANmonitor, i.e. **File** > **Add device** > **General** (see *General* on page 206). This page also contains further information about the manufacturer and device.

If you save the username and password permanently, any user who is permitted to run WLANmonitor also has access to the device.

3.3.4.5 View

This menu item is used to customize the behavior of the WLANmonitor graphical user interface.

Show status in systray

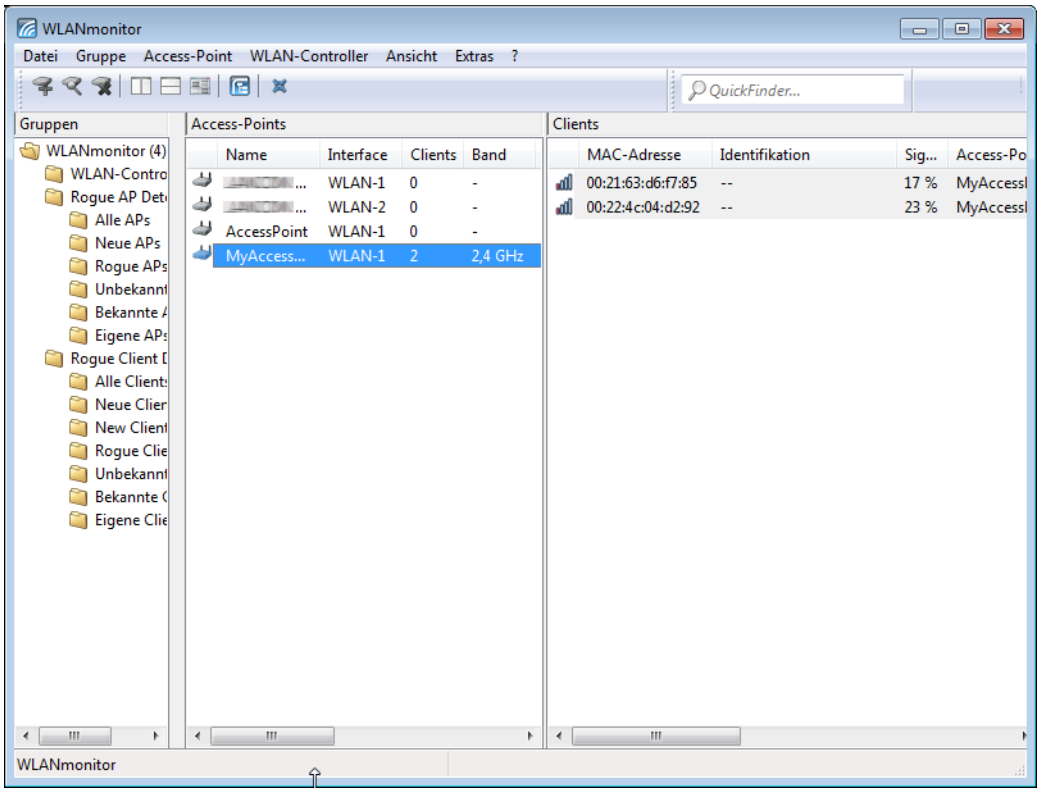
Shows the icon in the system tray.

Minimize WLANmonitor to systray

If you enable this setting, WLANmonitor is moved to the systray instead of the taskbar when minimized.

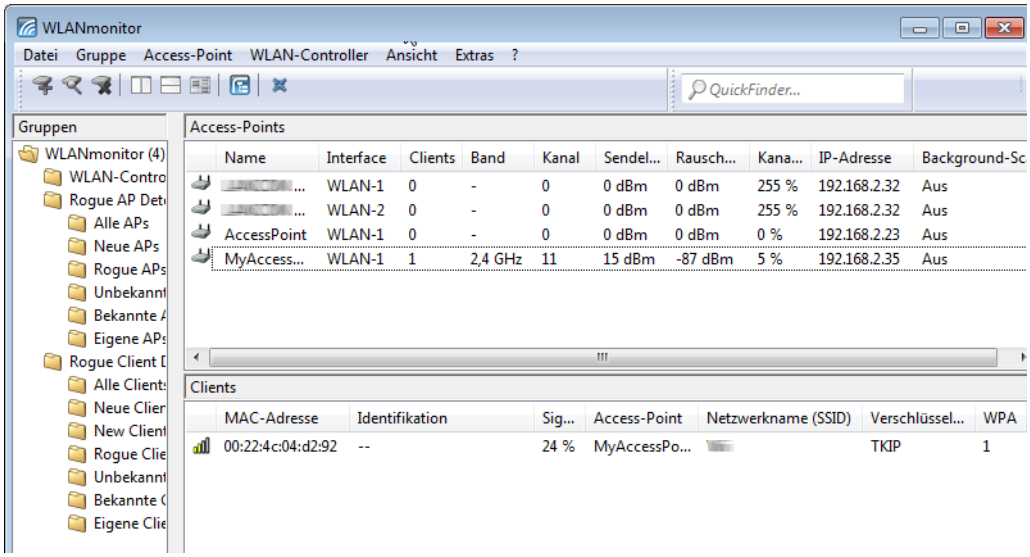
Windows adjust vertical

Adjusts the windows vertically, i.e. so that the lists for access points and clients are displayed next to each other.



Windows adjust horizontal

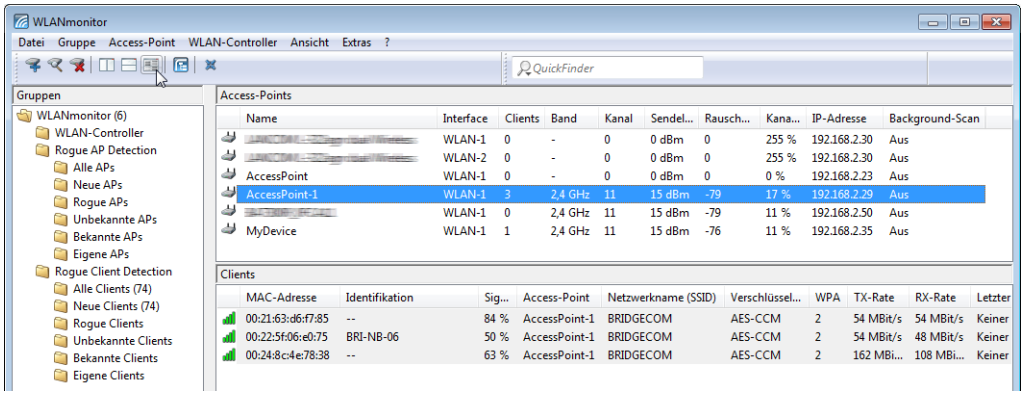
Aligns the windows horizontally, i.e. so that the lists for access points and clients are displayed one above the other.



Mark or filter rows

Use this option to filter the list of access points or clients for display.

- Select an access point and go to the option **View** > **Mark or filter rows**. The list of clients now contains only those clients associated with the selected access point.
- Mark one of the clients and click on the option **View** > **Mark or filter rows**. The list of access points now shows only the access point with which the selected client is associated.



Toolbar

Hides or displays the toolbar. Please also refer to *The toolbar in LANmonitor* on page 268.

Status bar

Hides or displays the toolbar.

3.3.4.6 Tools

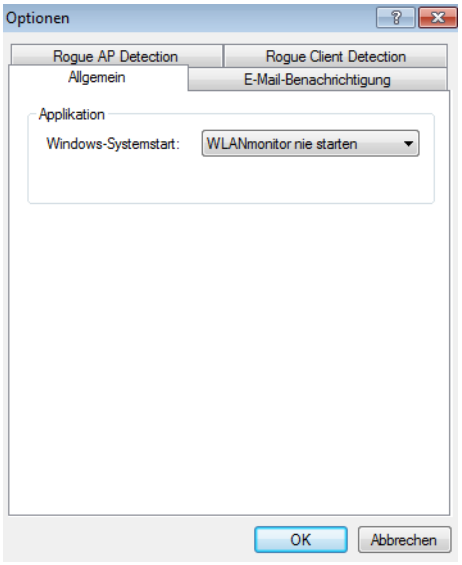
This menu item is used to start the other program components of LANtools and to configure the behavior of WLANmonitor, for example when it discovers unknown or unconfigured access points.

Options

With this menu item, you perform the program-related settings for WLANmonitor.

General

This dialog contains the general settings for the program.



Windows system startup

WLANconfig can be automatically started when the operating system starts. The following **Windows startup** types are available:

- **Start WLANmonitor never**

  The application does not start automatically with the operating system, and it has to be started manually.

- **Start WLANmonitor always**

  The application always starts automatically after Windows starts successfully.

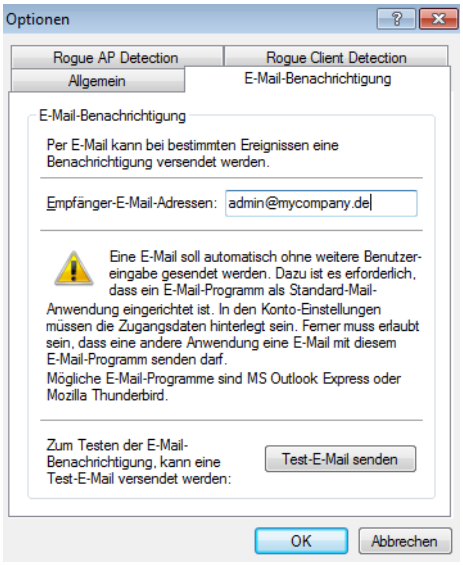
- **Start WLANmonitor like last time**

  The application starts in the same status as when Windows was shut down the last time. If the application was active then it will be started again; if inactive, it will not be automatically restarted.

When changing to a setting that enables the application to be started automatically, a change is made to the operating system's registry. Firewalls applications on the computer or the operating system itself may interpret this change as an attack and may issue a warning or even prevent the entry from being made. In order to allow the desired startup behavior, you can ignore these warnings and allow the changes to be made.

E-mail notification

This dialog contains the settings for the alert function in WLANmonitor.



WLANmonitor can inform the administrator automatically via e-mail whenever an unknown or unconfigured access point is discovered. Activate this option if you would like WLANmonitor to report unknown or unconfigured access points via e-mail.

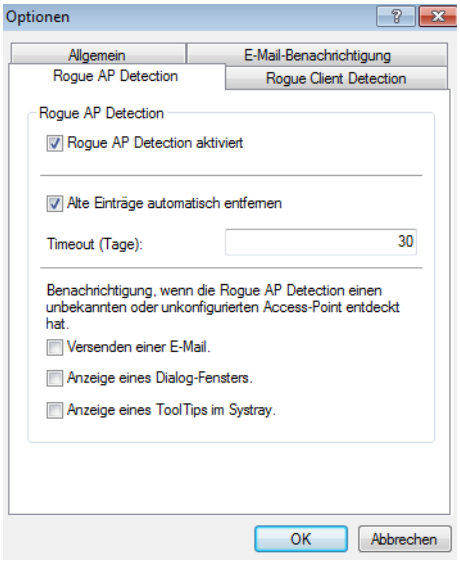
- **Recipient's e-mail address** Enter the e-mail address(es) of the administrators here that should be informed in the event of rogue AP detection. Multiple e-mail addresses should be separated by commas.

In order to send e-mail alerts, the computer on which WLANmonitor is running requires a standard e-mail client (MS Outlook Express or Mozilla Thunderbird) that allows automatic mail transmission to be configured and running.

- **Send test e-mail**: Some mail clients require a confirmation from the user before sending via third-party applications. Test the alert function with this button.

Rogue AP detection

This dialog contains the settings for the "Rogue AP detection". For further information on this feature refer to the section *Rogue detection* on page 275.



The dialog gives you the following options:

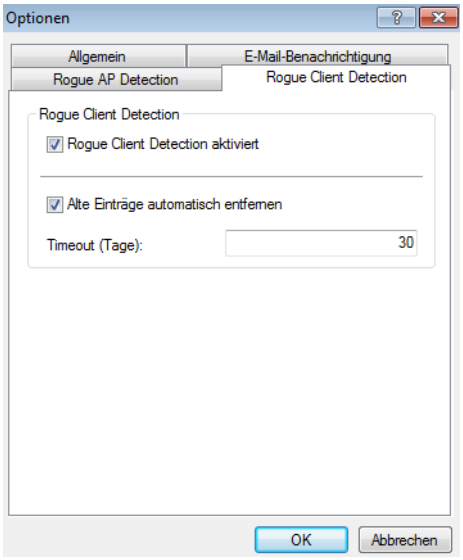
- **Rogue AP detection activated** Activates the automatic search for rogue access points.
- **Remove old entries automatically**: If enabled, WLANmonitor automatically removes entries for access points from the groups that were last seen longer ago than the number of days specified as **Timeout**.

You also have the option to specify how WLANmonitor notifies you of the discovery of an unknown or unconfigured access point.

- **Send notification per e-mail**: Sends a message to the recipient address(es) entered under **E-mail notification**.
- **Display a dialog box**: Opens a pop-up window
- **Display a tooltip in the systray**: Shows a tooltip in the system tray.

Rogue client detection

This dialog contains the settings for the "Rogue client detection". For further information on this feature refer to the section *Rogue detection* on page 275.



The dialog gives you the following options:

- **Rogue client detection activated**: Activates the automatic search for rogue clients.
- **Remove old entries automatically**: If enabled, WLANmonitor automatically removes entries for access points from the groups that were last seen longer ago than the number of days specified as **Timeout**.

Start LANmonitor

This starts LANmonitor. Refer to chapter *LANmonitor – monitoring devices on the LAN* on page 247 for more information on this.

Start LANconfig

This starts LANconfig. Refer to chapter *LANconfig – configuring devices* on page 173 for more information on this.

3.3.4.7 Help

This menu item offers help about the program and displays information about the software.

Help topics

This menu item gives you access to the help topics. Alternatively you can press F1.

Info

This menu item shows you which software version you are operating and its build date.

3.3.5 The toolbar in WLANmonitor



The toolbar in LANmonitor provides the following functions:

- Add device

- Find devices
- Delete device
- Windows adjust vertical
- Windows adjust horizontal
- Mark or filter rows
- Start LANmonitor
- Minimize window to systray
- QuickFinder

You can show or hide the toolbar with the menu item **View** > **Toolbar**.

3.3.6 WLANmonitor context menu

Clicking on a device in WLANmonitor with the right-hand mouse key opens a context menu.

The contents of the context menu depends on the type of the selected device: If an access point is marked, the context menu will resemble the **Access point** menu; if a controller is marked, the context menu will resemble the **WLAN controller** menu.

3.3.7 WLANmonitor keyboard shortcuts

Alt+F4	Exit
Ins	Add group
Del	Delete group
F2	Rename group
Ins	Add access point
Del	Delete access point
F3	Find access points
F5	Refresh all access points
Ctrl+F5	Refresh display
Space	Access point > Options
Ins	Add WLAN controller
Del	Delete WLAN controller
F3	Find WLAN controller
Space	WLAN Controller > Options
F7	Tools > Options
F1	Help topics

3.3.8 WLANmonitor application concepts

This section describes various applications of WLANmonitor.

3.3.8.1 Enabling background scans for access points

In order to identify other access points within the device's local radio range, access points and wireless routers can record the beacons received (management frames) and store them in the scan table. Since this recording occurs in the background in addition to the access points' 'normal' radio activity, it is called a "background scan". Wireless routers in access-point

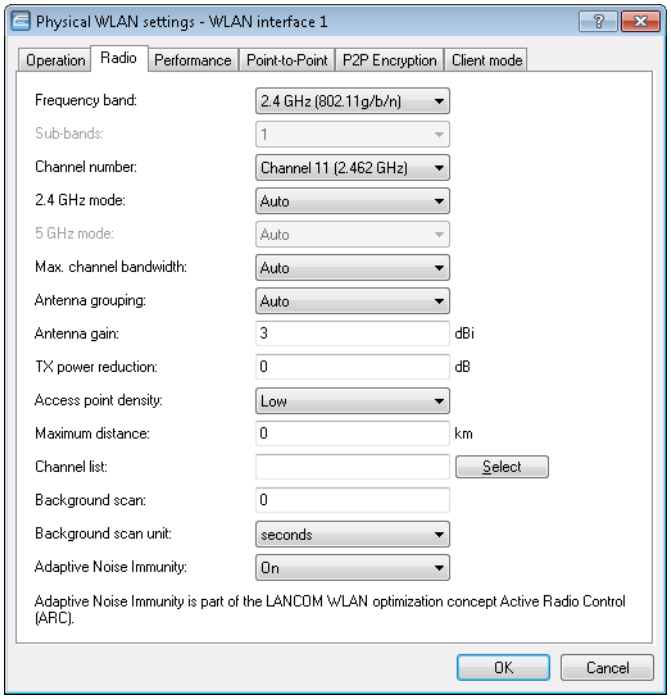
mode normally use the background scan function for rogue AP detection. Without the background scan activated, the rogue detection in WLANmonitor is limited to the detection of rogue clients.

When configuring the background scan, you specify a time period in which all available WLAN channels are scanned once for the receiving beacons. The following tutorial describes how to set this time.

1. Start LANconfig and open the manual configuration dialog for your device.
2. In the dialog **Wireless LAN** > **General**, click **Physical WLAN settings.** and select the WLAN interface for which the background scanning is to be enabled.
3. In the dialog window that opens, navigate to the **Radio** tab.
4. Select a time unit in the selection list **Background scan unit** and enter a corresponding duration in the input field **Background scan interval**.

   This scan interval should correspond to the time span within which rogue access points should be recognized, e.g. `3600 seconds`. The minimum meaningful value in both the 2.4-GHz and the 5-GHz bands is `260 seconds`.

   In the case of 13 possible channels, this value prompts another channel to be scanned each 20 seconds (interval/number of channels).



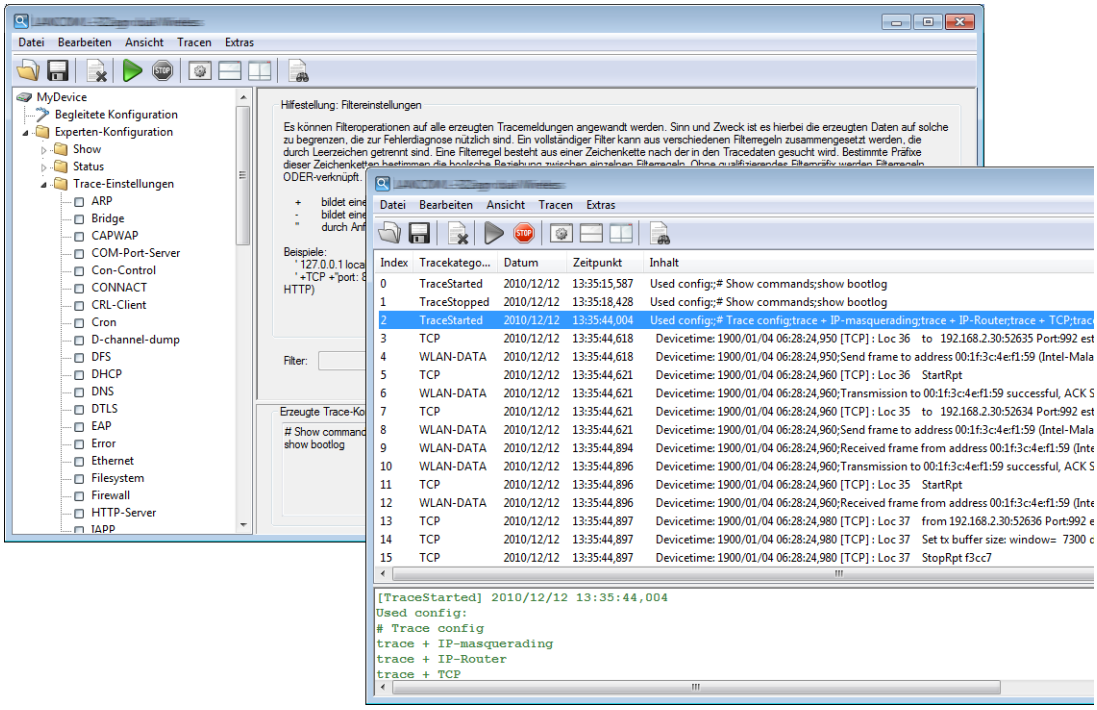
5. Close all of the dialogs and write the configuration back to the device.

That's it! From now on, at the specified scan interval your WLAN device cyclically searches the currently unused frequencies of the active band for available access points.

3.4 LANtracer – tracing with LANconfig and LANmonitor

The trace function in LANconfig and LANmonitor goes beyond the standard trace functions available at the command-line interface and offers greater convenience in the generation and analysis of traces. For example, a trace configuration that activates the relevant trace commands can be stored to a configuration file. An experienced service technician can

set up a trace configuration and provide it to a less experienced user for executing specialized trace requests for a device. Also, the trace results can be saved conveniently to a file for return to the technician for evaluation.



3.4.1 Starting LANtracer

Traces can be executed very easily with LANconfig or LANmonitor. To open the trace window for a device, right-click the device entry and select **Create trace output** from the context menu.

Telnet-access to the device (preferably SSL-secured) needs to be enabled to carry out trace requests with LANconfig or LANmonitor. When starting the trace dialog, LANconfig or LANmonitor first attempts to establish an SSL-encrypted Telnet connection to the device. If the device does not support SSL connections, LANconfig or LANmonitor automatically switches to unencrypted Telnet. If access to the device configuration is password-protected, the access data for an administrator with trace rights is also required.

The **Guided configuration** wizard facilitates the analysis of detailed trace data. The wizard guides you through a number of dialogs, where you simply select the trace parameters for the analysis of certain problems. Once these entries have been completed, the wizard automatic enables the corresponding trace configuration.

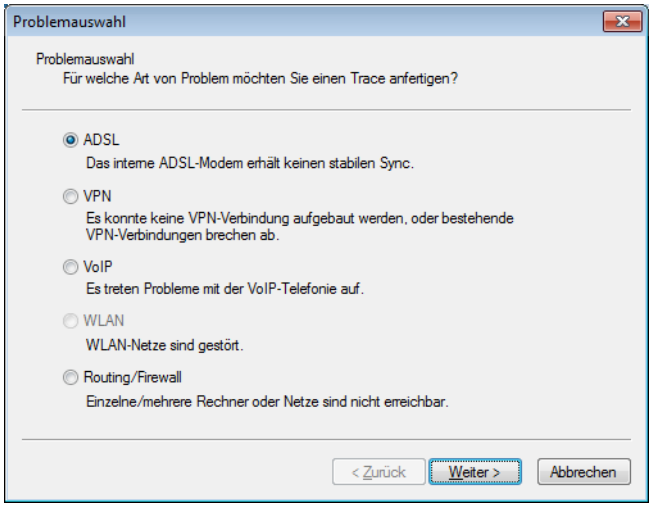
3.4.2 Working with LANtracer

The following chapter describes how to use certain functionalities of LANtracer for outputting and storing traces.

3.4.2.1 Guided configuration of trace output

As an alternative to the expert configuration of the trace output, LANtracer also features an optional guided configuration. This Wizard simplifies the setup of trace output by displaying a selection of potential problems for which you need diagnostic information. The Wizard then sets the necessary parameters and settings for you in the expert configuration.

The Wizard is started from the left-hand part of the LANtracer window by clicking **Guided configuration** > **Start wizard**. Navigate further by using the **Problem selection**.



3.4.2.2 Expert configuration of trace output

Going beyond the settings of the **Guided configuration**, traces and other displays can be set up precisely using the Expert configuration. The Expert Configuration is divided into three areas: ***Show***, ***Status*** and ***Trace properties***.

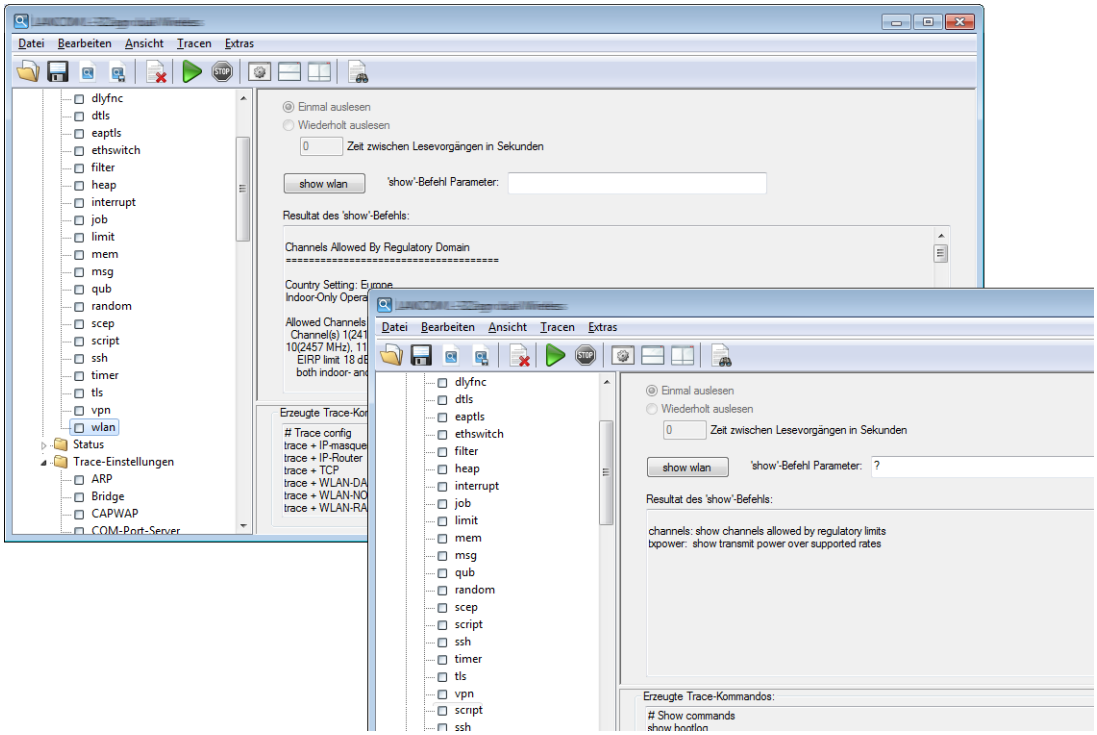
Show

Relevant information can be retrieved from any device type using Show commands, which are usually applied at the command line (Telnet). In the Expert configuration of the trace, this Show command can be invoked very conveniently from the Windows user interface.

- To access the current dump of the Show command (e.g. **show** > **wlan**), click the name of a Show command in the left-hand area of the trace dialog and then the Show button (e.g. **show wlan**).
- Depending on the entry selected you can, or may be required to, specify additional parameters. For an overview of the available parameters, type a question mark ('?') in the input box and click the Show button.

To include the dump of a Show command in the trace data, click the appropriate checkbox to the left of the entry name. Any Show command can be activated to run just once when the trace is started or at regular intervals (set in seconds).

The settings of the Show commands are stored in the trace configuration together with the actual trace settings.



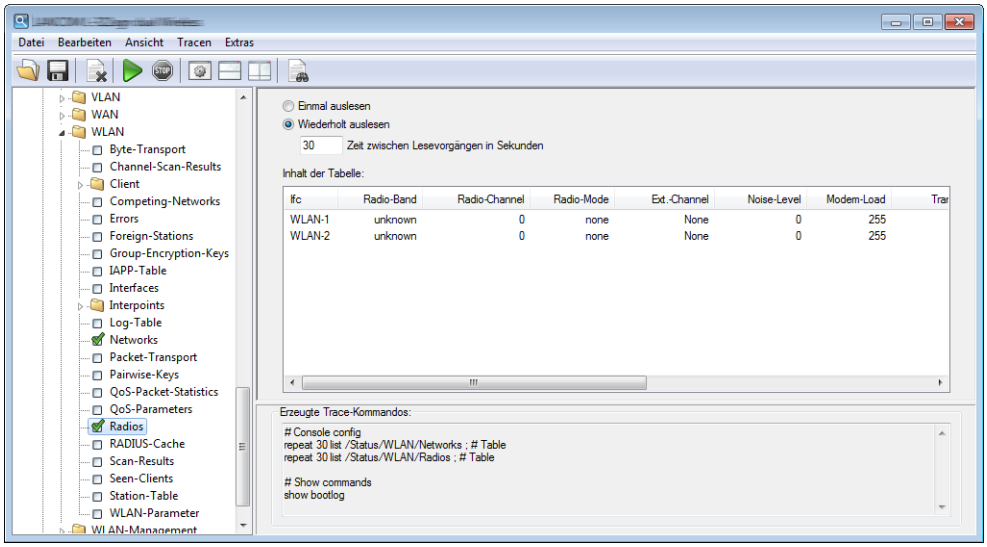
Status

You can access detailed status information and statistics about a device from the command line (Telnet) or via WEBconfig. All of the available status information can also be shown via the trace dialog.

› To display the current contents of the table or value, click the name of a status entry in the left-hand area of the trace dialogue.

To include the dump of a status entry into the trace data, click the appropriate checkbox to the left of the entry name. Any activated status entry can be read-out just once when the trace is started or at regular intervals (set in seconds).

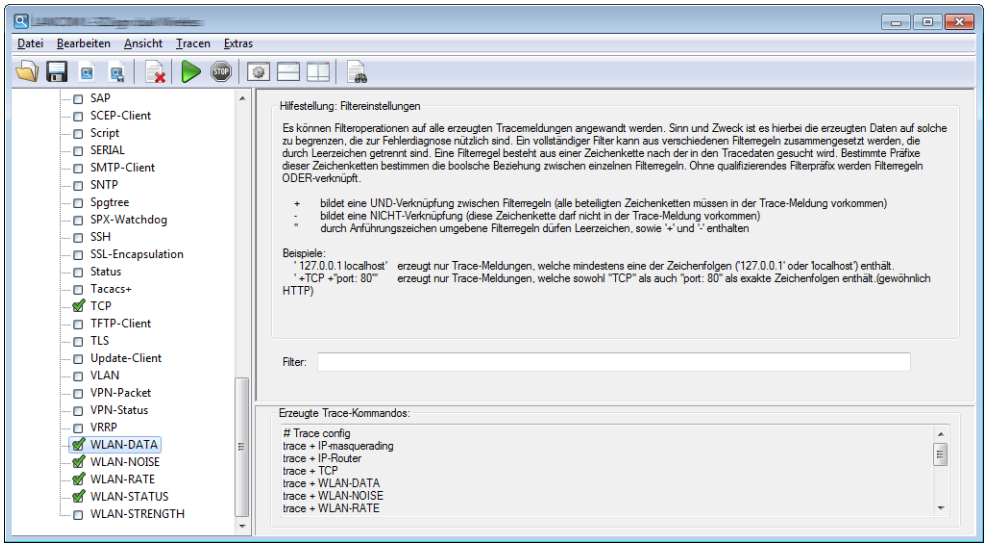
The settings of the Status information are stored in the trace configuration together with the actual trace settings. Similarly, the output of the status information is stored along with the actual trace data.



Trace settings

The traces to be dumped for the current device are enabled in the Trace settings area. To include the trace commands into the trace results, click the appropriate checkbox to the left of its name.

A filter can also be entered for any trace. For example, to display only the IP address of a particular workstation, enter the appropriate IP address as a filter of the IP router trace. To find out more about the filter function, read the section *Filtering trace output* on page 293.



3.4.2.3 Filtering trace output

Trace output from the command line or the LANtools trace dialog can often be very long, because the trace receives information from the device at a very high frequency. To make the trace output easier to understand, you can apply appropriate filters. The filters use a search function to analyze the trace output and present the desired information only.

In the following example, the administrator activates a simple IP router trace on a device with three Internet connections and sends pings to different destinations. The unfiltered trace output shows all packets processed by the IP router in the device:

```
root@MyDevice:/
> trace # ip-router
IP-Router ON

root@MyDevice:/

>[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cde
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1ccf
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1ccf
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cde
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1cea
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1cea
Route: LAN-1 Tx (INTRANET2):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cd0
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cdf
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cd0
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cdf
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1ceb
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (INTERNET2, RtgTag: 2):
```

```
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1ceb
Route: LAN-1 Tx (INTRANET2):
```

The output in just 2 seconds is enough to produce a large amount of data. For a better overview of the output, add a filter to the trace command. The filters start with the @ symbol and enter a search criterion. In this example, the filter reduces the output to that containing the search criterion "Internet1", in order to output only the packets from this remote site.

The filter is not case-sensitive.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1

IP-Router ON @ INTERNET1

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfb
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfb
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfc
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfc
Route: LAN-1 Tx (INTRANET1):
```

Again, the time frame of the trace is about two seconds, but the amount of data has already been reduced significantly. The only data to be displayed is that relating to remote site "INTERNET1". However, further filter criteria can also be specified simply by placing a space between the first and second criteria. As well as a space symbol, the symbols "+" and "-" can also be used as operators. With a "+" both criteria must be met; with a "-" the criterion must not be fulfilled; a space means that one or the other of the associated criteria must be fulfilled. The option to use strings containing operators as a filter is implemented by quotation marks:

If you want to apply multiple search terms, you can separate the terms with the following operators:

- Space: A space before a search term is a logical OR operation. The trace output is only displayed if it contains one of the strings marked in this way.
- +: A plus sign before a search term is a logical AND operation. The trace output is only displayed if it contains all of the strings marked in this way.
- -: A minus sign before a search term is a logical NOT operation. The trace output is only displayed if it contains none of the strings marked in this way.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 -"echo request"

IP-Router ON @ INTERNET1 -"echo request"

[IP-Router] 2010/12/20 17:12:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0b
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:12:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0c
Route: LAN-1 Tx (INTRANET1):
```

The trace now shows only the entries that contain the remote site 'INTERNET1', but **not** the string 'echo request'. This displays only the responses to a ping as they return from the remote site.

You can use multiple traces simultaneously and filter by different criteria. In the following example, an Ethernet trace is run in addition to the IP router trace to see the packet associated with the ping on the Ethernet:

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 +"echo reply"
IP-Router ON @ INTERNET1 +"echo reply"

root@MyDevice:/
> trace # eth @ ICMP +"echo reply"
Ethernet ON @ icmp +"echo reply"

[IP-Router] 2010/12/21 14:17:21,000
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0002, seq: 0x2654
Route: LAN-1 Tx (INTRANET1):

[Ethernet] 2010/12/21 14:17:21,000
Sent 98 byte Ethernet packet via LAN-1:
HW Switch Port : ETH-1
-->IEEE 802.3 Header
Dest : 00:a0:57:12:a9:21 (LANCOM 12:a9:21)
Source : 00:a0:57:12:f7:81 (LANCOM 12:f7:81)
Type : IPv4
-->IPv4 Header
Version : 4
Header Length : 20
Type of service : (0x00) Precedence 0
Total length : 84
ID : 18080
Fragment : Offset 0
TTL : 59
Protocol : ICMP
Checksum : 24817 (OK)
Src Address : 11.11.11.1
Dest Address : 192.168.1.100
-->ICMP Header
Msg : echo reply
Checksum : 18796 (OK)
Body : 00 00 00 02 00 00 26 54 ......
 7e c9 6d 8c 00 00 00 00 ~.m.....
 00 01 02 03 04 05 06 07 ........
 08 09 0a 0b 0c 0d 0e 0f ........
 10 11 12 13 14 15 16 17 ........
 18 19 1a 1b 1c 1d 1e 1f ........
 20 21 22 23 24 25 26 27 !"#$%
```

3.4.2.4 Display of the trace results

To commence the trace data, click the Start button () and switch from the configuration view to the results view in LANtracer. The ongoing trace dumps are displayed in this view:

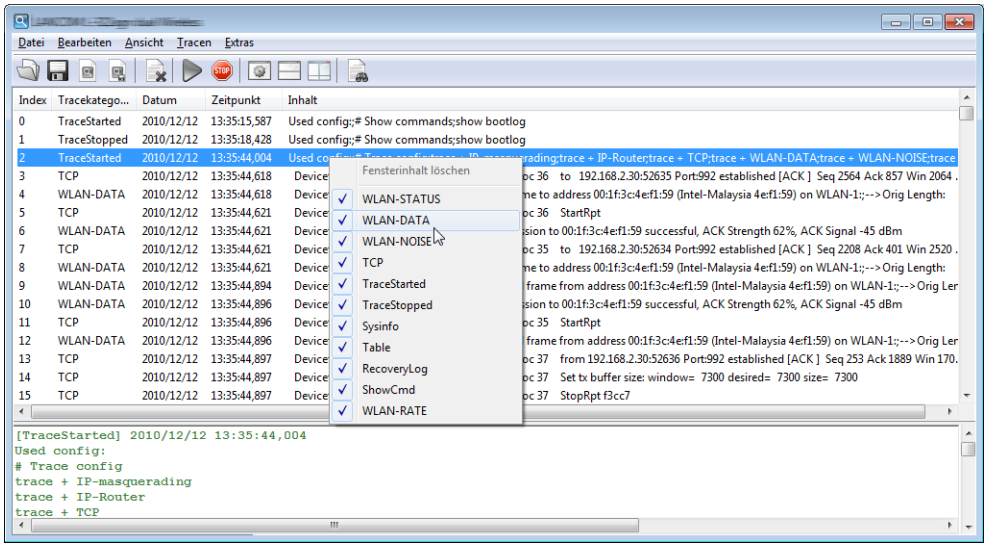
- The upper section lists the results for the executed trace commands chronologically line by line.
- The lower pane presents the results of the trace command selected in the upper pane. All of the active Trace, Status and Show entries are listed here with their respective filters and parameters. The output contains multiple lines because the results for a single trace command can be extensive.

A right-hand mouse click on a trace event opens a context menu, which you can use to display or hide the individual trace categories by filtering.



Trace data is collected as long as the trace dump is enabled. To prevent overloading the main workstation memory using LANconfig or LANmonitor, trace data is automatically written to a backup file. You set the time intervals

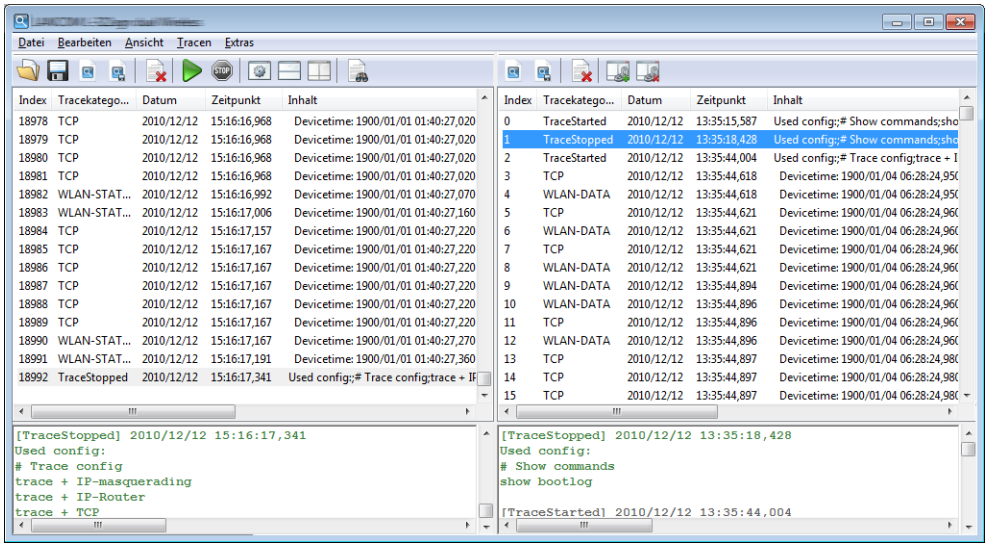
and the maximum size of a backup file for LANtracer under **Extras** > **Miscellaneous settings** > **Trace preferences**.



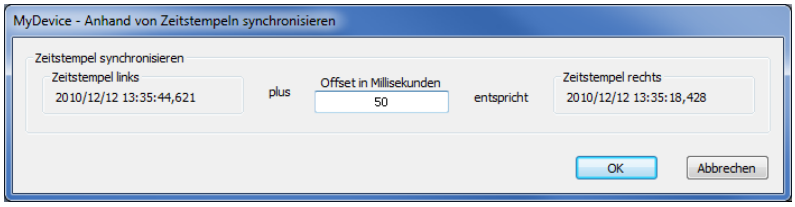
Comparing trace data

In order to compare the results of two traces with one another, you can display two traces side by side in the split-screen mode.

1. Stop the currently running trace and select from the menu **View** > **Result twin view**.
2. Load your current or previously saved trace data into the empty pane.

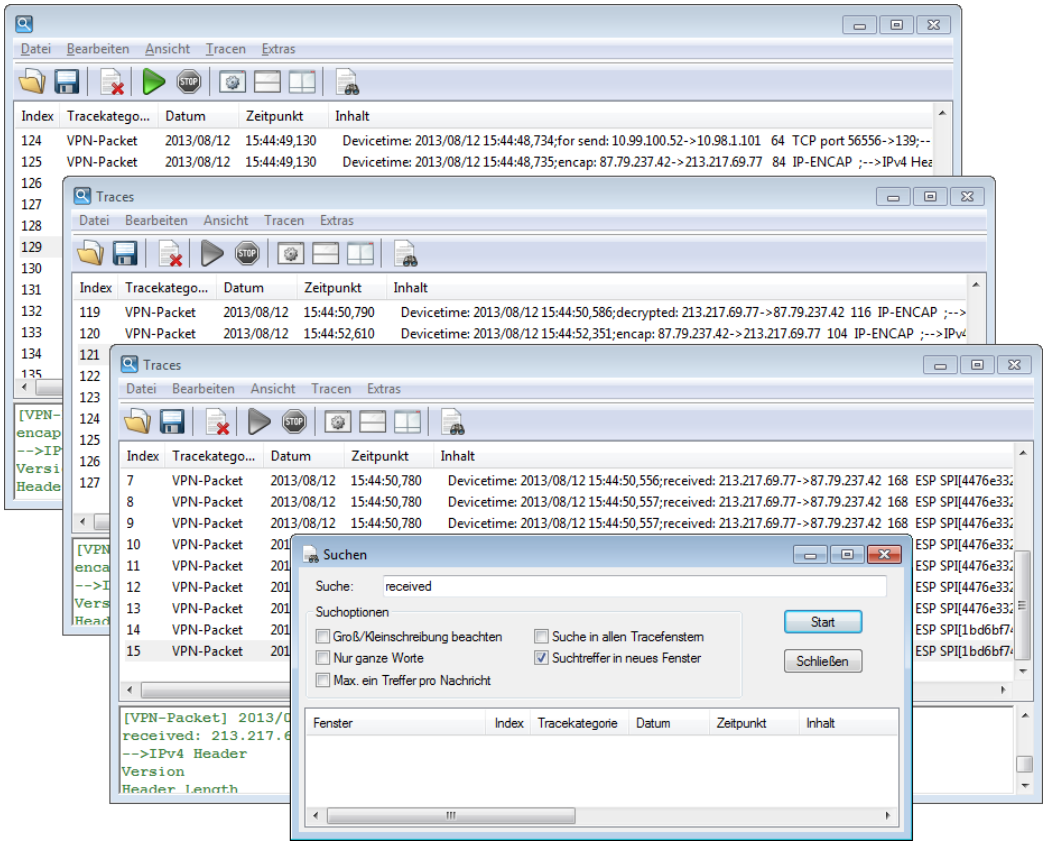


3. Start the time-stamp based synchronization of the two traces with the button. In the following window, enter a suitable value for the offset in milliseconds and start the synchronization.



3.4.2.5 Cascaded find

You have the option of intelligently nesting your Find queries to perform a cascaded (multi-level) search of the trace results. Do this *before* starting the first Find by activating the option **Search results in new window** and leave the option for all other searches enabled. You then search successively for the various terms in the each of the recently opened windows, which further refines your hit list.



In order to generalize a query again, or to go back a step, simply close the most recent results window and return to the previous results window.

For more about the **Find** setup options, see the chapter *Find* on page 300.

3.4.2.6 Backup settings for traces

When starting a trace with LANconfig or LANmonitor, a backup file with the current trace data is saved automatically. Find more about the corresponding setting options in the section *Trace preferences* on page 302.

3.4.2.7 Backing up and restoring the trace data

For later editing, or for transfer to another user, the actual trace data can be written to a storage medium with **File** > **Save trace data/support configuration** and later re-opened with **File** > **Load trace data**.

Alternatively, you can also use the buttons  to load and  to save the trace data.

3.4.2.8 Backing up and restoring the trace configuration

The entire configuration of the trace dump can be written to a storage medium for later re-use or for transfer to another user. Click on **File** > **Save trace config** and re-open it later with **File** > **Load trace config**.



Trace configurations themselves are non-device-specific, so they can be used in combination with any device. Any options, status values, or show commands that are not supported by the target device are skipped during the process of loading. LANtracer emits a warning message with a list of the components of the trace configuration that are not supported by the target device.

3.4.2.9 Exporting a configuration file for Support

LANtracer optionally creates a special configuration file that you can pass on for support with troubleshooting or other assistance. This file contains the current configuration and further information about the device, which facilitates troubleshooting by employees in Support.

If you do not wish to share certain information, LANtracer has an option to hide sensitive information when saving the file. Find more about the corresponding setting options in the section *Support configuration file* on page 302.

3.4.3 The menu structure in LANtracer

The menu bar enables you to load and save trace configurations and data, start and stop traces, and to customize the appearance of LANtracer and the way it works.

3.4.3.1 File

This menu item allows you to save and load trace configurations/data, and to exit LANtracer.

Load trace data

This menu item loads the trace data stored in an *.lct file into the results view.

Save trace data/support configuration

This menu item allows you to save the recorded trace data to an *.lct file after a trace. In parallel, a support configuration file is stored to the same directory. This file is identical to that described in the section *Save support configuration* on page 300.

Load trace configuration

This menu item loads the trace configuration stored in an *.lcg file into the configuration view.



Trace configurations themselves are non-device-specific, so they can be used in combination with any device. Any options, status values, or show commands that are not supported by the target device are skipped during the process of loading. LANtracer emits a warning message with a list of the components of the trace configuration that are not supported by the target device.

Save trace configuration

This menu item allows you to save the settings you made in the configuration view to a non-device-specific *.lcg file.

Import trace data

This menu item imports the trace data stored in an *.lct file into the results view. This allows you to graphically process the trace data created from the command line (e.g. with Telnet or PuTTy).

Save support configuration

This menu item allows you to save the settings you made in the configuration view to a device-specific *.spf file.

A support configuration file contains the current configuration and additional information about the device. Because this file is used for technical support purposes and will leave your hands, you can use the *settings for the support configuration file* to hide sensitive areas of the configuration, if you prefer.

Close

Closes and terminates LANtracer.

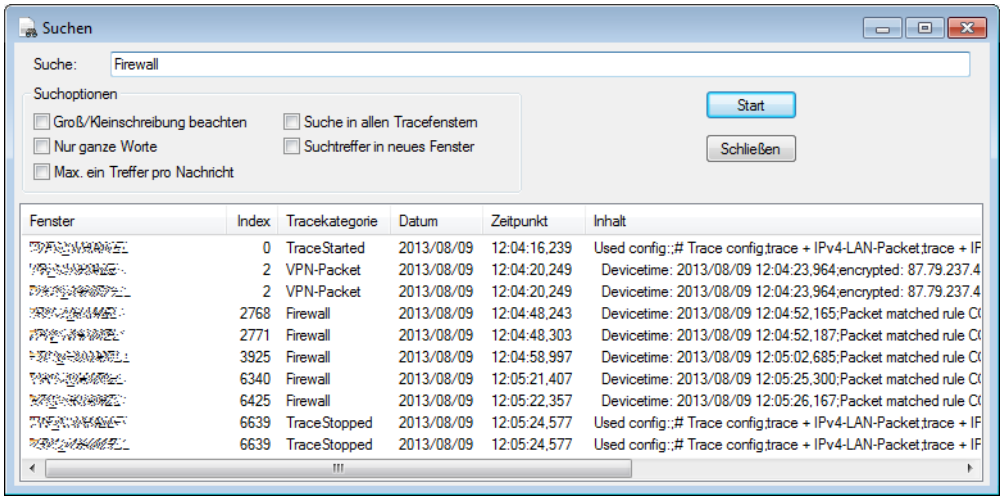
3.4.3.2 Edit

This menu item allows you to search through the displayed traces or delete them.

Find

This menu item opens the Find dialog, which allows you to search for specific terms in the recorded or restored trace data. As long as no other search options have been selected, this feature performs a wildcard search for the entered search term in all of the available columns. The results window lists all hits containing the entered search term.

In order to specifically search for trace entries of a certain category or with a specific date, enter for example `firewall` or `2013/08/09` and click **Start**.



You also have the following search options:

- **Match case**: Enables a case-sensitive search.
- **Match whole word**: Enables the search for whole words or disables the search for substrings. In this case a search, for example, for `VPN` only returns entries where the term as such is present. Terms such as `VPN-Packet` fall outside of the search pattern.
- **Max. one hit per message**: Collects multiple hits for a term within a trace entry into a single search hit.
- **Find in all trace windows**: Extends the search to all open result windows. Otherwise the search is limited to the results of your last search. Also see the chapter *Cascaded find* on page 298.
- **Show results in new window**: The results are displayed in a new window.

Delete trace data

Using this menu item, you delete the trace data currently displayed in the results section.

3.4.3.3 View

This menu item is used to customize the behavior of the LANtracer graphical user interface.

Trace results

Switches to the mode for displaying the trace output

Result twin view

Switches to the split-screen mode to display the trace results in two parallel windows (twin view).

Configuration

Switches to the mode for configuring the trace output.

3.4.3.4 Traces

This menu item is used to start and stop the trace output.

Start tracing

This menu item starts the trace output.

Start tracing

This menu item stops the trace output.

3.4.3.5 Extras

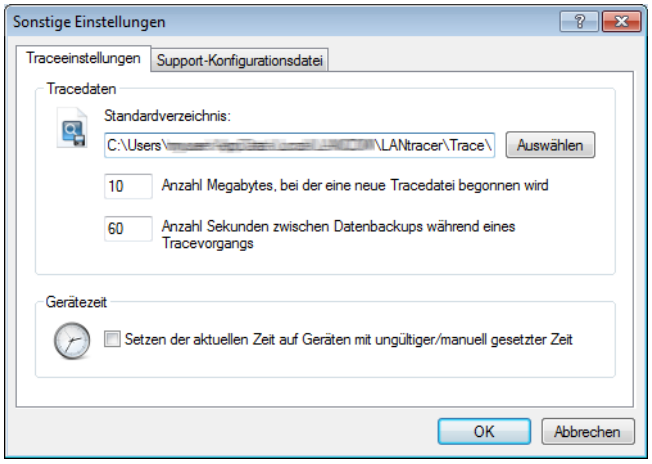
This menu item contains the program-related optional settings for LANtracer, e.g. for automatic logging of trace output or to define the support configuration file.

Miscellaneous settings

With this menu item, you perform the program-related settings for LANtracer.

Trace preferences

This menu item enables you to adjust the settings for the trace data and the device time.



Trace data

When starting a trace with LANconfig or LANmonitor, a backup file with the current trace data is saved automatically. The settings for the trace backup are located in the **Trace data** section. Enter

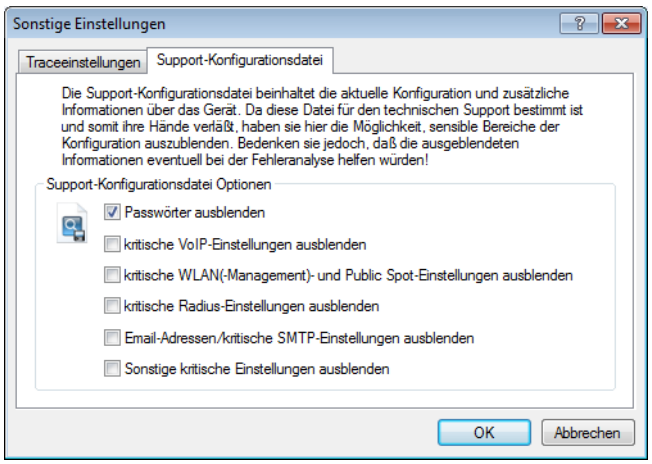
- ... the maximum size of a trace-backup file in megabytes. When this size is reached with an ongoing trace, a new trace backup file is created automatically.
- ... an interval (in seconds) after which the LANtracer stores the trace output to the file.
- ... a directory where LANtracer stores the trace files by default.

Device time

To obtain trace output containing the correct time, enabling this option allows LANtracer to check the device time before running a trace: If the time of the device is wrong or was set manually, it is corrected automatically.

Support configuration file

This menu item allows you to set which content is automatically removed when a support configuration file is saved. The support file created in this way contains all information in cleartext. The file can be opened using an editor and checked for any critical entries.



Please consider that hiding sensitive areas of the configuration can possibly complicate the fault analysis by our Support department.

3.4.4 The toolbar in LANtracer

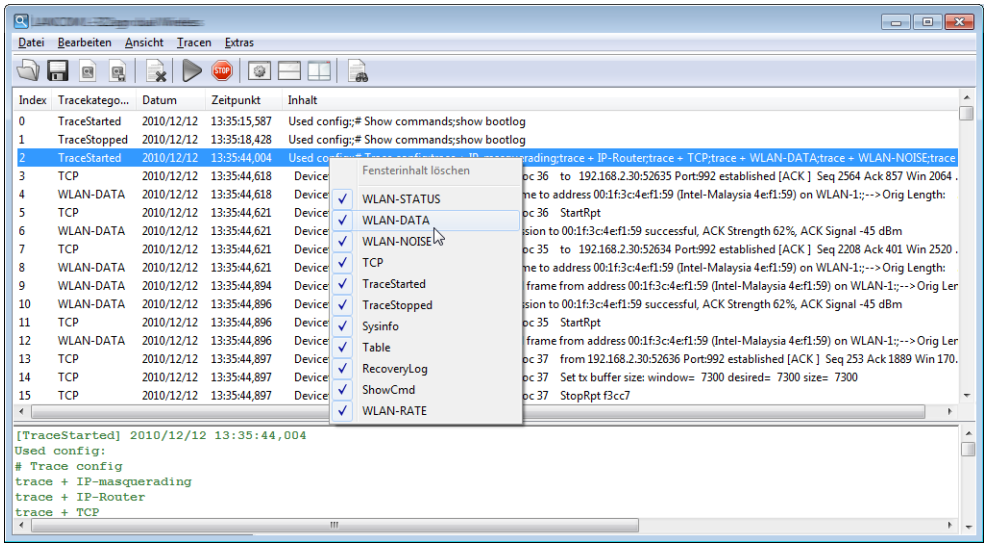
The Trace module provides the following buttons:

Table 21: Icon meanings

	Loads a file containing trace data
	Stores the current trace data for passing on to a user.
	Clears the current display of trace results
	Starts outputting the trace results as produced by the current configuration and automatically switches to the trace-result display mode. As soon as the trace results are returned, the other buttons are deactivated.
	Stops the output of trace results
	Switches to the mode for configuring the trace output
	Switches to the mode for displaying the trace output
	Switches to the split-screen mode to display the trace results in two parallel windows (twin view)
	Starts the time-stamp based synchronization of the two traces in the split-screen display
	Stops the synchronization of the two traces in the split-screen display
	Opens the window to search through the trace results.

3.4.5 LANtracer context menu

The context menu is only available in the results view. Here you can hide individual trace categories as a rough filtering of the displayed results, or you can completely empty the window of its contents.



3.4.6 LANtracer keyboard commands

Alt+L	Load trace data
Alt+I	Import trace data
Alt+S	Save trace data/support configuration
Ctrl+L	Load trace configuration
Ctrl+S	Save trace configuration
Ctrl+F	Opens the window to search through the trace results.
Alt+D	Clears the current display of trace results
Ctrl+R	Switches to the mode for displaying the trace output
Ctrl+T	Switches to the split-screen mode to display the trace results in two parallel windows (twin view)
Ctrl+K	Switches to the mode for configuring the trace output
Spacebar, Enter	Marks the selection box in the Expert configuration
Alt+C	Closes LANtracer

4 Diagnosis

4.1 Trace information

Trace outputs may be used to monitor the internal processes in the router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. A particular advantage of this is: The errors being tracked may stem from the configuration of your own router or that of the remote site.

The trace outputs are slightly delayed after the actual event, but are always in the correct sequence. This will not usually hamper interpretation of the displays but should be taken into consideration if making precise analyses.

4.1.1 How to start a trace

Trace output can be started in a Telnet session. Set up a Telnet connection to your device. The command to call up a trace follows this syntax:

```
> trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces.

4.1.2 Overview of the keys

This code…	… in combination with the trace causes the following:
?	displays a help text
+	switches on a trace output
-	switches off a trace output
#	switches between different trace outputs (toggle)
no code	displays the current status of the trace

4.1.3 Parameter overview for the trace command

The traces available for a particular model can be displayed by the CLI by entering `trace` without any arguments.

Table 22: Overview of some executable traces

This parameter ...	...causes the following message in the trace:
`ACME`	Automatic Certificate Management Environment (ACME) client
`ADSL-CTRL`	Output of all management packets for the internal ADSL interface
`ADSL-DATA`	Output of all packets transmitted via the internal ADSL interface
`ADSL-Modem`	Extended status information regarding the internal ADSL interface

This parameter ...	...causes the following message in the trace:
ADSL-Status	Information regarding the connection status as well as the connection and disconnection of the internal ADSL interface
ARP	Address resolution protocol
ATM-cell	ATM packet layer
ATM-error	ATM error
Autoload	Information regarding the automatic firmware and configuration load during a device rollout
Automatic-Firmware-Updater	Information regarding the automatic firmware update
B-Analog	Status information regarding the analog audio channel
BGP-Adj-RIB-In	Information regarding Border Gateway Protokoll Updates received from neighbors (BGP-Adj-RIB-In)
BGP-Adj-RIB-Out	Information regarding Border Gateway Protokoll Updates sent to neighbors (BGP-Adj-RIB-Out)
BGP-Connection	Event processing and State changes of the individual Statemachines as well as readably formatted BGP messages sent / received by the Statemachine
BGP-Control	Information regarding the processing of the BGP configuration
BGP-Message	Internal messages between the BGP threads (Note: Creates a lot of messages, usually only the number of the State Machine)
BGP-Network	Information regarding the creation of an outgoing BGP connection and accepting or rejecting of incoming BGP connections
BGP-Packet	Shows received and sent BGP packets as a hexdump (associated State Machine can only be resolved by number at the time of data retrieval)
BGP-Phase-Two	Shows, why BGP Phase 2 prefers or ignores a prefix (Note: Can create a lot of messages)
BGP-Policy	Information regarding the processing of Border Gateway Protokoll routes when using rules
Bonjour-Proxy-Packet	Packets of the Bonjour-Proxy
Bonjour-Proxy-Status	Status information of the Bonjour-Proxy
Bridge	Information on the LAN bridge
BT-Status	Status information regarding the BLE interface
Callmanager	Status information regarding the Voice Call Manager
CAPWAP-CTRL	Status information regarding the control channel between a WLAN-Controller and managed access point
CAPWAP-DATA	Packets transmitted via the Layer3-Tunnel between the WLAN-Controller and a managed access point
CAPWAP-RF-Opt	Status information regarding the WLC-based radio field optimization
CAPWAP-Firmware	Informationen zum zentralen Firmwaremanagement auf WLAN-Controllern
CF-Status	Status information regarding the Content-Filter
CF-Urls	Status information regarding URLs in the Content-Filter
COM-Port-Server	Status information about the Com-Port-Server

This parameter ...	...causes the following message in the trace:
Config-Sync:	Status information regarding Config-Sync (automatic configuration synchronisation)
Connact	Messages from the activity protocol
CRL-Client	Status information regarding the Certificate Revocation List (CRL) Client
Cron	Activities of the scheduler (cron table)
D-channel	Shows communication via ISDN D-Channel (Call setup and termination)
DFS-Pulse	Shows radar pulses in the 5 GHz band (DFS - Dynamic Frequency Selection)
DFS-Status	Shows ecvents which are related to dynamic frequency detection and radar detection
DHCP	Dynamic host configuration protocol
DHCPv6-Client	Status information regarding the DHCPv6-Client
DHCPv6-Relay-Agent	Status information regarding the DHCPv6-Relay-Agent
DHCPv6-Server	Status information regarding the DHCPv6-Server
DNS	Domain name service protocol
DS-Lite	Status information regarding Dual Stack Lite (DS-Lite)
DSLoL	Status information regarding DSLoL (DSL over LAN)
DSR-CTRL	Status information regarding the setup and termination of connections to Analog/ISDN devices
DSR-IPT	Shows received and sent voice packets between SIP and Analog/ISDN (Note: Similar to the MEDIA-PCM trace, but more specialised towards Analog/ISDN devices)
DTLS	Status information regarding DTLS connection (is used by CAPWAP)
DYN-AUTH-Client	Status information regarding the client for dynamic authorization by RADIUS CoA (Change of Authorization)
DYN-AUTH-Server	Status information regarding the server for dynamic authorization by RADIUS CoA (Change of Authorization)
EAP	Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1X
Error	Connection error messages
Ethernet	Information on the Ethernet interfaces
Filesystem	Status information regarding the filesystem
Firewall	Displays firewall events
Firmware-Upload	Status information regarding the firmware upload
FPing	Status information regarding the FPing command
FRONTPANEL-Serial	Information regarding the display monitor controller on WLC-1000/WLC-2000/ISG series
FW-DNS	Changes to the firewall database of DNS destinations: › If a DNS packet arrives, it outputs the packet along with the affected wildcard expressions and destinations. › If the TTL (time-to-live) of an entry expires, it outputs the associated record along with the relevant wildcard expressions and destinations.

This parameter ...	...causes the following message in the trace:
	› If one of the two firewalls registers or de-registers a DNS destination because its configuration has changed. › If there is a change to the table **Set up** > **Firewall** > **DNS-Destinations** or **Set up** > **Firewall** > **DNS-Destination-List**.
GRE	Messages to GRE tunnels
hnat	Information on hardware NAT
HTTP-Client	Status information regarding HTTP-Client events
HTTP-Client-DNS	Status information regarding DNS-based HTTP-Client events
HTTP-Server	Status information regarding HTTP-Server events
HWMON-Serial	Information regarding the Hardware Monitor Controller on WLC-1000/WLC-2000/ISG series
IAPP	Trace on inter access point protocol giving information on wireless LAN roaming.
ICMP	Internet control message protocol
ICMPv6	Status information regarding the Internet Control Message Protocol for IPv6
IGMP-Snooping	Information regarding IGMP snooping in the LAN bridge (IGMP - Internet Group Management Protocol)
Iperf-Server-Daemon	Status information regarding the iPerf server
IP-masquerading	Events in the masquerading module
IPv4-Config	Information regarding the internal IPv4-Control-Plane
IPv4-Host	Shows IPv4 packets, which the router itself sends or receives
IPv4-Interfaces	Information about the internal management of logical IPv4 interfaces
IPv4-LAN-Packet	Shows IPv4 LAN packets (without packets destined for the router itself and packets created by the router)
IPv4-Packet	Shows all IPv4 packets (without packets destined for the router itself and packets created by the router)
IPv4-RIB	Status information regarding the IPv4 Routing Information Base (RIB)
IPv4-WAN-Packet	Shows IPv4 WAN packets (without packets destined for the router itself and packets created by the router)
IPv6-config	Information about the IPv6 configuration
IPv6-firewall	IPv6 firewall events
IPv6-Interfaces	Information about the IPv6 interfaces
IPv6-LAN-Packet	Data packets over the IPv6 LAN connection
IPv6-router	Information about the IPv6 routing
IPv6-WAN-Packet	Data packets over the IPv6 WAN connection
L2TP	L2TPv2 / v3 protocol
L7-Detection	Shows the connections recognised by the Layer-7 detection
L7-Detection-Status	Shows general status information regarding the Layer-7 detection

This parameter ...	...causes the following message in the trace:
LANAUTH	LAN authentication (e.g. Public Spot)
LACP	Information regarding the Link Aggregation Control Protocol (LACP)
LBS-Client	Information regarding the Location Based Services Client
License-Management	Information regarding license files (vRouter)
LISP-Config	Information regarding the Locator / ID Separation Protocol (LISP)
LISP-Control	Information regarding the Control-Plane of the Locator / ID Separation Protocol (LISP)
LISP-Data	Shows data packets of the Locator / ID Separation Protocol (LISP)
LISP-Error	Shows error messages of the Locator / ID Separation Protocol (LISP)
LL2M	Information regarding the LANCOM Layer 2 Management Protokoll
Load-balancer	Information on load balancing
Mail-client	E-mail processing by the internal mail client
MEDIA	Status information regarding the Media Receiver (Setup/Termination of media endpoints and streams)
MEDIA-CODECS	Status information regarding the Media Receiver with focus on Codec negotiation
MEDIA-PCM	Shows data between SIP and Analog/ISDN (Note: Similar to the DSR-IPT trace, but more specialised towards the Media Receiver)
MLD	Information regarding the IPv6 Multicast Listener Discovery (MLD)
ND-CACHE	Information regarding the IPv6 Neighbor Discovery Protocol Cache
ND-DAD	Information regarding the Duplicate Address Detection of the IPv6 Neighbor Discovery Protocol
NETFLOW-Common	For more information about NetFlow/IPFIX, please see *Netflow / IPFIX* on page 1641.
NETFLOW-Error	
NETFLOW-Export	
NETFLOW-Metering	
NTP	Timeserver trace
OAM	Information regarding Ethernet OAM
OCSP-Client	Information regarding the Online Certificate Status Protocol (OCSP) Client
OCSP-Server	Information regarding the Online Certificate Status Protocol (OCSP) Server / Responder
OSPF-Expert	Expert information regarding the Open Shortest Path First (OSPF) protocol
OSPF-LSA	Information regarding the Open Shortest Path First (OSPF) Link State Advertisements (LSA)
OSPF-Neighbor	Information regarding the Open Shortest Path First (OSPF) neighbors
OSPF-Packet	Shows Open Shortest Path First (OSPF) packets

This parameter ...	...causes the following message in the trace:
OSPF-Redistribution	Information regarding the Open Shortest Path First (OSPF) redistribution of routes with a different routing protocol source
OSPF-Router	Information regarding the Open Shortest Path First (OSPF) Router
Outband	Information regarding the outband interface (serial)
Packet-dump	Displays the first 64 bytes of a packet in hexadecimal
PbSpot-Advertisement	Information regarding the insertion of advertising in the Public Spot
PCAP	Information regarding Packet Capture (PCAP)
PMS	Information regarding the Fidelio interface (PMS - Property Management System)
Port-Listener-Switch	Information regarding the switch between PSec and IPSec-over-HTTPS
PPP	PPP protocol negotiation
PRP	Information regarding the Parallel Redundancy Protocol (PRP)
Provisioning	Information regarding provisioning of DECT base stations
PSTN-MNGMT	Information regarding the setup and termination of connections between PSTN devices (Analog/ISDN) and betweem PSTN and SIP
Q.931	Information regarding the ISDN D-Channel Layer 3 Protocol
RADIUS-Client	Informationen about the RADIUS-Client
RADIUS-Server	Information about the RADIUS-Server
RADSEC	Information about RADSEC
RIP	IP Routing Information Protocol
Rollout-Agent	Information regarding the Rollout-Agent
Rollout-Wizard	Information regarding the Rollout-Wizard
Route-Monitor	Information regarding the Route-Monitor
SCEP-CA	Information regarding the Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA)
SCEP-Client	Information regarding the Simple Certificate Enrollment Protocol (SCEP) Client
Script	Script negotiation
Serial	Information on the state of the serial interface
SFP	Status information regarding SFP ports
SI3220	Status information regarding the SI3220 SLIC chip
SIP-ALG	Status information regarding SIP-ALG (Application Layer Gateway)
SIP-ALG-Packet	Shows packets transmitted via the SIP-ALG (Application Layer Gateway)
SIP-Connection	Status information regarding the setup and termination of SIP connections
SIP-packet	SIP information that is exchanged between a VoIP router and a SIP provider or an upstream SIP telephone system

This parameter ...	...causes the following message in the trace:
SLIC	Status information about the analog telephony interface
SMTP-client	E-mail processing by the internal mail client
SNTP	Simple network time protocol
Spgtree	Information on spanning tree protocol
Status	Connection status messages
SSH	Information regarding SSH connections to the SSH server and from the SSH client
SSL-Encapsulation	Information regarding VPN encapsulation via IPSec-over-HTTPS
T.38	Debug output for the T.38 library
Tacacs+	Information regarding the TACACS+ protocol
TCP	Information regarding TCP connections orifginating from or directed to the device
TFTP-Client	Information regarding TFTP connections initiated by the TFTP-Client
TLS	Information regarding SSL/TLS connections originating from or directed to the device
TR064-StateEngine	Information about the State-Machine in TR-064
TR069-Engine	Information regarding TR-069/CWMP
TR069-Message	Information regarding messages in TR-069/CWMP
TR069-State	Information regarding the State-Machine in TR-069/CWMP
USB	Information on the state of the USB interface
UserDef-Wizards	Information regarding the user-defined wizards in WEBconfig
VCM-DNS	Information regarding the DNS resolution of the Voice Call Manager
VDSL-CTRL	Shows all management packets of the internal VDSL modem
VDSL-DATA	Shows all packets transmitted via the internal VDSL modem
VDSL-Modem	Extended status regarding the internal VDSL modem
VDSL-Status	Information about the connection status as well as the setup and termination of the internal VDSL modem
VLAN	Information about VLAN tagging for individual packets
VLB-Packet	Packet information regarding the IKEv2 Server-Loadbalancer
VLB-Status	Status information regarding the IKEv2 Server-Loadbalancer
VPN-Debug	Extensive debug information for VPN connections
VPN-IKE	Shows IKE packets in the VPN
VPN-Mesh	Trace for *LANCOM Advanced Mesh VPN (AMVPN)* on page 886.
VPN-Packet	IPSec and IKE packets
VPN-Status	IPSec and IKE negotiations
VRRP	Information on the virtual router redundancy protocol

This parameter ...	...causes the following message in the trace:
VRRP-Status	Information about processing the Virtual Router Redundancy Protocol (VRRP), e.g. information regarding states, roles, neigbors and errors
VRRP-Packet	Information regarding packets of the Virtual Router Redundancy Protocol (VRRP)
WISPr-PbSpot	Information about the Wireless Internet Service Provider Roaming (WISPr) protocol in the Public Spot
WePaper-Coordination	Status information regarding the coordinated ePaper channel selection
WireGuard	Enables the basic WireGuard traces of negotiation packets as well as status and debug information.
WG-Packet	Displays the WireGuard payload packets.
WLAN	Information on activity in the wireless networks
WLAN-ACL	Status messages about MAC filtering rules. The display depends on how the WLAN data trace is configured. If a MAC address is specified there, the trace shows only the filter results relating to that specific MAC address.
WLAN-Adapt-RF-Opt	Information regarding Adaptive RF Optimization events
WLAN-AGGREGATION	Information regarding aggregation of WLAN packets (Note: Only works with 802.11n chipsets)
WLAN-ANI	Information regarding Adaptive Noise Immunity
WLAN-CCA	Information regarding WLAN-CCA (Clear Channel Assessment) (Note: Only works with 802.11n chipsets)
WLAN-DATA	Output of all packets transmitted via the internal WLAN interfaces
WLAN-NOISE	Status information regarding the noise level of the WLAN modules
WLAN-POWERSAVING	Status information regarding WLAN-Power-Saving (Note: Only works with 802.11n chipsets)
WLAN-OFFLOAD	Additional statis information regarding WLAN modules with 802.11ac or newer chipsets
WLAN-OWE	Status information regarding Opportunistic Wireless Encryption (Enhanced Open)
WLAN-RATE	Status information regarding rate adaption of WLAN modules with 802.11n chipset
WLAN-SAE	Status information regarding SAE authentication, which is used with WPA3
WLAN-STATUS	General WLAN status information
WLAN-STEERING	Status information regarding WLAN-Client-Management
WLAN-STRENGTH	Status information regarding the seen signal strength of connected WLAN clients or P2P connections
WLC-Steering	Status information regarding WLC-based Client-Steering
WLC-Tunnel	Information regarding Status connections between two WLAN-Controllers
WWAN-Control	Output of the management communication of the internal WWAN interface
WWAN-Data	Output of all packets transmitted via the internal WWAN interface
WWAN-Modem	Extended status information regarding the internal WWAN interface

This parameter ...	...causes the following message in the trace:
XML-Interface-PbSpot	Messages from the Public Spot XML interface

4.1.3.1 Advanced wireless LAN traces

To support better diagnostics in the WLAN, a number of trace parameters can be specifically adjusted under **Setup** > **WLAN**.

Trace-Data-Packets

The output of the trace messages can be restricted to certain data packets.

Possible values:

Normal

ZERO

Other

Default:

Normal

ZERO

Other

Trace MAC

For the WLAN data trace, the output of the trace messages can be restricted to the particular client with the MAC address entered here.

Possible values:

Max. 12 hexadecimal characters from

0123456789abcdef

Default:

000000000000

Special values:

000000000000: Deactivates this function and outputs trace messages for all clients.



This filter is effective for the traces WLAN-DATA, WLAN-STRENGTH and WLAN-AGGREGATION, but not for WLAN-STATUS.

Trace-Mgmt-Packets

With this selection it is possible to set which type of management frames should automatically appear in the WLAN-DATA trace

Possible values:

Association: (Re)Association Request/Response, Disassociate

Authentication: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Other: all other management frame types

Default:

Association

Authentication

Probes

Action

Other

Trace packets

Similar to Trace MAC and Trace level, the output from WLAN DATA traces can be restricted by the type of packet sent or received, e.g. management (authenticate, association, action, probe-request/response), control (e.g. powersave poll), EAPOL (802.1x negotiation, WPA key handshake).

Possible values:

Management

Control

Data

EAPOL

All

Default:

All

Trace level

The output of trace messages for the WLAN data trace can be restricted to contain certain content only. The value entered here restricts the packets in the WLAN-DATA trace to the specified level.

Possible values:

0 to 255

Special values:

0: Reports that a packet has been received/sent

1: Adds the physical parameters for the packets (data rate, signal strength, etc.)

2: Adds the MAC header

3: Adds the Layer-3 header (e.g. IP/IPX)

4: Adds the Layer-4 header (TCP, UDP...)

5: Adds the TCP/UDP payload

255: No restrictions on content. The trace includes the entire packets.

Default:

255

4.1.4 Combination commands

This combination command…	… brings up the following display for the trace:
Display	status and error outputs
Protocol	LANCOM and PPP outputs
TCP-IP	IP-Routing, IP-RIP, ICMP and ARP outputs

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

4.1.5 Trace filterss

Some traces, such as the IP router trace or the VPN trace, produce a large number of outputs. The amount of output can become unmanageable. The trace filters allow you to sift out the information that is important to you.

A trace filter is activated by adding the parameter "@" that induces the following filter description. In filter description uses of the following perators:

Operator	Description
(space)	OR: The filter applies if one of the operators occurs in the trace output
+	AND: The filter applies if the operator occurs in the trace output
-	Not: The filter applies if the operator does not occur in the trace output
"	the output must match the search string exactly

An operator can be entered as any string of characters, such as the name of a remote station, protocols or ports. The trace filter then processes the output according to the operator rules, much like an Internet search engine.

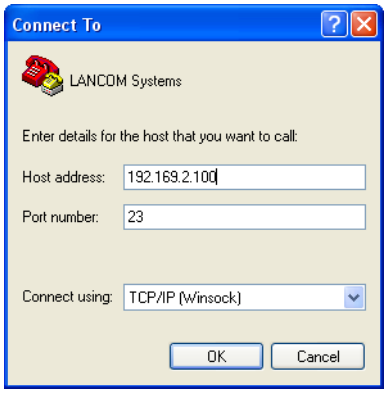
4.1.6 Examples of traces

This code…	… in combination with the trace causes the following:
trace	displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF)
trace + protocol display	switches on the output for all connection protocols together with the status and error messages
trace - icmp	switches on all trace outputs with the exception of the ICMP protocol
trace ppp	displays the status of the PPP
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B	switches on all trace outputs for IP routers related to remote site A or B
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B -ICMP	switches on all trace outputs for IP routers related to remote site A or B that do not use ICMP
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B +ICMP	switches on all trace outputs for IP routers related to remote site A or B that use ICMP
trace + ip-router @+TCP +"port: 80"	switches on all trace outputs from the IP router wiht TCP/IP and port 80. "port: 80" is in quotes so that the space is recognised as a part of the string.

4.1.7 Recording traces

Traces can be conveniently recorded under Windows (e.g. as an aid to Support), and we recommend you do this as follows:

Start a terminal program, e.g. HyperTerminal. Enter a name of your choice when prompted to do so.



In the window 'Connect to' use the pulldown menu 'Connect using' and select the entry 'TCP/IP'. As 'Host address' enter the local/official IP address or the FQDN of the device. After confirmation, HyperTerminal dipslays a request to log in. Enter the configuration password.

You record the traces by clicking on **Transmit** / **Capture text**. Enter the path of the directory where the text file is to be saved. Now change back to the dialog window and enter the required trace command.

To stop the trace, click on the HyperTerminal menus **Transmit** / **Stop text capture**.

4.1.8 Trace to an attached USB drive

It is possible to save traces to a connected USB drive, e.g. a USB stick to save in the background. An active console session is not required for this, as the recording is carried out in the background.

After recording, the file can be accessed by plugging the USB stick into a computer. Alternatively, the /usb/ directory on the device can be accessed remotely via SCP.

The USB drive must be FAT32 formatted. The device writes to the USB stick until it is full, after which the capture stops.

It is not possible to write or load a file to the internal flash of the device.

An ICMP trace on the console is e.g. redirected to a USB drive as follows:

```
Trace # ICMP > /usb/file.lct
```

The ICMP trace is stopped as follows:

`Trace # ICMP > /usb/file.lct` or `Trace - all > /usb/file.lct`

The show command “show trace-file” shows active trace sessions on USB.

A `Trace - all` does not terminate the running sessions that are being recorded on USB, only the active traces of the active console session.

```
root@lc1900ef-aa:/
> tr # icmp >/usb/my
created trace session for '/usb/my.lct'
/usb/my.lct:
ICMP                        ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                  ON

root@lc1900ef-aa:/
> tr # tcp >/usb/my
/usb/my.lct:
TCP                         ON
```

```
root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                 ON
  TCP                  ON

root@lc1900ef-aa:/
> tr - all >/usb/my
/usb/my.lct:
remove trace session for '/usb/my.lct'
```

4.2 Tracing with LANmonitor

You find information about this topic in the chapter *LANtracer – tracing with LANconfig and LANmonitor* on page 289.

4.3 Recording and analyzing data packets

LCOS offers you two ways of recording data packets for the purpose of troubleshooting.

One way is to execute the console command **lcoscap**. This command enables the capture of packets and writes the results to a file that you can open and analyze with a tool like "Wireshark".

Another way is to use the much more convenient method with WEBconfig. This allows you to specify different parameters and record the data packets of selected interfaces, which you subsequently write to a results file for analysis.

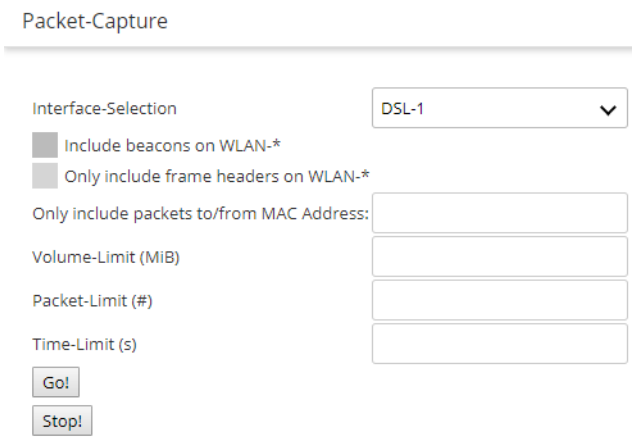
This method offers you several advantages:

- You do not need any special software, because you can run WEBconfig on any Web browser.
- There is no need to input any CLI commands. Instead, you work with a convenient menu.
- If you use WEBconfig over HTTPS, the confidentiality and security of captured traffic is guaranteed.

The LCOScap client is able to connect to the device via IPv4 or IPv6.

4.3.1 Data capture with packet capturing

The **Extras** > **Packet capture** function offers you a simple way to capture data packets from different interfaces and then analyze them with a program such as Wireshark.



To specify the output file the following general menu items are available:

Interface selection

Use this drop-down menu to choose the interface that you want to capture data packets for.

Include beacons on WLAN-*

Enable this option to capture beacon information in addition to the data packets if the selected interface is a WLAN interface.

Include packet headers only on WLAN-*

Enable this option to limit the capture of data packets to the packet header if the selected interface is a WLAN interface.

Only include packets to/from MAC address

If you only want to record data packets for a particular physical address within the selected interface, you can specify it here.

Volume limit (MiB)

Enter the maximum volume of the recorded packets in Mebibytes.

Packet limit (#)

Here you can set the maximum number of packets to be recorded.

Time limit (s)

Enter the maximum time in seconds, after which the recording ends.

After you set the parameters and click on **Go!** you create a file that you can save anywhere and open with Wireshark, for example. After a certain period of time (depending on the connection speed), a window opens for you to save the generated files. You can now save the file locally with the suffix *.cap. By default, the file name is composed of the description and interface associated with the device for which the data packets were recorded (e.g. MyDevice-LAN-2.cap). You can change the name when saving or later.

You can stop a recording at any time by clicking on **Stop!**. This is useful for correcting or adjusting parameters before the data capture.

If you start recording without setting any limits, the device keeps recording the packets until you manually halt the process by clicking on **Stop**.

Flexible WLAN capture format

A variety of different formats are available to you for storing WLAN packet-capture data. **Setup** > **WLAN** > **Packet-Capture**).

4.3.2 Data capture with LCOSCAP

With "LCOSCAP" you have the option to capture and store data traffic in a format compatible with Wireshark. You operate "LCOSCAP" from the command line interface by appending the appropriate parameters.

The following parameters control LCOSCAP:

-o

Target file containing the captured data.

-p

Password of the device for which LCOSCAP captures the data.

-i

Interface of the device for which LCOSCAP captures the data.

If you omit the -i parameter, LCOSCAP outputs the device's interface list.

-b

Switch to include the beacons in the data traffic (WLAN only).

-h

Switch to include the 802.11 headers, although without payload (WLAN only).

-l

Specifies the maximum size of the capture file. If the specified value is reached, LCOSCAP creates a new file. The files are given sequential numbers.

-n

Specifies the number of files produced by LCOSCAP. If the maximum number of files is reached, LCOSCAP overwrites the first file.

--h

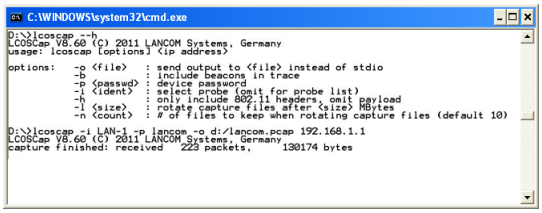
With `LCOSCAP --h` you invoke LCOSCAP's Help function.

Enter the following command to record the data traffic for a device:

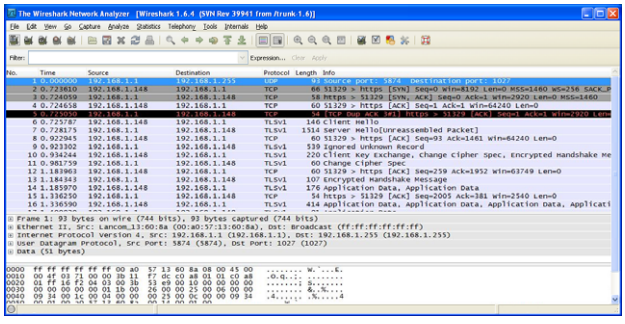
```
LCOSCAP -i LAN-1 -p lancom -o d:\lancom.pcap 192.168.1.1
```

- The device in this example has the IP address "192.168.1.1".
- The password is "lancom".
- You are recording the data traffic on the interface "LAN-1".
- File name and location are `d:/lancom.pcap`.

Use the keyboard shortcut **Ctrl + C** to stop the recording.



For the analysis, open the file generated by LCOSCAP with "Wireshark".



4.3.3 Data capture with RPCap

The RPCap interface integrated in LCOS allows you to use the packet analysis tool “Wireshark” to capture data packets from any interface of a LANCOM router.

In contrast to data capture with LCOSCap, using RPCap allows the captured data to be analyzed in real time and you can create capture filters.

Please note that a running Wireshark instance consumes significantly more resources on the PC than an LCOSCap instance. For long-term data capture, we therefore recommended the use of LCOSCap.

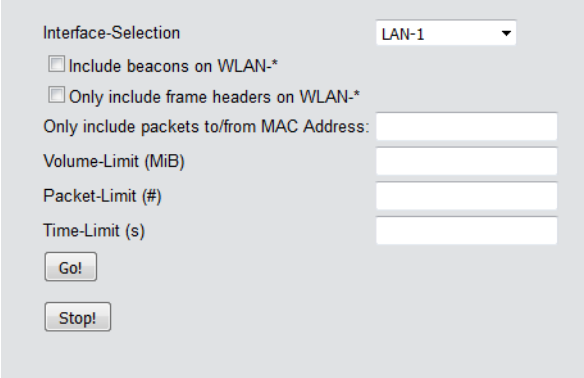
Packet capture with RPCap has the following prerequisites:

- Current versions of Wireshark and WinPcap under Microsoft Windows
- LCOS version 8.80 or later
- IP connectivity between the PC running Wireshark and the router being analyzed

4.3.3.1 Activating packet capture with WEBconfig

Proceed as follows to use WEBconfig to capture data packets:

1. Open the router configuration in WEBconfig and switch to the menu item **Extras** > **Packet-Capture**.
2. Select the interface for packet capture (e.g. LAN-1).
3. Click on the button **Go!** to start the data capture.



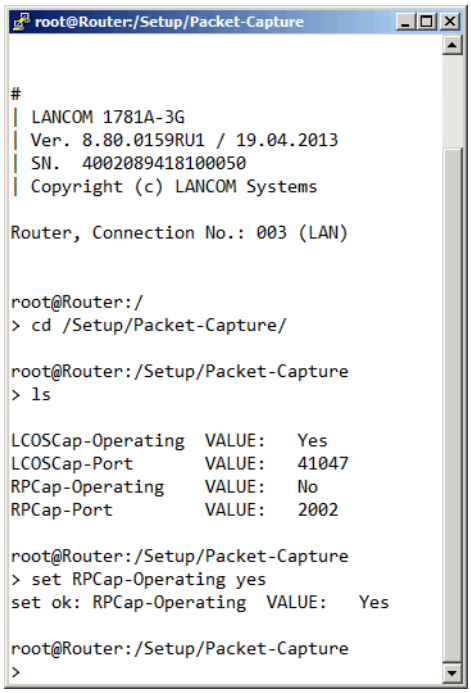
The data packets on the selected interface are now captured. Click the **Stop!** button to halt the data capture.

4.3.3.2 Activating packet capture from the command line

Proceed as follows to capture data packets from the command line:

1. Start a CLI session on the router from which packets are to be captured.
2. Change to the path `/Setup/Packet-Capture`.

3. Activate the RPCap interface with the command `set RPCap-Operating yes`.



The data packets on the selected interface are now captured. Deactivate packet capture with the command `set RPCap-Operating no`.

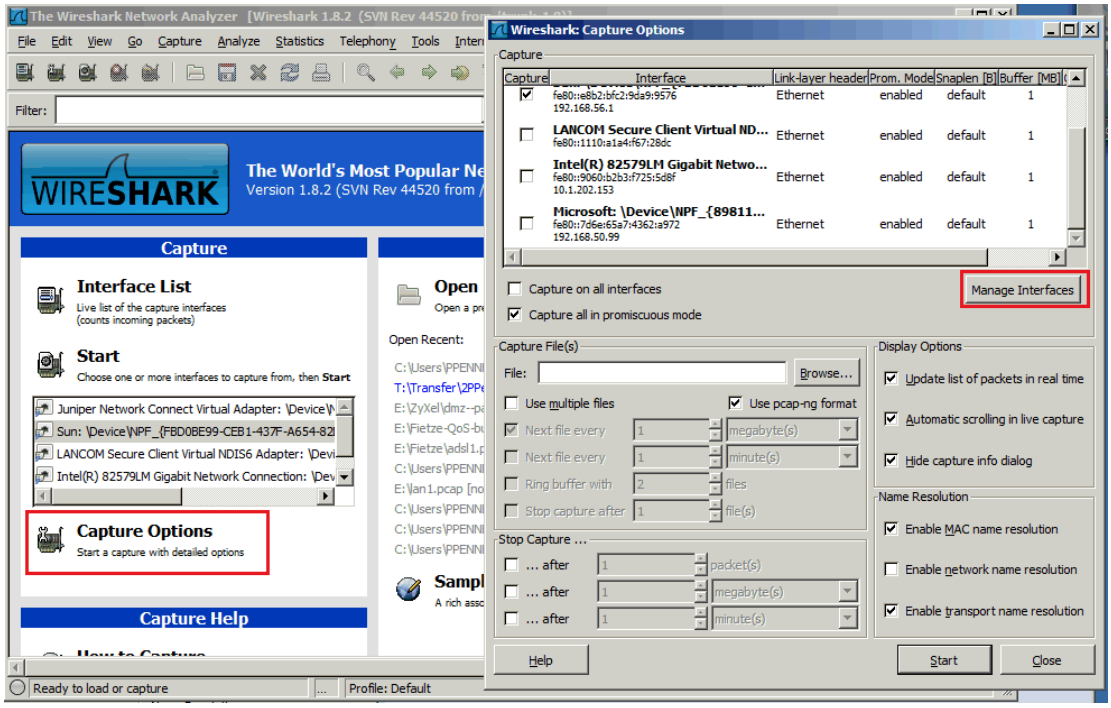
4.3.3.3 Analyzing captured packets with Wireshark

To analyze the captured packets with the packet analysis tool “Wireshark”, proceed as follows:

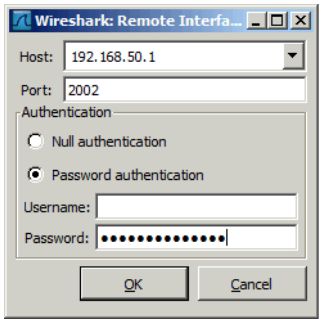
1. Start Wireshark.

   Please note that using the RPCap interface only works properly in combination with the Windows version of Wireshark. This is because PRCap is only supported by the WinPcap driver available for Windows and included in Wireshark.

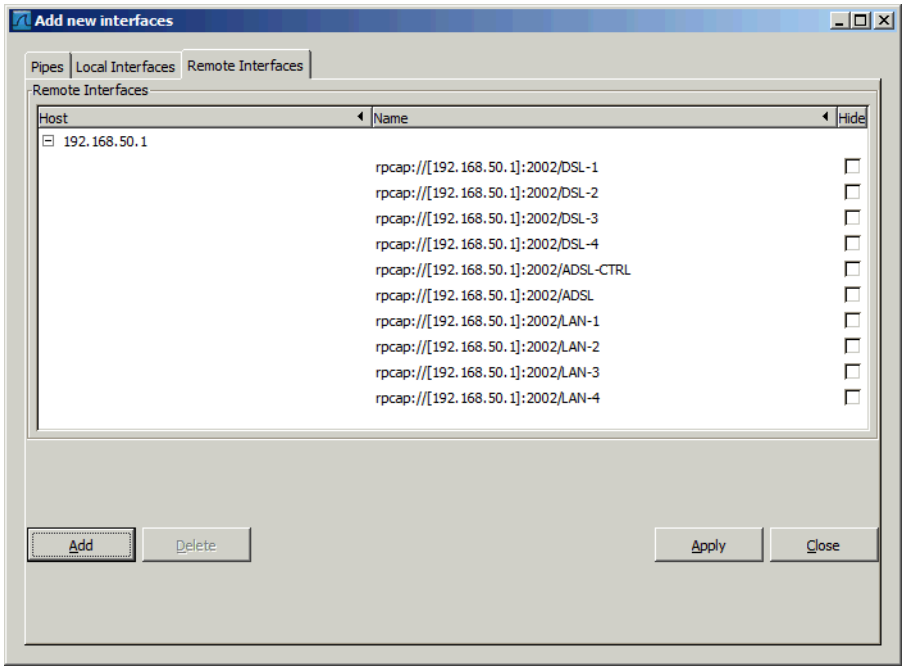
2. After starting the program, select **Capture Options**. In the window that appears, click on the button **Manage Interfaces**.



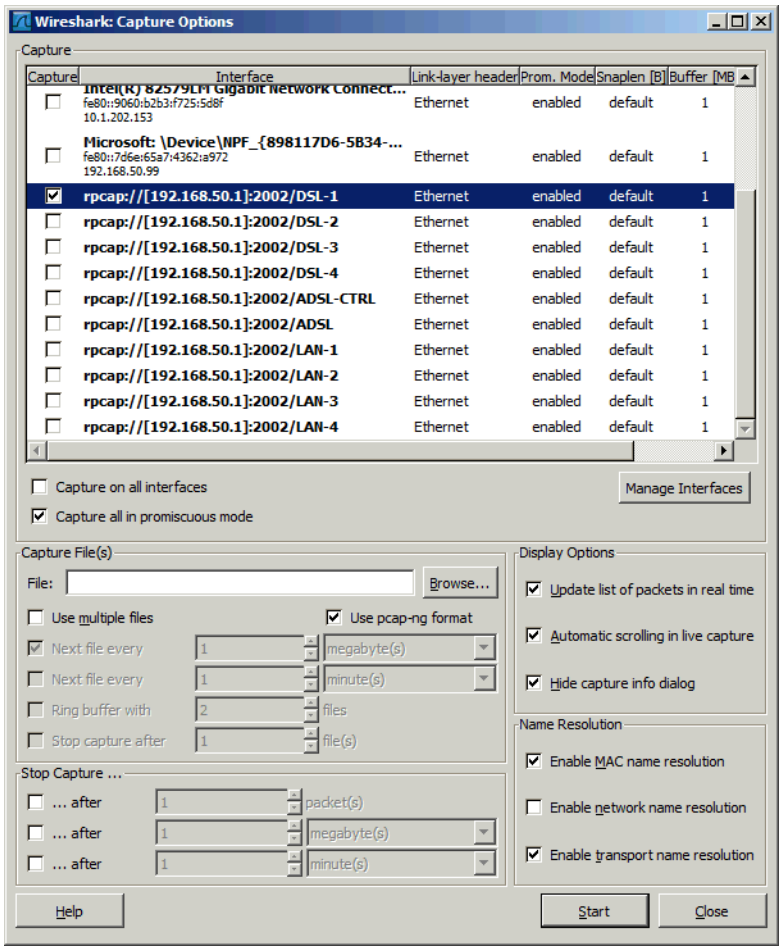
3. In the following window, select the tab **Remote Interfaces** and add your router. The field **Username** can be left blank. Set the password as the **main device password for the router**.



4. A list of all of the interfaces on the router available for data capture is displayed. Confirm the dialog by clicking on **Apply** and **Close**.



5. In the **Capture Options**, select which of the interfaces are to be captured. Now click on the **Start** button.



The packets passing through the selected interfaces are now captured.

4.3.4 Output capture data to a USB drive

You can do Wireshark captures in the background from the router to an attached USB drive, e.g. write to a USB stick. An active management session from the computer to the device is not required for this.

After recording, the file can be accessed by plugging the USB stick into a computer. Alternatively, the /usb/ directory on the device can be accessed remotely via SCP.

The USB drive must be FAT32 formatted. The device writes to the USB stick until it is full, after which the capture stops.

It is not possible to write or load a file to the internal flash of the device.

Enter the file name and all other necessary information using the command line in the table **Setup** > **Packet-Capture** > **Capture-to-File** > **Files**. See the Menu Reference Guide for the values.

4.4 The SYSLOG module

The SYSLOG module allows accessing of the device to be logged. This function is especially interesting for system administrators as it optionally records a complete history of all activities in the device.

A corresponding SYSLOG client or daemon is required to receive the SYSLOG messages. Logging under UNIX/Linux is generally performed by the SYSLOG daemon that is set up by default in these operating systems. The daemon either establishes contact with the CLI or writes its log to an appropriate SYSLOG file.

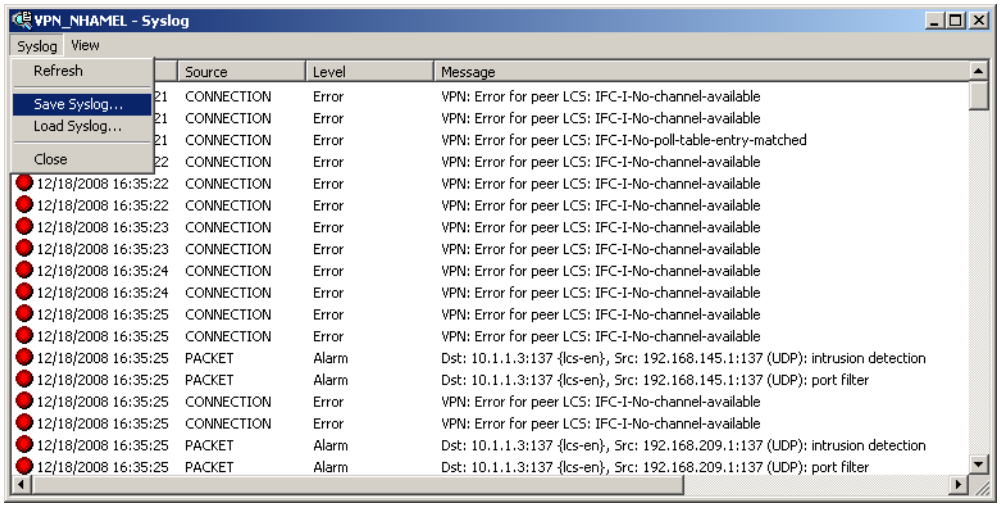
Under Linux, the file `/etc/syslog.conf` contains a definition of which facilities (service or component that issued the message) should be written to which log file. Please check your daemon's configuration to see if it explicitly listens to network connections.

Windows does not provide a corresponding system function. You require special software to provide the functionality of a SYSLOG daemon.

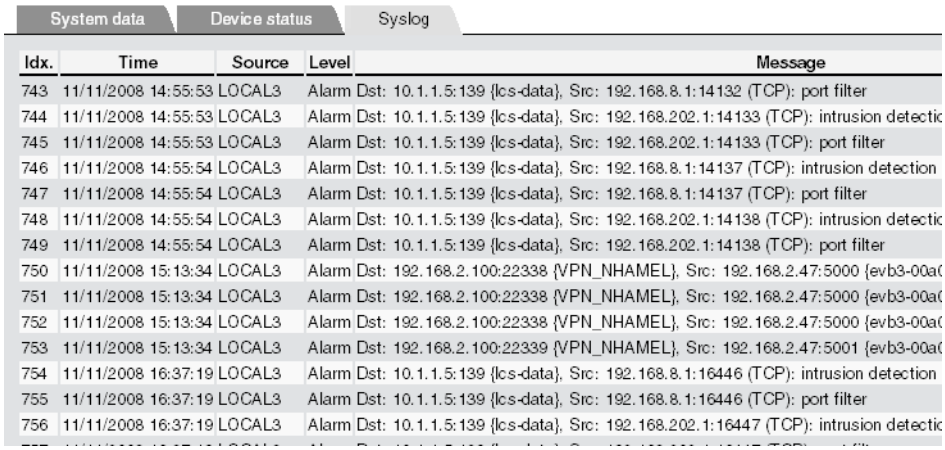
To extend the output of the SYSLOG information over an appropriate SYSLOG client, the most recent SYSLOG messages are stored in the device's RAM. Depending on the memory fitted, this can vary from 100 to 23,000 syslog messages. These internal syslogs can be viewed in various ways:

- In the device statistics on the command line
- In WEBconfig under /System information/Syslog
- LANmonitor additionally lets you export the syslog from the device and save it to a file. Simply click on the entry for the device with the right mouse button and select **View Syslog** from the context menu. A snapshot of the current status is displayed. Clicking on **Refresh** exports a copy of the current syslog and this is displayed in the window. **Save syslog...** stores the current display to a file. The content of syslog files can be viewed with **Load syslog...**.

SYSLOG messages will only be written to the device's internal memory if the device was entered as a SYSLOG client with the loopback address 127.0.0.1 or if boot-persistent storage is enabled. See *Boot-persistent SYSLOG, event log and boot log*.



Alternatively you can view the current SYSLOG messages on the first page of WEBconfig on the **SYSLOG** tab:



4.4.1 Structure of SYSLOG messages

SYSLOG messages consist of three parts:

- Priority
- Header
- Contents

4.4.1.1 Priority

The priority in a SYSLOG message contains information about the the message severity and the facility (service or component that triggered the message).

The eight severity levels originally defined in SYSLOG have been reduced to five levels in the device. The table below shows the correlation between the alert level, the meaning and the SYSLOG severities.

Priority	Meaning	SYSLOG severity
Alert	This category includes all messages requiring the system administrator's close attention.	PANIC, ALERT, CRIT
Error	All error messages which can occur under normal conditions are communicated at this level; no special attention is required by the administrator (e.g. connection errors).	ERROR
Warning	This level communicates messages which do not compromise normal operating conditions.	WARNING
Information	At this level, all messages are sent that have a purely informational character (e.g. accounting information).	NOTICE, INFORM
Debug	Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting.	DEBUG

The table below provides an overview of the meaning of all internal message sources that you can set in the device. The final column in the table also provides the default correlation between the internal sources of the device and the SYSLOG facilities. This mapping can be changed, if necessary.

Source	Meaning	Facility
System	System messages (boot events, timer system, etc.)	KERNEL
Logins	Messages about successful connection and disconnection as well as about login and logout of a user during PPP negotiation as well as errors that occur in the process	AUTH
System time	Messages about changes to the system time	CRON
CLI login	Messages about CLI logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.	AUTHPRIV
Connections	Messages about any errors that occurred during establishment and termination of connections (display trace)	LOCAL0
Accounting	Accounting information stored after termination of a connection (user, online time, transfer volumes)	LOCAL1
Administration	Messages on changes to the configuration, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.	LOCAL3

4.4.1.2 Header

The header contains the name or the IP address of the device which sent the SYSLOG message. The chronological sequence is also very important for evaluating the messages. Time information is only added to the messages at the SYSLOG client in order not to disturb their chronological consistency due to different device times.



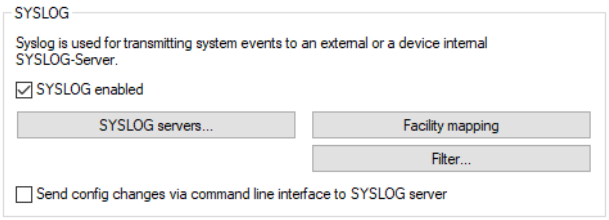
The devices must have a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

4.4.1.3 Contents

The actual contents of the SYSLOG messages describe the event, for example a login occurrence, the establishment of a WAN connection, or firewall activities.

4.4.2 Configuring SYSLOG

In LANconfig you configure SYSLOG under **Logging/Monitoring** > **Protocols** in the section **SYSLOG**.



SYSLOG enabled

Activate the SYSLOG protocol.

Send config changes via command line interface to SYSLOG server

Configuration changes made via the command line interface are sent to the configured servers via SYSLOG.

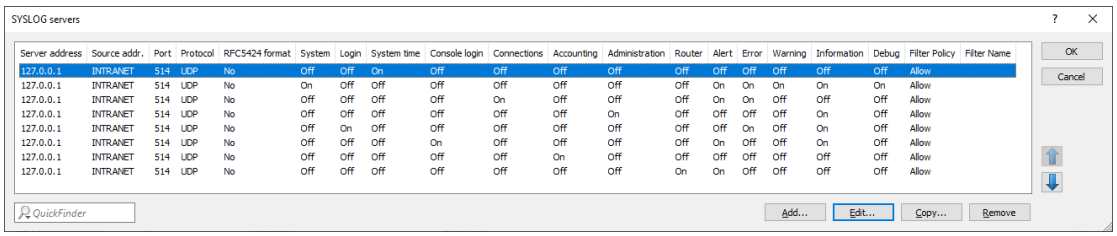
This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

4.4.2.1 SYSLOG server

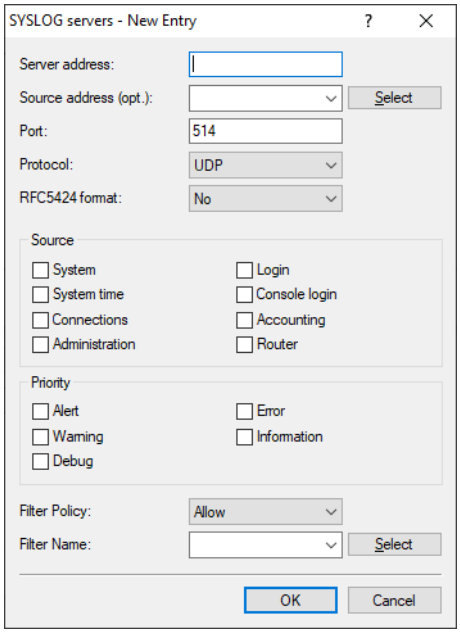
In LANconfig, you configure the settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **SYSLOG servers**.

Click on **SYSLOG servers** to see the entries available for SYSLOG.

With the factory settings, the table of SYSLOG entries is set up to display important events which are relevant to diagnostics, and to save these to the internal SYSLOG memory. These settings correspond to the specifications in the UNIX world, where SYSLOG originates from. The following screenshot shows these pre-defined SYSLOG entries under LANconfig:



Click on **Add**, or select an entry and click **Edit**.



Server address

Used to set the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a host name.

Source address (optional)

You can optionally specify a source address that the SYSLOG client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

Port

Specifies the port number (e.g. 514 for TCP/UDP).

Protocol

Defines the protocol used. Possible values:

UDP

User Datagram Protocol

TCP

Transmission Control Protocol

TLS

The syslog client supports three scenarios in TLS mode:

1. The syslog client accepts all TLS server certificates from the syslog server. For this purpose, no trusted CA certificate is stored in the router.
2. The syslog client only accepts server certificates signed by a trusted CA. To do this, the CA certificate must be uploaded to the corresponding certificate slot on the router.
3. The syslog client authenticates itself with the syslog server using a TLS client certificate and the syslog server authenticates itself with its CA certificate. To do this, both the TLS client certificate for the router and the CA certificate must be uploaded to the corresponding certificate slot on the router, e.g. in a container as a PKCS#12 file.

Certificates for syslog can be loaded into the device either via WEBconfig or LANconfig.

- **LANconfig**:**Right-click on the device** > **Configuration Management** > **Upload Certificate or File**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**
- **WEBconfig**: **Extras** > **File management** > **Upload Certificate or File** > **File Type**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**

RFC5424 format

Specifies whether the syslog client should send messages to the syslog server in RFC5424 format.

Source

The table below provides an overview of the meaning of all message sources that you can set in the device. The final column in the table also provides the correlation between the internal sources of the device and the SYSLOG facilities.

Source	Meaning	Facility
System	System messages (boot events, timer system, etc.)	KERNEL
Login	Messages concerning the user's login or logout during the PPP negotiation, and any errors that occur during this.	AUTH
System time	Messages about changes to the system time	CRON
Console login	Messages about CLI logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.	AUTHPRIV
Connections	Messages about establishment and termination of connections and any errors that occurred (display trace)	LOCAL0
Accounting	Accounting information stored after termination of a connection (user, online time, transfer volumes)	LOCAL1
Administration	Messages on changes to the configuration, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.	LOCAL3

Priority

The eight priority levels originally defined in SYSLOG have been reduced to five levels in the device. The table below shows the correlation between the alert level, the meaning and the SYSLOG priorities.

Priority	Meaning	SYSLOG priority
Alert	This category includes all messages requiring the system administrator's close attention.	PANIC, ALERT, CRIT
Error	All error messages which can occur under normal conditions are communicated at this level; no special attention is required by the administrator (e.g. connection errors).	ERROR
Warning	This level communicates messages which do not compromise normal operating conditions.	WARNING
Information	At this level, all messages are sent that have a purely informational character (e.g. accounting information).	NOTICE, INFORM
Debug	Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting.	DEBUG

Filter Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the following field, are allowed or denied.

Filter Name

Select one of the configured filters.

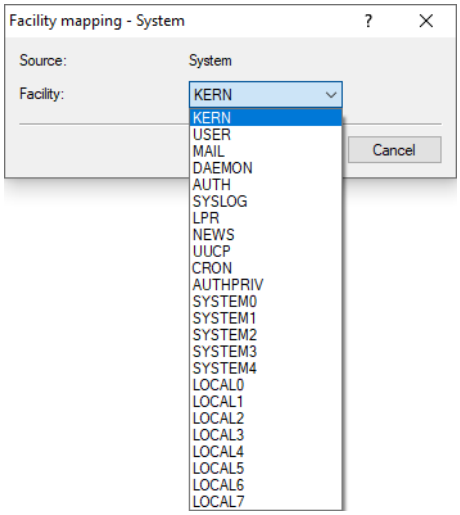
Once you have set all of the parameters, confirm your entries with **OK**. The SYSLOG table shows the SYSLOG client with its parameters.

4.4.2.2 SYSLOG facility mapping

The SYSLOG protocol uses certain designations for message sources, the so-called facilities. Each internal source in the devices that can generate a SYSLOG message must therefore be assigned to a SYSLOG facility.

The standard mapping can be changed, if necessary. In this way you can, for example, send all SYSLOG messages from a device with a specific facility (Local7). It is thus possible to collect all messages in a common log file by configuring the SYSLOG client appropriately.

Under **Logging/Monitoring** > **Protocols** in the section **SYSLOG** under **Facility mapping**, the internal sources can be assigned to the corresponding SYSLOG facilities.



Messages from the device are mapped to a facility, so that the SYSLOG client can write them to a special log file without any additional effort.

All facilities are set to 'local7'. Under Linux, the file `/etc/syslog.conf` with the entry

```
local7.* /var/log/lancom.log
```

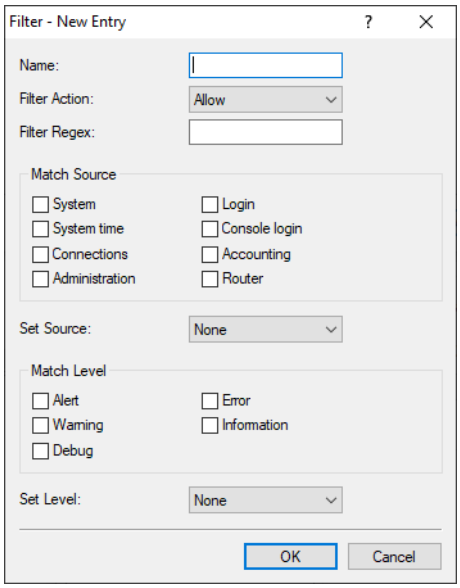
writes all of the device output to the file `/var/log/lancom.log`.

4.4.2.3 Filter

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages

depending on the source, priority and/or message text. Configure these filters here, which you can then use for entries on the SYSLOG server.

In LANconfig, you configure the filter settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **Filter**.



Name

Give the filter a descriptive name. Several rules can be created with the same filter name. These are then checked in the order in which they are created in the filter table when sending the messages. If there is no matching rule in this filter chain, the message is sent or discarded according to the server's default policy in the server table.

Filter action

Action when the rule applies; "Allow" enables messages to be sent to the server, "Deny" rejects the message.

Filter regex

Regular expression in Perl syntax (also see *Regular expressions in Perl*) to which the message text must apply. An empty string means that the message text is ignored, and therefore all message texts apply.

Match source

Source of the message to which this rule applies. The value "none" stands for any source.

Set source

New source of the message if the rule applies. The value "none" means that the source is not changed.

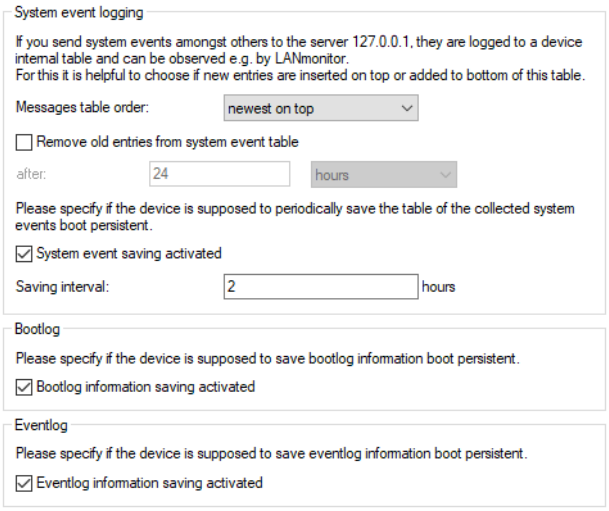
Match level

Priority of the message to which this rule applies. The value "none" stands for any priority.

Set level

New priority of the message if the rule applies. The value "none" means that the priority is not changed.

4.4.2.4 System event logging



Define for how long system events are saved

Under **Logging/Monitoring** > **System events** > **System event logging** you specify how long the device saves system events. To do so, select the option **Remove old entries from the system event table** and specify a time (0-9999) in hours, days or months.

In this case, a month is 30 days.

Boot-persistent SYSLOG, event log and boot log

The settings for the boot-persistent SYSLOG, event log and boot-log messages are to be found under **Logging/Monitoring** > **System events** (if available for your device). Activate the following options:

- SYSLOG: **System event saving activated**

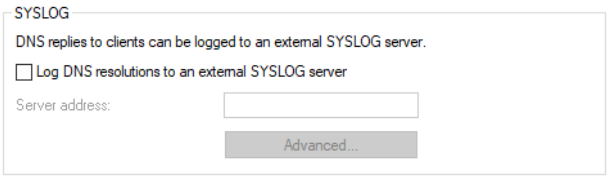
  Use the entry **Saving interval** to set the time in hours after which the SYSLOG system events are saved to boot-persistent memory.
- Bootlog: **Bootlog information saving activated**
- Eventlog: **Eventlog information saving activated**

4.4.2.5 Logging DNS requests and responses to external SYSLOG servers

The DNS server in LANCOM devices resolves the DNS queries from clients. SYSLOG provides an overview of the clients, the names they requested, and the responses they received.

It is not possible to use the router/access points own internal SYSLOG. For this reason it is necessary to employ an external SYSLOG server.

DNS logging is configured in LANconfig under **DNS** > **General** in the section **SYSLOG**.



Log the DNS resolutions on an external SYSLOG server

Select this option to enable the DNS logging.

> This option is independent of the setting in the SYSLOG module. Even if the SYSLOG module is disabled (setting under **Logging/Monitoring** > **Protocols** in the section **SYSLOG**), DNS logging is carried out nevertheless.

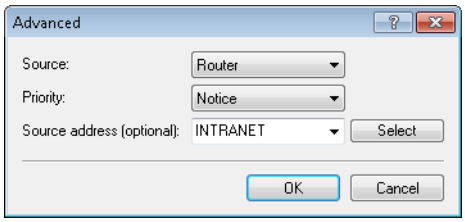
The corresponding SYSLOG message is structured as follows:

```
PACKET_INFO: DNS for <IP address>, TID {Hostname}: Resource record
```

Server address

Contains the IP address or the DNS name of the SYSLOG server.

The settings behind the button **Advanced** influence the content of SYSLOG messages.



Source

Contains the log source as displayed in the SYSLOG messages.

Priority

Contains the log level as displayed in the SYSLOG messages.

Source address (optional)

Contains the source address that is shown in the SYSLOG messages.

4.4.3 Meaning of SYSLOG messages

4.4.3.1 Extended status display of the login to the cellular network

In order to more quickly analyze connection problems in a cellular network, WWAN-capable routers report all logon procedures to the SYSLOG. In this manner, the user can recognize if and why the cellular service provider rejected the connection, for example.

The device generates a SYSLOG entry for each of the following events:

Status	Meaning	SYSLOG severity
WWAN: Currently not searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Registered to home network	The modem has registered on its service provider's cellular network.	INFORM
WWAN: Registered to foreign network	The modem has successfully registered on the cellular network of the service provider's roaming partner.	INFORM

Status	Meaning	SYSLOG severity
WWAN: Unknown registration	Initial value. The modem has not yet received a response from the radio module regarding the registration status.	INFORM
WWAN: Network registration denied	The cellular service provider has rejected the login on the cellular network.	ERROR
WWAN: Lost network registration	The modem lost the connection to the registered cellular network.	NOTICE
WWAN: Failed to set network	The modem has replied to the command to assign the network with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Failed to set network mode	The modem has replied to the command to assign the network mode with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using modem '...'.	Displays the modem in use.	INFORM
WWAN: Modem is gone.	Modem no longer available.	INFORM
WWAN: Resetting modem.	Re-init by modem reset	WARNING
WWAN: Local disconnect.	D-channel disconnect	INFORM
WWAN: Local disconnect (Release).	D-channel release	INFORM
WWAN: Force 2G mode at ... dB.	Modem starts the 2G fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem ends the 2G fallback	INFO
WWAN: Forced 2G mode disabled.	The 2G fallback mode is disabled.	INFO
WWAN: PIN missing in profile.	PIN is missing from the profile.	ERROR
WWAN: PUK required.	Modem requires the PUK.	ERROR
WWAN: Invalid PIN.	Incorrect PIN	ERROR
WWAN: Failed to set APN	Error when setting the APN The modem has replied to the command to assign the APNs with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using profile '...'.	Name of the profile in use.	NOTICE
WWAN: Cannot find profile '...'.	Profile not available.	ERROR
WWAN: Disconnected.	Physical connection is terminated.	INFORM
WWAN: Connected: '...'.	The modem has established a data connection and can now transmit data over the cellular network.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Cell ID and country code.	INFORM
WWAN: Current Network is '...'.	Network (text)	INFORM
WWAN: Current Network is	Network (number)	INFORM
WWAN: Mode ..., Band '...'.	Display of network mode and band	INFORM

Status	Meaning	SYSLOG severity
WWAN: Mode ..., Band '...', Bandwidth in MHz: ..., Channel (Rx/Tx): .../....	Display of network mode, band, bandwidth and channel (transmit and receive direction).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Display of network mode, band and channel (transmit and receive direction).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Current QoS data rate (down/upstream)	INFORM
WWAN: Network mode is '...'.	Current mode. Possible values are: › GPRS › EDGE › UMTS › HSPA › LTE/4G	INFORM
WWAN: Signal strength is ... dBm.	Current signal strength	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Access point currently being used in the network.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Change of network access point	INFORM
WWAN: Temperature is ...°C.	Current temperature of the module	INFORM
WWAN: Temperature status: '...'.	Current temperature status of the module. Possible values are: › Normal › High warning › High critical › Low critical	INFORM (normal), WARNING (high warning), CRITICAL (high critical, low critical)
WWAN: Closing device: '...'.	The device running the connection to the WAN is shutting down.	INFORM
WWAN: Hangup: '...'.	The modem terminates the network connection.	INFORM
WWAN: Error in modem init: '___'.	An error has occurred when initializing the modem.	ERROR

4.4.3.2 Documenting events on the xDSL interface

The device generates a SYSLOG entry for each of the following xDSL interface events:

Status	Meaning	SYSLOG severity
xDSL: Booting modem: ...	The modem is restarting.	NOTICE
xDSL: Set up line to <line mode>/<line type>	The xDSL module establishes the connection with the mode and type specified. The following values are possible: › Line mode: Disabled, auto and all modes configured in **Setup** > **Interfaces** > **ADSL or VDSL interface**. › Line type: POTS, ISDN	INFORM
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ...,	The modem connected successfully with the specified values.	NOTICE

Status	Meaning	SYSLOG severity
DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:		
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. This can lead to a change in the line values. After one minute, the modem transmits the current line values.	NOTICE
xDSL: Line data update.	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. After one minute, the modem transmits this message if the line values do not change after the synchronization.	NOTICE
xDSL: Line disconnected due to	The connection was disconnected for the specified reason. The following values are possible: › modem reboot › retrain › silence › high line error rate › protocol setting › line type setting › automode line type switch › modem timeout › VC parameter change	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	The value between the required and measured signal-noise ratio (SNR) has changed by more than 1dB.	INFORM

4.5 Parameter overview for the ping command

The ping command entered at the command prompt of a Telnet or terminal connection sends an “ICMP echo-request” packet to the destination address of the host to be checked. If the receiver supports the protocol and it is not filtered out in the firewall, the destination host will respond with an “ICMP echo reply”. If the target computer is not reachable, the last device before the host responds with a “network unreachable” or “host unreachable” message.

The syntax of the ping command is as follows:

```
ping [-46dfnoqrmb] [-s n] [-i n] [-c n] [-x x][-p <dscp>][-a ...] destination [%scope] [%scope@rtg-tag]
[%%interface] [@rtg-tag]
```

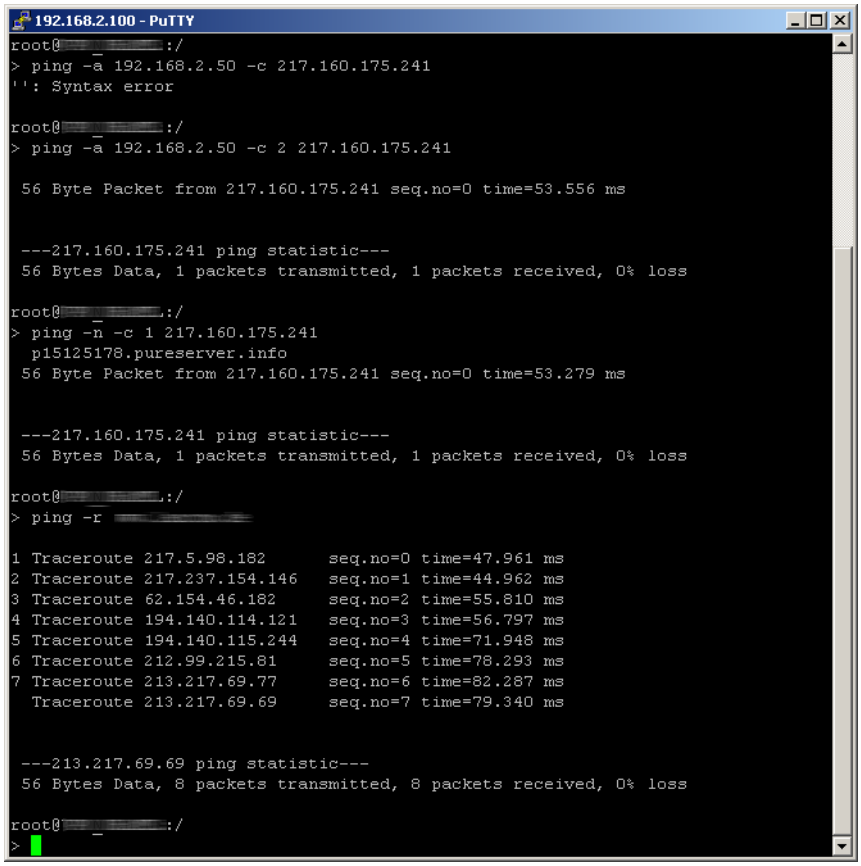
The meaning of the optional parameters is explained in the following table:

Table 23: Overview of optional parameters for the ping command

Parameter	Meaning
`-4`	Force IPv4
`-6`	Force IPv6
`-d`	Forbid fragmentation

Parameter	Meaning
`-f`	flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example. It is easy for flood ping to be misinterpreted as a denial-of-service (DoS) attack.
`-n`	Returns the computer name of a specified IP address.
`-o`	Immediately sends another request after a response.
`-q`	Ping command returns no output to the CLI (quiet).
`-r`	Switches to the traceroute mode. The path taken by the data packets to the target computer is displayed with all intermediate stations.
`-m`	Switches to the tracepath mode to determine the path MTU to the specified IP address.
`-b`	Do not stop pinging after receiving a PacketTooBig (DF), in order to achieve “Path MTU Discovery”.
`-s n`	Sets the packet size to n bytes (max. 65500).
`-i n`	Time between packets in seconds.
`-c n`	Send n pings.
`[-x x]`	Atomic fragments: (n)ever, (f)orce, (a)utomatic
`[-p <dscp>]`	Use a specific DSCP value for this ping. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible DSCP values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF
`-a a.b.c.d`	Sets the ping's sender address (default: IP address of the device.
`-a <name>`	Uses a named network, interface, or loopback address as the sender address
`-l <Load-Balancer-Policy>`	If the ping target is reached via a load balancer, the policy makes a load-balancer decision when the pings are sent. Possible values are default, traffic, bandwidth, round-robin, mst-used and all defined Dynamic Path Selection policies. If an invalid policy is specified, no pings are sent It is not possible to use this CLI option in combination with the specification of a scope or an interface binding in the destination.
`-6 <IPv6-Address>%<Scope>`	Performs a ping command to the link-local address via the interface specified by <scope>. For IPv6, the scope of parameters is of central importance: IPv6 requires a link-local address (fe80::/10) to be assigned to every network interface (logical or physical) on which the IPv6 protocol is enabled, so you must specify the scope when pinging a link-local address. This is the only way that the ping command knows which interface it should send the packet to. A percent sign (%) separates the name of the interface from the IPv6 address. **Examples:** › `ping -6 fe80::1%INTRANET` Pings the link-local address “fe80::1”, which is accessible via the interface and/or the network “INTRANET”. › `ping -6 2001:db8::1` Pings the global IPv6 address “2001:db8::1”.

Parameter	Meaning
`destination`	Address or host name of the target computer
`%scope`	Name of the interface used to send the packet when link-local addresses are used as the destination.
`%scope@rtg-tag`	Name of the interface used to send the packet when link-local addresses are used as the destination, with additional specification of the routing tag.
`%%interface`	Name of the destination interface. The packet is sent directly to the interface without taking the routing table into account.
`@rtg-tag`	Routing tag used to send the packet.
`stop /<RETURN>`	Entering `stop` or pressing the RETURN button terminates the ping command.

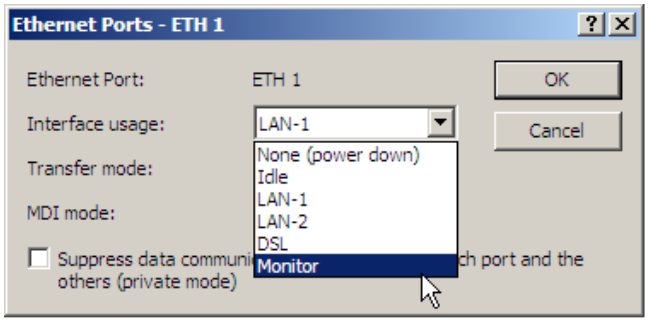


4.6 Monitoring the switch

The data transmission over the switch of LANCOM devices only takes place on the port the target computer is attached to. Therefore the connections on the other ports are not visible.

For monitoring data traffic between ports, the ports must be set to monitor mode. In this state all data is issued, that is transmitted over the switch of the devices between stations of the LAN and WAN.

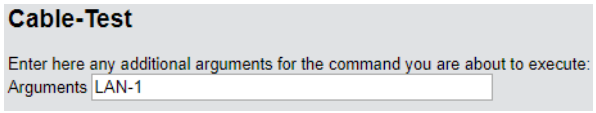
For the configuration with LANconfig open the Ethernet switch settings under **Interfaces** > **LAN** with the button **Ethernet ports**.



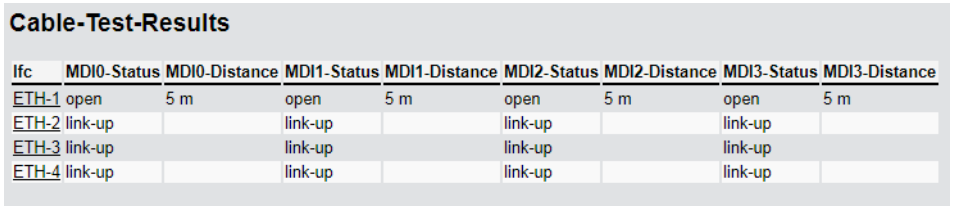
4.7 Cable test

If your LAN or WAN connection cannot not transfer any data even though the configuration of the equipment appears to be correct, there may be a fault in the cabling.

The cable test allows you to test the cabling from the device. This is done in WEBconfig by navigating to **Extras** > **LCOS menu tree** > **Status** > **LAN** > **Cable-Test**. Enter the name of the interface that you want to test (e.g. "DSL1" or "LAN-1"). Make sure you spell the name of the interface correctly. Start the cable test for the specified interface by clicking on the **Execute** button.



This is done by navigating to **Extras** > **LCOS menu tree** > **Status** > **LAN** > **Cable-Test-Results**. The list displays the results produced by the cable test for each interface.



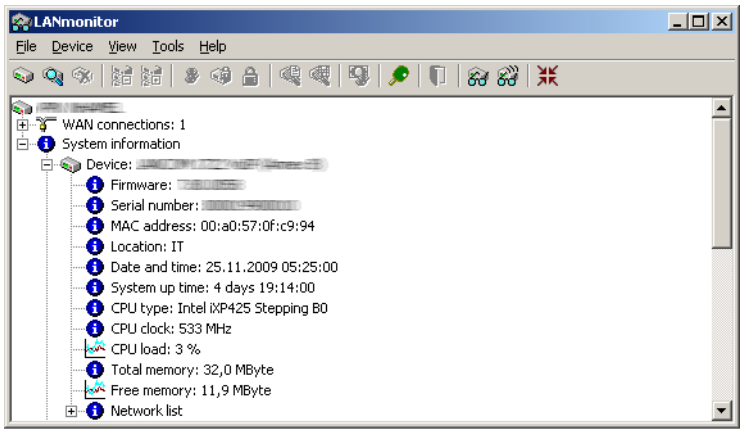
Cable-Test-Results

Ifc	MDI0-Status	MDI0-Distance	MDI1-Status	MDI1-Distance	MDI2-Status	MDI2-Distance	MDI3-Status	MDI3-Distance
ETH-1	open	5 m	open	5 m	open	5 m	open	5 m
ETH-2	link-up		link-up		link-up		link-up	
ETH-3	link-up		link-up		link-up		link-up	
ETH-4	link-up		link-up		link-up		link-up	

4.8 Average value of the CPU load display

4.8.1 Introduction

The current CPU load of the devices is displayed via various output options (LANmonitor, via WEBconfig or CLI in the status area, on some models in the display).



4.8.2 Configuration

You can set the time period over which the displayed CPU load is to be averaged as required.

Command line: **Setup** > **Config**

CPU-Load-Interval

Here you can select the time period for averaging the CPU load display. The display of CPU load in LANmonitor, status area, display (if available) as well as in any SNMP tools used is based on the averaging time frame. In the status area under WEBconfig or CLI, the CPU load values for all four possible averaging time frames are displayed.

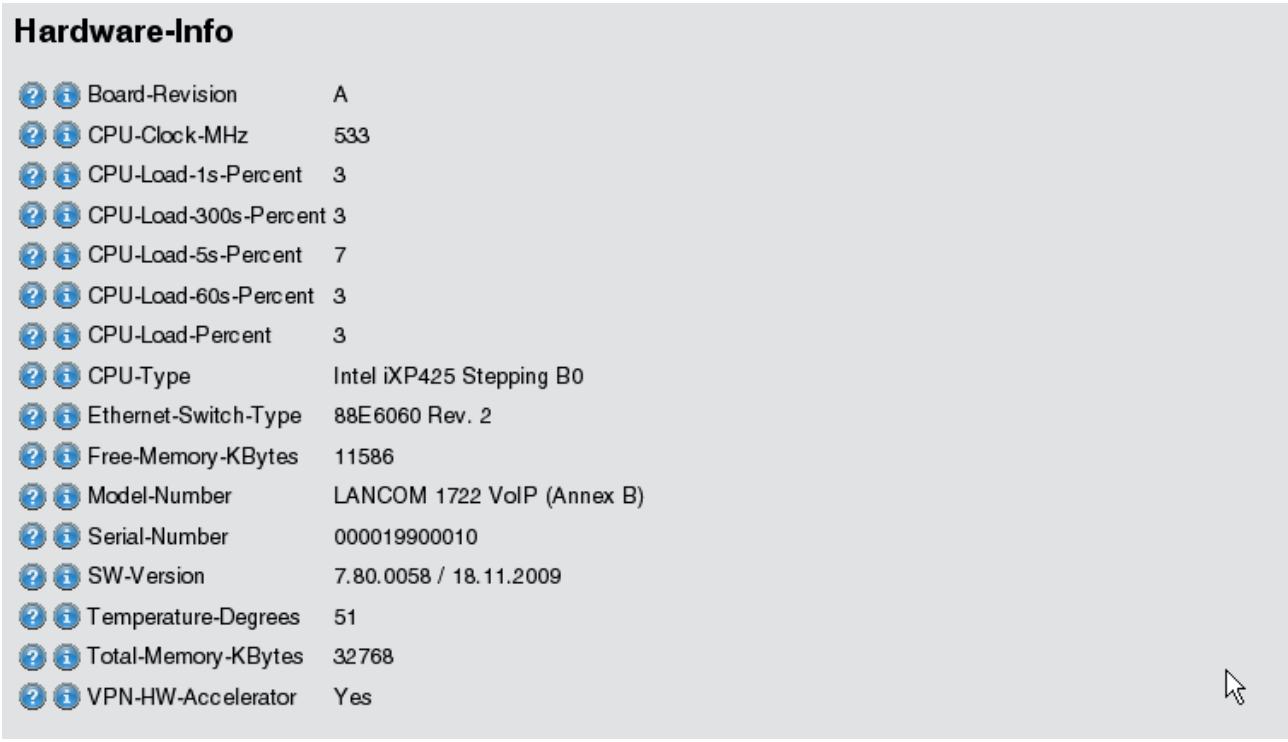
Possible values:

› 1, 5, 60 or 300 seconds.

Default:

› 60 seconds.

The default averaging over 60 seconds is prescribed in the HOST-RESOURCES-MIB, which is used by common SNMP tools to display the CPU load in a tachometer display. Please note this when adjusting the CPU load interval.



4.9 Sending attachments with the mailto command

E-mails with information on device status can be sent automatically if certain events occur. To do this, just include the mailto command into entries in the action table or cron table.

Attachments can be sent with the e-mails. This allows the results of console commands executed on the device before sending the mail to be sent as an attachment. In this way, the content of tables or menus (e.g. detailed status messages) can be sent by e-mail.

- Action (action table) or command (cron table) (max. 250 characters)

  Here you describe the action that is be executed at a certain time or when a change in the status of the WAN connection occurs. Only one action can be triggered per entry.

  Possible values for the actions (max. 250 characters):

  - mailto: – This prefix causes an e-mail to be sent.

  Optional variables for the actions:

  - attach=`console command`

  Any console command can be entered which outputs useful information. The console command is enclosed in "backquotes" also known as backticks. This character is produced with the aid of the "accent grave" key.

  The output of the console command is written to a text file for attachment to the mail. This text file is headed by the command and a time/date stamp, followed by the output.

Default:

› Blank

Examples:

The following action enables you to sent the ADSL status by e-mail:

```
mailto:admin@mycompany.de?subject=ADSL_status?attach=`dir /status/adsl`
```

An action can be used to send mutliple console commands:

```
mailto:admin@mycompany.de?subject=Status_reports?attach=`dir /status/adsl`?attach=`dir /status/config`
```

The attached files are named 'cmd1.txt', 'cmd2.txt', etc.

4.10 Enhanced Sysinfo

To determine whether changes have been made to the configuration, and to find the time/date when a change was made, Sysinfo contains additional entries in the field CONFIG_STATUS.

The devices store the value CONFIG_STATUS each time a change is made to the configuration (via the command line, via SNMP or by loading a script or complete configurations). The value CONFIG_STATUS consists of the following components:

› Hash value of the device configuration as a unique identifier of configuration status.
› Timestamp of the last change to the configuration in the format HHMMSSddmmyyyy based on Coordinated Universal Time UTC. The reference to UTC guarantees unique values without being influenced by time zone or daylight-saving settings.
› Counter of configuration changes, sequential.

The field CONFIG_STATUS contains, along with a value for the configuration status switches and a value for the configuration flash status, the additional components in the form <Hash>.<Date>.<Counter>.

Changes to the configuration can be implemented in the appropriate files or scripts (e.g. with LANtools) or on the devices directly (by command line or WEBconfig). The content of CONFIG_STATUS is influenced by the method by which configuration changes are made.

The device configuration hash value

Hash values are calculated solely by LCOS, the operating system used by the devices. The hash value differs for every state of configuration, and a modified hash value indicates that a device configuration has been changed.

LCOS stores the calculated hash value to the device during the flash process.

Timestamp of the last configuration change

Both LCOS and LANtools can set the timestamp, assuming that they have a valid time.

If the chosen method of configuration does not have a valid time, the device sets the timestamp to the value '00: 00:00 0000-00-00'.

Configuration changes counter

When the devices are shipped, the counter of configuration changes is set to '0'. Every configuration change after this increases the value by 1. The configuration-changes counter allows changes to the current version of the configuration to be determined, even if no valid time of configuration was available and the timestamp is therefore set to '00: 00:00 0000-00-00'.

A configuration counter that shows '0' after changes have been made to the configuration indicates an error while reading or writing the counter during flashing.

Displaying CONFIG_STATUS

To display the value for CONFIG_STATUS, enter the command `sysinfo` on the command line for the device.

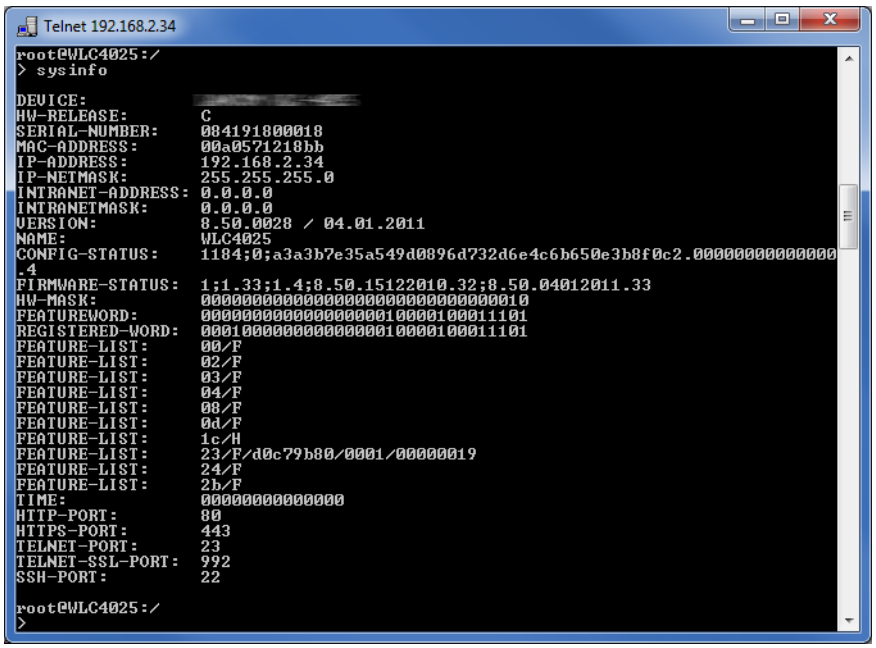


Figure 1: Displaying system information on the command line

4.10.1 Output additional ports in SYSINFO at the console

As of LCOS version 9.00, the `sysinfo` command also outputs the numbers of the following ports:

- HTTP
- HTTPS
- TELNET
- TELNET-SSL
- SSH
- SNMP
- TFTP

4.10.2 Output the configuration date

As of LCOS version 9.10, you have the option to read out the date and time of the device configuration via `status/config/config-date`.

SNMP ID: 1.11.20

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

The values are displayed in UTC format.

4.10.3 Output the configuration hashes

As of LCOS version 9.10, you have the option to read out the hash value of the device configuration via `status/config/config-hash`.

SNMP ID: 1.11.21

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

The displayed value is a SHA1 hash.

4.10.4 Output the configuration version

As of LCOS version 9.10, you have the option to read out the version number of the device configuration via `status/config/config-version`.

SNMP ID: 1.11.22

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

4.11 Bandwidth measurements with iPerf

Measurements of network performance determine values such as the throughput, latency, jitter and error rates over a network connection. The measured values are used, among other things, for network optimization, error detection and troubleshooting, and for assessing the performance of network infrastructures.

iPerf has become established as a free program for generating and evaluating data streams over data connections. An iPerf server daemon receives TCP and UDP streams and measures the throughput for the corresponding applications along with the latency, jitter, packet loss and packet reordering over UDP connections.

To conduct a bandwidth measurement between two hosts, you start the iPerf server on one device and the iPerf client on the other one. The iPerf client then connects to the iPerf server. The server and client exchange data packets for a certain time or a certain amount of data and generate statistics about this. These statistics provide information about the quality of the connection between the two devices.

When measuring the quality of the TCP connection, the iPerf client transmits completely filled TCP data packets at the fastest speed possible. The average data rate of successful data transfer (“goodput”) is the result of what the iPerf server received correctly.

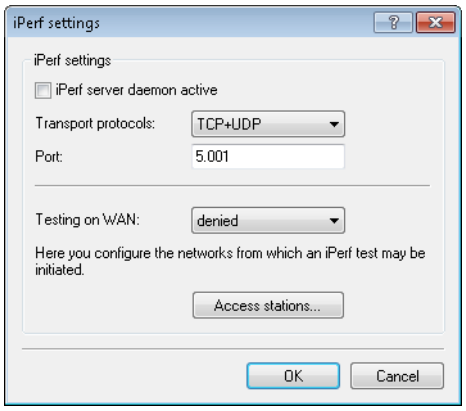
When measuring UDP connection quality, the iPerf client transmits data over a specified bandwidth (1 Mbps by default), although this is without flow or performance control. The “goodput” relates to the maximum bandwidth with which the client's transmission buffer remains permanently filled without data packets being lost.

LANCOM devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

Measurements can be carried out between two LANCOM devices or between a LANCOM device and another iPerf2 instance.

4.11.1 Setting up iPerf with LANconfig

In LANconfig, you configure iPerf under **Log & Trace** > **General** and clicking on **iPerf settings**.



iPerf server daemon active

Activates or deactivates the iPerf server daemon.

Rather than setting up the iPerf server to run permanently at this point, you can optionally start a one-off test by accessing the command-line console via SSH and starting a temporary iPerf server.

Transport protocols

Here you set which transport protocols are to be measured for bandwidth.

Port

This port is used for communications between the iPerf client and server ("5001" by default).

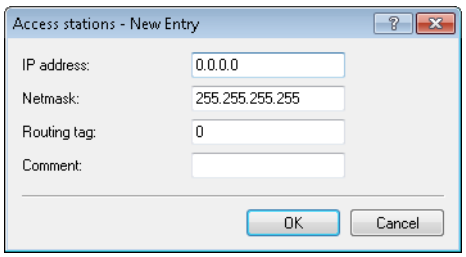
Testing on WAN

Here you determine whether measurements are also permitted over a WAN connection.

Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

Access stations

In order restrict iPerf access to certain stations only, enter the connection data into this table.



IP address

Enter the IPv4 address of the remote station.

Netmask

Enter the netmask of the remote station.

Routing tag

Enter the routing tag that specifies the connection to the remote station.

Comment

Enter a descriptive comment for this entry.

4.11.2 Temporary iPerf server and client

If you configure iPerf with LANconfig, the iPerf function remains permanently active. You can optionally start a temporary iPerf daemon, which remains active for just one test, by using SSH to connect to the command-line console.

To do this, start a terminal program (e.g. PuTTY) and open a connection to the device where you want to perform the iPerf test. Use the console command `iperf` and the appropriate option switches to start the temporary iPerf daemon.

The following examples illustrate some standard commands.



More information about the option switches for `iperf` is available in the section *Commands for the console*.

Running the iPerf server in TCP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s
[Iperf-TCP-Server|1526] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

Running the iPerf server in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s -u
[Iperf-UDP-Server|1524] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

Running the iPerf client in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -u -c 172.16.30.23
WARN: Using default UPD bandwidth limitation of 1 MBit/s
WARN: Using default UDP payload length of 1472 bytes (for matching Ethernet MTU via IPv4)
[Iperf-UDP-Client|2100] Connecting to server...
[Iperf-UDP-Client|2100] Connection established to 172.16.30.23:5001

root@device:/
>
```

Press the Enter key to exit the test.

```
[Iperf-UDP-Client|2100] Connection closed actively
[Iperf-UDP-Client|2100] Sent 1249728 bytes within 10s (10000ms) -> 0 Mbit/s (999 Kbit/s)
[Iperf-UDP-Client|2100] Server reports 1249728 bytes received within 9s (9985ms) -> 1 Mbit/s (1001
Kbit/s)
[Iperf-UDP-Client|2100] Server received 849 packets (0 lost / 0 out-of-order) with 62us jitter

root@device:/
>
```

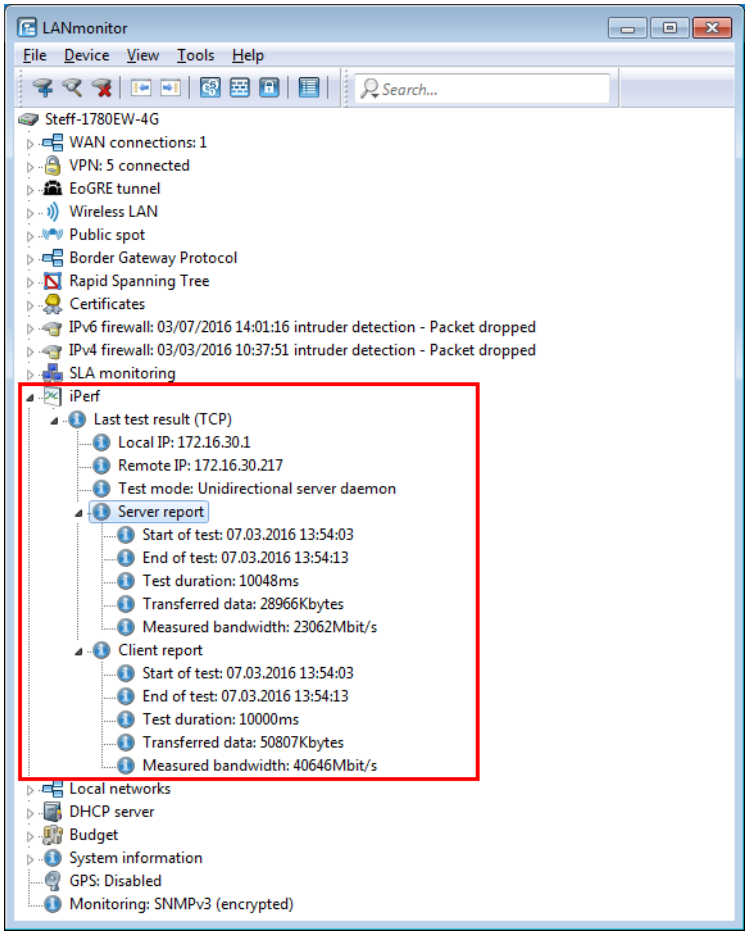
4.11.3 Analyzing iPerf results with LANmonitor

LANCOM devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.



For more information on iPerf, see the section *Bandwidth measurements with iPerf*.

The last iPerf test result can also be viewed in LANmonitor under “iPerf”. In this case it is unimportant whether the device initiated a connection or was contacted externally. The connection type “Test mode” displays the mode accordingly:



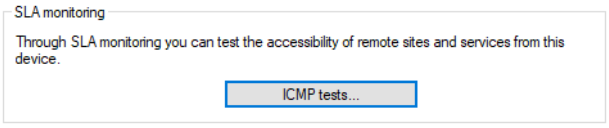
LANmonitor displays the test results stored in the device under **Status** > **Iperf** > **Last results**.

4.12 SLA monitoring

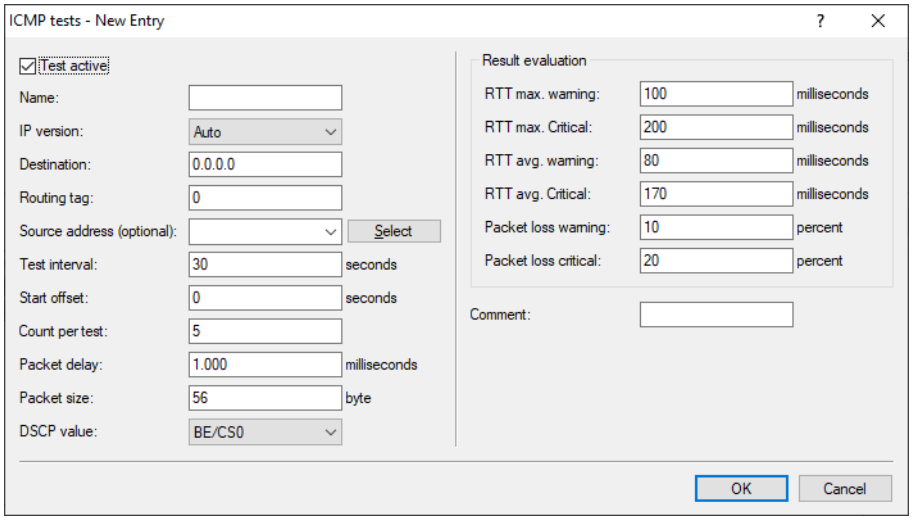
SLA monitoring is used to monitor the connections to remote stations within a network infrastructure. Ping tests to specified targets provide information about peer availability, packet transmission times and the number of lost packets. You can optionally define alerts that are issued when certain threshold values are exceeded, and to output these with LANmonitor. The history of past checks is also stored, so helping administrators to stay up to date about the quality of the connections.

4.12.1 Configuring SLA monitoring with LANconfig

For configuration with LANconfig, the SLA monitor is located under **Logging/Monitoring** > **General** on the **SLA monitoring** pane.



Click the button **ICMP tests**, add new queries and set guideline values for the connection tests.



Test active

With this check box enabled, the device uses the specified settings for the connectivity test.

Name

Name of connection

IP version

Specifies the use of IPv4 or IPv6.

The setting "Auto" is selected by default.

Destination

Specifies the destination for testing (ICMP/PING destination).

Routing tag

Specify a routing tag if a particular route is to be used.

Source address (optional)

You can optionally configure a source address if you want to use a specific network as the source interface.

Test Interval:

Specifies the time interval in which the device sends ICMP packets (**default: 30 seconds**).

Start offset

Set a delay time before ICMP packets are sent.

Count per test

Specifies how many ICMP packets are sent per test (**default: 5**).

Packet delay

Set a delay before packets are sent.

Packet size

Sets the packet size for the ICMP message.

DSCP value

Specifies the DSCP value of the ICMP message. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service). Possible values: BE/CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF

Result evaluation

In this section, you specify the threshold limits for packet handling.

RTT max. warning

Specify a maximum packet transmission time (**R**ound **T**rip **T**ime). A warning message is generated if an ICMP packet takes longer than the transmission time specified here.

RTT max. critical

An error message is generated if an ICMP packet takes longer than the transmission time specified here.

RTT avg. warning

Specify an average packet transmission time here. A warning message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

RTT avg. critical

Specify an average packet transmission time here. An error message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

Packet loss warning

A warning message is generated if the percentage of lost packets reaches the value specified here.

Packet loss critical

An error message is generated if the percentage of lost packets reaches the value specified here.

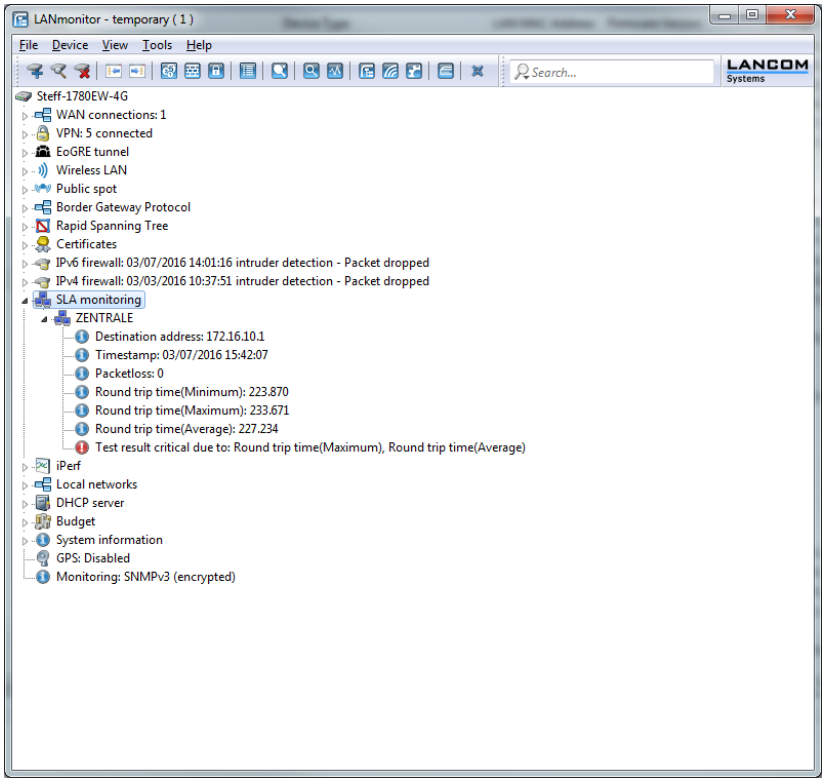
Comment

Enter a descriptive comment for this entry.

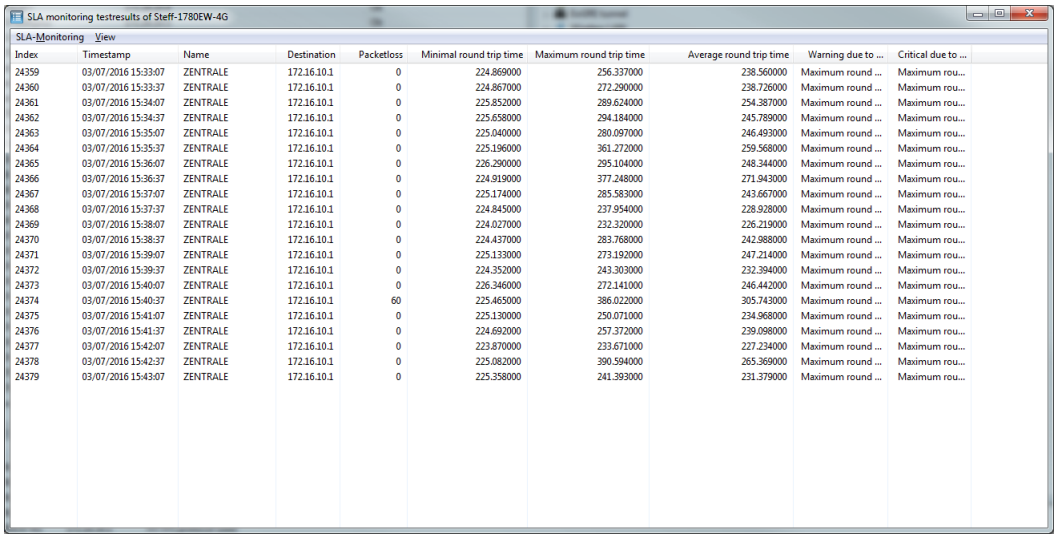
4.12.2 Displaying the SLA monitoring results in LANmonitor

LANmonitor displays the configured tests under **SLA monitoring**.

It shows the results of the most recently collected information from the connection test.



You also have the option to display the history of the connection tests. Click with the right mouse button on the entry **SLA monitoring**. In the following dialog, select **SLA monitoring history**.



Index	Timestamp	Name	Destination	Packetloss	Minimal round trip time	Maximum round trip time	Average round trip time	Warning due to ...	Critical due to ...
24359	03/07/2016 15:33:07	ZENTRALE	172.16.10.1	0	224.869000	256.337000	238.560000	Maximum round ...	Maximum rou...
24360	03/07/2016 15:33:37	ZENTRALE	172.16.10.1	0	224.867000	272.290000	238.726000	Maximum round ...	Maximum rou...
24361	03/07/2016 15:34:07	ZENTRALE	172.16.10.1	0	225.852000	289.624000	254.387000	Maximum round ...	Maximum rou...
24362	03/07/2016 15:34:37	ZENTRALE	172.16.10.1	0	225.658000	294.184000	245.789000	Maximum round ...	Maximum rou...
24363	03/07/2016 15:35:07	ZENTRALE	172.16.10.1	0	225.040000	280.097000	246.493000	Maximum round ...	Maximum rou...
24364	03/07/2016 15:35:37	ZENTRALE	172.16.10.1	0	225.196000	361.272000	259.568000	Maximum round ...	Maximum rou...
24365	03/07/2016 15:36:07	ZENTRALE	172.16.10.1	0	226.290000	295.104000	248.344000	Maximum round ...	Maximum rou...
24366	03/07/2016 15:36:37	ZENTRALE	172.16.10.1	0	224.919000	377.248000	271.943000	Maximum round ...	Maximum rou...
24367	03/07/2016 15:37:07	ZENTRALE	172.16.10.1	0	225.174000	285.583000	243.667000	Maximum round ...	Maximum rou...
24368	03/07/2016 15:37:37	ZENTRALE	172.16.10.1	0	224.845000	237.954000	228.928000	Maximum round ...	Maximum rou...
24369	03/07/2016 15:38:07	ZENTRALE	172.16.10.1	0	224.027000	232.320000	226.219000	Maximum round ...	Maximum rou...
24370	03/07/2016 15:38:37	ZENTRALE	172.16.10.1	0	224.437000	283.768000	242.988000	Maximum round ...	Maximum rou...
24371	03/07/2016 15:39:07	ZENTRALE	172.16.10.1	0	225.133000	273.192000	247.214000	Maximum round ...	Maximum rou...
24372	03/07/2016 15:39:37	ZENTRALE	172.16.10.1	0	224.352000	243.303000	232.394000	Maximum round ...	Maximum rou...
24373	03/07/2016 15:40:07	ZENTRALE	172.16.10.1	0	226.346000	272.141000	246.442000	Maximum round ...	Maximum rou...
24374	03/07/2016 15:40:37	ZENTRALE	172.16.10.1	60	225.465000	386.022000	305.743000	Maximum round ...	Maximum rou...
24375	03/07/2016 15:41:07	ZENTRALE	172.16.10.1	0	225.130000	250.071000	234.968000	Maximum round ...	Maximum rou...
24376	03/07/2016 15:41:37	ZENTRALE	172.16.10.1	0	224.692000	257.372000	239.098000	Maximum round ...	Maximum rou...
24377	03/07/2016 15:42:07	ZENTRALE	172.16.10.1	0	223.870000	233.671000	227.234000	Maximum round ...	Maximum rou...
24378	03/07/2016 15:42:37	ZENTRALE	172.16.10.1	0	225.082000	390.594000	265.369000	Maximum round ...	Maximum rou...
24379	03/07/2016 15:43:07	ZENTRALE	172.16.10.1	0	225.358000	241.393000	231.379000	Maximum round ...	Maximum rou...

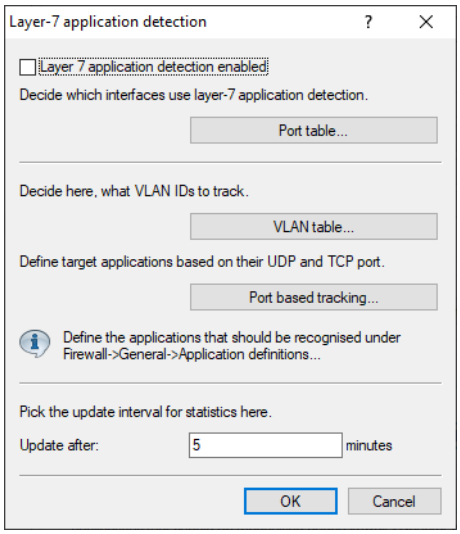
4.13 Layer-7 application detection

Layer-7 application detection helps you to identify services on your network that are frequently accessed and therefore consume high levels of bandwidth. This feature also allows you to isolate the clients that use these services most intensively and to inspect their traffic.

To use this function, you need to activate the layer-7 application detection. It is not enabled by default.

Application detection analyzes the inbound and outbound connections at each tracked interface, and it stores the statistics of the specified applications. As of LCOS version 10.12, layer-7 application detection captures *IPv4 and IPv6 traffic* separately.

In LANconfig, you enable and configure layer-7 application detection under **Firewall/QoS** > **General** > **Layer-7 application detection**.



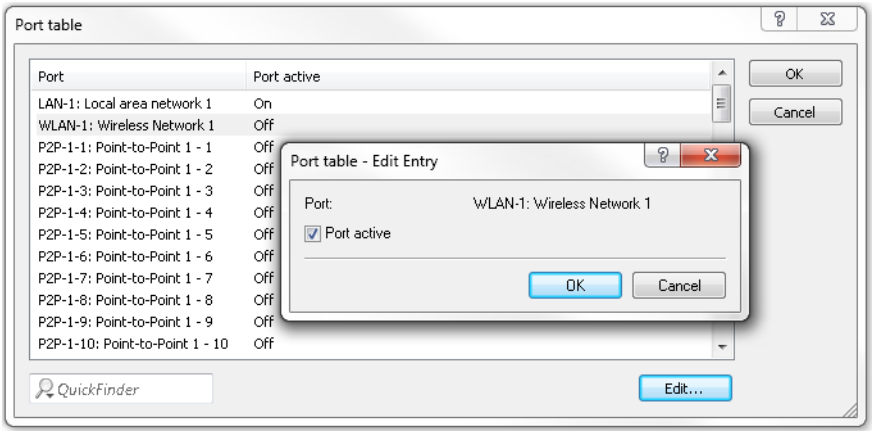
Use this dialog to specify the following parameters:

Layer-7 application detection enabled

This entry is used to enable or disable layer-7 application detection.

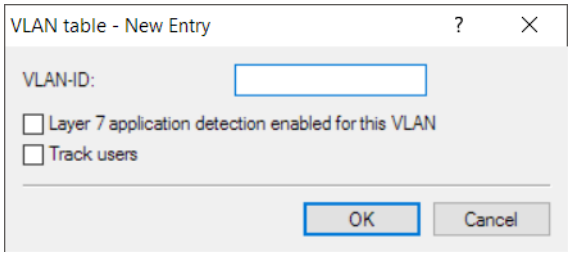
Port table

Here you specify the ports that are to be tracked by layer-7 application detection. Enable or disable the available ports correspondingly.



VLAN table

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

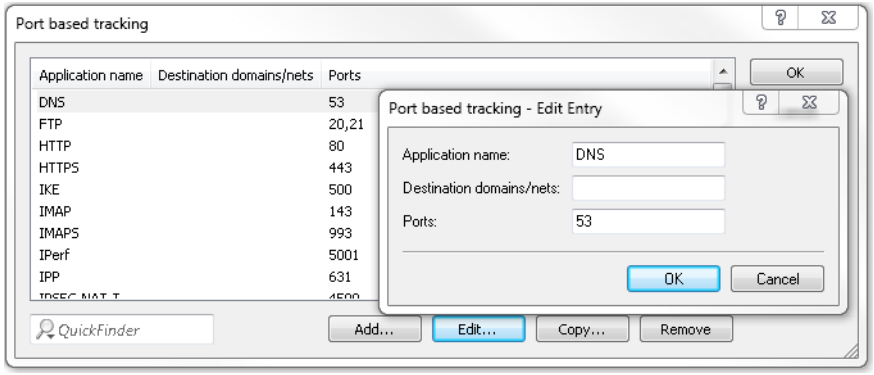


- **Layer-7 application detection enabled for this VLAN**: The device tracks general and application-specific data.
- **Track users:** The device tracks user-specific data (user or client name and MAC address) in the specified VLAN.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

Port-based tracking

Here you select the applications to be tracked. Optionally you can chose default applications or you can specify your own applications. You also specify the destination domains or the destination networks of the application. Extend the list according to your needs.



You can specify several destination domains, destination networks or ports by using a comma-separated list in CIDR notation (classless inter-domain routing). You have the option of using IPv4 or IPv6 destination networks.

Update after

Specify an interval in minutes for updating the usage statistics.

When a client establishes a connection over a tracked interface, layer-7 application detection begins analyzing and recording the traffic volumes.

The results of the recording and the usage statistics depend on the configuration that was specified for this connection.

Layer-7 application detection monitors the destination port of an application. If a connection Is detected arriving at port 80 or 443 (HTTP or HTTPS), the connection establishment is further analyzed. If a different destination port is used, the application is identified according to the applications entered into the "Port-based tracking" list.

You define the applications to be detected under **Configuration** > **Firewall/QoS** > **General** > **Application definitions**. See *Application definitions for layer-7 detection and layer-7 application control* on page 662.

If the establishment of an HTTP/HTTPS connection is detected, this connection is subjected to deeper analysis. For HTTP connections, the application detection additionally extracts the destination host from the destination URL in the HTTP GET request.

The only part to be used is the host; additional parts of the URL are truncated

If an HTTPS connection is detected, the layer-7 application detection attempts to identify the destination host in the following sequence:

- Server name indication from the TLS "Client Hello"
- Common name from the transmitted TLS server certificate
- Reverse DNS request to the server IP address

For HTTP and HTTPS connections, the destination host name found is compared with the "HTTP/HTTPS tracking" list. This list contains the most widely used Web services/applications, including the components of their host names.

If neither the service nor the connection appear in the list, i.e. the application cannot be identified, then it is classified as a general HTTP or HTTPS service on the port.

Allocation in this way requires the "Port-based tracking" list to include the entries HTTP and HTTPS.

If the destination service is known for every connection on a tracked interface, the combination with the connecting client makes is possible to track the connection and to determine which client caused what amount of traffic to / from a service.

The values found are available from the corresponding tables in the LCOS menu tree under **Status** > **Layer-7-App-Detection**.

Layer-7 application detection can be operated either centrally or decentrally on your network. Both options prevent traffic being listed multiple times:

Central

Layer-7 application detection is enabled on a central router in the LAN, and it is disabled on all other LANCOM devices.

Decentral

Layer-7 application detection is enabled only on the final bridges in the LAN, e.g. on access points or LANCOM routers with the clients connected directly to their LAN interfaces.

To avoid distorted results, the traffic should pass through just one single device or bridge running the layer-7 application detection.

4.13.1 IPv4/IPv6 traffic accounting

Layer-7 application detection captures IPv4 and IPv6 traffic separately.

There is no need to switch on this feature separately. With layer-7 application detection is active, both IPv4 and IPv6 applications are automatically resolved separately.

Layer-7 application detection logs details about the traffic transmitted over the relevant interface.

This is presented in the following status table:

```
root@LN-1700Esc:/Status/Layer-7-App-Detection/Total-Traffic-per-Protocol
> ls -a

[1.3.6.1.4.1.2356.11][1.95.8]
Protocol-Name  Tx-KBytes  Rx-KBytes  Tx-KBytes-Curr.-Day  Rx-KBytes-Curr.-Day
[1]            [2]        [3]        [4]                  [5]
```

```
===============-------------------------------------------------------------------
IPv4            522        259        522                259
IPv6            2696       18         2696               18
```

The inbound (RX) and the outbound (TX) traffic are listed separately for IPv4 and IPv6 in kBytes.

5 Security

You probably would not be happy about strangers viewing or modifying the data on your computers. Furthermore, the configuration settings of your devices need to be protected against unauthorized changes. This chapter is therefore dedicated to a very important topic: Security. The security settings are described in the following sections:

- Protecting the configuration
  - Password protection
  - Login barring
  - Access control

The most important security settings are summarized in a checklist at the end of the chapter. This list will help you to secure your device properly.

Further functions of the LCOS contribute to the security of your data, and some of these are described in separate chapters:

- *Firewall*
- *Router functions*
- *VLAN*

5.1 Protecting the configuration

By configuring the device, you specifiy a range of important parameters for data communication: This includes the security of your own network, cost controls, and the authorization of individual network users.

Obviously, the parameters you have set should not be changed by unauthorized persons. For this reason, the device offers various means of protecting the configuration.

5.1.1 Password protection

The simplest way of protecting the configuration is to agree upon a password.

If no password has been agreed for the device, the configuration is open to be changed by anybody. For example, your Internet access credentials could be exposed or the router reconfigured to disable the security mechanisms.

Among other things, the power LED flashes on devices that have no password set, assuming that the configuration can be accessed via WAN or WLAN.

5.1.1.1 Handling passwords properly

At this point we would like to make a few recommendations for handling passwords:

- **Keep your password as secret as possible.**

  Never write down a password. Popular but completely unsuitable are, for example: Notebooks, wallets and text files on the computer. It sounds trivial, but it cannot be repeated often enough: Do not share your password with anybody else. Even the securest systems are defenseless against talkativeness.

- **Communicate passwords securely.**

Once set, a password must be communicated to the remote site. Choose the most secure method possible. Avoid using: Unencrypted e-mail, letter, fax. It is better to communicate personally and face to face. The highest level of security is achieved when you enter the password personally at both ends.

› **Choose a secure password.**

Use random sequences of letters and numbers. Passwords that are normal words are not secure. Special characters such as '&"?-*_:;,!°' make it even more difficult for attackers to guess your password, which is a plus for your security.

The password for the configuration is case sensitive.

› **Never use a password twice.**

Using the same password for multiple purposes makes it less secure. If a remote site is compromised, the other connections that use this password are endangered all at once.

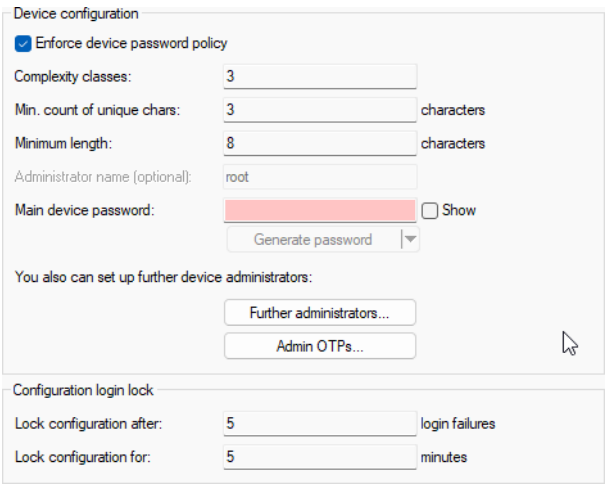
› **If you suspect anything, change the password immediately.**

When an employee with access to a password leaves the company, then it is high time to change that password. If you have even the slightest suspicion of a leak, change the password.

If you follow these simple rules, you will achieve a high level of security.

5.1.1.2 Entering the password

In LANconfig, the field for entering the password can be found under **Management** > **Admin** > **Device configuration** > **Main device password**. In a CLI session, you set or change the password with the command `passwd`. The maximum length of the main device password is 128 characters.



The **Show** option is only available if the device stores the passwords in such a way that it can restore them. You can adjust this with the value **Setup** > **Config** > **Passwords** > **Keep-Cleartext**.

The switch **Enforce device password policy** sets the following policies for the main device password and the administrator passwords:

Complexity classes

Configure the required number of different complexity classes for passwords. Complexity classes include lower and upper case letters, numbers, and special characters. With a setting of 2, the password must include characters from at least two of these complexity classes.

Minimum count of unique chars

Configure the required number of unique characters for passwords.

Minimum length

Configure the minimum number of characters for passwords.

As soon as a password is set for the "root" administrator in the device's configuration, WEBconfig will display the button Login that starts the login window. After entering the correct user name and password, the WEBconfig main menu will appear.

In the **Configuration login lock** section you can block access to the configuration for a few minutes after a configurable number of failed login attempts. This is an important aid against brute-force attacks on login data. A brute-force attack is the attempt by an unauthorized person to crack a password to gain access to a network, a computer or another device. To achieve this, a computer, for example, can go through all the possible combinations of letters and numbers until the right password is found. As a measure of protection against such attacks, the maximum allowed number of unsuccessful login attempts can be set. If this limit is reached, access will be barred for a certain time. The login lock only applies to the access path being used. The other access paths are still available.

For technical reasons, SSH and Telnet can only be locked and unlocked together.

5.1.1.3 Protecting the SNMP access

At the same time you should also protect the SNMP read access with a password. SNMP uses the general configuration password. More information can be found under *SNMPv3 access settings for administrators*

5.1.2 Further administrators with restricted rights

There is no need for every administrator to have full rights and access to all parts of the configuration. As root administrator, you can add further administrators with restricted rights under **Configuration** > **Management** > **Admin** > **Further administrators**. Consequently, there is no need for every administrator to know the main device password. Further details are available under *Managing rights for different administrators* on page 113.

5.1.3 Two-Factor Authentication (2FA) for Device Access

Access to management protocols (e.g., WEBconfig, SSH, Telnet) can be secured using two-factor authentication (2FA) in addition to the regular password. The feature can be configured separately for additional administrators or for the default root user.

In certain cases, management protocols must be allowed over unsecure channels, such as the Internet. To provide additional protection and safeguard the device against brute-force attacks, two-factor authentication can be enabled granularly for different access paths.

Common authenticator apps for mobile devices, such as smartphones, are supported.

Note that in the event of loss of the authenticator, a complete device reset may be required in the worst case. It is therefore recommended not to require 2FA for all configuration access methods — for example, not for serial console access or local LAN access — so that in the event of loss or misconfiguration, the device can still be accessed through normal means without 2FA.

It is especially recommended to enable 2FA protection for access via the WAN interface, including the use of encrypted protocols such as HTTPS or SSH.

Using 2FA requires the device to have the correct time. Therefore, the time reference should always be configured via the NTP client on the router in LANconfig under **Date & Time** > **Synchronization**.

The basic configuration process for two-factor authentication is as follows:

1. Create an entry in the "Admin-OTPs" table (LANconfig: **Management** > **Admin** > **Device configuration** > **Admin OTPs**), specifying the administrator account name to which this entry applies.
2. Open WEBconfig under **Extras** > **Admin-OTPs**. From there, the generated QR code for the user can be displayed, saved, or scanned by an external authenticator app.

3. When the management connection for the admin user is initiated, the user will be prompted to enter the one-time password (OTP) after entering their regular password.

The use of 2FA with OTPs is currently not natively supported by LANconfig/LANmonitor or LANtracer, i.e., through a separate OTP input field. However, it is possible to enter the OTP directly after the password in the password input field (without spaces or separators). The password must then not be saved, because the OTP will already have expired the next time it is used. Each time the password is entered, the currently valid OTP must be appended. In this way, the procedure also enables the use of OTPs with external applications that do not natively support OTPs.

Generating QR Codes for Connection with the Authenticator

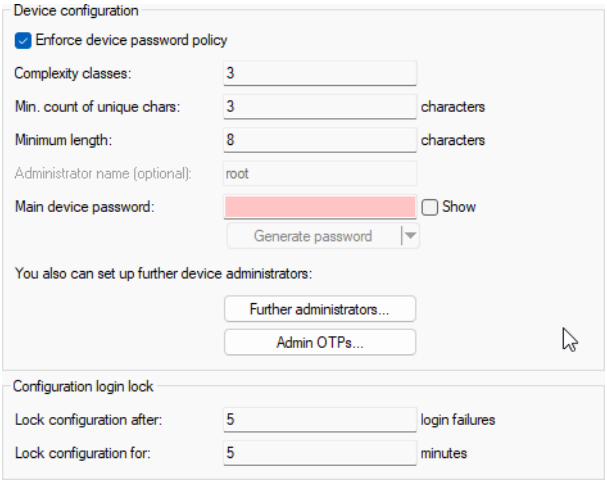
The QR codes used to connect the authenticator with the device are generated in WEBconfig under **Extras** > **Admin-OTPs** or alternatively via the CLI command "show Admin-OTP-QR".

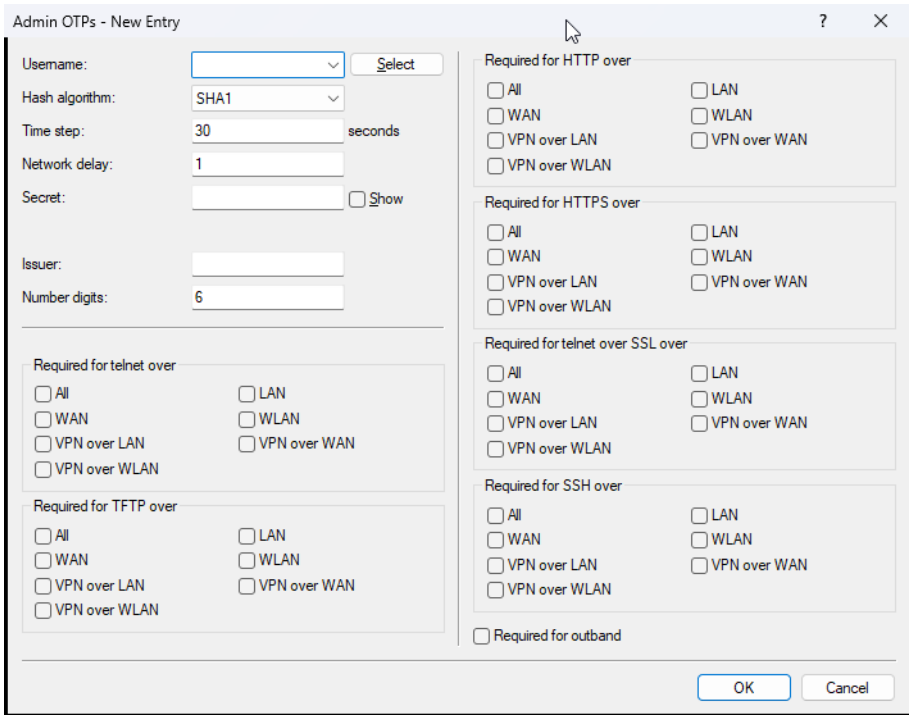
Show Commands

- show Admin-OTP *<Administrator>* – Displays the administrator OTP profiles
- show Admin-OTP-CODES *<Administrator>* – Displays the administrator OTP profiles (codes only)
- show Admin-OTP-QR *<Administrator>* – Displays the administrator OTP profiles (QR code only)
- show Admin-OTP-URI *<Administrator>* – Displays the administrator OTP profiles (URI only)

5.1.3.1 Admin OTPs

The settings for OTPs for administrator accounts can be found in LANconfig under **Management** > **Admin** > **Device configuration** > **Admin OTPs**.





Username

Username of the administrator for whom two-factor authentication is to be enabled, e.g., “root”.

Hash algorithm

Defines the hash algorithm to be used.

Make sure that the authenticator app supports the highest possible hash algorithm.

Time step

Defines the interval in seconds after which a new OTP is generated.

Network delay

Defines the maximum number of time steps by which the client’s clock may differ. The device checks the OTP that is older or newer by this value.

Secret

Defines the actual shared secret that must be shared with the authenticator app. The secret must be unique for each user. There are currently three input options in the table:

Base32 (Default)

Prefix “base32:” followed by the Base32-encoded secret. The prefix may also be omitted.

Hexadecimal

Prefix “hex:” followed by an even number of hex digits.

Plain text passphrase

Prefix “ascii:” followed by the characters.

For Google Authenticator, the secret must be 16 characters long (80 bits, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G.

Issuer

Freely definable text used in the authenticator to distinguish between multiple keys or for general display purposes when the same username is used. The value must not contain a colon.

Number digits

Length of the OTPs.

For Google Authenticator, the value should be set to 6.

Required for *protocol* over

Defines whether two-factor authentication is required for this user when logging in via this *protocol* and whether the device should prompt for it. You can configure granularly over which access paths two-factor authentication is required, e.g., only via a WAN connection.

All

Two-factor authentication is required for all access protocols.

WAN

Two-factor authentication is required for access via "WAN".

VPN over LAN

Two-factor authentication is required for access via "VPN over LAN".

VPN over WLAN

Two-factor authentication is required for access via "VPN over WLAN".

LAN

Two-factor authentication is required for access via "LAN".

WLAN

Two-factor authentication is required for access via "WLAN".

VPN over WAN

Two-factor authentication is required for access via "VPN over WAN".

Required for outband

Defines whether two-factor authentication is required for this user when logging in via the serial interface, or whether the device should request it.

5.1.4 Login barring

The configuration in the device is protected against "brute-force attacks" by barring logins. A brute-force attack is the attempt by an unauthorized person to crack a password to gain access to a network, a computer or another device. To achieve this, a computer, for example, can go through all the possible combinations of letters and numbers until the right password is found.

As a measure of protection against such attacks, the maximum allowed number of unsuccessful login attempts can be set. If this limit is reached, access will be barred for a certain time.

The login lock only applies to the access path being used. The other access paths are still available.

For technical reasons, SSH and Telnet can only be locked and unlocked together.

To configure the login lock, the following entries are available in the configuration tools:

- Activate lock after (`number of login errors`)
- Duration of the lock (`lockout in minutes`).

LANconfig: Management / Admin

If you fill out the field **Lock configuration after** with the value "0", the login lock is deactivated.

WEBconfig: LCOS menu tree / Setup / Config

The login lock has no function if RADIUS or TACACS are being used for authentication.

5.1.5 Restricting access to the configuration

Access to the internal functions can be configured for each interface separately:

- LAN
- Wireless LAN (WLAN)
- WAN (e.g. DSL or ADSL)

Access to the network configuration can be further restricted so that, for example, configurations can only be edited from certain IP addresses. Furthermore, the following internal functions can be switched on/off separately:

- LANconfig (TFTP)
- WEBconfig (HTTP/HTTPS)
- SNMP
- Terminal/Telnet

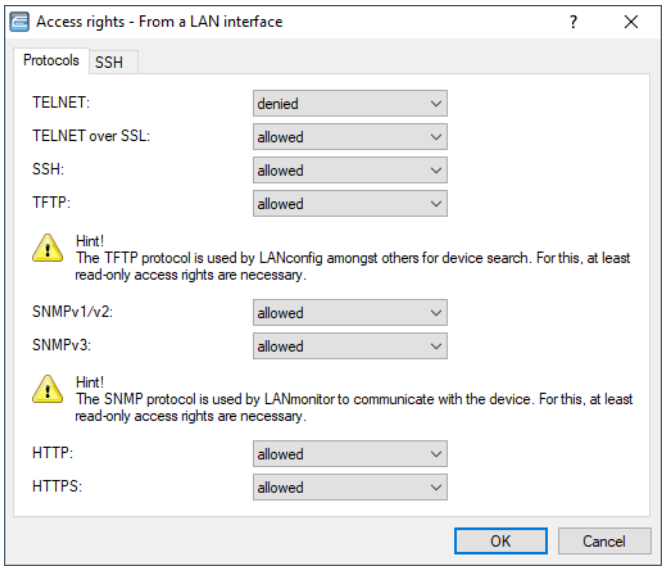
For devices supporting VPN, it is also possible for internal functions that operate over WAN interfaces to be restricted to VPN connections only.

5.1.5.1 Restricting network configuration access

Access to the internal functions can be controlled for each of the configuration services individually according to whether they are accessed from the local network, from remote networks, or from wireless LANs.

Access to the configuration can be allowed or denied in general, as purely read-only access or, if your model is so equipped, via VPN only.

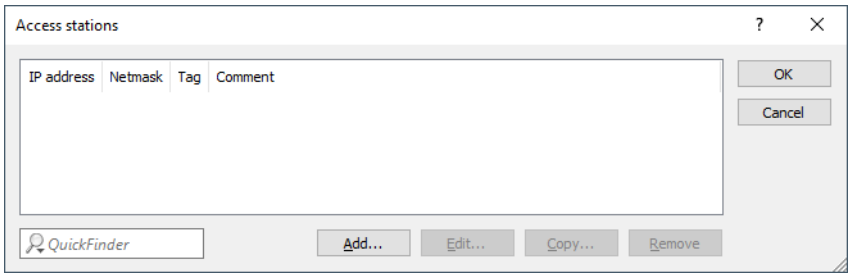
To open the LANconfig configuration dialogs containing the access rights from the local network (LAN), from the WLAN or via remote networks (WAN), go to **Management** > **Admin** in the section **Device access** and use the **Access settings** button. You then click on **Configurations access ways** > **Access rights** and select the appropriate interface:



To completely block access to the router from the WAN, set the configuration access rights from remote networks to “denied” for all protocols.

5.1.5.2 Restricting access to the network configuration to specific IP addresses

By means of a special filter list, you can restrict access to the internal functions of a device to specific IP addresses only. In LANconfig, the configuration dialog for entering the addresses that are permitted to access the stations is located in the **Access stations** table to be found under **Management** > **Admin** > **Device access** > **Access settings** > **Configuring access ways**.

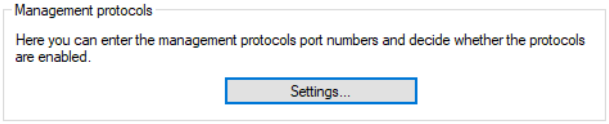


By default, this table contains no entries. This means that you can access your device from any IP address. You activate the filter by entering an IP address and the corresponding subnet mask. After that, only the IP addresses entered are entitled to use the internal device functions. Further entries will expand the selection of users with the associated rights. The filter entries can include individual computers or even entire networks.

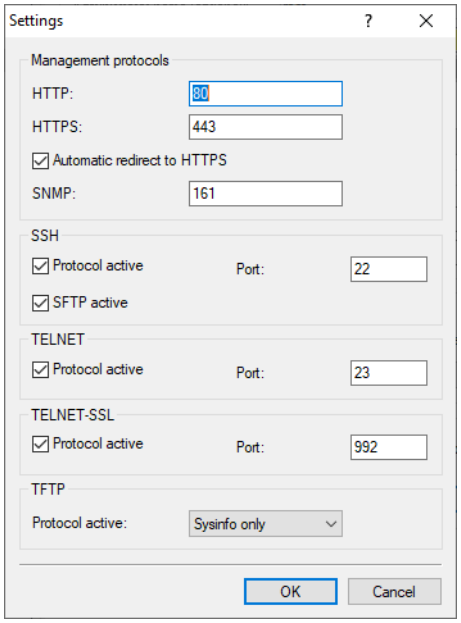
5.1.6 Management protocols

The management protocols allow you to define the protocols and their ports that should always be active for the configuration. In LANconfig, these settings are located under **Management** > **Admin** > **Management protocols**. You

can also set which protocols should be used on certain interfaces. Further details are available under *Restricting access to the configuration* on page 362.



Click on **Settings** to enable the following protocols and configure the port to be used:



HTTP/ HTTPS

Access via WEBconfig.

Automatic redirect to HTTPS

If WEBconfig is accessed with HTTP, this option automatically switches to an encrypted HTTPS connection. As a result, confidential data such as the login password or the configuration itself are secured with the encrypted connection.

SNMP

The SNMP protocol is active on the specified port.

SSH

Access to the command line via SSH. Additionally the protocol SFTP can be switched on or off here.

TELNET

Access to the command line via TELNET.

TELNET-SSL

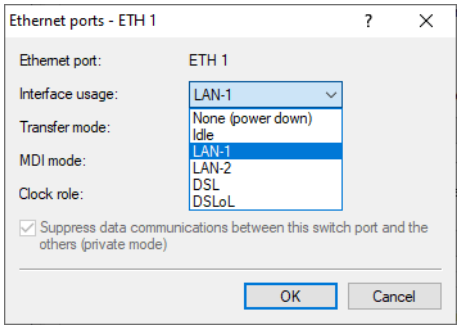
Access to the command line via TELNET-SSL.

TFTP

Access is via TFTP The trivial file transfer protocol (TFTP) is a simpler variant of the file transfer protocol (FTP). In contrast to FTP, TFTP permits the reading or writing of files via UDP only. The setting **Sysinfo only** leaves the port open, but the device responds only to a Sysinfo request. As a result it is displayed in LANconfig and, in particular, it will be found when searching for devices. However, no configuration can be uploaded to the device. Since this protocol transmits unencrypted, sensitive data could be intercepted on the network.

5.1.7 Deactivating Ethernet interfaces

The Ethernet interfaces on any publicly accessible device can potentially be used by unauthorized persons to gain physical access to a network. The Ethernet interfaces on the device can be disabled to prevent this.



LANconfig: **Interfaces** > **LAN** > **Ethernet switch settings** > **Ethernet ports**

Interface usage

Here you select how this interface is to be used.

Possible values:

None (power down)

The interface is deactivated.

Idle

The interface is not allocated to any particular task, but it remains physically active.

LAN-1 to LAN-n

The interface is allocated to a logical LAN.

DSL-1 to DSL-n

The interface is allocated to a DSL interface.

DSLoL

IPv4 addresses can only be masked (“NAT”) on WAN connections. If you want to masquerade in the direction of a LAN or WLAN interface, then the corresponding LAN or WLAN interface must be declared as a DSL port in order for it to establish a WAN connection (typically by IPoE or DHCPoE).

Monitor

The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Wireshark/Ethereal can be connected to this port, for example.

Default: Depends on the particular interface or the hardware model.

5.2 Location verification by GPS

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations do not stop third parties from operating RAS access, LAN connectivity or VPN connections that are set up in the device: A thief could gain access to a protected network.

The device’s operation can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

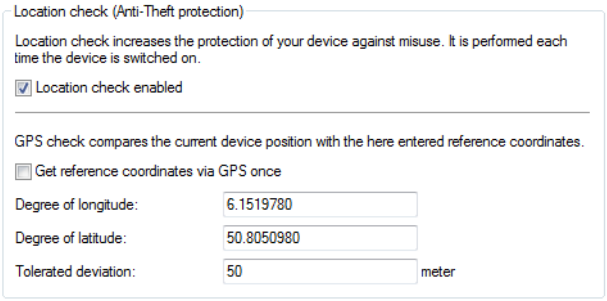
5.2.1 GPS location verification

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically activates the GPS module and checks if it is located at the "correct" position. The router module only switches on if the check is positive. After location verification has been carried out the GPS module is switched off again, unless it was activated manually.

5.2.2 Configuring location verification

Parameters for location verification are to be found in LANconfig under **Management** > **Location**.

Under **Management** > **Advanced** > **GPS module** you can switch on the GPS module so that it operates independently of the location check, for example to monitor the coordinates of the current location with LANmonitor.

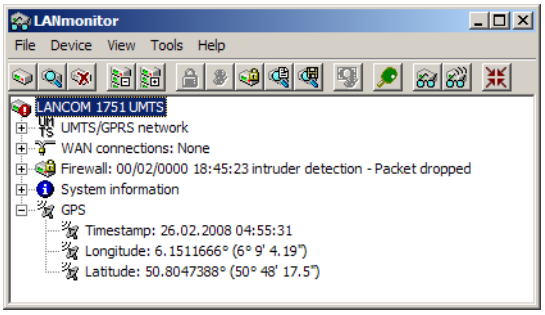


- Activate location verification with the option **Location check enabled**.
- Select the method for the location check:
  - 'GPS verification' for a check on the geographical coordinates.

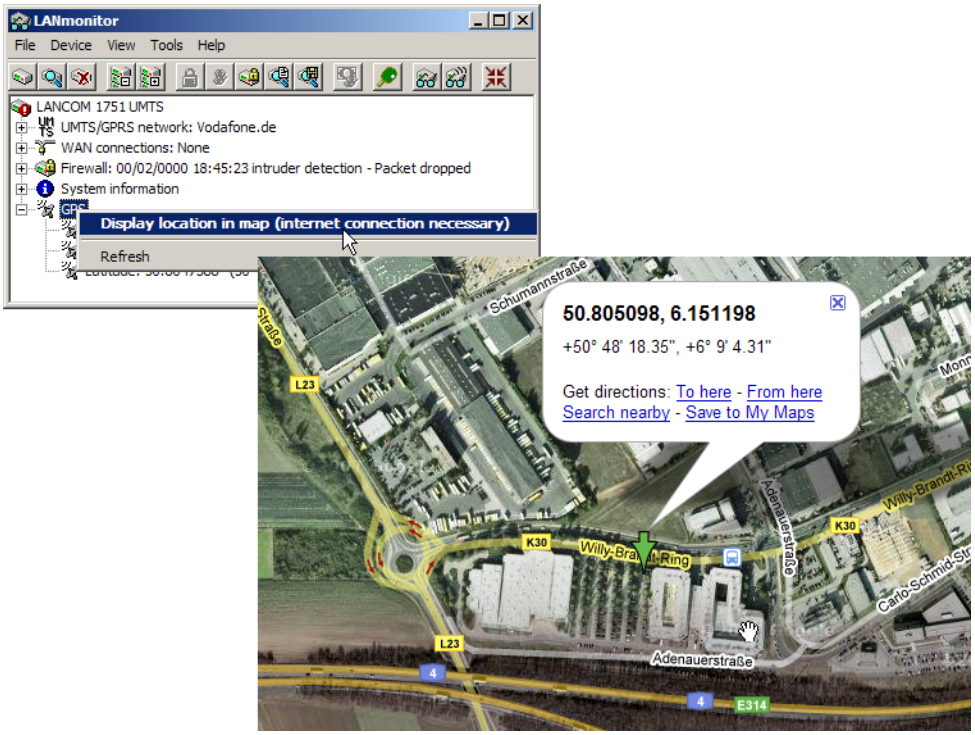
    For a location check by GPS an appropriate GPS antenna must be connected to the AUX connector on the device. Additionally, a SIM card for mobile telephone operation has to be inserted and the device must be logged on to a mobile phone network.
- For the location check enter 'Self call' or 'Call forwarding check' and enter the destination number as the telephone number to be used for the check.
- For location verification by GPS enter the necessary parameters:
  - Degrees latitude and longitude
  - Deviation from the intended position in meters

    The device is itself able to determine the geographical coordinates for its current position by activating the **Once get reference coordinates via GPS** checkbox. Once the configuration is written back to the device, the current longitude and latitude are entered automatically, assuming that location verification is activated and a valid GPS position is available. Subsequently this option is automatically deactivated again.

As an alternative you can determine the geographical coordinates from tools such as Google Maps.

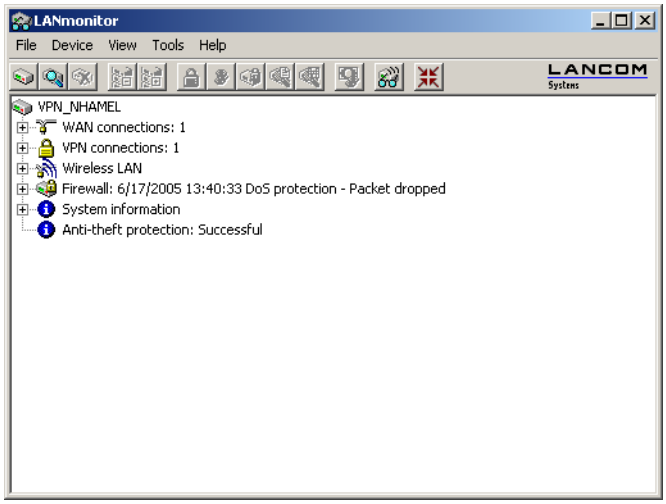


When the current geographical coordinates are displayed in LANmonitor, you can right-click with the mouse on the entry 'GPS' to call up that location in Google maps.



5.2.2.1 Status request, location verification

The status of location verification can be viewed with LANmonitor:



With WEBconfig (**LCOS menu tree / Status / Config / Location verification**) or Telnet (`Status/Config/Location-verification`) you can view the status of the location verification:



Only when the location verification has the status 'Successful' will the router data be transferred over the WAN interfaces.

› Location verification via GPS is successful when the GPS position is valid and within the tolerated range deviation from the known position.

5.3 Preventing password form fields in the browser from storing passwords

Input dialogs on web pages allow web browsers to store any passwords that are entered. This makes things easier for a user accessing the page again in future. This web browser feature is a vulnerability that malicious software can exploit to read out the confidential form data.

To force the manual input of login passwords each time a page is accessed, open WEBconfig and navigate to **Setup** > **HTTP** > **Disable-Password-Autocompletion** and prevent the storage of passwords with the setting “Yes”.

5.4 The security checklist

The following checklists provide an overview of all of the important security settings. Most of the points in this checklist are uncritical for simple configurations. In these cases, the security settings in the basic configuration or that were set with the Security Wizard are sufficient.

Have you secured your wireless network with encryption and access control lists?

With the help of 802.11i, WPA or WEP, you can encrypt the data in your wireless network with different encryption methods such as AES, TKIP or WEP. LANCOM recommends the strongest possible encryption with 802.11i and AES. If the WLAN client adapters do not support these, then you should use TKIP or at least WEP. Make sure that the encryption function in your device is activated, and that at least one passphrase or WEP key has been entered and selected for application.



For security reasons, LANCOM strongly advises you not to use WEP! You should only ever use WEP under exceptional circumstances. When using WEP encryption, use additional security mechanisms additionally.

To check encryption settings in LANconfig, go to **Wireless LAN** > **Encryption** > **WLAN encryption settings** and select the settings for the logical WLAN interfaces.

With the access control list (ACL) you can permit or prevent individual clients accessing your wireless LAN. The decision is based on the MAC address that is permanently programmed into wireless network adapters. To configure the access-control list in LANconfig, go to **Station rules** under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC**.

The LANCOM Enhanced Passphrase Security (LEPS) uses an additional column in the ACL to assign an individual passphrase consisting of any 8 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA2 is only possible with the right combination of passphrase and MAC address. See also *Configuration* on page 966.

Access control is takes place in phases. First, a search is made for a LEPS-MAC entry. If no such entry exists, a search is made for a LEPS-U entry. Finally, a search is made for a passphrase set for the WLAN under **Wireless LAN** > **Encryption** > **WLAN encryption settings**.



When operating LEPS-U and/or LEPS-MAC, this passphrase should be kept secret and preferably not used at all. Users or MAC addresses removed from the system should not be able to gain access by means of the WLAN passphrase instead.

Have you protected the configuration with a password?

The simplest way of protecting the configuration is to agree upon a password. If no password has been agreed for the device, the configuration is open to be changed by anybody. In LANconfig, the field for entering the password is located under **Management** > **Admin**. It is absolutely imperative to assign a password to the configuration if you want to enable remote configuration!

Have you permitted remote configuration?

If you do not require remote configuration, please ensure to switch it off. If you need to make use of remote configuration, ensure that you do not fail to password-protect the configuration. In LANconfig, the field for disabling remote configuration is located under **Management** > **Admin** > **Device access** > **Access settings**. In the section **Configuration access ways Access rights** > **From a WAN interface** set all protocols to **denied**. You also have the option of blocking the HTTP port for web-server services. To do this, go to the section **Access to web server services** and under **Access rights** > **From a WAN interface** select the option **disabled**.

Have you allowed configuration from the wireless LAN?

If you do not need to configure the device from the wireless LAN, switch this function off. In LANconfig, the field for disabling configuration from a wireless LAN is also located under **Management** > **Admin** > **Device access** > **Access settings**. In the section **Configuration access ways Access rights** > **From a WLAN interface** set all protocols to denied. You also have the option of blocking the HTTP port for web-server services. To do this, go to the section **Access to web server services** and under **Access rights** > **From a WAN interface** select the option **disabled**.

Have your password-protected the SNMP configuration?

Protect the SNMP configuration with a password too. The field for password-protecting the SNMP configuration is also to be found in LANconfig under **Management** > **Admin**.

Have you activated the firewall?

The stateful inspection firewall of devices ensures that you local network cannot be attacked from the outside while your WLAN controller is operating as a Public Spot. Activate the firewall in LANconfig under **Firewall/QoS** > **General**.



Note that firewall security mechanisms (incl. IP masquerading, port filters, access lists) are active only for data connections that are transmitted via the IP router. Direct data connections via the bridge are not protected by the firewall!

Are you using a "deny all" firewall strategy?

Maximum security and control is initially achieved by denying all data traffic from passing the firewall. The only connections to be accepted by the firewall are those that are to be explicitly permitted. This ensures that "Trojan horses" and certain types of e-mail virus are denied communication to the outside. The firewall rules in LANconfig are located under **Firewall/QoS** > **IPv4 rules** > **Rules** and **Firewall/QoS** > **IPv6 rules** > **IPv6 inbound rules** or **Firewall/QoS** > **IPv6 rules** > **IPv6 forwarding rules**.

The stateful inspection firewall of devices ensures that you local network cannot be attacked from the outside while your WLAN controller is operating as a Public Spot. Activate the firewall in LANconfig under **Firewall/QoS** > **General**.



Note that firewall security mechanisms (incl. IP masquerading, port filters, access lists) are active only for data connections that are transmitted via the IP router. Direct data connections via the bridge are not protected by the firewall!

Have you activated IP masquerading?

With "IP masquerading", local computers remain invisible to the outside while they access the Internet. All that is revealed to the Internet is the IP number of the router module of the device. The IP address can be fixed or dynamically assigned by the provider. The computers in the LAN use the router as a gateway and are not visible individually. The router separates the Internet from the intranet like a wall. The application of IP masquerading is set in the routing table for every route individually. The routing tables for IPv4 and IPv6 in LANconfig are located under **IP router** > **Routing**.

Have you used filters to close critical ports?

The firewall filters in the device offer filter functions for individual computers or entire networks. It is possible to set up source and destination filters for individual ports or port ranges. Furthermore, filters can be set for individual protocols or any combination of protocols (ICMP). It is especially convenient to set up the filters with the aid of LANconfig. You can create and modify filter rules under **Firewall/QoS** > **IPv4 rules** > **Rules** and **Firewall/QoS** > **IPv6 rules** > **IPv6 inbound rules** or **Firewall/QoS** > **IPv6 rules** > **IPv6 forwarding rules**.

Have you excluded certain stations from accessing the device?

A special filter list can be used to limit access to the device's internal functions via TCP/IP. The phrase "internal functions" refers to configuration sessions via LANconfig, WEBconfig, Telnet or TFTP. As standard this table

contains no entries, meaning that computers with any IP address can use TCP/IP and TFTP to commence accessing the device. The first time an IP address is entered with its associated netmask, the filter is activated and only the IP addresses contained in this entry are entitled to make use of internal functions. Further entries can be used to extend the circle of authorized parties. The filter entries can describe individual computers or even entire networks. The access lists in LANconfig are located under **Firewall/QoS** > **IPv4 rules** and **Firewall/QoS** > **IPv6 rules**.

Do you store your saved configuration to a safe location?

Protect your saved configurations in a location that is safe from unauthorized access. Otherwise, byway of example, an unauthorized person may load your stored configuration file into another device and they can access the Internet at your expense.

Concerning the exchange of your particularly sensitive data via wireless LAN; have you set up the functions offered by IEEE 802.1X?

If you move especially sensitive data via wireless LAN you can provide even stronger security by using the IEEE 802.1X technology. In LANconfig, the IEEE 802.1X settings are configured under **Wireless LAN** > **802.1X**.

Have you activated the protection of your WAN access in case the device is stolen?

After being stolen, the device can theoretically be operated at another location by unauthorized persons. Password-protected device configurations do not stop third parties from operating RAS access, LAN connectivity or VPN connections that are set up in the device: A thief could gain access to a protected network.

The device's operation can be protected by various means; for example, it will cease to function if there is an interruption to the power supply, or if the device is switched on in another location.

GPS location verification enables a geographical position to be defined within the device. After being switched on the device automatically checks if it is located at the "correct" position. Only after a positive check is the router module activated.

The scripting function can store the entire configuration in RAM only so that restarting the device will cause the configuration to be deleted. The configuration is not written to the non-volatile flash memory. A loss of power because the device has been relocated will cause the entire configuration to be deleted.

Is the storage of configuration files adapted to your security requirements?

For "standalone operation", the configuration for a WLAN interface being managed by a WLAN controller is stored in flash memory for a certain time only, or even in the RAM only. This device configuration is deleted if contact to the WLAN controller is lost or if the power supply is interrupted for longer than the set time period.

Have you ensured that the reset button is safe from accidental configuration resets?

Some devices simply cannot be installed under lock and key. There is consequently a risk that the configuration will be deleted by mistake if a co-worker presses the reset button too long. The behavior of the reset button can be set so that a press is either ignored or it causes a re-start, depending on the time for which it is held pressed.

6 Routing and WAN connections

This chapter describes the most important protocols and configuration entries that relate to WAN connections. It also describes how WAN connections can be optimized.

6.1 General information about WAN connections

WAN connections are used for the following applications.

- Internet access
- LAN-LAN links
- Remote access

6.1.1 Bridges for standard protocols

WAN connections differ from direct connections in that the data in the WAN are transmitted via standardized network protocols that are also used in the LAN. Direct connections, on the other hand, use proprietary methods that are specifically designed for point-to-point connections.

WAN connections act to extend a LAN, while direct connections merely connect one individual PC to another PC. WAN connections form bridges for the communication between networks (or for connecting individual computers to the LAN).

6.1.1.1 Which protocols are used on WAN connections?

WAN connections over high-speed connections (e.g. DSL) use the IP standard for transmitting packets.

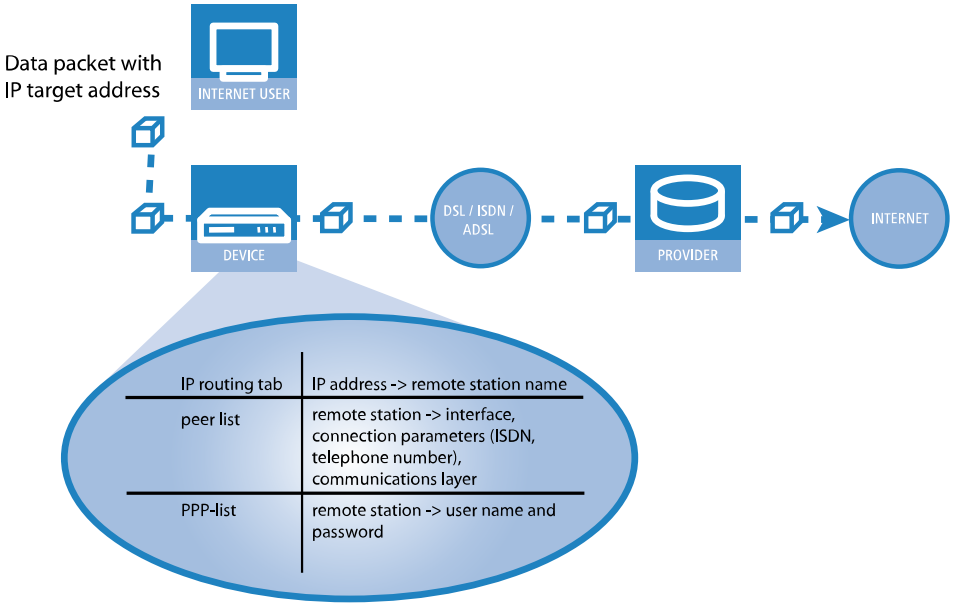
6.1.1.2 Close cooperation with the router modules

Characteristic of WAN connections is the close cooperation with the router modules in the device. The router modules (IP) provide the connection between LAN and WAN. They use the WAN modules to respond to requests from LAN-based PCs for external resources.

6.1.2 What happens with a request from the LAN?

Initially, the router modules only determine which remote site a data packet should be sent to. In order for the required connection to be selected and/or established, various parameters need to be agreed for all of the necessary connections. These parameters are stored in different lists, which interact to allow the correct connections.

A simplified example will illustrate this process. Here we assume that you know the Internet IP address of the computer you are looking for.



1. **Selecting the right route**

   A data packet from a computer initially finds its way to the Internet by means of the IP address of the recipient. The computer sends the packet with this address through the LAN to the router. The router refers to its IP routing table to determine which remote site is used to reach the IP address in question, e.g. 'Provider'.

2. **Connection data for the remote site**

   The router uses this name to check the list of remote sites and find the connection data required for the provider. This connection data includes, for example, the WAN interface (DSL) used to reach the provider, or protocol information. The router also refers to the PPP list to obtain the corresponding user name and password.

3. **Establishing the WAN connection**

   The router then establishes a connection to the provider via a WAN interface. It authenticates itself by user name and password.

4. **Transmission of data packets**

   Once the connection is established, the router sends the data packet to the Internet.

6.2 IP routing

An IP router works between networks that use TCP/IP as the network protocol. In order for data to be transmitted, the destination addresses must be available in the routing table. This section explains the structure of the IP routing table of a LANCOM router, as well as the additional functions available to support IP routing.

6.2.1 Routing behavior

LCOS implements the routing via the **FIB** (**F**orwarding **I**nformation **B**ase).

There is also the **RIB** (**R**outing **I**information **B**ase), which prioritizes routes from different sources that have the same destination network and the same routing tag. Prioritization is influenced by the **administrative distance**.

The **FIB** is based on the following sources:

› **Automatically generated sources:**

- **Dynamic routing protocols (RIP, BGP, LISP, OSPF)**
- **DHCP**
- **IPv6 auto config**

- **Manually generated sources:**
  - **Routing table** (IPv4 routing table or IPv6 routing table)
  - **LAN interface** (IPv4 or IPv6 network)
  - **WAN interface** (IPv4 or IPv6 Internet- and VPN connection)
  - **WAN tag table** (IPv4 only)
  - **Loopback addresses**

A separate table is created in the **FIB** for each routing tag.

6.2.1.1 General rules

For each routing tag assigned, a route with this tag must exist in the **FIB** for communication to be possible. There is **no fallback to a route with routing tag 0**.

A table with tag 0 always exists, but it may be empty.

6.2.1.2 Specific rules

When entries are added to the **FIB**, the following specific rules are processed in sequence:

Rule 1: Routes with the same destination

Route collisions should be avoided if possible.

1. **Adding a route when a route to the same destination exists but with a different routing tag**

   If a **routing entry is to be entered into the FIB** and **a route with the same destination but a different routing tag already exists** there, then **the existing route is overwritten by the newly added routing tag**.

   Example:

   - The INTRANET network (192.168.1.0/24) is set up on the router.
   - The IPv4 routing table already contains a routing entry with the destination 192.168.45.0/24 and routing tag 0, which refers to the Internet remote site INTERNET-DEFAULT (DHCPoE). Since this is a routing entry for a WAN connection with routing tag 0 (see **rule 5**), this route is also entered into all other routing tables.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                10        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)

Rtg-Tag 5

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 10.0.0.0/24       192.168.1.253   INTRANET                10        no           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)
```

   - A new entry is made in the IPv4 routing table for the destination 192.168.45.0/24 with routing tag 5, which refers to the Internet remote site INTERNET-DEFAULT.

› The static route with routing tag 5 overwrites the DHCPoE route in the table with tag 5.

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 10.0.0.0/24        192.168.1.253   INTRANET                10        no           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24     0.0.0.0         INTRANET                10        no           Down           Connected LAN (2)
 192.168.1.254/32   0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32  0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32  0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)

Rtg-Tag 5

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 10.0.0.0/24        192.168.1.253   INTRANET                10        no           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.45.0/24    0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 192.168.45.139/32  0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32  0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)
```

2. **Adding multiple routes with the same destination but different routing tags and tags that are unknown to the FIB**

   If multiple **routes with the same destination and different routing tags** are entered **into the FIB** and **the routing tag of the routes is unknown to the FIB**, the **route is copied** to **all tables** that do not yet know this route.

   Example 1:

   › Along with the network INTRANET (192.168.45.0/24), two DMZ networks are set up (DMZ1 with 192.168.10.0/24 and DMZ2 with 192.168.20.0/24).

   › A routing entry for destination 10.0.0.0/24 with routing tag 5 already exists in the IPv4 routing table, so there is a table for routing tag 5 in the FIB.

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 10.0.0.0/24        192.168.45.254  INTRANET                4         no           Redistribute   Static (5)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.10.0/24    0.0.0.0         DMZ1                    7         no           Redistribute   Connected LAN (2)
 192.168.10.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.20.0/24    0.0.0.0         DMZ2                    8         no           Redistribute   Connected LAN (2)
 192.168.20.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    0.0.0.0         INTRANET                4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 10.0.0.0/24        192.168.45.254  INTRANET                4         no           Redistribute   Static (5)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.10.0/24    0.0.0.0         DMZ1                    7         no           Redistribute   Connected LAN (2)
 192.168.10.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.20.0/24    0.0.0.0         DMZ2                    8         no           Redistribute   Connected LAN (2)
 192.168.20.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
```

   › Two routes with the destination 192.168.1.0/24 are added to the IPv4 routing table for routing tags 1 and 2, each of which point as next hop to an IP address in one of the DMZ networks (routing tag 1 to the IP address 192.168.10.253 in the DMZ1 and routing tag 2 to the IP address 192.168.20.253 in the DMZ2).

   › The route for the DMZ1 interface is entered into the FIB both in the table with tag 0 and in the table for tag 5.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 1

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 2

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.20.253  DMZ2                     12        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.10.253  DMZ1                     11        no           Redistribute   Static (5)
 192.168.10.0/24   0.0.0.0         DMZ1                     11        no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.20.0/24   0.0.0.0         DMZ2                     12        no           Redistribute   Connected LAN (2)
 192.168.20.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

Example 2:

- In addition to the network INTRANET (192.168.45.0/24) with tag 0, a DMZ (192.168.10.0/24) with tag 0 is set up on the router and thus both are entered into the FIB in the table for routing tag 0.
- A routing entry for destination 10.0.0.0/24 with routing tag 5 already exists in the IPv4 routing table, so there is a table for routing tag 5 in the FIB.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      9         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTRANET                 4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)

Rtg-Tag 5

 Prefix            Next-Hop        Interface                ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT         3         on           Down           Static Ifc Down (255)
 10.0.0.0/24       192.168.45.254  INTRANET                 4         no           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback                1         no           Never          Loopback (0)
 192.168.10.0/24   0.0.0.0         DMZ                      9         no           Redistribute   Connected LAN (2)
 192.168.10.254/32 0.0.0.0         #Loopback                1         no           Redistribute   Local LAN (0)
```

- A route with the destination 192.168.45.0/24 and tag 1 is added to the IPv4 routing table. The next hop for this route is set to the IP address 192.168.10.253 in the DMZ.

› The route for the DMZ is entered in the FIB into the table with tag 5 but not in the table with tag 0, since an entry with tag 0 exists already (INTRANET) and the existing entry is preferred.

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 10.0.0.0/24        192.168.45.254  INTRANET                4         no           Redistribute   Static (5)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.10.0/24    0.0.0.0         DMZ                     13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    0.0.0.0         INTRANET                4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)

Rtg-Tag 1

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.10.0/24    0.0.0.0         DMZ                     13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    192.168.10.253  DMZ                     13        no           Redistribute   Static (5)

Rtg-Tag 5

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 10.0.0.0/24        192.168.45.254  INTRANET                4         no           Redistribute   Static (5)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.10.0/24    0.0.0.0         DMZ                     13        no           Redistribute   Connected LAN (2)
 192.168.10.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24    192.168.10.253  DMZ                     13        no           Redistribute   Static (5)
```

3. **Adding multiple routes with the same destination and different routing tags and inserting the route into the FIB into the table with tag 0**

   If **multiple routes with the same destination and different routing tags** are added, the **route with the lowest tag is added to the table with tag 0** unless it already contains a route with tag 0.

   Example:

   › The router is set up with the INTRANET network (192.168.45.0/24).

```
Rtg-Tag 0

 Prefix             Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0          0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 127.0.0.0/8        0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.45.0/24    0.0.0.0         INTRANET                4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
```

   › Two routes with the destination 192.168.1.0/24 are added to the IPv4 routing table for routing tags 2 and 5, each of which point as next hop to an IP address in the INTRANET network (tag 2 to 192.168.45.253 and tag 5 to 192.168.45.254).

   › The route with tag 2 is transferred to the table with tag 0.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.45.253  INTRANET                4         no           Redistribute   Static (5)
 192.168.45.0/24   0.0.0.0         INTRANET                4         no           Redistribute   Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)

Rtg-Tag 2

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.45.253  INTRANET                4         no           Redistribute   Static (5)

Rtg-Tag 5

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         0.0.0.0         INTERNET-DEFAULT        3         on           Down           Static Ifc Down (255)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    192.168.45.254  INTRANET                4         no           Redistribute   Static (5)
```

4. **Different rule for routes with the DMZ interface**

   In contrast, **routes with the DMZ interface and arriving from another tag can displace routes of the type Connected WAN, provided they have the same destination network**.

   Example:

   - The router is set up with the INTRANET network (192.168.1.0/24).
   - A routing entry for the destination 192.168.45.0/24 with the tag 0 already exists. This is a separate route of a DHCPoE connection (Connected WAN).

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                14        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   Connected WAN (2)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)
```

   - A DMZ (192.168.45.0/24) with tag 1 is created.
     - The original route of the type Connected WAN is overwritten by the route of the DMZ.

```
Rtg-Tag 0

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.1.0/24    0.0.0.0         INTRANET                14        no           Down           Connected LAN (2)
 192.168.1.254/32  0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.0/24   0.0.0.0         DMZ                     15        no           Down           Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)

Rtg-Tag 1

 Prefix            Next-Hop        Interface               ID        Masquerading Redistribution Type (Distance)
 ------------------------------------------------------------------------------------------------------------------
 0.0.0.0/0         192.168.45.254  INTERNET-DEFAULT        3         on           Redistribute   Static (5)
 127.0.0.0/8       0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 127.0.0.1/32      0.0.0.0         #Loopback               1         no           Never          Loopback (0)
 192.168.45.0/24   0.0.0.0         DMZ                     15        no           Down           Connected LAN (2)
 192.168.45.100/32 0.0.0.0         #Loopback               1         no           Redistribute   Local LAN (0)
 192.168.45.139/32 0.0.0.0         #Loopback               1         no           Redistribute   Local WAN (0)
 192.168.45.254/32 0.0.0.0         INTERNET-DEFAULT        3         on           Redistribute   DHCP (15)
```

Rule 2: Dynamic routing protocols

If the **route is generated by a dynamic routing protocol** (**eBGP**, **iBGP**, **OSPF**, **RIP**, **LISP**), the **route in the FIB is inserted into the table with the routing tag** that was handed over.

Rule 3: Configuring a loopback address

- If **routing tag 0** is handed over, the **route is inserted into all tables of the FIB**.
- If the **routing tag handed over is not equal to 0**, the **route** is entered **into the FIB in the table with the assigned routing tag** and **also into the table with the routing tag 0**.

Rule 4: Routes with the destination DMZ can be reached from all networks

Routes with the DMZ as their destination (e.g. an **IP network with the type DMZ**) can be addressed via any routing tag, since an entry is **automatically created for the DMZ in the FIB** for each routing tag configured in the router.

Rule 5: Routes with a destination in the WAN and handling static routes

- If the **route has the routing tag 0** and the **destination interface is the WAN** (Internet remote site), **or** you are configuring a **static route with routing tag 0** (in the IPv4/IPv6 routing table), the **route is inserted in the FIB into all tables**.
- If the **route has a tag other than 0**, the **route is inserted into the FIB with the configured tag**.

Rule 6: Routes with a destination in the LAN

- If a **route is entered with a destination in the LAN** (i.e. an **IPv4/IPv6 network**) **with the routing tag 0**, the **route is only inserted into the FIB table with the routing tag 0**.
- If a **route is entered with a destination in the LAN** (i.e. a **IPv4/IPv6 network**) **and a routing tag other than 0**, the **route is entered into the FIB table with the assigned routing tag** and **is also entered into the table with routing tag 0**.

Rule 7: Behavior in cases not described above

If none of the above rules apply, the route is **only inserted into the FIB table with the routing tag** as handed over.

If a **routing entry is removed from the FIB**, there is a search for an **equivalent replacement** that meets the rules described in rule 1 – 7. If the **FIB no longer contains** a routing entry for a specific routing tag, the **associated table is deleted**.

6.2.1.3 Other examples

SIP line with routing tag 10:

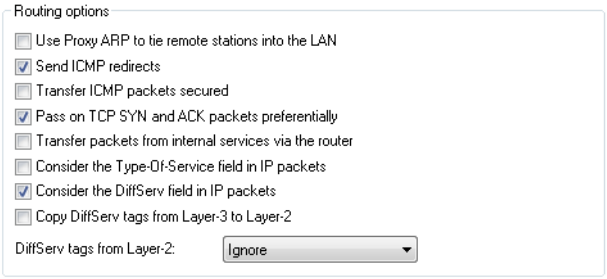
1. A **SIP line** is given the **routing tag 10**. There is an **IP network** named **INTRANET** with the **interface tag 0** and a **default route** named **INTERNET** with the **routing tag 0**.
   - In this case **the SIP line cannot register** because the **routing tag 10 does not exist in any of the tables**.
2. A **SIP line** is given the **routing tag 10**. There is an **IP network** named **INTRANET** with the **interface tag 10** and a **default route** named **INTERNET** with the **routing tag 0**.
   - In this case **the SIP line can register** because the **routing tag 10 exists in the IP network INTRANET**.
3. A **SIP line** is given the **routing tag 10**. There is an **IP network** named **INTRANET** with the **interface tag 0** and a **default route** named **INTERNET** with the **routing tag 10**.
   - In this case **the SIP line can register** because that **routing tag 10 exists in the DEFAULT route INTERNET**.

Special case: WAN tag table

If a **port is to be forwarded** or a **VPN dial-in** operates on an Internet connection that uses a **routing tag other than 0** and the **forwarding destination has tag 0**, then the **WAN tag table** needs to have an **entry for the Internet connection** with the **same routing tag** (in this example **tag 1**) so that the response packets can be routed over this Internet connection. Instead the response packets will be sent via the **Internet connection with routing tag 0**. Furthermore, a **firewall rule with the routing tag 65535** has to be created, which then removes the tag set by the **WAN tag table**. Otherwise, packets intended for the local network will be sent out over a suitable route (such as the Internet connection).

6.2.2 Routing options

In LANconfig, you configure the general routing options under **IP router** > **General**.



Use Proxy ARP to tie remote sites into the LAN

Use this option to enable or disable the proxy ARP mechanism. The use of proxy ARP integrates remote computers into your local network as if they were physically located within it.

Send ICMP redirects

You know how workstations behave in a local network: If the computer wants to send a packet to an IP address that does not exist in the local LAN, it looks for a router for further help. The computer's operating system generally points to this router by means of an entry for the default router or standard gateway. If a network has several routers, it is generally only possible to specify one default router that is theoretically able to reach all of the IP addresses that are unknown to the workstation. Occasionally this default router may be unable to reach the target network, but it knows of another router that is able to find this target.

By default, the router sends the computer a response containing the address of that router which knows the route to the target network (this response is called the "ICMP redirect"). The workstation then uses this address to send the packet straight to the other router.

However, some computers are unable to process ICMP redirects. In order for the data packets to be delivered despite this, you make use of the local routing. You instruct the router in your device to send the packet to the other responsible router. Also, it is no longer able to send ICMP redirects to the clients.

Local routing can be very helpful in individual cases, but it should be used only in situations of this type. This is because local routing leads to a doubling of all network packets to the target network. The packets are first sent to the default router, which then sends them to the appropriate router in the local network.

You use this option to determine whether the device sends ICMP redirects.

Transfer ICMP packets secured

Here you determine whether the device sends secured ICMP redirects.

Pass on TCP-SYN and ACK packets preferentially

The SYN/ACK-speedup method is used to accelerate IP traffic. With SYN/ACK-speedup, IP control characters (`SYN` for synchronization and `ACK` for acknowledge) in the transmit buffer are given priority over standard data packets. This avoids the situation where control characters are caught up in the transmit queue, so causing the remote site to stop sending data.

SYN/ACK-speedup is most effective with high-speed connections like ADSL, where data are transferred at high speed in both directions at the same time.

In the factory settings, SYN/ACK-speedup is activated by default.

The preferential treatment of individual packets leads to a change from the original packet order. Although TCP/IP provides no guarantee of a specific packet order, this can lead to problems with some applications. This only affects applications which, in divergence from the standard protocol, require a certain packet order. In this case, disable the SYN/ACK-speedup.

Transfer packets from internal services via the router

By default, local services always bypass the router. Acknowledgments are always returned directly to the MAC address where the request originated. Select this option if you wish packets from internal services to be sent via the router. Packets will then be sent not directly to the MAC address of the sender but via the router (provided an appropriate route has been configured).

Consider the Type-of-Service field in IP packets

If you have selected "Type-Of-Service", the router searches the IP packets for options that indicate whether the packets should be transmitted particularly quickly or secured.

Consider the DiffServ field in IP packets

If the router considers the DiffServ field in IP packets, it applies preferential transmission according to the standardized DSCP (DiffServ code point) `AFxx` (Assured Forwarding) for secured transmission and `EF` (Expedited Forwarding). All other IP packets will be transmitted normally. This option is enabled by default.



This option cannot be used in combination with ToS since the DiffServ field replaces the ToS field within the IP packet.

For more information about DiffServ, see the chapter *Quality-of-Service*.

Copy DiffServ tags from layer 3 to layer 2

The setting for Layer3-Layer2 tagging regulates the behavior when a data packet is transmitted. With this option enabled, VLAN tags with priority bits originating from the DSCP precedence are generated if the recipient has sent at least one tagged packet.

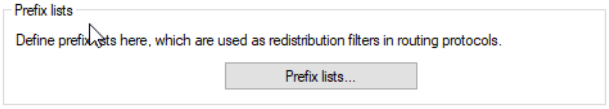
DiffServ tags from Layer 2

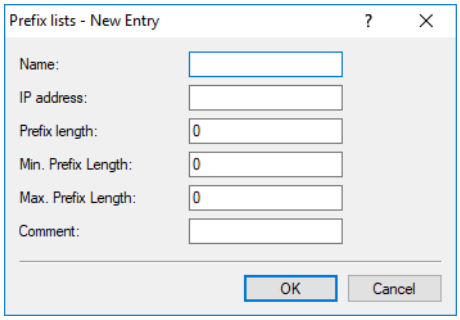
The setting for Layer2-Layer3 tagging regulates the behavior when a data packet is received.

- **Ignore**: VLAN tags are ignored.
- **Copy to layer 3**: Priority bits in the VLAN tag are always copied to the precedence of the DSCP.
- **Copy automatically**: Priority bits in the VLAN tag are only copied to the DSCP precedence if this is "000".

6.2.3 Prefix lists

Filter lists can be used to allow or deny certain prefixes during redistribution by the BGP. LISP and OSPF. To do this, create the prefix filter list under **IP router** > **General** > **Prefix lists**.





Name

Give this entry a name here. Prefixes that should belong to a list are referenced by the same name, e.g. List1.

IP address

Specify the IPv4 or IPv6 address of the network here.

Prefix length

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Min. prefix length** and **Max. prefix length** are set to values not equal to zero.

If the value is "0", the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

Min. prefix length

Here you specify the minimum prefix length value required for the prefix to match.

Max. prefix length

Here you specify the maximum prefix length value required for the prefix to match.

Comment

Comment on this entry.

Using prefix lists with BGP

These **prefix lists** can be referenced for the IPv4 and IPv6 address families of the BGP protocol, and you can specify whether these prefix lists should be allowed or rejected

Using prefix lists with LISP

These **Prefix lists** can be used to allow or deny certain prefixes during route redistribution by LISP. Use the prefixes defined here for redistributing static routes, BGP, OSPF and connected routes.

Using prefix lists with OSPF

These **Prefix lists** can be used to allow or deny certain prefixes during route redistribution by OSPF. Use the prefixes defined here for redistributing static routes, BGP and connected routes.

6.2.4 The routing table

The routing table specifies exactly where the router (i.e. to which other router or computer) sends the data for any given IP addresses or IP address ranges. This type of entry is called a "route" since it is used to describe the path that the data packet should take. This procedure is also known as "static routing" since these entries are made manually and remain unchanged until you edit or delete them. In contrast to this, there is also "dynamic routing". Here, the various routers independently exchange information about the routes and keep this information up to date. Dynamic routing protocols include RIP, OSPF, BGP or LISP. When dynamic routing protocols are enabled, the router respects the static routing entries as well as the dynamic routing information.

The static unicast routes for IPv4 and IPv6 are each configured in separate tables. Multicast routes are configured using IGMP/MLD, PIM, and the tables for static multicast routes.

With the help of the static IPv4 routing table you also inform the router about the length of the route so that, in conjunction RIP, the most effective path is used where multiple routes exist to the same destination. The default setting for the RIP distance to another router is 0, i.e. the router is directly accessible. All locally accessible devices, i.e. other routers in the same LAN or workstations that are connected via proxy ARP, are entered with the distance 0. Setting a higher RIP distance (up to 14) reduces the "quality" of a route. These "unfavorable" routes will only be used if no other route to the corresponding remote site is available.

6.2.4.1 Administrative distance

The administrative distance can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. This mechanism can be used, for example, to configure simple backup mechanisms.

The manipulation of the administrative distance for routes that are dynamic is handled by the respective dynamic routing protocol.

Example 1: Two VPN tunnels are to be configured with the route 192.168.2.0/24. The second VPN tunnel is to be configured as the "always-on" backup for the first VPN tunnel.

For the first tunnel, the prefix 192.168.2.0/24 is set up to the remote site VPN-1 with an administrative distance of 10. For the second tunnel, the prefix 192.168.2.0/24 is set up to the remote site VPN-2 with an administrative distance of 20. Both VPN tunnels will be established, but the route is only active for the first VPN tunnel as it has the better/lower administrative distance. If the first VPN tunnel disconnects, the operating system sets this route to the administrative distance of 255 (interface down), which automatically activates the route using the second tunnel.



Entries of type "DHCP Automode" are added by the operating system when the DHCP client is started in automode. The automode is configured in the DHCP server table and is the default setting after a factory reset.

In this case, the DHCP client routes have a higher priority than static routes to enable zero-touch commissioning via LAN.

Example 2: There is a static route for 192.168.1.0/24 to the remote peer VPN-Tunnel1. If the same prefix 192.168.1.0/24 is received via BGP, the static route has a better/lower administrative distance by default, so it has preference over the route via BGP.

If you now set the administrative distance of the static route to the value 210, then the route learned via BGP is preferred and active, since (e)BGP has an administrative distance of 20 or 200 (iBGP). The static route thus serves as a backup for the dynamic BGP route.

This feature does not replace the backup table, but it does offer a different kind of "backup". When using the backup table, only one connection is active at a time. If the backup is required, the system attempts to activate the backup connection. While the backup connection is active, the system attempts to reestablish the primary connection and will switch back to it, if successful. The backup strategy based on the administrative distance assumes that connections to all remote sites are always established. This may be undesirable in certain scenarios, e.g. with backups via cellular networks, and the backup table would be the preferred choice.

The backup table and backups over administrative distances are mutually exclusive ways of implementing backups.

The value 0 has a special function and is internally the lowest value reserved for the device's own addresses (i.e. for the sources Loopback, Local LAN, Local WAN, Broadcast, VRRP).

In the configuration, 0 has the special role of assigning the default value for the route source to a route marked with this administrative distance. This can be seen in `show admin-distance`.

The value 255 has the special role for the "route disabled" or "interface down" state.

If administrative distances are to be used for prioritizing routes in the configuration, values from 1-254 must be used. The values 0 and 255 have a special function.

The commands `show ipv4-static-routes` and `show ipv6-static-routes` displays all active and inactive static routes. The current administrative distances for route sources can be viewed from the CLI using the command `show admin-distance`.

The most important administrative distances are:

Table 24: Administrative Distances

Route type	Administrative distance
Device's own addresses, VRRP, Broadcast	0
Connected LAN and WAN networks	2
DHCP Automode	4
Static routes	5
VPN, VPN Mesh, PPP server, 464XLAT, DHCP, Autoconfig, Framed, CAPWAP, Rollout Agent	15
eBGP	20
OSPF	110
RIP	120
iBGP	200
LISP	240
Automatic default	254
Interface down	255

Static routes are defined as routes that a user manually configured in the IPv4 or IPv6 routing table.

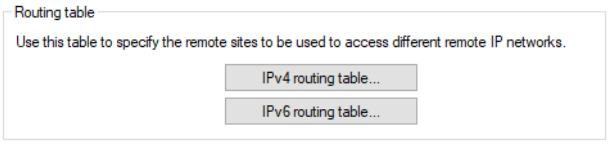
VPN routes are defined as routes that are automatically entered into the routing table by the VPN, e.g. by IKEv2 routing.

Entries of type "DHCP Automode" are added by the operating system when the DHCP client is started in automode. The automode is configured in the DHCP server table and is the default setting after a factory reset.

In this case, the DHCP client routes have a higher priority than static routes to enable zero-touch commissioning via LAN.

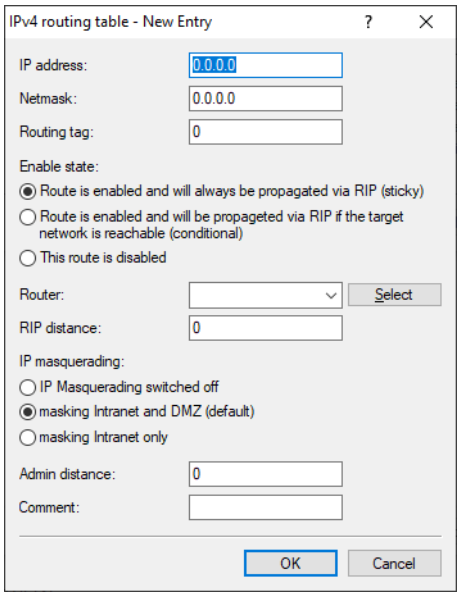
6.2.4.2 Routing tables for IPv4/IPv6

Static routing entries are configured in the separate tables for IPv4 and IPv6. The tables are located in LANconfig under **IP router** > **Routing** > **Routing table**



IPv4

The routing table for the static routing of IPv4 packets is located under **IP router** > **Routing** > **Routing table** > **IPv4 routing table**.



IP address/Netmask

This is the address of the destination network, to which data packets may be sent, together with its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network.

The default route has the IP address '255.255.255.255' and the network mask '0.0.0.0'. All data packets that cannot be routed by other routing entries are sent over this route.

Routing tag

The routing tag allows the selection of the destination route to be controlled more precisely. This route is active only for packets with the same tag. In this case, route selection relies not only on the target IP address, but also on further information added to the data packets by the firewall (see *Policy-based routing* on page 388). With the routing tag “0” the routing entry applies to all packets.

Enable state

Specify the switch status here. The route can be activated and either always propagated via RIP or only propagated via RIP when the destination network can be reached.

Router

Data packets that match the IP address and netmask are transmitted by the router to this remote site or IP address.

- If the remote site is a router in another network or an individual workstation computer, then the name of the remote site is entered here.
- If a router is unable to reach the remote site, the IP address entered here is that of another router in the LAN that knows the route to the destination network.
- If the router or next-hop is to be resolved in a different routing context, the syntax 'IP address@tag' can be used.

  This is the case, for example, if a static route has been created with a tag where this tag can only be assigned by a firewall rule.

  Example: If the router 192.168.1.1 is to be resolved in routing context 1, the entry is '192.168.1.1@1'.

Routes with the entry '0.0.0.0' identify excluded or blocked routes. Data packets for this “zero route” are discarded and not forwarded. This means that routes prohibited on the Internet (private address spaces as per RFC1918, e.g. '10.0.0.0/8') are excluded from transmission.

If the remote site is entered as an IP address, then this is a locally accessible router that is responsible for transmitting the corresponding data packets.

RIP distance

Number of routers between your own and the destination router. This value is often equated with the cost of transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered here are propagated as follows:

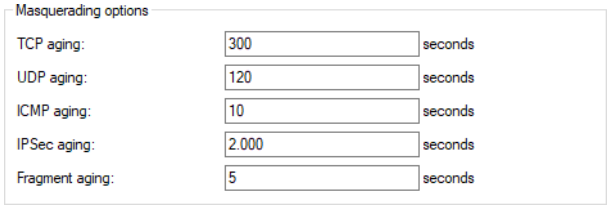
- While a connection is established to a destination network, all networks reachable via this connection are propagated with a distance of 1.
- All non-connected networks are propagated with the distance entered in the routing table (at least with a distance of 2), as long as a free transmission channel is still available.
- If no channels are available, the remaining networks are propagated with a distance of 16 (unreachable).
- Exceptions are the remote sites that are connected via proxy ARP. These “proxy hosts” are not propagated at all.

IP masquerading

This option in the routing table tells the router which IP address to use when forwarding packets.

Please refer to section *IP masquerading* on page 420 for further information.

Die Optionen zum maximalen Alter der verschiedenen Arten von Paketen finden Sie unter **IP Router** > **Masq.** > **Masquerading options**.



TCP aging

The connection list keeps track of open sessions of TCP packets for any communication that passes through the router so that they can be mapped during communication. Typically, a TCP connection is terminated after communication is complete. In some cases, however, TCP connections are not terminated by the initiator or responder. So that the connection list does not continue to fill up and performance is reduced as a result, TCP connections are automatically terminated after this timer expires.

Specify here after which time of inactivity of an TCP connection the corresponding entry in the masking table should be removed.

UDP aging

Specify here after which time of inactivity of an UDP connection the corresponding entry in the masking table should be removed.

ICMP aging

Specify here after which time of inactivity of an ICMP connection the corresponding entry in the masking table should be removed.

IPSec aging

Enter the default lifetime for entries in the IPSec masking table in seconds here.

Fragment aging

If an IP packet cannot be completely unmasked because not all fragments were received, then the incomplete fragments are discarded after the time set here.

Administrative distance

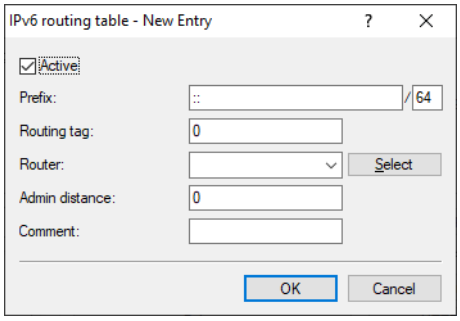
Administrative distance for this route. The default is 0 (set automatically by the operating system). The administrative distance parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. See *Administrative distance* on page 383.

Comment

Optionally enter a meaningful comment as a description.

IPv6

The routing table for the static routing of IPv6 packets is located under **IP router** > **Routing** > **Routing table** > **IPv6 routing table**.



Active

Activates or deactivates this entry in the routing table.

Prefix

This prefix and prefix length denote the network range from which the current remote site (e.g. 2001:db8::/32) is to receive data. The value ::/0 denotes the default route.

Routing tag

The routing tag allows the selection of the destination route to be controlled more precisely. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall (see *Policy-based routing* on page 388) or depending on the LAN or WAN interface used. Detailed information on the routing behavior in LCOS can be found in the chapter *Routing behavior* on page 373.

Router

This is where you specify the destination or remote site for this route. Enter one of the following options:

- An interface name
- An IPv6 address (e.g. 2001:db8::1)
- An interface name supplemented with a link-local address (e.g. fe80::1%INTERNET)
- An IPv6 address with TAG (e.g. 2001:db8::1@1) if the router or next hop is to be resolved in a different routing context.

  This is the case, for example, when a static route has been created with a tag, where this tag can only be assigned by a firewall rule.

  Example: If router 2001:db8::1 is to be resolved in routing context 1, enter '2001:db8::1@1'

Routes with the entry "::" identify excluded or blocked routes. Data packets for this "zero route" are discarded and not forwarded. This means that routes prohibited on the Internet (private address spaces, e.g. unique local address 'fc00::/7' as per RFC 4193) are excluded from transmission.

Administrative distance

Here you set the administrative distance of this route. This parameter can be used to configure several identical routes or prefixes to different remote sites. The route with the lowest administrative distance is the preferred active route. The default is 0, i.e. the value is assigned automatically by the operating system. See *Administrative distance* on page 383.

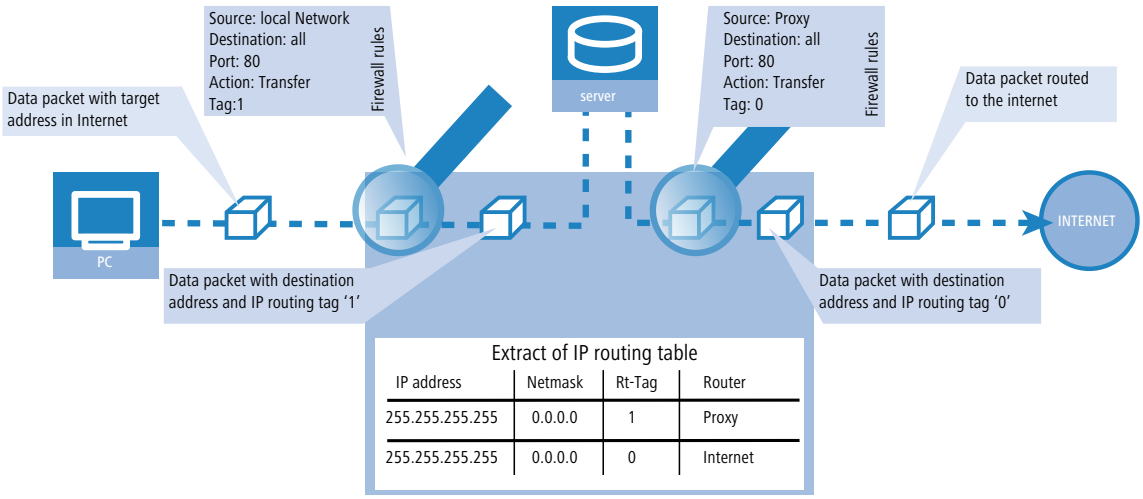
Comment

Optionally enter a meaningful comment as a description.

6.2.5 Policy-based routing

Policy-based routing does not rely exclusively upon the destination IP address to define the destination route (i.e. the remote device to be used for transferring the data). Further information can be used—such as the service or the protocol used, sender addresses, or the destination for the data packets—to select the destination route. Policy-based routing can be used to achieve a significantly finer-grained routing behavior, such as in the following application scenarios:

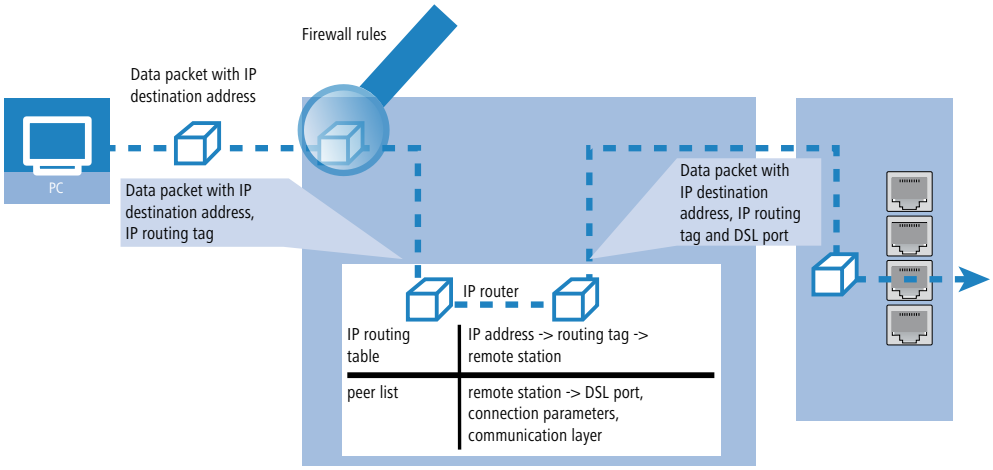
- The LAN's entire Internet traffic is diverted to a proxy without entering the proxy address into the browsers. As the users do not notice the proxy routing, the scenario is named "transparent" proxy.



- With load balancing, the data traffic for selected protocols is diverted over a certain DSL port that uses an additional external ADSL modem.
- A server in the local network is routed via a specific WAN interface as it needs to be accessible from the WAN at a fixed IP address.
- VPN traffic is forwarded to a VPN tunnel with dynamic end points by using the routing tag '0'; the company's remaining Internet traffic is diverted to another firewall by means of another suitable routing tag.

In order for channel selection to be decided according to information other than just the destination IP address, suitable entries can be made in the firewall. These entries are supplemented with a special “routing tag” that is used to control the channel selection with the routing table. For example, a rule adds the routing tag ‘2’ to the entire data traffic for a local group of computers (defined by an IP address range). Alternatively, certain protocols receive a different supplementary routing tag.

The diagram demonstrates the application of policy-routing with load balancing:



- When establishing a connection, the firewall initially checks if the packets for transmission fit to a rule which contains a routing tag. The routing tag is entered into the data packet.
- The IP routing table combines the routing tag and destination IP address to determine the appropriate remote site. The IP routing table is processed from top down in the usual fashion.
- If an entry is found corresponding to the network, then the second step is to check the routing tag. The required remote site can be found with the help of the appropriate routing tag. During load balancing, the device can use the remote site from the list of remote sites/peers to determine the correct DSL port.

  If the routing tag has a value of “0” (default) then the routing entry applies to all packets.

- Internal services implicitly use the default tag. If the user wishes to direct the default route through a VPN tunnel with a dynamic tunnel endpoint, for example, then the VPN module uses the default route with the routing tag “0” as standard.

  To direct the default route through the VPN tunnel anyway, create a second default route with routing tag "1" and the VPN remote site as router names. With the appropriate firewall rule you can transfer all services from all source stations to all destination stations with routing tag “1”.

- Routing tags and RIP: The routing tag is also sent in RIP packets and evaluated upon receipt, so you can, for example, change the distances in the correct routes.

6.2.5.1 Routing tags for VPN and PPTP connections

Routing tags are used on the device in order to evaluate criteria relevant to the selection of the target route in addition to the IP address. In general, routing tags are added to the data packets using special firewall rules. However, in some cases, it is desirable to assign the tags directly.

› Routing tags for VPN connections

The VPN name list can be used to enter the routing tag for every VPN connection. The routing tag is used in order to determine the route to the remote gateway (default '0').

In addition, every gateway can be assigned a specific routing tag in the gateway table. The tag 0 has a special function in this table: If the tag is set at 0 on a gateway, then the tag from the VPN name list table is used.

The VPN routing tag parameters can be found under Setup/VPN/VPN Peers or Setup/VPN/Additional Gateways and under LANconfig in the configuration section 'VPN' on the 'General' tab by clicking on 'Connection List' and 'Further remote gateways' in the list.

› Routing tags for PPTP connections

In the PPTP table, a routing tag can be entered in addition to the IP address of the PPTP server. Using this routing tag, two or more DSL modems that use a single IP address can be operated on different DSL ports.

Peer	IP address	Rtg tag	Port	SH-Time
PEER01	10.0.0.138	1	1723	9999
PEER02	10.0.0.138	2	1723	9999

In the IP routing table, two appropriately tagged routes are required:

IP address	IP-Netmask	Rtg tag	Peer-or-IP	Distance	Masking
10.0.0.138	255,255,255,255	2	PEER02-PPTP	0	No
10.0.0.138	255,255,255,255	1	PEER01-PPTP	0	No
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No
172.16.0.0	255.240.0.0	0	0.0.0.0	0	No
10.0.0.0	255.0.0.0	0	0.0.0.0	0	No
224.0.0.0	224.0.0.0	0	0.0.0.0	0	No
255,255,255,255	0.0.0.0	0	PEER-LB	0	Yes

Using these settings and the corresponding entry in the load balancing table, load balancing can be performed that would also work in Austria.

Peer	Bundle-Peer-1	Bundle-Peer-2	Bundle-Peer-3
PEER-LB	PEER01	PEER02	

6.2.6 Dynamic routing with IP RIP

In addition to the static routing table, routers from LANCOM also have a dynamic routing table. Unlike the static table, you do not fill out this table manually as this is handled by the router itself. It does this by means of the routing information protocol (RIP). All devices that support RIP use this protocol to exchange information about the available routes.

6.2.6.1 What information is propagated via IP RIP?

A router uses the IP RIP information to inform the other routers in the network of the routes it finds in its own static table. The following entries are ignored:

› Rejected routes with the '0.0.0.0' router setting.
› Routes referring to other routers in the local area network.
› Routes that link individual computers to the LAN via proxy ARP.

Although the entries in the static routing table are set manually, this information nevertheless changes depending on the connection situation of the routers, which in turn influences the RIP packets transmitted.

- If the router has established a connection to a remote site, it uses RIPs to propagate all of the networks that can be reached over this route and gives them the distance '1'. This informs other routers in the LAN that a connection to this remote site is available using this router. This saves other routers from accessing their dial-up connections, which in turn reduces connection costs.
- Furthermore, if this router is unable to connect to any other remote sites, all of its other routes are propagated by RIP with the distance '16'. The '16' stands for “This route is not available at the moment”.

6.2.6.2 What information does the router extract from received IP RIP packets?

When the router receives IP RIP packets, it incorporates them into its dynamic IP routing table, which looks something like this:

IP address	IP-Netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

6.2.6.3 What do the entries mean?

IP address and network mask identify the destination network, the distance shows the number of routers between the transmitter and receiver, and the last column shows which router advertised this route. With the 'Time', the dynamic table shows how old the route is. The value in this column acts as a multiplier for the interval at which the RIP packets arrive, so a '1' stands for about 30 seconds, a '5' for about 2.5 minutes, and so on. When new information about a route arrives, this route is considered to be directly accessible and receives the time '1'. The value in this column is automatically incremented when the corresponding amount of time has elapsed. After 3.5 minutes, the distance is set to '16' (route unavailable), and after 5.5 minutes the route is deleted.

If the router now receives an IP RIP packet, it must decide whether or not to include the routes it contains in its dynamic table. This is done as follows:

- The route is included if it is not yet listed in the table (if there is enough space in the table).
- The route is present in the table with the time from '5' or '6'. The new route will be used if it has the same or a better distance.
- The route is present in the table with the time from '7' to '10', so it has the distance '16'. The new route will always be used.
- The route is present in the table. The new route comes from the same router that also communicated this route, but has a worse distance than the previous entry. If a device communicates the degradation of its own static routing table in this way (e.g. a disconnect increases the distance from 1 to 2, see below), the router accepts this and includes the poorer entry in its dynamic table.

RIP packets from the WAN are ignored and immediately discarded. RIP packets from the LAN will be evaluated and are not propagated in the LAN.

6.2.6.4 Interaction of static and dynamic tables

The router combines the static and dynamic tables to assemble the actual IP routing table used to determine the path for data packets. In doing so, it combines the routes from its own static table with the routes from the dynamic table which it does not know itself or which indicate a shorter distance than its own (static) route.

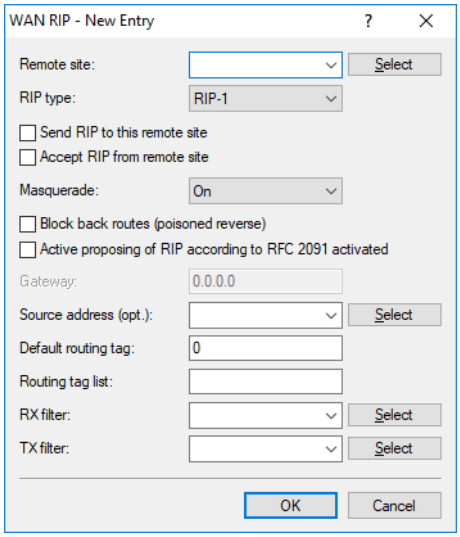
6.2.6.5 Scaling with IP RIP

If you use several routers in a local network with IP RIP, you can represent the routers outwardly as one large router. This procedure is also called “scaling”. Due to the constant exchange of information between the routers, this type of router theoretically has no limits to the transmission options available to it.

6.2.6.6 Configuring the IP RIP function

In order for statically defined routes and routes learned from RIP to be broadcast across the WAN, or for routes to be learned from the WAN, the respective remote sites can be entered into the WAN RIP table.

LANconfig: **Routing protocols** > **RIP** > **WAN RIP**



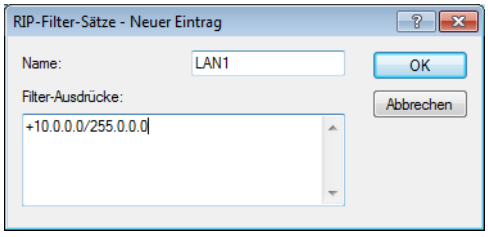
Command line: **Setup** > **IP-Router** > **RIP** > **WAN-Sites**

RIP-capable routers send the RIP packets approximately every 30 seconds. The router will only send and receive RIPs if it has a unique IP address. In the default setting with the IP address xxx.xxx.xxx.254 the IP RIP module is switched off.

6.2.6.7 RIP filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses (e.g. "Only learn routes in the network 192.168.0.0/255.255.0.0"). First of all a central table is used to define the filters that can then be used by entries in the LAN and WAN RIP table.

LANconfig: **Routing protocols** > **RIP** > **RIP filter sets**

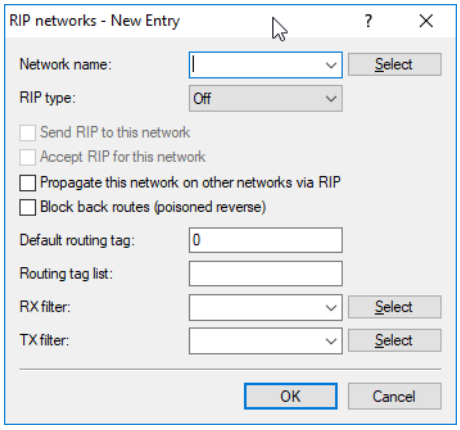


Command line: **Setup** > **IP-Router** > **RIP** > **Filter**

6.2.6.8 Setting up RIP for separate networks

In most cases, it is not desirable for the local network structure to be propagated to the DMZ via RIP. Furthermore it is sometimes desirable to propagate routes to a network, but not to learn routes from that network (e.g. in the WAN). For this reason, the RIP function can be configured separately for each network.

LANconfig: **Routing protocols** > **RIP** > **RIP networks**



Command line: **Setup** > **IP-Router** > **RIP** > **LAN-Sites**

6.2.6.9 Timer settings

The Routing Information Protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information.

Command line: **Setup** > **IP-Router** > **RIP** > **Parameter**

6.2.6.10 Triggered update in the LAN

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay stops faulty configurations from causing excessive update messages.

› Update delay

The update delay starts as soon as the routing table, or parts of it, are propagated. As long as this delay is running, new routing information is accepted and entered into the table but it is not reported any further. The router actively reports its current entries only after expiry of this delay.

The value set here sets the upper limit for the delay – the actual delay is a random value between one second and the value set here.

6.2.6.11 Triggered update in the WAN

Other than in the LAN, WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN once only when the connection is established. After this, updates only are transmitted.

Because updates are explicitly requested here, broadcasts or multicasts are not to be used for delivering RIP messages. Instead, the subsidiary device must be statically configured with the IP address of the next available router at the central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it then sends any messages on route changes directly to the subsidiary device.

The WAN-RIP table has been extended for configuring the triggered update in the WAN.

6.2.6.12 Poisoned reverse

Poisoned reverse prevents the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

However, this has a significant disadvantage over WAN connections: The central location transmits a high number of routes which would then suffer from route poisoning, so leading to a heavy load on the available bandwidth. For this reason, poisoned reverse can be manually activated for every LAN/WAN interface.

The LAN and WAN RIP tables have been extended for the configuration of poisoned reverse.

6.2.6.13 Static routes for constant propagation

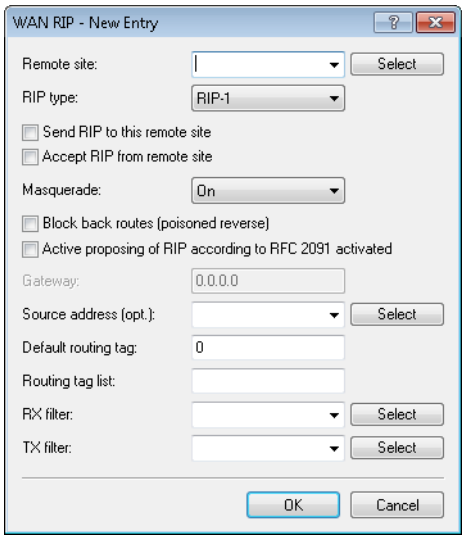
Routers use RIP to propagate not only dynamic routes but statically configured routes as well. Some of these static routes may not be constantly available, for example when an Internet connection or dial-up access is temporarily unavailable.

For a static route, the setting for "Active" in the routing table defines whether it should be propagated constantly or only when it is actually reachable.

Command line: **Setup** > **IP-Router** > **IP-Routing-Table**

6.2.7 WAN RIP

In order for routes learned from RIP to be broadcast across the WAN, the respective remote sites can be entered into the WAN RIP table under **IP Router** > **General** > **WAN RIP**.



The WAN RIP table contains the following values:

Remote site

Contains the name of the remote site.

RIP type

Specifies the RIP version used to propagate the local routes.

Send RIP to this remote site.

Specify whether RIP is to be propagated on the WAN routes. The RIP type must be set for this.

Accept RIP from this remote site

Specify whether RIP is to be accepted from the WAN. The RIP type must be set for this.

Please bear in mind that WAN-side RIP represents a potential security risk.

Masquerading

Specify whether and how the device is masked on the route. This entry makes it possible to start WAN RIP even in an empty routing table. The following values are possible:

- **Auto**: The masquerade type is taken from the routing table (value: 0). If there is no routing entry for the remote site, then masquerading is not performed.
- **On**: All connections are masqueraded (value: 1).
- **Intranet**: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently (value: 2).

Block back routes (poisoned reverse)

When blocking the return route (poisoned reverse), all routes learned/received on this interface are marked and returned as "unavailable "by directly setting the number of hops to 16 (or the maximum).

Active proposing of RIP according to RFC 2091 activated

The device supports RIP according to RFC 2091.

The setting "propose RFC 2091" is only relevant for active connection establishment. Passive connections accept the RIP version proposed by the remote site, regardless of how this switch is set.

For active connections that propose RIP as per RFC 2091, there is an optional fallback to "normal" RIP as per RFC 2453: A fallback occurs if the remote site does not respond to 10 retries of the first packet (10 retries take about 30 seconds).

The entry for the gateway is taken to be the IP address of the RIP partner at the other end of the WAN route. 0.0.0.0 can be entered here if a PPP negotiation is conducted over the WAN route and the IP address of the remote site is transmitted.



In a central gateway, the setting "RFC 2091" can always be off and the "Gateway" entry always set to 0.0.0.0 because the central gateway always considers the gateway as specified at the subsidiary.

Gateway

Enter the IP address of the RIP partner.

Source address (optional)

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If you have configured loopback addresses, you can specify them here as source address. As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.



If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Default routing tag

This indicates the "default routing tag" applicable for the WAN link. When the device transmits over the WAN, it gives this tag to all untagged routes.

Routing tag list

This is a comma-separated list of the tags that the device accepts on the interface. If this list is empty, the device accepts all tags. If at least one tag is in the list, then the device only accepts the tags in this list. When sending tagged routes on the WAN, the device only propagates routes with valid tags.

The device internally treats all routes learned from the WAN as untagged routes and propagates them on the LAN with the default tag (0). Over the WAN, however, it propagates routes with the tag that it learned.

RX filter

Specify here the filter to be applied when receiving (RX) RIP packets.

You must first define the filter in the RIP filter list in order to use it here.

TX filter

Specify here the filter to be applied when sending (TX) RIP packets.

You must first define the filter in the RIP filter list in order to use it here.

6.2.8 SYN/ACK speedup

The SYN/ACK speedup procedure is used to speed up IP data traffic. In SYN/ACK speedup, IP control characters (SYN for synchronization and ACK for acknowledge) within the send buffer are given priority over simple data packets. This avoids the situation where control characters remain in the send queue for a longer time and the remote terminal therefore stops sending data.

The greatest effect of SYN/ACK speedup occurs with fast connections (e.g. ADSL) when data is transmitted simultaneously in both directions at high speed.

The SYN/ACK speedup is switched on at the factory.

6.2.8.1 Switch off in case of problems

Preferential treatment of individual packages changes the original package order. Although TCP/IP does not guarantee a specific packet order, problems may occur in individual applications. This only affects applications that require a specific packet sequence in deviation from the protocol standard. In this case, the SYN/ACK speedup can be switched off:

LANconfig: **IP Router** > **General** > **Pass on TCP SYN and ACK packets preferentially**

6.3 Advanced Routing and Forwarding (ARF)

6.3.1 Introduction

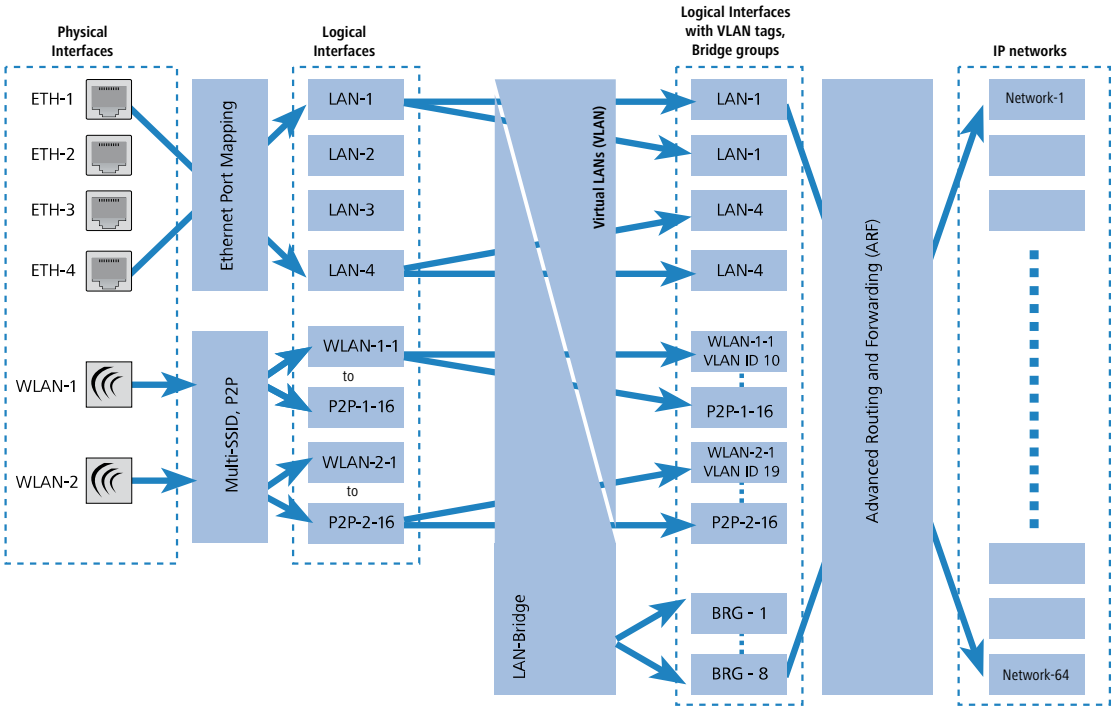
In simple use cases, a device manages two local networks only: The intranet and the DMZ. In more complex environments, however, it is often desirable to realize more than one intranet and one DMZ with a device, for example to provide Internet access to multiple IP networks by means of a central device. Depending on the model, current devices support up to 64 different IP networks.

Various scenarios are possible when realizing multiple IP networks:

- One network per interface.
- Multiple networks per interface.
- Multiple VLANs per interface; one or more networks per VLAN (which corresponds with a combination of the first two scenarios).

The realization of these scenarios is facilitated by advanced routing and forwarding (ARF), which provides very flexible options in the definition of IP networks and the assignment of these networks to the interfaces. The diagram below

illustrates the network/interface assignment at various levels. The configuration options applied here are described in the following chapters.



The assignment of IP networks to interfaces proceeds as follows:

- The various models have different numbers of physical interfaces, i.e. Ethernet ports or WLAN modules. The logical interface(s) is/are assigned to the physical interface:
  - For the Ethernet ports, assignment is handled by Ethernet port mapping.

    For some but not all models, the number of logical LAN interfaces corresponds to the number of physically available Ethernet ports.
  - In the case of the WLAN modules, the establishment of point-to-point connections (P2P) and/or the use of Multi-SSID can mean that multiple WLAN interfaces are assigned to each physical WLAN module: Up to 16 wireless networks and up to 16 P2P connections per module
- These logical interfaces are further specified and grouped in the next stage:
  - For devices supporting VLAN, multiple VLANs can be defined for each logical interface simply by using VLAN-IDs. Although the data traffic for the various VLANs flows via a common logical interface, the VLAN-ID ensures that the different VLANs remain strictly separated. From the perspective of the device, the VLANs are completely separate interfaces, meaning that a single logical interface becomes multiple logical interfaces for the device, and each of which can be addressed individually.
  - For devices with WLAN modules, the individual logical interfaces can be grouped together. This is handled by the LAN bridge which regulates data transfer between the LAN and WLAN interfaces. The formation of bridge groups (BRG) allows multiple logical interfaces to be addresses at once and they appear as a single interface to the device—in effect achieving the opposite of the VLAN method.
- In the final stage, the ARF forms a connection between the logical interfaces with VLAN tags and the bridge groups on the one side, and the IP networks on the other. For this reason, an IP network is configured with a reference to a logical network (with VLAN-ID, if applicable) or to a bridge group. Furthermore, for each IP network an interface tag can be set, with which the IP network can be separated from other networks without having to use firewall rules.

The definition of routing tags for IP networks as described above is one of the main advantages of Advanced Routing and Forwarding. This option allows “virtual routers” to be realized. By using the interface tag, a virtual router uses only

a part of the routing table for an IP network, and in this way controls the routing specifically for that one IP network. This method allows, for example, several default routes to be defined in the routing table, each of which is given a routing tag. Virtual routers in the IP networks use the tags to select the default route which applies to the IP network with the appropriate interface tag. The separation of IP networks via virtual routers even permits multiple IP networks with one and the same address range to be operated in parallel on a single device.

An example: Within an office building, a number of companies have to be connected to the Internet via a central device, even though each of these companies has its own Internet provider. All of the companies want to use the popular IP network '10.0.0.0' with the netmask '255.255.255.0'. To implement these requirements, each company is given an IP network '10.0.0.0/255.255.255.0' with a unique name and a unique interface tag. In the routing table, a default route with the corresponding routing tag is created for each Internet provider. This allows the clients in the different company networks, all of which use the same IP addresses, to access the Internet via their own provider. Employing VLANs enables logical networks to be separated from one another even though they use the same physical medium (Ethernet).

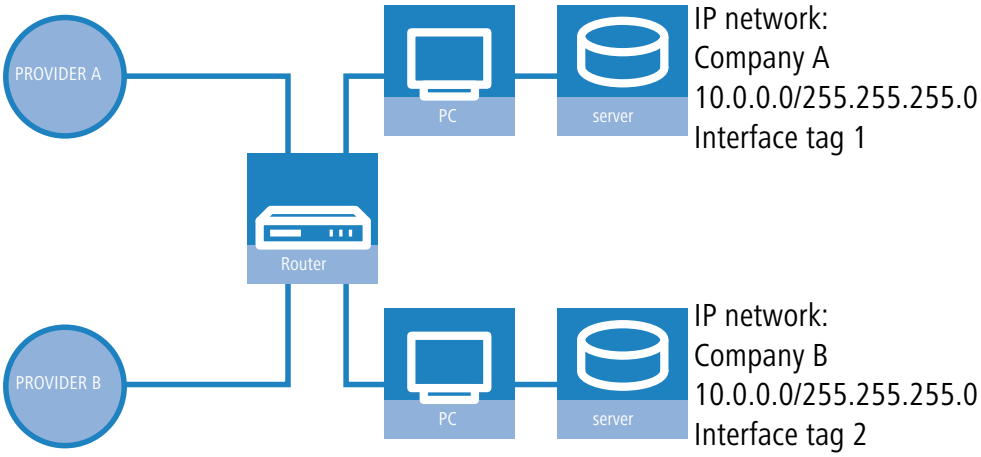
The differences between routing tags and interface tags

Routing tags as assigned by the firewall and interface tags as defined by the IP networks have a great deal in common, but also some important differences:

- The router interprets both tags in the same way. Packets with the interface tag '2' are valid for routes with the routing tag set to '2' in the routing table (and all routes with the default route tag '0'). The same routes apply for packets which the firewall has assigned with the routing tag '2'.

  Thus the interface tag is used in the same way as a routing tag.

- Interface tags have the additional ability to delimit the visibility (or accessibility) between different networks:
  - In principle, only networks with the same interface tag are “visible” to one another and thus able to interconnect.
  - Networks with the interface tag '0' have a special significance; they are in effect supervisor networks. The networks can see all of the other networks and can connect to them. Networks with an interface tag not equal to '0' cannot make connections to supervisor networks, however.
  - Networks of the type 'DMZ' are visible to all other networks, independent of any interface tags—this is useful as the DMZ often hosts public servers such as web servers, etc. The DMZ networks themselves can only see networks with the same interface tag (and any other DMZ networks, of course).
  - A special case involves networks of the type ’DMZ’ with the interface tag '0': As “supervisor networks” they can see all other networks and they are visible to all other networks.



For cases which do not allow IP addresses to be uniquely assigned by interface tag, the Advanced Routing and Forwarding can be supported by firewall rules. In the above example, this would be the case if each of the networks were to support a public web or mail server, all of which use the same IP address.

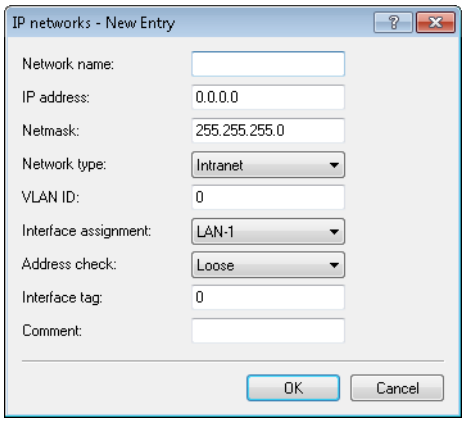
6.3.2 Defining networks and assigning interfaces

When defining a network, the first setting is for the IP address range which is to be valid for a certain local interface on the router. "Local interfaces" are logical interfaces that are assigned either to a physical Ethernet port (LAN) or a wireless port (WLAN). To realize the scenarios outlined above, it is possible for several networks to be active on one interface: Conversely, a network can also be active on multiple interfaces.

The networks are defined in a table under **IPv4** > **General** > **IP networks**. A unique name for the networks is set along with definitions for the address range and interface assignment. The network name allows the identification of networks in other modules (DHCP server, RIP, etc.) and to enable control over which services are available in which networks.

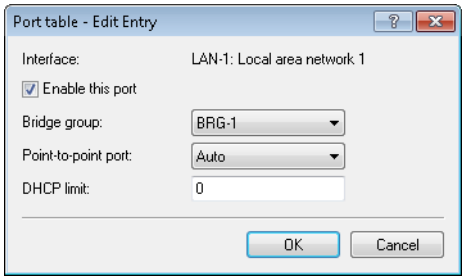
The network name must not be the same as the name of a remote site (e.g. a VPN connection). Otherwise the communication on the network and the remote site won't be reliable anymore.

The network name must contain at least one letter as otherwise in the routing table there is no way to distinguish between IP address and interface.



6.3.3 Assigning logical interfaces to bridge groups

Located under **Interfaces** > **LAN** > **LAN bridge**, the **Port table** is used to specify the properties of the logical interfaces.



Enable this port

This option activates or deactivates the logical interface.

Bridge group

Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the router to be a single interface. This can then be used for Advanced Routing and Forwarding, for example.

If the interface is removed from all bridge groups by setting **none**, then there is no communication between the LAN and WLAN via the LAN bridge (isolated mode). With this setting, LAN/WLAN data transfers over this interface are only possible via the router.

A requirement for data transfer from/to a logical interface via the LAN bridge is the deactivation of the global "isolated mode" which applies to the whole of the LAN bridge. Furthermore, the logical interface must be assigned to a bridge group. With the setting **none**, no transfers can be made via the LAN bridge.

Point-to-point port

This item corresponds to the "adminPointToPointMAC" setting as defined in IEEE 802.1D. By default, the point-to-point setting for the LAN interface is derived from the technology and the concurrent status: However, this automatic specification can be revised if this is unsuitable for the required configuration.

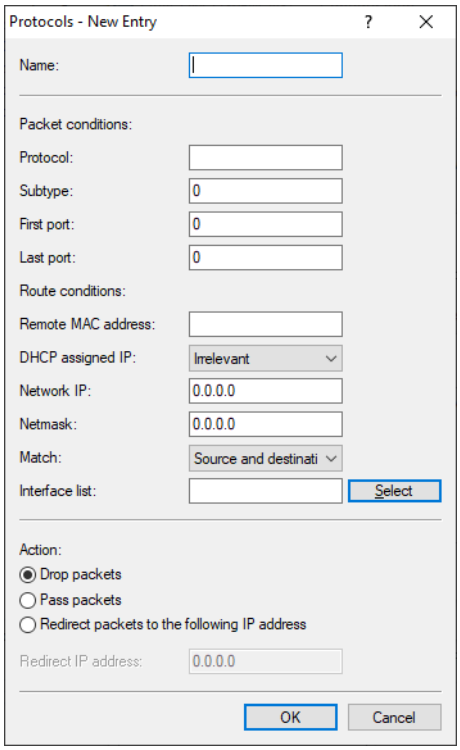
Interfaces in point-to-point mode have various specialized capabilities, such as the accelerated port status change for working with the Rapid Spanning Tree Protocol.

DHCP limit

Number of clients which can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filer table to limit access to just one logical interface.

6.3.4 Filtering protocols

With the protocol filter you can influence the handling of certain protocols for transmissions between interfaces, e.g. from the WLAN to the LAN. The use of appropriate rules allows the definition of which data packets should be inspected, interfaces for which the filter applies and which action should be performed on the data packets.



LANconfig: **Interfaces** > **LAN** > **LAN bridge** > **Protocols**

Command prompt: **Setup** > **LAN-Bridge** > **Protocol-Table**

Similar to a firewall rule, a protocol filter consists of two parts:

- The packet conditions defines the conditions that must be satisfied in order for the filter to be applied to a packet.
- The action defines what happens to the packet if the condition is met.

A packet filter is described by the following parameters:

Name

A name of your choice for the filter entry.

Protocol

The protocol that this filter is valid for. If '0' is entered as the protocol, the filter applies to **all** packets.

Subtype

The sub-protocol for which this filter is valid. If '0' is entered as the sub-protocol, the filter applies to **all** packets of the specified protocol.

First port / Last port

The port range that this filter is to be valid for. If '0' is entered as the start port, this filter will be applied to **all** ports of the corresponding protocol/sub-protocol. If '0' is entered as the end port, the start port becomes an end port.

Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

Remote MAC address

The MAC address of the client to which the packet is to be sent. If no destination MAC address is entered, the filter is applied to **all** packets.

IP assigned by DHCP

Setting this option to **Yes** or **No** activates the DHCP tracking. This checks whether the table **Status** > **LAN-Bridge** > **DHCP-Table** contains the source MAC address of a packet from a network user who obtained an IP address via DHCP. Additionally, a network can be specified for a filter rule. However, if a rule has set this parameter to **Yes**, a specified network could be ignored.

Possible values:

- **Yes:** The rule applies if the source MAC address of the packet is listed in the table under **Status** > **LAN-Bridge** > **DHCP-Table** as an address that obtained an IP address via DHCP.
- **No**: The rule applies if this is not the case.
- **Irrelevant**: The source MAC address is not considered.

If DHCP address tracking is enabled, any IP addresses usually entered are disregarded.

Network IP / Netmask

The IP address of the network mask to which this filter applies. Only those IP packets whose source and destination IP addresses lie within this network are captured by the rule.

If no network is entered, the filter applies to **all** packets.

Match

By default, the source and the destination address are both checked. Here you can specify whether only the source or only the destination address is checked instead.

Interface list

List of the interfaces to which the filter applies.

All of the LAN interfaces, DMZ interfaces, logical WLAN networks and point-to-point connections in the WLAN may be entered as interfaces.

The following examples illustrate how interfaces are specified: 'LAN-1' for the first LAN interface, 'WLAN-2-3' for the third logical WLAN network on the second physical WLAN interface, 'P2P-1-2' for the second point-to-point connection on the first physical WLAN interface.

Groups of interfaces may be specified in the form 'WLAN-1-1~WLAN-1-6' (logical WLANs 1 to 6 on the first physical WLAN interface) or with a wildcard as 'P2P-1-*' (all P2P connections on the first physical interface).

Only filter rules with valid entries in the interface list are active. A rule with no specification of the interfaces does not apply to all of them - it is ignored instead.

Action

Action performed for the data packets processed by this rule:

Redirect IP address

Destination IP address for the "Redirect" action

On redirection, the destination IP address of the packets is replaced by the Redirect IP address entered here. Furthermore, the destination MAC address is replaced by the MAC address determined using ARP for the Redirect IP address.

If ARP was unable to determine the destination MAC address, the packet is dropped rather than redirected.

Example:

Name	DHCP-Src-MAC	Dest-MAC-Addr.	Prot.	IP address	IP network	Subtype	First port	Last port	Interface list	Action	Redirect IP address
ARP	irrelevant	000000000000	0806	0.0.0.0	0.0.0.0	0	0	0	WLAN-1-2	Pass	0.0.0.0
DHCP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	17	67	68	WLAN-1-2	Pass	0.0.0.0
TELNET	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	23	23	WLAN-1-2	Redirect	192.168.11.5
ICMP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	1	0	0	WLAN-1-2	Pass	0.0.0.0
HTTP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	80	80	WLAN-1-2	Redirect	192.168.11.5

ARP, DHCP, ICMP are allowed to pass, Telnet and HTTP are redirected to 192.168.11.5 and all other packets are dropped.

If no filter rules are defined for an interface, all packets from and destined to it are transmitted without alteration. As soon as a filter rule has been defined for an interface, all packets to be transferred via this interface are checked prior to being processed.

1. As a first step, the information required for checking is read out of the packets:
   - DHCP source MAC
   - Destination MAC address of the packet
   - Protocol, e.g. IPv4, ARP
   - Sub-protocol, e.g. TCP, UDP or ICMP for IPv4 packets, ARP Request or ARP Response for ARP packets
   - IP address and network mask (source and destination) for IPv4 packets
   - Source and destination port for IPv4 TCP or IPv4 UDP packets
2. As a second step, this information is checked against the information from the filter rules. All those rules in which the source **or** destination interface is included in the interface list are considered. Checking of the rules for the individual values is as follows:
   - For DHCP source MAC, protocol and sub-protocol, the values read out of the packets are checked for consistency with the values defined in the rule.
   - With IP addresses, the source **and** destination address of the packet are checked to see whether they lie within the range formed by the IP address and the network mask of the rule.
   - Source and destination ports are checked to see whether they lie in the range between start port and end port.

If none of the rule values specified (not filled by wildcards) agree with the values read out of the packet, the rule is not considered applicable and is disregarded. If several rules apply, the most accurate rule action is carried out. Parameters are more accurate the further down the list of parameters they are or the further right they appear in the protocol table.

If rules are defined for an interface, but there is no match with one of the rules for a packet from/for this interface, the default rule for this interface is used for the packet. The default rule is preconfigured for each interface with the 'drop' action but this is not visible in the protocol table. To modify a default rule for an interface, a rule with the name 'default-drop' is defined. Besides the interface naming, this rule can only contain wildcats and the required action.

Checking of MAC addresses in packets sent over the respective interface takes on a different form to that with in-coming packets.

- With out-going packets, the source MAC address read out of the packet is checked against the destination MAC address entered in the rule.
- The destination MAC addresses read out of the packet are then checked to see whether they are listed as currently active DHCP clients.
- Rules with the 'Redirect' action are ignored if they apply for an interface over which the packet is to be sent.

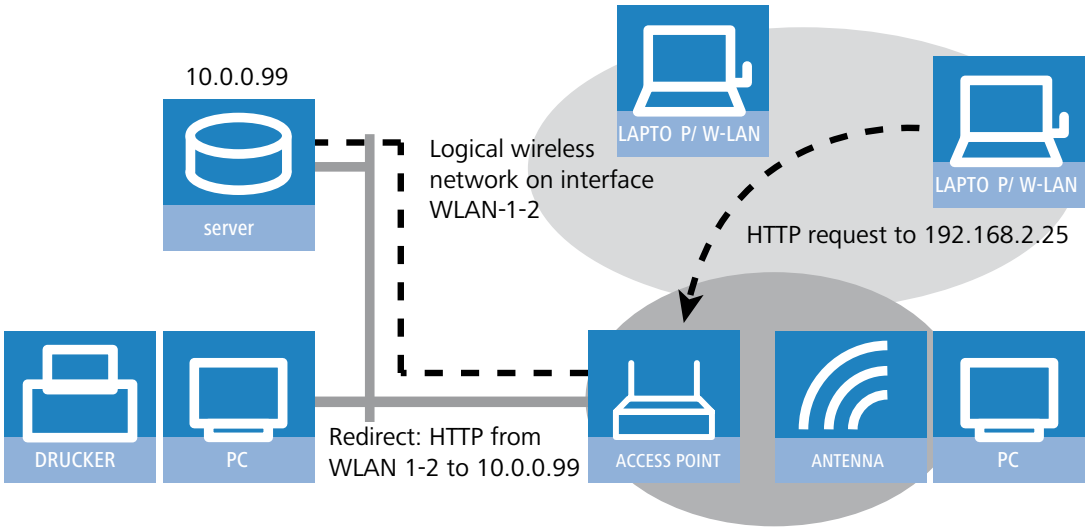
3. In the third step, the action associated with the applicable rule is carried out.

With the Redirect action, IPv4 packets can not only be transferred and dropped, they can also be communicated specifically to a particular destination. As a general rule, the destination IP address of the packet is replaced by the Redirect IP address entered. The destination MAC address of the packet is replaced by the MAC address determined by ARP and associated with the Redirect IP address.

In order for the redirected packets to find the correct sender on their “return trip”, a dynamic table is compiled with automatic filter rules that apply to packets leaving via this interface. This table can be viewed under `Status > LAN bridge > Connection table`. Rules in this table have a higher priority than other matching rules with the 'Transfer' or 'Drop' actions.

Clients within wireless networks often have one aspect in common: They are highly mobile. Consequently, clients are not necessarily always connected to the same AP, but frequently change between APs and the related LANs.

The redirect function assists WLAN client applications to automatically find the correct target computer in the LAN. If a WLAN client's HTTP request from a particular logical wireless network is to be always directed to a particular server in the LAN, a filter setting with the "Redirect" action is set up for the appropriate protocol for the desired logical WLAN interface.



All requests with this protocol from this logical wireless network are automatically redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, ensuring trouble-free operation in both directions.

DHCP address tracking keeps a record of which clients have received their IP addresses using DHCP. The relevant information for an interface is automatically maintained in a table under `Status > LAN Bridge > DHCP Table`. DHCP tracking is enabled on an interface if, for this interface, a minimum of one rule is defined where 'DHCP Source MAC' is set to 'Yes'.

The number of clients which may be connected to an interface via DHCP can be configured in the Port table under `Setup > LAN Bridge > Port Data`. Setting the entry to '0' means that any number of clients can register at this interface via DHCP. If the maximum number of DHCP clients is exceeded by a further attempt to register, the oldest entry in the list is deleted.

When checking data packets, IP addresses and the IP network mask defined in the rule are not used. Consequently no check is made as to whether the destination IP address of the packet lies within the range specified. Instead, a check is made as to whether the source IP address of the packet matches the IP address assigned to the client via DHCP. The connection of the two IP addresses is made based on the source MAC address.

This check can be used to block clients which have received an IP address via DHCP, but which actually use a different IP address (either intentionally or inadvertently). A rule in which the DHCP Source MAC parameter is set to 'Yes' would not apply since the two addresses do not match. The packet would instead be processed either by other rules or the default rule.

In order for DHCP tracking to work, at least two more rules must be set up for this interface, rules which are not dependent on DHCP tracking. This is necessary since the required DHCP information is not exchanged until the end of DHCP handshake. This is why packets due to be sent beforehand must be allowed by rules which do not use DHCP tracking. These usually included TCP/UDP packets on port 67 and 68 and ARP packets.

If DHCP tracking is enabled on an interface, packets received on this interface from HDCP servers are automatically dropped.

6.3.5 Interfaces tags for remote sites

The definition of interface tags in Advanced Routing and Forwarding (ARF) facilitates the use of virtual routers, which only use a part of the overall routing table. For inbound data packets from the WAN, the assignment of interfaces tags can be regulated in different ways:

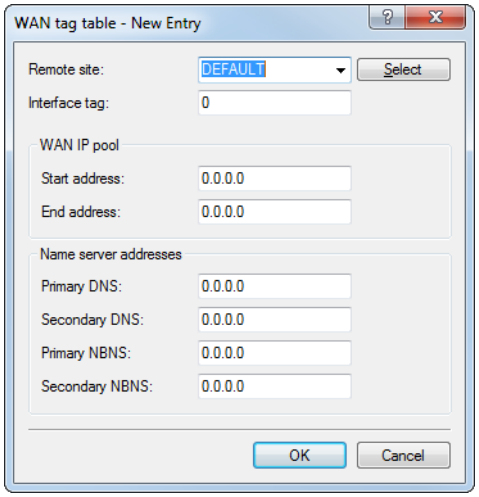
- By using appropriate firewall rules that only capture data packets from particular remote sites, IP addresses or ports
- Via an explicit assignment of tags to remote sites.

This assignment of tags to the remote sites to separate ARF networks can also be conveniently used for packets received at the WAN-side (which by default contain Tag 0). Without controlling the assignment of tags explicitly with the firewall, the virtual router can be determined directly from the remote site or source route from the form of the interface tag. Inbound and outbound communication can thus be easily divided between virtual routers bidirectionally.

The interface tags determined via the tag table can be overwritten with an appropriate entry in the firewall.

6.3.5.1 Assigning interface tags via the tag table

LANconfig: **Communication** > **Remote sites** > **WAN tag table**



Interface tags assign remote sites to a unique ARF network or tag. This assignment must be done manually for each ARF network.

From LCOS 10.20, automatic WAN-tag generation is no longer supported. All remote sites have to be assigned manually.

6.3.6 Setting the routing tag for local routes

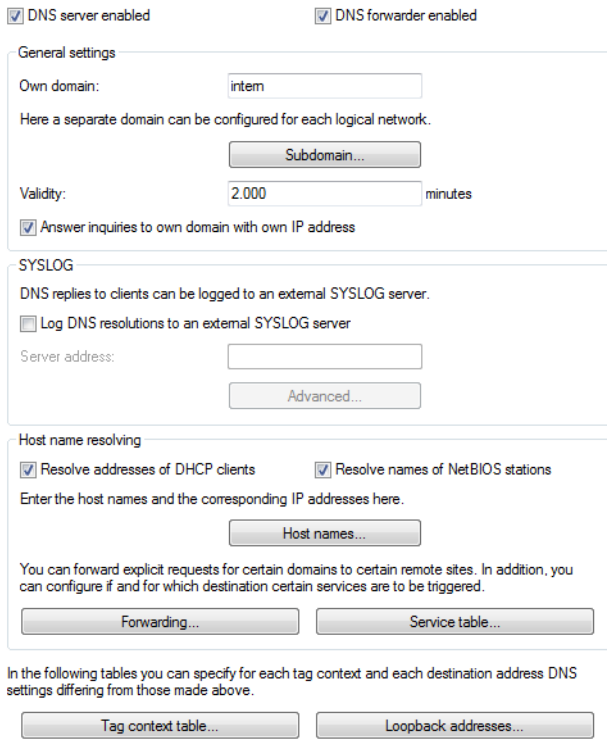
The definition of interface tags in Advanced Routing and Forwarding (ARF) facilitates the use of virtual routers, which only use a part of the overall routing table. The interface tag for a packet received from another local router is set according to the following procedure:

1. If there is only one ARF network on a LAN interface/VLAN pair, this is selected automatically.
2. If there are multiple ARF networks on a LAN descriptor / VLAN pair, then a check is made to see if the source address of the packet is local to one of the ARF networks. If so, this network is then selected.
3. If not, a reverse ARP lookup is performed for the source MAC address, which determines the address of the next hop to the source address. If the address can be resolved, then a check is made to see whether it is local to one of the ARF networks. If so, this network is then selected.
4. If the address cannot be resolved, then the first ARF network of the LAN interface / VLAN pair is selected.
5. The selected ARF network determines the interface tag to be used.

6.3.7 Routing tags for DNS forwarding

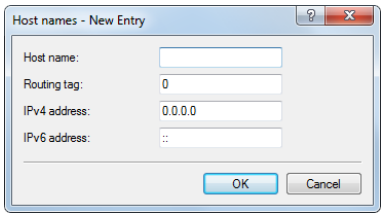
With DNS forwarding, it is possible to set up multiple forwarding definitions (especially general wildcard definitions with "*") that are independent of one another by marking them with unique routing tags. Depending on the routing context

of the requesting client, the router considers only those forwarding entries that are correspondingly tagged and any general entries that are marked with “0”.



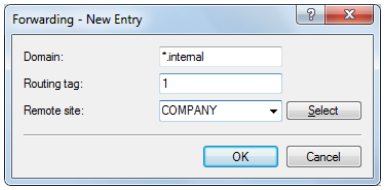
Station name

The item **DNS** > **General** > **Host names** is used to define the tag context and IP number used by the device to resolve the station names.



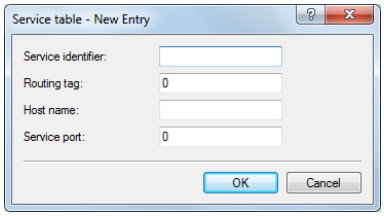
DNS destinations

The item **DNS** > **General** > **Forwarding** is used to set the routing tags for the forwarding rules, so ensuring they only apply when the correct routing tags are used.



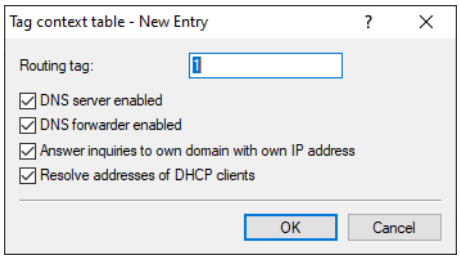
Service table

The item **DNS** > **General** > **Service table** is used to assign routing tags to the services, so ensuring that they are only available when the correct routing tags are used.



Tag context table

In LANconfig under **DNS** > **General** > **Tag context table**, tag contexts can be defined which override the global settings of the DNS server for specific interface and routing tags (routing context):



If an entry for a tag context exists, then only the DNS settings in this table apply for this context. However, if there is no entry in this table, then the global settings of the DNS server apply.

The following options are possible for each tag context:

Routing tag

Unique interface or routing tag in the range of 1 to 65535, the subsequent settings will override the global settings of the DNS server.

DNS server enabled

Enables the DNS server of the device.

DNS forwarder enabled

Enables DNS forwarders for this device.

Answer inquiries to own domain with own IP address

If enabled, DNS requests relating to the router's own domain will be answered with the router's IP address.

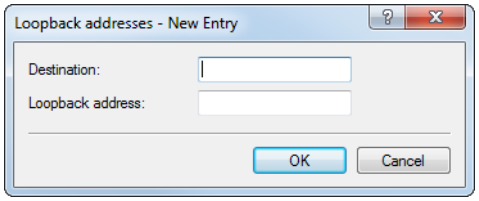
Resolve addresses of DHCP clients

Enables resolution of station names that have requested an IP address through DHCP.

Loopback addresses

LANconfig allows loopback addresses to be specified for every remote site under **DNS** > **General** > **Loopback addresses**. Consequently, there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one

remote site and loopback address. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.



The following options are possible for each loopback address:

Destination

The remote site for a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an "@". The remote site must also be in the DNS Destinations table.

Source address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

6.3.8 Virtual routers

Interface-dependent filtering—in combination with policy-based routing—allows virtual routers to be defined for every interface:

Example:

Two separate IP networks are used by the Development and Sales departments. Both networks are connected to different switch ports although they use the same network '10.1.1.0/255.255.255.0'. Sales should be able to enter the Internet only, whereas Development should also have access to a partner company's network ('192.168.1.0/255.255.255.0').

The result is the following routing table (where the Development dept. has tag 2, Sales has tag 1):

IP address	IP-Netmask	Rtg tag	Peer-or-IP	Distance	Masking	Active
192.168.1.0	255.255.255.0	2	PARTNER	0	No	Yes
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No	Yes
255,255,255,255	0.0.0.0	2	INTERNET	2	Yes	Yes
255,255,255,255	0.0.0.0	1	INTERNET	2	Yes	Yes

If Development and Sales were in IP networks with different address ranges, then it would be no problem to assign the routing tags with firewall rules. Since both departments are in the same IP network, the only available method of assignment is with network names.

Tag assignment can be carried out directly in the network definition:

Network name	IP address	Netmask	VLAN ID	Interface	Source check	Type	Rtg-Tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1	Strict	Intranet	2
SALES	10.1.1.1	255.255.255.0	0	LAN-2	Strict	Intranet	1

Alternatively the assignment of tags can be carried out with a combination of network definitions and firewall rules. The networks are defined as follows:

Network name	IP address	Netmask	VLAN ID	Interface	Source check	Type	Rtg-Tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1	Strict	Intranet	0
SALES	10.1.1.1	255.255.255.0	0	LAN-2	Strict	Intranet	0

Routing tags can be used to define the following firewall rules:

Name	Protocol	Source	Destination	Action	Linked	Prio	(...)	Rtg tag
DEVELOPMENT	ANY	%Ldevelopment	ANYHOST	%a	Yes	255		2
SALES	ANY	%Lsales	ANYHOST	%a	Yes	255		1

Important for these rules is the maximum priority (255) so that these rules are always checked first. Since filtering is still possible by services, the option "Linked" has to be set in the firewall rule.

6.4 Configuring remote sites

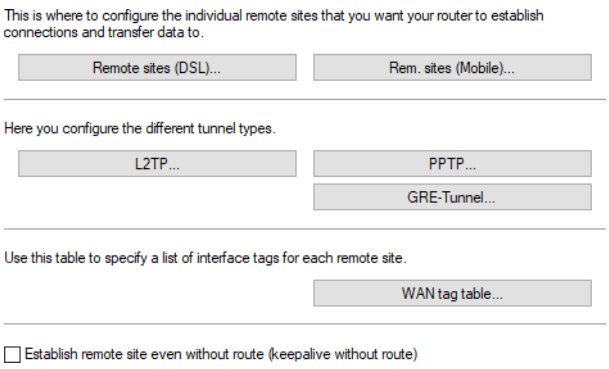
Remote sites are configured in two tables:

- The Remote site list (or lists) contain(s) all the information that applies individually to only one remote site.
- Parameters for the lower protocol levels (under IP) are specified in the Communication layers table.

This section does not include how to configure the authentication (protocol, user name, password). Refer to section *Connection establishment with PPP* on page 454 for information on authentication.

6.4.1 Remote sites

The available remote sites are specified in this list, along with a suitable name and additional parameters. Each WAN interface has its own separate list of remote sites. The lists of remote sites are located under **Communication** > **Remote sites**.



Establish remote site even without route (keepalive without route)

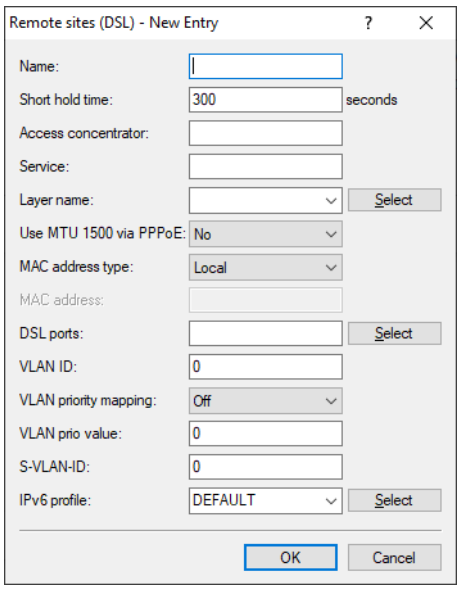
Specifies whether a connection to a remote site, e.g. a VPN tunnel or an Internet connection, should be established even without a route. Connecting to the remote site without an explicit route in the routing table is necessary if the remote site transmits the routes, e.g. by DHCP (Classless Static Route Option) or a dynamic routing protocol.

Please observe the following advice when editing the remote-sites lists:

- If two remote-site lists contain identical names for remote sites (e.g. DSL broadband peers and Dialup peers), the device automatically takes the “fastest” interface when establishing the connection. The other interface is available for backup purposes.
- If the list does not specify DSL broadband remote sites, access concentrators or services, then the router connects to the first access concentrator that responds to the request over the exchange line.
- For an existing DSLoL interface, the same entries apply as for a DSL interface. This information is entered into the list of DSL broadband remote sites.

DSL broadband peers

You set up DSL broadband remotes under **Remote sites (DSL)**.



Name

This name is used to identify the remote site in the router modules. As soon as the router modules have used the IP address to determine where the remote site can be reached, the corresponding connection parameters are taken from the remote site list.

Short hold time

This time defines how long a connection is kept active if data is no longer being transferred. If a zero is entered as hold time, the connection will not be interrupted automatically. If the short hold time is set to 9999, interrupted connections will be reestablished automatically (see *Permanent connection for flat rates – keep-alive* on page 462).

VPI / VCI

Enter the VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) for your ADSL connection here.

These values are communicated to you by your ADSL network operator. Typical values for VPI/VCI are, for example: 0/35, 0/38, 1/32, 8/35, 8/48.

Access concentrator

The access concentrator (AC) is the server that can be reached at this remote site. If multiple providers can be accessed via your ADSL connection, use the name of the AC to select the provider responsible for the IP-address range of this remote site. Your provider will inform you of the values to be entered for the AC. If no value is entered for the AC, all ACs will be accepted that offer the requested service.

Service

Enter the provider's service that you wish to use. This can be, for example, simple Internet surfing or even video downstreaming. Your provider will inform you of the values to be entered for the service. If no value is entered for the service, all services will be accepted that are offered by the requested access concentrator.

Layer name

Select the communication layer to be used for this connection. How to configure this layer is described under *Layer List* on page 414.

Use MTU 1500 via PPPoE

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

MAC address type

Here you select the MAC address to be used. If you need to specify an explicit MAC address for the remote gateway (**user-defined**), then enter it under **MAC address**. With **Local** selected, additional virtual addresses based on the MAC address of the device are generated for each WAN connection. **Global** uses the MAC address of the device for all connections.

MAC address

Enter the user-defined MAC address here, if applicable.

DSL ports

Select the DSL ports to use if your device has more than one DSL port. Activate channel bundling in the relevant layer to bundle the DSL lines.

VLAN ID

See *VLAN IDs for DSL interfaces* on page 947.

VLAN priority mapping

This entry controls how the VLAN priority mapping functions.

Off

VLAN priority mapping is disabled.

1TR-112

The value "1TR112" maps the precedence (i.e., the top 3 bits) of the DSCP into the VLAN priority field. Additionally, PPP-LCP echo packets are marked with VLAN priority 6, and IGMP packets are marked with 4.

DSCP

The "DSCP" value maps the precedence (i.e. the top 3 bits) of the DSCP into the VLAN Prio field.

Value

All packets sent to the WAN are marked with the priority tag configured under **VLAN- Prio-Value**. However, this only happens if a VLAN other than 0 is also configured. Otherwise it would be equivalent to being set to "Off".

VLAN prio value

This value is set as the VLAN priority value when **VLAN priority mapping** is set to "Value".

S-VLAN ID

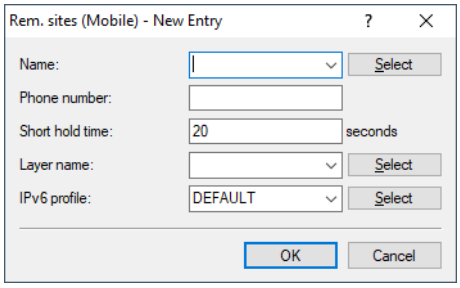
See *Q-in-Q VLAN* on page 943.

IPv6 profile

This entry specifies the IPv6 remote site. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **IPv6 interfaces** > **WAN profiles**.

Dial-in peers

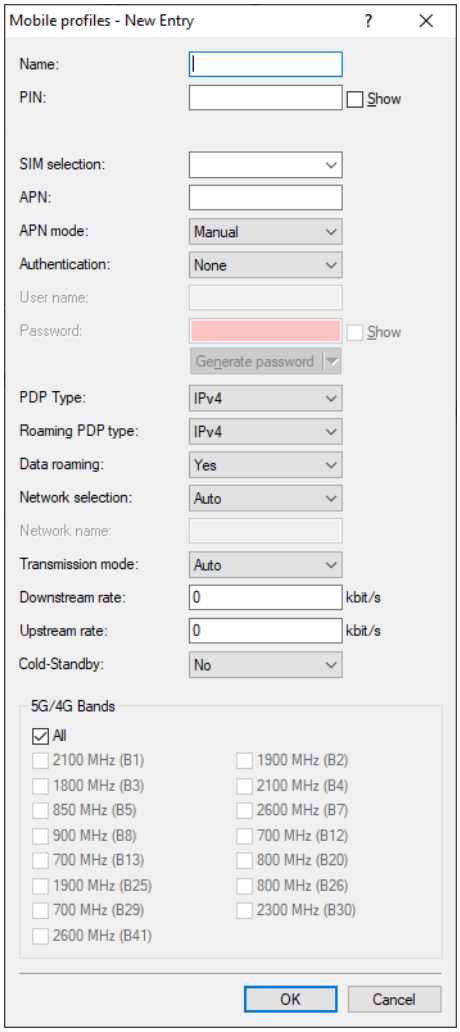
The remote dial-in peers are set up under **Remote sites (mobile)**. Depending on the device, other dial-in options are available here.



Name

This name is used to identify the remote site in the router modules. As soon as the router modules have used the IP address to determine where the remote site can be reached, the corresponding connection parameters are taken from the remote site list.

The name of the remote site corresponds to a **Mobile profile**from **Interfaces** > **WAN** > **Mobile settings**.



Name

Enter a unique name for this mobile profile here. This profile can then be selected in the WAN-interface settings (mobile).

PIN

Enter the 4-digit PIN of the mobile phone SIM card used at the mobile interface. The router needs this information to operate the mobile interface.

The SIM card records each attempt to enter an incorrect PIN. The number of Failed attempts is "remembered" even after the power supply is interrupted. After 3 failed attempts, the SIM card is locked and it is no longer possible to access it with the PIN. In this state, the SIM card needs to be unlocked with the (normally) 8-digit PUK or SuperPIN number.

APN

Here you enter the name of the access server for mobile data services known as the APN (Access Point Name). This information is specific to your mobile telephony service provider, and you will normally find this information in the documentation for your mobile telephony contract.

APN mode

Defines in which mode the APN is to be used.

- With Automatic, the APN is taken from the internal database of the provider settings of the operating system. For this purpose, the provider is queried from the SIM card (MCC/MNC) and searched for in the internal database. The "Automatic" mode only works with public provider APNs and not with private APNs. For private APNs, the mode must be set to "Manual" and the APN entered in the "APN" field.
- For Manual, the APN from the APN field is used

Authentication

Specify whether authentication is required for logging in to the APN. Possible values: None, PAP, CHAP.

User name

If authentication is required for logging in to the APN, enter the user name here.

Password

If authentication is required for logging in to the APN, enter the password here.

PDP type

Defines the IP type of the Packet Data Protocol (PDP) context.

- IPv4: A purely IPv4 data connection is established
- IPv4+IPv6: A dual-stack data connection, i.e. IPv4 and IPv6, is established
- IPv6: A purely IPv6 data connection is established

Network selection

If you have opted for automatic mobile network selection, then the cellular networking interface will login to any available and valid cellular network. If you select manual mobile network selection, then the mobile interface will only login to the specified mobile network.

Manual selection of the mobile network is recommended if the router is operated in a fixed location and the mobile interface should be prevented from logging into other networks, which may offer strong signals, but which may be undesirable or more expensive.

Network name

If you have opted for manual mobile network selection, then the mobile interface will login only to the mobile network specified here with its long name.

Transmission mode

This item selects the cellular data transmission standard that is preferred to be used by the mobile interface.

Downstream rate / Upstream rate

The transfer rates used by the WWAN connection must be entered here to ensure that the Quality of Service (QoS) functions in the firewall work properly.

If you enter 0 for downstream or upstream rate, the interface is set to unlimited. This means QoS rules will not work.

5G/4G Bands

If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result. This selection allows you to control which frequency bands the mobile router can or should use.

Phone number

A telephone number is only required if the remote is to be called. The field can be left empty if calls are to be received only. Several numbers for the same remote can be entered in the **Round-robin list**.

Short hold time

This time defines how long a connection is kept active if data is no longer being transferred. If a zero is entered as hold time, the connection will not be interrupted automatically. If the short hold time is set to 9999, interrupted connections will be reestablished automatically (see *Permanent connection for flat rates – keep-alive* on page 462).

Layer name

Select the communication layer to be used for this connection. How to configure this layer is described under *Layer List* on page 414.

IPv6 profile

This entry specifies the IPv6 remote site. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **IPv6 interfaces** > **WAN profiles**.

6.4.2 Layer List

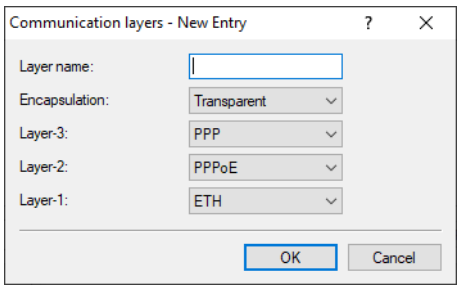
A layer defines a collection of protocol settings to be used for connecting to specific remote sites. The list of communication layers can be found under:

LANconfig: **Communication** > **General** > **Communication layers**

Console: **Setup** > **WAN** > **Layer**

The communication layer list includes predefined common protocol combinations. Changes or additions should only be made if the remote sites are incompatible with the existing layers. The possible options are shown in the following overview.

Please note that the parameters available on the device depend on its functionality. Your device may not offer all the options described here.



Layer name

The layer is selected by this name in the remote site lists.

Encapsulation

Additional encapsulations can be set for the data packets:

Transparent

No additional encapsulation.

Ethernet

Encapsulation as Ethernet frames.

LLC-ETH

Ethernet over ATM with LLC encapsulation according to RFC 2684.

LLC-MUX

Multiplexing over ATM with LLC/SNAP encapsulation according to RFC 2684. Multiple protocols can be transmitted within the same VC (Virtual Channel).

VC-MUX

Multiplexing over ATM by creating additional VCs according to RFC 2684.

Layer-3

The following options are available for the network layer (Layer 3):

Transparent

No additional header is added.

PPP

The connection is established according to the PPP protocol (in synchronous mode, i.e., bit-oriented). Configuration data is taken from the PPP table.

DHCP

Assignment of network parameters via DHCP.

DHCP (Broadcast Flag)

The connection is established using a DHCP client with the broadcast flag set in DHCP.

Layer-2

This field configures the upper part of the Data Link Layer (Layer 2). The following options are available:

Transparent

No additional header is added.

PPPoE

Encapsulation of PPP protocol information into Ethernet frames.

Layer-1

This field configures the lower part of the Data Link Layer (Layer 1). The following options are available:

ETH

Transparent Ethernet according to IEEE 802.3.

WWAN

For connections via the internal WWAN modem.

XDSL

For connections via the internal DSL modem.

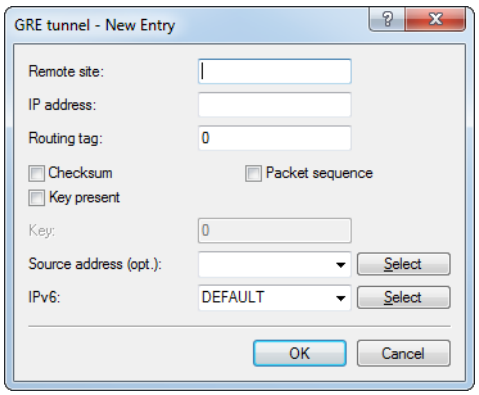
6.5 Generic routing encapsulation (GRE)

6.5.1 Understanding the generic routing encapsulation (GRE) protocol

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. This is very useful, among other things, when the two communication partners wish to use a particular transport protocol (for example, IPSec) that is unavailable on the transmission path. Since GRE itself does not encrypt the tunneled data, the two communication partners themselves must ensure that the data is protected.

6.5.1.1 Configuring a GRE tunnel

To configure a GRE tunnel with LANconfig, navigate to **Communication** > **Remote sites** > **GRE tunnel** and click **GRE tunnel**.



Remote site

The name of the remote site for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

IP address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing tag

Routing tag for the connection to the GRE tunnel endpoint. The device maps data packets to this GRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this GRE tunnel. Two devices connected via several GRE tunnels use this key to map the data packets to the appropriate GRE tunnel.

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.



If the list of IP networks or loopback addresses contains an entry named "DMZ" then the associated IP address will be used.

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **WAN interfaces**.

If you need to specify an IP address for the tunnel interface, proceed as follows:

IPv4

Create a new entry under **Communication** > **Protocols** > **IP parameters** and set the name of the remote site as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **IP address** and **Netmask**.

IPv6

Create a new entry under **IPv6** > **General** > **IP addresses** and set the interface name as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **Address/Prefix length**.

6.5.2 Ethernet-over-GRE (EoGRE)

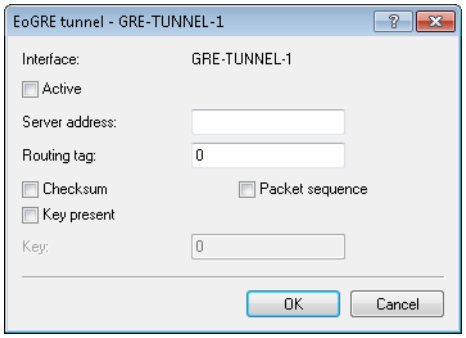
For more information about the GRE protocol, see *Understanding the generic routing encapsulation protocol (GRE)*.

The current version of LCOS provides a number of "Ethernet over GRE" tunnels (EoGRE) to transmit Ethernet packets via GRE. Since these Ethernet packets move on OSI layer 2 only, the EoGRE tunnel only functions as a bridge.

This can be used to implement L2VPN (VPN as a simple level-2 bridge) or a transparent Ethernet bridge over WAN.

6.5.2.1 Configuring an EoGRE tunnel

To configure an EoGRE tunnel with LANconfig, navigate to **Communication** > **Remote sites** > **GRE tunnel**, click **EoGRE tunnel** and select the appropriate tunnel.



Interface

Name of the selected EoGRE tunnel.

Active

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

Server address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing tag

Routing tag for the connection to the EoGRE tunnel endpoint. The device maps data packets to this EoGRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this EoGRE tunnel. Two devices connected via several EoGRE tunnels use this key to map the data packets to the appropriate EoGRE tunnel.

Sequencing

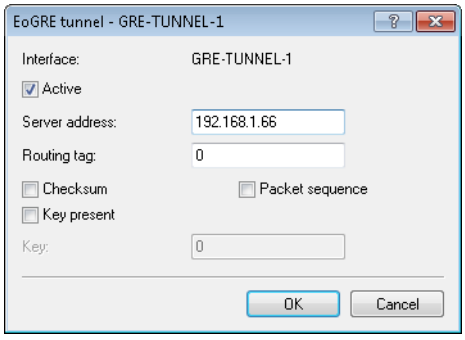
Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

6.5.2.2 Connecting a local interface to an EoGRE tunnel

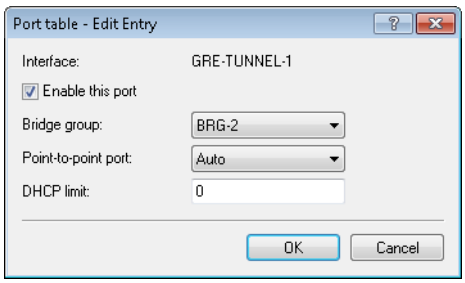
Connecting a local interface to an EoGRE tunnel involves the following steps:

1. Create a new entry under **Communication** > **Remote sites** > **GRE tunnel** > **EoGRE tunnel**.



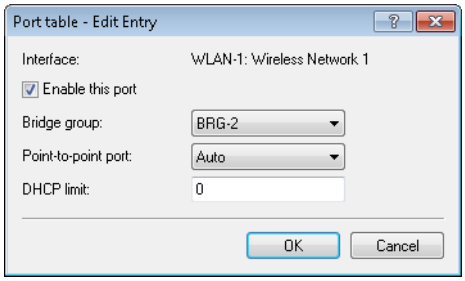
Activate the tunnel and, under **Server address**, enter the address of the remote device to which the EoGRE tunnel is to connect (IPv4 address, IPv6 address, or FQDN).

2. Add a bridge group for the activated EoGRE tunnel under **Interfaces** > **LAN** > **Port table**.



Enable the port and select the required bridge group.

3. Again under **Interfaces** > **LAN** > **Port table**, supplement the same bridge group with the local interface that you want to connect through the EoGRE tunnel (e.g. WLAN-1).



Enable the port and select from the list the bridge group that contains the EoGRE tunnel.

6.6 IP masquerading

One of the most common tasks for a router nowadays is connecting many workstations in a LAN to the mother of all networks, the Internet. Everyone should, if possible, have direct access to the Internet for the latest work-related information.

"IP masquerading" is used as a means of concealing intranet clients so that individual computers and their IP addresses are not visible from the Internet. IP masquerading places two conflicting demands on the router: Whereas each computer needs a valid intranet IP address in order to be reachable from the LAN, it also needs a valid, public IP address (either fixed or assigned dynamically by the provider).

As a matter of principle these two addresses cannot co-exist in a single logical network, so the router must have two IP addresses:

- The intranet IP address for communication with the clients in the LAN
- The public IP address for communication with remote devices in the Internet

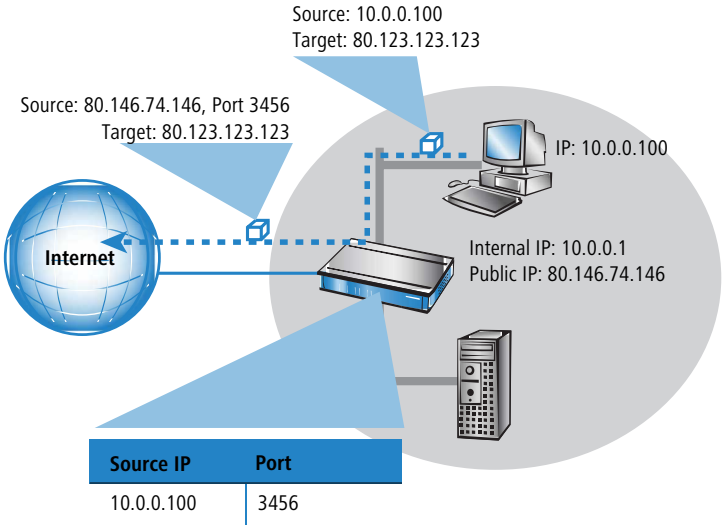
The computers in the LAN use the router as a gateway and are not visible individually. The router separates the Internet from the intranet.

In addition to the options "simple masquerading" and "port forwarding" listed below, LCOS also supports *WAN policy-based NAT* on page 693, which allows masquerading via firewall rules.

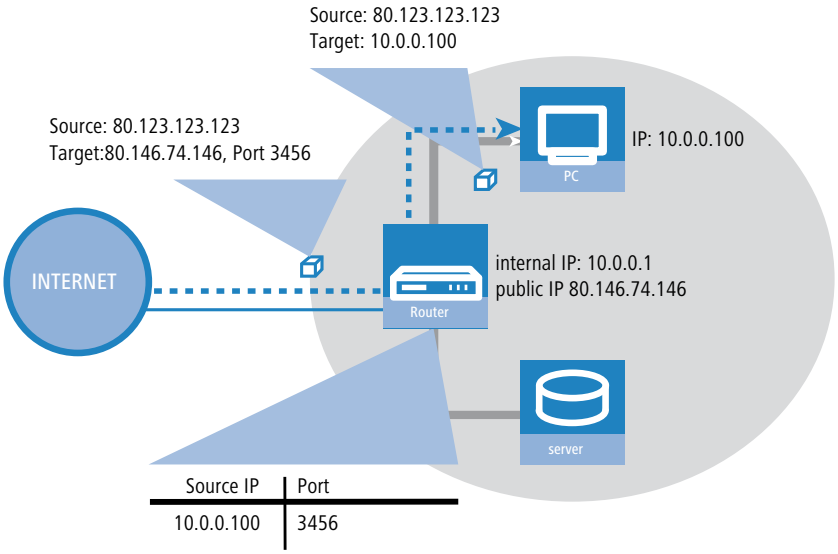
6.6.1 Simple masquerading

6.6.1.1 How IP masquerading works

Masquerading exploits a characteristic of TCP/IP data transmission, in that source and destination port numbers are used in addition to the source and destination addresses. When a router receives a data packet for transmission, it notes the IP address and the port of the sender in an internal table. The packet is then given the IP address of the router and an arbitrary new port number. This new port number is also entered in the table, and the packet is forwarded with its new IP address and port number.



The response to this packet is now returned to the router's IP address together with the sender port number. The router can now forward the response to the original sender by using the entry in the internal table.



6.6.1.2 Which protocols can be transmitted with IP masquerading?

IP masquerading works well for all IP protocols that are based on TCP, UDP, or ICMP, and that communicate exclusively over ports. These uncomplicated protocols include, among others, the basic protocol of the World Wide Web: HTTP.

Although some IP protocols do use TCP or UDP, they do not communicate exclusively through ports. Protocols of this type require special treatment during IP masquerading. Protocols supported by IP masquerading in the device and requiring special treatment include:

- FTP (using the standard ports)
- PPTP
- IPSec
- IRC

6.6.1.3 Configuring IP Masquerading

The application of IP masquerading is set in the routing table for every route individually. The routing table can be accessed as follows:

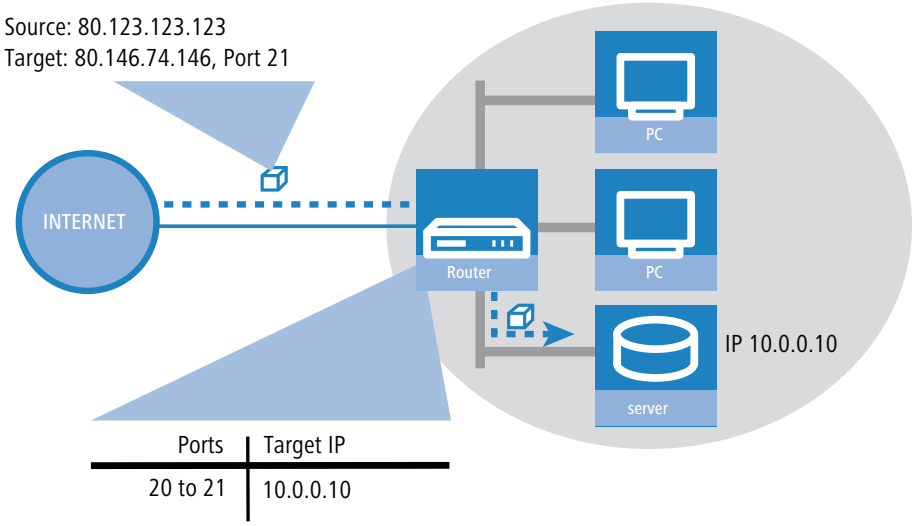
LANconfig: **IP-Router** > **Routing** > **Routing-Table**

Console: **Setup** > **IP-Router** > **IP-Routing tab**

6.6.2 Port forwarding (inverse masquerading)

With simple masquerading, all of the IP addresses on the local network are masked behind the router's IP address. If now a certain computer on the LAN, such as an FTP server, needs to be accessible from the Internet, simple masquerading means that the IP address of the FTP server remains hidden from the Internet. This makes it impossible to connect to this FTP server from the Internet.

To enable access to this type of server ("exposed host "), the IP address of the FTP server is entered in a table (the port-forwarding table) along with the services (ports) that it should also present outside the LAN. For a computer sending a packet from the Internet to the FTP server on the LAN, the router itself appears to be the FTP server. Using the protocol used, the router reads the IP address of the FTP server in the LAN from the entry in the port forwarding table and forwards the packet to the local IP address entered there. Packets sent by the FTP server in the LAN (responses from the server) are masked behind the IP address of the router.



The general difference between simple and inverse masquerading:

- For inverse masquerading, external access to a service (port) on the intranet must be defined in advance by specifying a port number. This is done in the port forwarding table, where the destination port is specified along with the intranet address of the FTP server, for example.
- When accessing the Internet from the LAN, on the other hand, the router itself automatically enters the port and IP address information into the table.

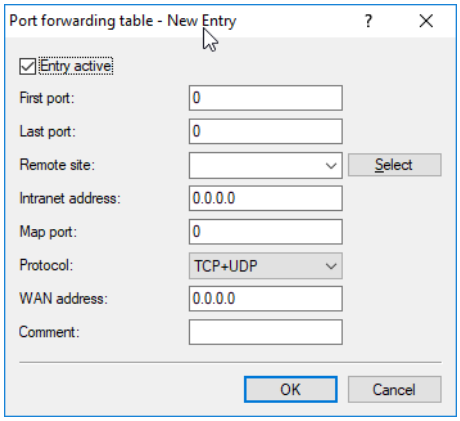
The table concerned can hold up to 2048 entries, thus enabling 2048 simultaneous transmissions between the masked and the unmasked network.

After an adjustable time period, however, the router assumes that the entry is no longer necessary and deletes it from the table automatically.

Stateful inspection and inverse masquerading: If a port is exposed in the masquerading module (i.e. all packets received on this port are forwarded to a computer in the local network), a deny-all firewall strategy requires an **additional** entry in the stateful-inspection firewall to allow computers to access that server.

On occasion it is desirable for the “exposed host” not to be contacted over this standard port, e.g. when security reasons demand the use of another port. In this case it is not only necessary to map the ports to an IP address, but to translate between ports as well (port mapping). Another use of port mapping would be to translate multiple WAN ports to one common port in the LAN, although to different IP addresses (N-IP mapping).

The configuration of port mapping involves the assignment of a port or port range (start port to end port) to an IP address from the LAN as the target and the port (map port) to be used in the LAN.



LANconfig: **IP router** > **Masquerading** > **Port forwarding table**

Console: **Setup** > **IP-Router** > **1-N-NAT** > **Service-Table**

› First port

D-port from (start port)

› Last port

D-port to (end port)

› Peer

Remote site which applies for this entry. The use of virtual routers (*Advanced Routing and Forwarding (ARF)* on page 396) when using port forwarding demands an exact selection of the remote site. If no peer is entered then the entry applies to all peers.

› Intranet-Address

Internet address that a packet within the port range is forwarded to.

› Map-Port

Port used for forwarding the packet.

If “0” is entered for the map port, the ports used in the LAN will be the same as those used in the WAN. If a port range is to be mapped, then the map port identifies the first LAN port to be used. For example, mapping the port range '1200' to '1205' to the internal map port '1000' means that the ports 1000 to 1005 will be used for data transfer in the LAN.

Port mapping is static, meaning that two ports or port ranges cannot be mapped to the same map port of a target computer in the LAN. The same port mapping can be used for different target computers.

› Protocol

Protocol which applies for this entry.

› WAN address

WAN address which applies for this entry. If the device has more than one static IP address, then this allows port forwarding to be limited to certain connections.

› Entry active

Switches the entry on or off.

› Comment

Comment on the defined entry (64 characters)

6.7 Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) makes certain routers in a network accessible from the Internet. These computers in the DMZ are generally used to offer Internet services such as e-mail or similar services. The rest of the network should of course be inaccessible for attackers on the Internet.

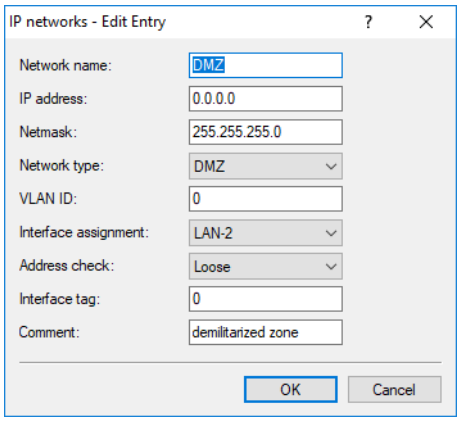
In order to allow this architecture, data traffic between the three zones Internet, DMZ and LAN must be analyzed by a firewall. The firewall's tasks can also be consolidated in a single device (router). For this, the router needs three interfaces that can be monitored separately from each other by the firewall:

› LAN interface
› WAN interface
› DMZ interface

The table lists the devices supporting this feature.

6.7.1 Assigning network zones to the DMZ

Various network zones (address ranges) are assigned to the DMZ, the LAN and the ARF using the address settings. Depending on availability, WLAN interfaces can also be selected.



LANconfig: **IPv4** > **General** > **IP networks**

Console: **Setup** > **TCP-IP**

6.7.2 Address check with DMZ and intranet interfaces

To shield the DMZ (demilitarized zone) and the Intranet from unauthorized attacks, you can activate an additional address check for each interface using the firewall's Intrusion Detection System (IDS).

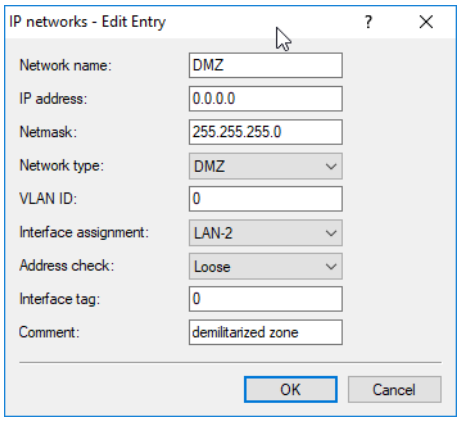
The relevant buttons are called 'DMZ check' or 'Intranet check' and can have the values 'loose' or 'strict':

› If the button is set to 'loose', then every source address is accepted if the device is addressed directly.
› If the switch is set to 'strict', then a return route has to be explicitly available so that no IDS alert is triggered. This is usually the case if the data packet contains a sender address to which the relevant interface can also route data.

Sender addresses from other networks to which the interface cannot route, or sender addresses from its own address range therefore lead to an IDS alert.

For all devices, the default is 'loose'.

You will find the button for activating the DMZ and Intranet address check in LANconfig:



LANconfig: **IPv4** > **General** > **IP networks**

Console: **Setup** > **TCP-IP**

6.7.3 Unmasked Internet access for servers in the DMZ

While the inverse masquerading described in the previous section allows at least one service of each type (e.g. one web, mail and FTP server) to be exposed, the method is subject to some restrictions.

- The service of the exposed host must be supported and 'understood' by the masking module. For example, some VoIP servers use non-standard, proprietary ports for advanced signaling. As a result, these server services can only be operated on connections without masking.
- From the security standpoint, it must be noted that the exposed host is in the local network. If the computer is hijacked by an attacker, it would be open to abuse for attacks against other machines in the local network.

6.7.3.1 Two local networks – operating servers in the DMZ

This feature requires Internet access with multiple static IP addresses. Please contact your ISP for a quote.

An example: Your provider assigns you the Internet IP network address 123.45.67.0 with the netmask 255.255.255.248. Then you can assign the IP addresses as follows:

Public DMZ IP address	Meaning/use
123.45.67.0	Network address
123.45.67.1	Intranet gateway
123.45.67.2	Any device in the local network that should have unmasked access to the Internet, e.g. a web server on the DMZ port
123.45.67.7	Broadcast address

Computers and devices in the intranet have no public IP address and appear on the Internet with the IP address of the device (123.45.67.1).

6.7.3.2 Separation of intranet and DMZ

Even though the intranet and DMZ may already be separated from one another at the Ethernet level by dedicated interfaces, separating them at IP level requires the use of a firewall rule.

The server service should be accessible from the Internet and the intranet, but IP traffic should be prohibited from the DMZ to the intranet. For the example above, the following would result:

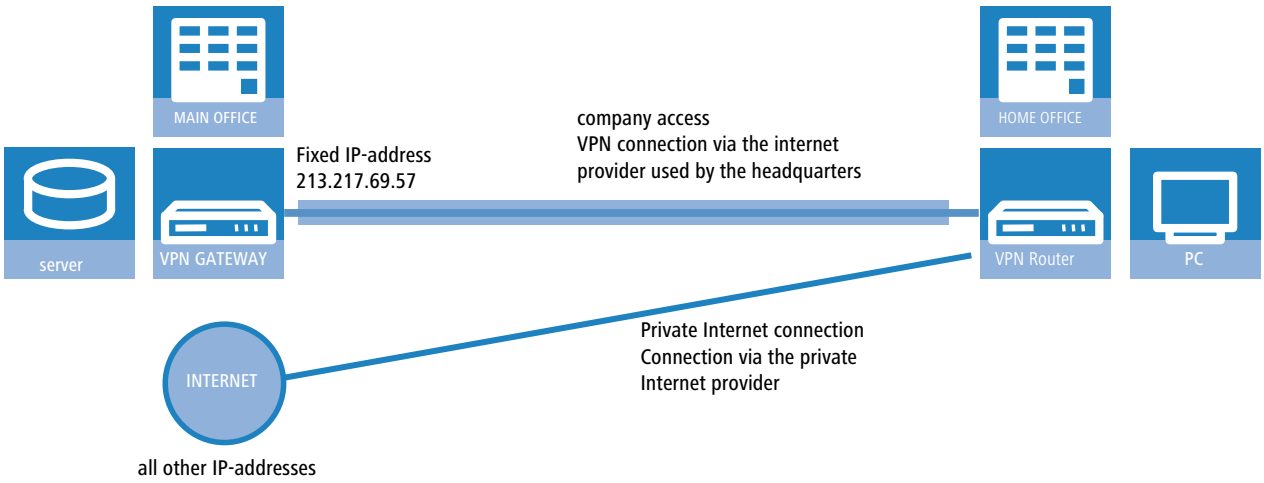
- For an "allow-all" strategy (default): Block access from "123.45.67.2" to "All stations on the local network"
- For a "deny-all" strategy: Allow access from "All stations on the local network" to "123.45.67.2"

6.8 Multi PPPoE

In most cases just one connection at a time is established over a DSL or ADSL WAN interface. However, there are applications where it makes sense to use multiple parallel connections on the WAN interface. Devices with a DSL or ADSL interface can establish up to eight different channels in parallel in the WAN using the same physical interface.

6.8.1 Example application: Home office with private Internet access

One possible application is the home office used by sales personnel who need access to the network at the headquarters via a VPN connection. The company pays for the VPN connection, the employee in the home office pays for Internet access privately.



To ensure a clean separation of the data links, two Internet connections are established, one to each provider. In the IP routing table, the default route is assigned to the private provider; the network with the headquarters via the VPN connection is routed over the headquarters' provider.

6.8.2 Configuration

The configuration of this scenario involves the following steps with the home-office router:

- Configuration of the private Internet access, for example with the LANconfig Wizard or with WEBconfig.
- Configuration of the Internet access that is invoiced to the headquarters.

- Selection of the private provider for the default route in the IP routing table (e.g. manually with LANconfig or with the Wizard for selecting Internet providers in WEBconfig.
- Configuration of the VPN connection to the network at the headquarters.
- Assignment of the VPN connection to the headquarters' provider.

  To ensure that the data traffic for the headquarters is routed via the desired Internet provider, one more entry in the IP routing table is required. Here, the VPN gateway at the headquarters is entered along with its fixed IP address and appropriate netmask, and is forwarded to the remote site used by the headquarters' provider.

  It is important that the route to the Internet provider used at the headquarters is masked; otherwise the device would apply the LAN address and not the WAN address, and the connection would never be established.

Further information about these steps in the configuration are to be found in the documentation for your device.

Administrator rights for the employee in the home office: To avoid the employee making accidental changes to the settings for the Internet provider or VPN access, he should be assigned the WEBconfig function rights for the “Internet connection” and “Selection of Internet provider” Wizards only.

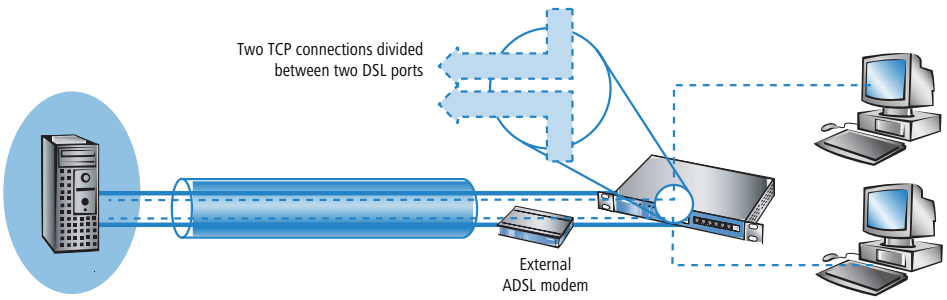
Use the necessary filter rules in the area 'Firewall/QoS' to ensure that the Internet traffic is not accidentally directed via the network at the headquarters.

6.9 Load balancing

Despite the ever increasing bandwidth of DSL connections, these remain the communications bottle-neck. In some cases it can be advisable to combine multiple DSL connections.

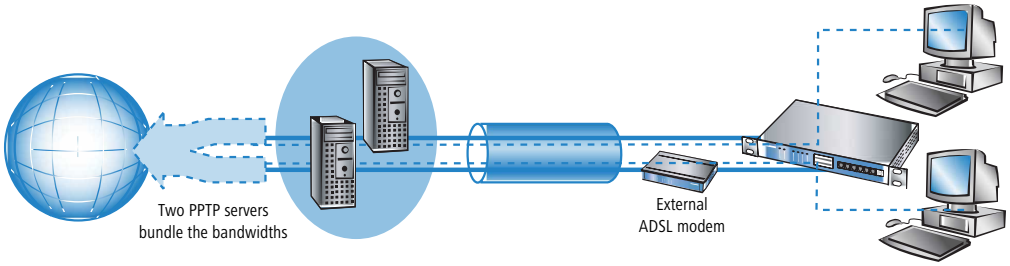
- Load balancing

  Load balancing dynamically divides TCP connections between independent DSL connections. The user has access to the sum of the bandwidths of the bundled channels, although each individual TCP connection is limited to the bandwidth of the DSL connection assigned to it.



- Indirect bundling for LAN-LAN links

  With indirect bundling, a PPTP connection is established on each of the two or more independent DSL connections. These PPTP connections are then bundled. For LAN-LAN links at least, genuine channel bundling is possible over the Internet even if the Internet provider itself does not offer channel bundling.



6.9.1 DSL port mapping

A basic requirement for DSL channel bundling is the support of more than one DSL interface per device. This means that one or more external DSL modems are connected to the switch of a router.

Please refer to the Quick Reference Guide for your device to see if it supports the connection of external DSL modems.

6.9.1.1 Assignment of switch ports to the DSL ports

Depending on the mode, devices with an integrated switch can enable some of the LAN ports to be used as additional WAN ports for connecting to external DSL modems. These ports are listed in the interface table as separate DSL interfaces (DSL-1, DSL-2, etc.). Each DSL port is enabled as a DSL interface in the list of WAN interfaces, where it is configured with the correct upstream and downstream data rates. It is assigned to the switch ports in the list of LAN interfaces.

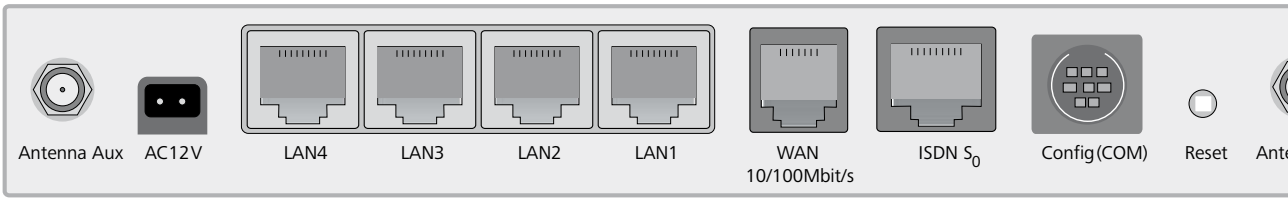
Example LANCOM Wireless 1811 DSL:

Port	Assignment	Connector	MDI-Mode	Private mode
LAN-1	LAN-1	Auto	Auto	No
LAN-2	LAN-1	Auto	Auto	No
LAN-3	LAN-1	Auto	Auto	No
LAN-4	LAN-1	Auto	Auto	No
WAN	DSL-1	Auto	Auto	No

- The column 'Port' contains the description of the associated port as marked on the back cover of the device.
- The utilization of the port is listed in the column 'Assignment':
  - None: The port is deactivated
  - LAN-1: The port is assigned to the LAN
  - DSL-1, DSL-2, ... : The port is assigned to one of the DSL interfaces
  - Monitor: The port is a monitor port, i.e. everything received at the other ports is output via this port. A packet sniffer such as Ethereal can be connected to this port, for example.

The assignment of DSL ports to the Ethernet ports can be chosen freely. An effective solution is to assign the DSL ports in the reverse order to the ports at the switch:

Example LANCOM Wireless 1811 DSL:



1. LAN4 / DSL-2
2. LAN3 / DSL-3
3. LAN2 / DSL-4
4. LAN1 / LAN-1: This port remains reserved for the LAN.
5. WAN / DSL-1: (dedicated WAN port for the device)

If the device is equipped with more than one DSL port, the DSL port to be used is entered in the list of DSL broadband peers:

- If no port is defined (or port "0"), the device selects the port after the one chosen for the connection's communication layer.
  - If Layer-1 is set with 'AAL-5', then the ADSL interface is chosen.
  - If Layer-1 is set with 'ETH', then the first DSL port (i.e. DSL-1) is chosen.
- If a particular port is defined (not "0"), then it will be used for the connection.

  Observe that the communication layer set for the connection over this port in Layer 1 is set to 'ETH'.
- To enable channel bundling via multiple DSL interfaces, the appropriate ports are entered into the peer list for the remote site (as a comma-separated port list '1,2,3' or as a port range '1-3'). With a port list, the bundled channels will be established in the given order; only in case of error will the channels be tested in ascending order. With a port range, the channels are always established in ascending order.
  - In the list of Ethernet ports, the ports must be switched to DSL port.
  - The DSL ports have to be activated as DSL interfaces in the list of the WAN interfaces and need to be configured with the correct up- and downstream rates.
  - In the layer used for the connection, a bundling method has to be activated that is also supported at the remote site.
  - To configure channel bundling for an internal ADSL interface, the ADSL port '0' is entered into the list of ports **at the top** of the list (e.g. '0,1,2,3' as port list or '0-3' as port range). In the remote device, the communications layer must be set to Layer 1 'AAL-5'.

    An entry in the peer list can contain various ports (e.g. ADSL and Ethernet), but it can only reference **one** communications layer in which just **one** layer-1 protocol can be defined. For bundled communications over ADSL and Ethernet ports, however, **two** different layer-1 protocols are required. For this reason, layer 1 is set to 'AAL-5' in these cases. As only one ADSL interface can exist in the devices, all of the interfaces bundled into this are automatically changed to layer 1 with 'ETH' for Ethernet DSL ports. This automatic change of the layer can only succeed if the ADSL interface is the first one to be selected for bundled connections.
  - For devices with a built-in DSL modem and an additional Ethernet interface (DSL or DSLoL), it is clear which ports are used for bundling. In this case it is not necessary to enter the ports into the remote site list. These devices always internally assume a port list '0,1' so that the internal DSL interface is the first one to be used for bundling.

For Multi-PPPoE (*Multi PPPoE* on page 426), multiple PPPoE connections share one physical DSL connection. With Multi-DSL, several PPPoE connection are divided between the available DSL interfaces. The maximum possible number of parallel connections is limited to 8 channels.

6.9.1.2 Assigning MAC addresses to the DSL ports

If a device uses switch ports to gain access to multiple DSL (WAN) interfaces, a corresponding number of MAC addresses is required to differentiate the DSL ports. As there are cases where the required MAC address depends upon the remote site which, for example, uses the MAC address to determine the DSL access charge, the MAC addresses are defined for the logical DSL remote sites and not for the physical DSL ports.

The following options are available for setting the MAC address:

- Global: Global system MAC address
- The unique, locally managed MAC address is calculated from the global address
- User defined: A MAC address that can be freely defined by the user

Every DSL connection contains its own MAC address. If two remote sites are configured with the same MAC address, this address is used for the first connection to be established. For the second connection, a "locally managed MAC address" is calculated from the user-defined MAC address, which is thus unambiguous. Similarly, for channel bundling the configured MAC address is used for the first connection; for the other bundle connections, a "locally managed" MAC address is calculated from the user-defined MAC address. If one of your connections is charged via the MAC address, configure this MAC address for the separately charged connection only. For all other connections you should use another address.

6.9.2 Dynamic load balancing

If the Internet provider does not directly support bundling, then multiple normal DSL connections can be coupled with a load balancer. First of all, the DSL accesses are set up for the necessary DSL ports. These are then coupled with a load-balancing table. This list assigns a virtual balancing connection (the connection that is entered into the routing table) to the other real DSL connections (bundle connections). Depending on the number of available DSL ports, several bundle connections can be assigned to one balancing connection.

The balancing connection is entered as a "virtual" connection. No access information or similar has to be entered for this connection. The entry merely serves as a "distributor" which uses the load-balancing table to assign several "real" bundled connections to an entry in the routing table.

DSL bundling is a static bundling. Any additional channels are **not** opened or closed according to the demand from data transfer volumes.

With load balancing, decisions about the routing of data packets can no longer be made simply based on the IP addresses because the individual bundled DSL connections all have different IP addresses. Thus load balancing also considers the information in the firewall connection list. This list has an entry for every established TCP connection, and for load balancing the list is supplemented with information about the DSL port used.

6.9.2.1 Connecting

A request for data transmission to a balancing remote site initially prompts the **first** bundle connection from the load balancing table to be established. Further progress depends upon the success of this connection establishment:

- If the connection is successfully established, the first step is the assignment of all pending TCP connections to this channel. Subsequently, all of the configured bundle connections will successively be established. As soon as at least two bundle connections are active, new TCP connections will be divided among the active bundle connections.
- Should establishment of the bundling connection fail, then attempts will be made to establish other bundle connections one after the other. As soon as one of the bundle connections is established, all of the pending TCP connections will be directed to this channel.

6.9.2.2 Spreading the data load

Two basic methods are available for balancing the data load:

- If the channel's bandwidth is known, then the connections will be assigned to the channel with the lowest workload (in percent).

- If the bandwidth is not known, then a differentiation is made according to the type of connection required; a TCP connection; or VPN or PPTP connections from the device.
  - If a TCP connection requests a channel, then the one with the lowest absolute workload will be chosen.
  - If a VPN or PPTP connection requests a channel, then the connections will be equally spread between all available channels.

For the most effective use of load balancing, the bandwidth should be entered into the list of WAN interfaces under LANconfig in the configuration section 'Interfaces' on the 'WAN' tab under the button Interface settings (Console: **Setup** > **Interfaces** > **DSL**).

6.9.2.3 Client binding

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

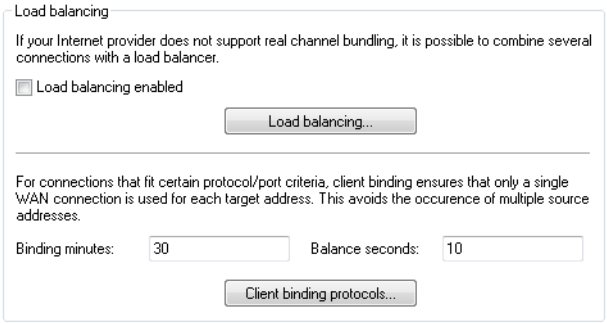
One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, the full volume of the traffic to that particular server would then be limited to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

6.9.2.4 Load balancing with client binding

In LANconfig, client binding is configured under **IP router** > **Routing** in the section **Load balancing**.



Binding minutes

Here you specify the time in minutes for the binding entries to be valid for a client.

Balance seconds

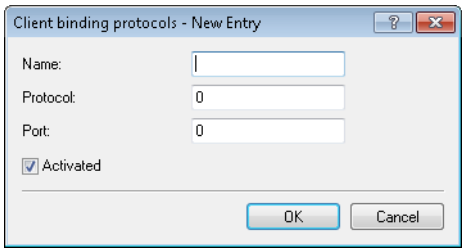
To prevent data from flowing via the main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new

session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

Client binding is protocol-oriented. You set the corresponding protocols under **Client binding protocols**. The table already contains the default entries

- HTTPS
- HTTP
- ANY



Name

Contains a descriptive name for this entry.

Protocol

Contains the IP protocol number.

Learn more about IP protocol numbers in the IANA *Online database*.

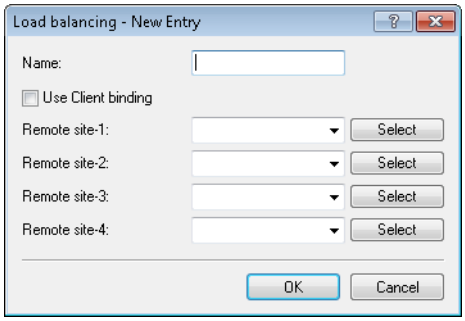
Port

Contains the port of the IP protocol.

Activated

Activates or deactivates this entry.

Client binding can be activated or deactivated for each of the entries under **Load balancing**.



6.9.2.5 Load balancer from RADIUS configuration

As of LCOS 10.40 your device adds to its existing ability to configure a load balancer via the load balancer's configuration table (see *Dynamic load balancing with multiple DSL connections* on page 438) in that it can now configure a load balancer based on RADIUS attributes for IKEv2 VPN tunnels.

In large-scale VPN scenarios, central configurations with all the necessary parameters of a VPN tunnel are not stored in the device itself; instead, this is outsourced to one or more central RADIUS servers. The aim of this is better scalability and administration. If these scenarios require several inbound IKEv2 VPN tunnels to be combined into a load balancer on the central-site VPN gateway, this can be implemented using additional RADIUS attributes.

The bundled peers of a dynamic load balancer are IKEv2 VPN clients that use RADIUS authorization. A VPN client becomes a part of a dynamic load-balancer cluster if the RADIUS response contains a corresponding RADIUS attribute (LCS-Load-Balancer). This attribute specifies the name of the load balancer cluster and also determines whether to activate client binding (see *Client binding* on page 431).

If this type of VPN connection terminates, the client is removed from its load-balancer cluster. A new connection must be established by the client.

A dynamic load-balancer cluster cannot have the same name as a statically configured cluster, so you cannot mix static and dynamic clients on the same load balancer.

For configuration via a RADIUS server, the syntax of the standard attributes "Framed-Route" and "Framed-IPv6-Route" have been extended to pass on dynamic routes that point to a load balancer. The attribute "LCS-Load-Balancer" ensures that routes used for IKEv2 routing automatically point to the load balancer instead of the dial-in interface.

This feature is also supported with IKEv2 routing. The route on the VPN gateway is then sent dynamically from the remote site instead of being received from the RADIUS server as a Framed-Route attribute. In this case, the RADIUS server only has to send the attribute "LCS-Load-Balancer".

Table 25: RADIUS attributes

ID	Name	Meaning
22	Framed-Route	IPv4 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client). Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv4 address + '/' + prefix length or netmask **ifc=<destination interface>** Name of the IP interface or a load balancer to which the route should point, or "#Ifc". If no destination interface is specified or it is "#Ifc", the route points to the VPN interface for the respective dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
99	Framed-IPv6-Route	IPv6 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client).

ID	Name	Meaning
		Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv6 address + '/' + prefix length **ifc=<destination interface>** Name of the IP interface or a load balancer to which the route should point, or "#Ifc". If no destination interface is specified or it is "#Ifc", the route points to the VPN interface for the respective dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
LANCOM 28	LCS load balancer	Format (string): <Load balancer name> [client_binding={no|yes}] The <load balancer name> can be up to 16 characters long and specifies a load-balancing remote site on the LANCOM routers. This remote site is used for dynamic IKEv2-VPN load balancing and therefore must not be already used for static load balancing under **IP router** > **Load balancing**. The option "client_binding" turns the client binding (see *Client binding* on page 431) on or off. Unless otherwise specified, client binding is off. The first IKEv2-VPN client to connect specifies this setting. Any subsequent settings for the client binding in connection with this load-balancing remote site are ignored.

Example: RADIUS attributes for a simple load balancer made up of IKEv2 VPN tunnels to the central site

```
LCS-Load-Balancer=LB1
Framed-Route=192.168.45.0/24 ifc=LB1;
```

6.9.3 Dynamic load balancing

Apart from the dynamic choice of connection outlined in the previous section, there are possible scenarios where certain TCP connections should always make use of the same DSL connection. Two cases are to be considered here:

- A server with a fixed IP address can only be contacted via a dedicated connection. All that is required for the selection here is the destination IP address.
- A server uses a protocol that requires a control channel and other channels for data transfer (e.g. FTP, PPTP). In establishing the data channels, servers accept only the same IP address as that used by the control channel.

6.9.3.1 Destination-based channel selection

Destination-based channel selection is handled by an entry in the routing table that directly uses one of the bundle connections to reach the destination instead of using the "virtual" balancing connection.

6.9.3.2 Policy-based routing

Suitable entries can be made in the firewall to select channels according to the destination port or the source address. These entries are supplemented with a special "routing tag" that is used to control the channel selection with the routing table. Please refer to *Policy-based routing* on page 388 for further information.

6.9.4 Indirect bundling for LAN-LAN links via PPTP

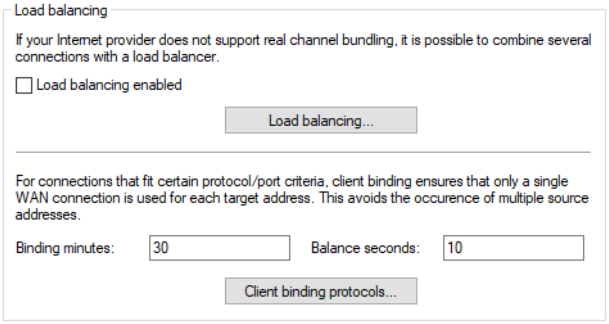
Indirect bundling is performed over bundled PPTP connections, which means that the full bandwidth of the bundled channels can be used over the LAN-LAN link. When considering PPTP bundling, there are three different scenarios:

- The client bundles the DSL channels, the server is behind a connection with sufficient bandwidth
- The client is behind a broadband connection, and the server handles the bundling
- The server and the client bundle the DSL channels

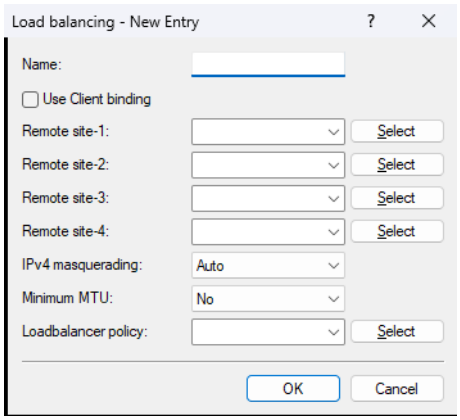
All the configuration involves is including the other PPTP addresses into the balancing table.

6.9.5 Configuring load balancing

To configure load balancing with LANconfig navigate to the view **IP Router** > **Routing** > **Load balancing**.



Activate load balancing with the item **Load balancing enabled**. Further settings are adjusted under **Load balancing**.



Name

Unique name for a virtual load-balancing remote site. This remote site can then be used in the routing table.

Use client binding

Activates or deactivates the client binding function.

Peer-1

Name of a previously configured remote site that is to be bound with others.

Peer-2

Name of a previously configured remote site that is to be bound with the first one.

IPv4 masquerading

This menu item contains the settings for IPv4 masquerading in the load balancer. Possible values:

Automatic

Adopts the masking option for each individual line from the routing table.

On

Activates NAT on all remote sites in the load balancer.

No

Deactivates NAT on all remote sites in the load balancer.

Only intranet

Activates NAT for networks of the type INTRANET. The DMZ will not be masked.

Minimum MTU

This value can be used to specify the use of a common minimum MTU for all channels of a load balancer. When using Dynamic Path Selection (DPS), it is recommended to set this parameter to "Yes".

If the MTU of the load balancer is explicitly overridden by an entry under **Communication** > **Protocols** > **MTU list**, then all channels use exactly the MTU specified there—regardless of how the "minimum-MTU" switch is set and regardless of what may have been negotiated on the channels.

Under **Status** > **WAN** > **MTU**, the MTU of the load balancer is only displayed if it has been explicitly configured.

Loadbalancer policy

Here are some predefined load balancer policies provided by LCOS.

DEFAULT

This load balancer policy always has the same effect as not specifying a policy or leaving the load balancer policy column empty. In the firewall and command-line ping, it falls back to the policy from the Dynamic Path Selection table.

TRAFFIC

This policy identifies the underlying physical connection for each channel and retrieves its absolute Rx load and Tx load from the columns Rx/s-average and Tx/s-average in **Status** > **WAN** > **Throughput**. If the physical bandwidth is known for all these physical connections (typically for wired connections but not for mobile networks), it calculates the relative loads by dividing the absolute loads by the respective bandwidth. Otherwise, it continues to work with the absolute loads. In the next step, it selects the larger value between the Rx and Tx loads. It then selects the channel with the lowest load.

BANDWIDTH

The load balancer policy BANDWIDTH selects a channel randomly. If the bandwidth is known for all underlying physical connections, the probability of selecting a particular channel is proportional to its bandwidth, i.e., a 50 Mbps channel is selected five times more often than a 10 Mbps channel. Otherwise, if at least one bandwidth is unknown, the channel is selected uniformly at random.

ROUND-ROBIN

The load balancer policy ROUND-ROBIN selects the channels in turn.

MOST-USED

With this policy, the load balancer selects the channel that currently has the most firewall sessions (regardless of whether in the sending or receiving direction and whether IPv4 or IPv6). This policy is only useful as a counterpart to Dynamic Path Selection, i.e., if a branch device uses Dynamic Path Selection on the load balancer, the central device should use MOST-USED on its corresponding load balancer. This effectively causes the central device to adapt to the branch's Dynamic Path Selection decisions without the branch explicitly communicating its decision to the central device.

Note: This feature only affects routed traffic. All internal services of the LANCOM router exclusively use the **ROUND-ROBIN** policy.

For each destination address, client binding can assign connections that correspond to certain protocol/port combinations to a fixed WAN connection. This avoids changing source addresses when using these connections. Client binding may be activated during load balancing.

Binding minutes

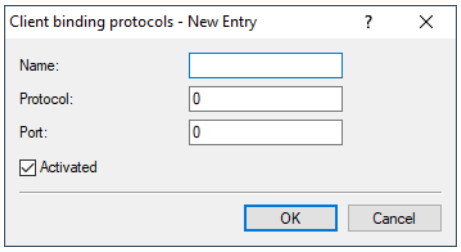
Here you specify the time in minutes for the binding entries to be valid for a client.

Balance seconds

To prevent data from flowing via the main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

Under **Client binding protocols** you configure the corresponding protocol/port combinations.



Name

Give this entry a name.

Protocol

Contains the IP protocol number.

Learn more about IP protocol numbers in the *IANA Online database*.

Port

Contains the port of the IP protocol.

Activated

Activate this entry.

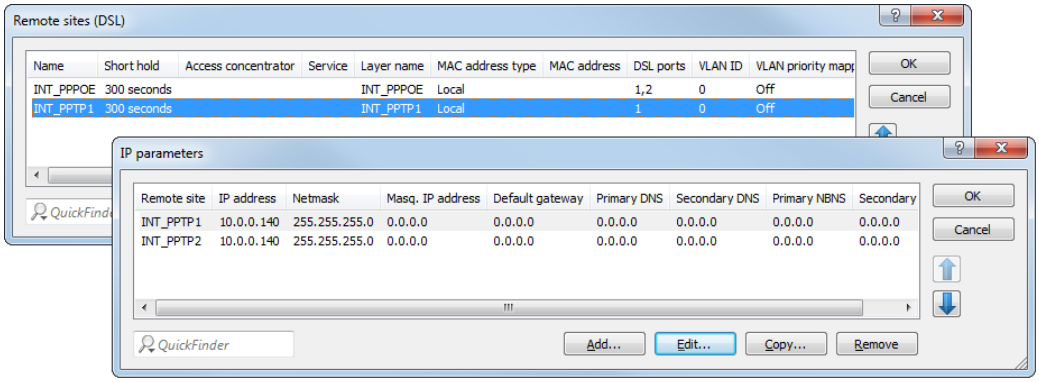
For the following example configurations we assume that the remote devices are already set up with all necessary access information.

6.9.5.1 Direct channel bundling via PPTP

The following method is for the configuration of channel bundling via PPTP:

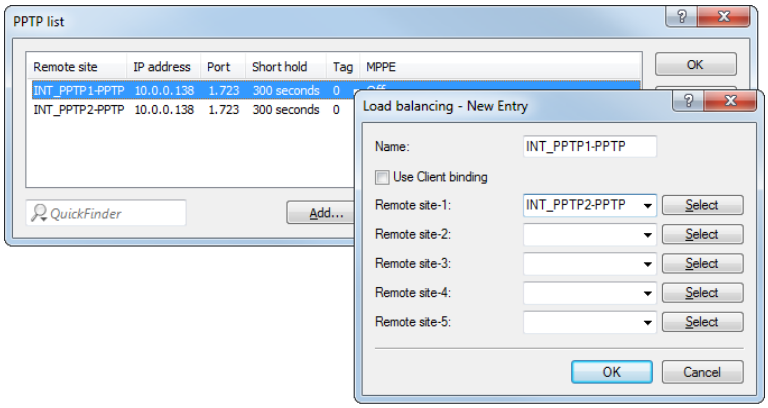
1. Configure several separate PPTP connections (e.g. using the LANconfig Wizard), each using a different DSL port. The connections are entered with the same values for the IP parameters as those that can be seen in LANconfig under **Communication** > **Protocols** > **IP parameters**.

   Console: **Setup** > **WAN** > **IP-List**



2. Bundling takes place if additional remote sites are defined in the load balancing list for the physical connection to the PPTP remote site. The PPTP connection then requests the next physical connection from the load balancer and establishes it there. Enter the bundled connections in LANconfig under **IP router** > **Routing** > **Load balancing**.

   Console: **Setup** > **IP-Router** > **Load-Balancer**

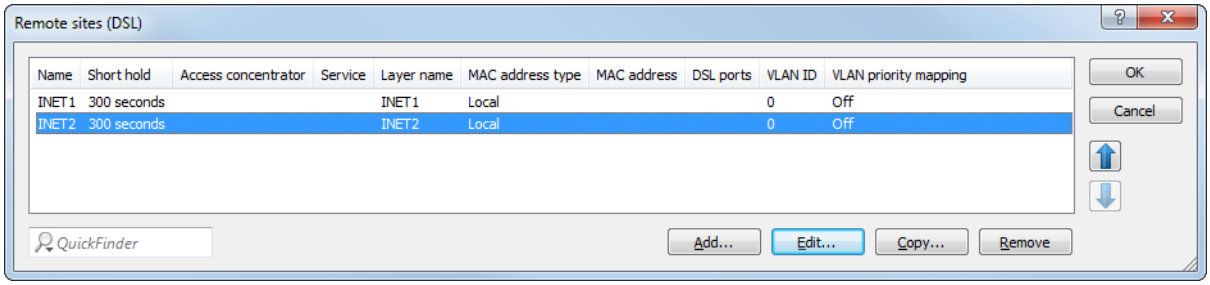


6.9.5.2 Dynamic load balancing with multiple DSL connections

The first step in setting up dynamic load balancing is to define the Internet accesses, e.g. 'INET1' and 'INET2', with the aid of the LANconfig Wizard.

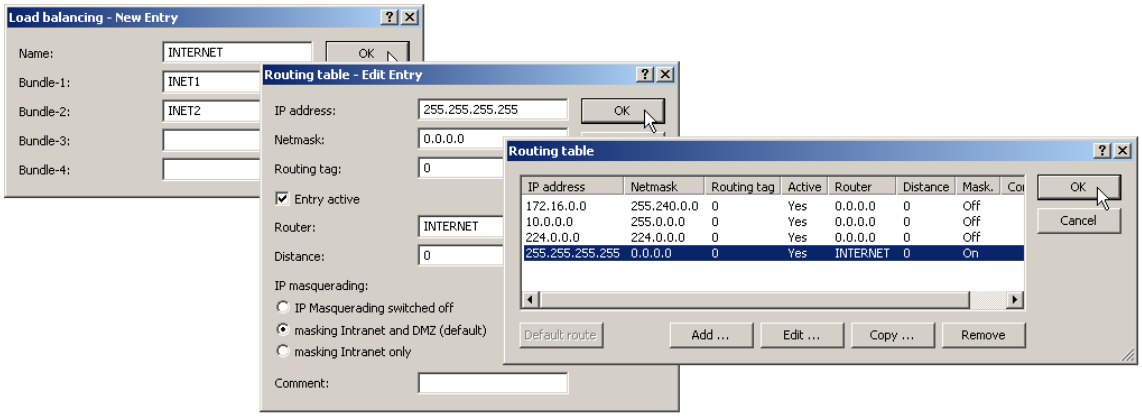
1. To distribute Internet traffic across different DSL interfaces, the individual remote sites are assigned to different DSL ports in LANconfig under **Communication** > **Remote sites** > **Remote sites (DSL)**.

Console: **Setup** > **WAN** > **DSL-Broadband-Peers**



2. The two DSL remotes are then assigned to a new virtual remote site 'INTERNET' in the load balancing list in LANconfig under **IP router** > **Routing** > **Load balancing**.

   Console: **Setup** > **IP-Router** > **Load-Balancer**



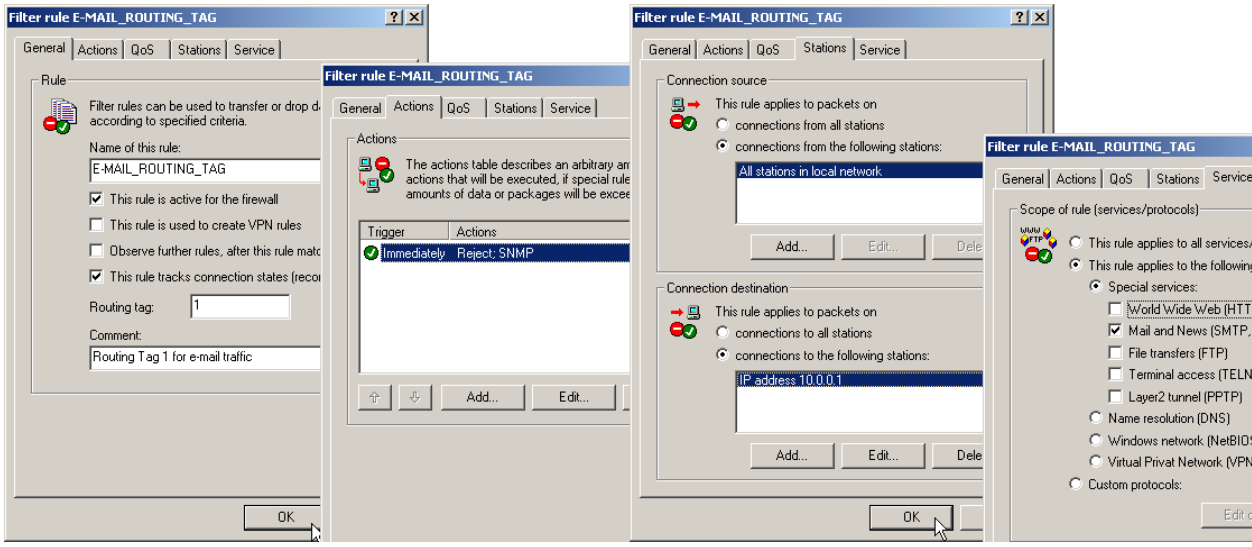
3. The virtual remote site is entered into the routing table as the router for the default route in LANconfig under **IP router** > **Routing** > **Routing table** / / .

   Console: **Setup** > **IP-Router** > **IP-Routing-Table**

   The virtual remote site 'INTERNET' is now to be used for Internet access. When data are routed over this connection, the load balancing table will cause the “real” DSL connections to be established and the data will be transmitted over the selected DSL ports.

4. Routing tags can be used for the application-dependent direction of data traffic to specific DSL ports. If, for example, outgoing e-mail traffic is to be routed over a certain DSL interface with a certain IP address, then the appropriate firewall rule must be created that transmits e-mail data traffic from all local stations to the mail server and sets the routing tag to '1'; do this with LANconfig under **Firewall/QoS** > **Rules**.

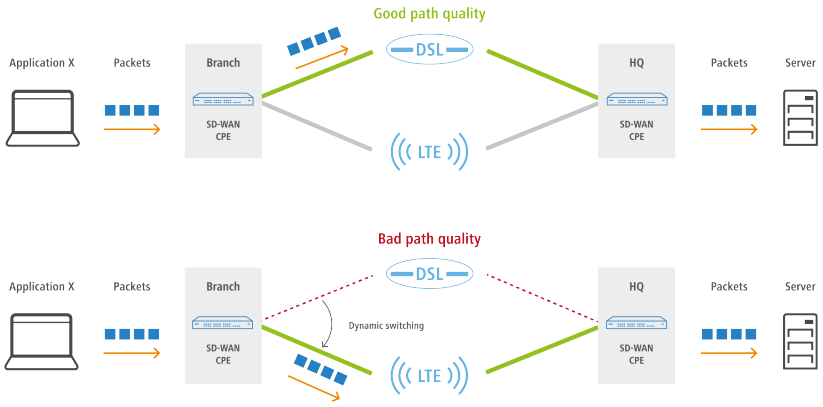
Console: **Setup** > **IP-Router** > **Firewall** > **Rules**



6.10 SD-WAN Dynamic Path Selection

Used in an SD-WAN scenario where several lines are available, Dynamic Path Selection (DPS) optimizes the performance of an application by directing data traffic over the line with the best quality as rated by metrics such as load, packet loss, latency or jitter.

In SD-WAN scenarios, MPLS lines should either be replaced or supplemented by cost-effective Internet connections such as DSL, cable Internet, fiber optic or 4G/5G. Load balancing helps to make use of the total bandwidth of all of the available lines. Dynamic Path Selection can be used to assure the performance of mission-critical applications. All lines are continuously, actively monitored with ICMP packets to calculate metrics for load, packet loss, latency and jitter. Policies are used to define the requirements of business applications: For example, the real-time data traffic on lines can be monitored for the allowed packet loss or the maximum latency of a possible path. The dynamic path selection algorithm selects the best quality line for sessions. If several lines meet the requirements, load balancing distributes the load across these lines by means of round-robin scheduling.



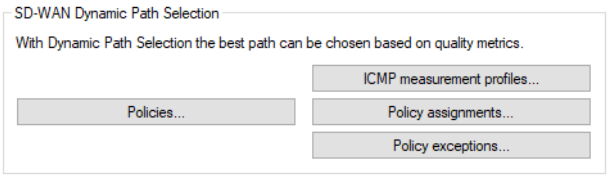
Policies can be defined as “critical”. If none of the lines fulfill the policy, no data traffic is transported at all.

Dynamic path selection is activated on a load balancer. A load balancer can be defined either for Internet connections or for SD-WAN overlay tunnels (VPN). The end point for ICMP test packets can either be any IP address or the central-site SD-WAN gateway.

In the firewall, the defined (load balancer) policies for the applications are used in corresponding firewall rules. There, the traffic or applications to which the load balancer policy is to apply are defined.

6.10.1 Configuring Dynamic Path Selection

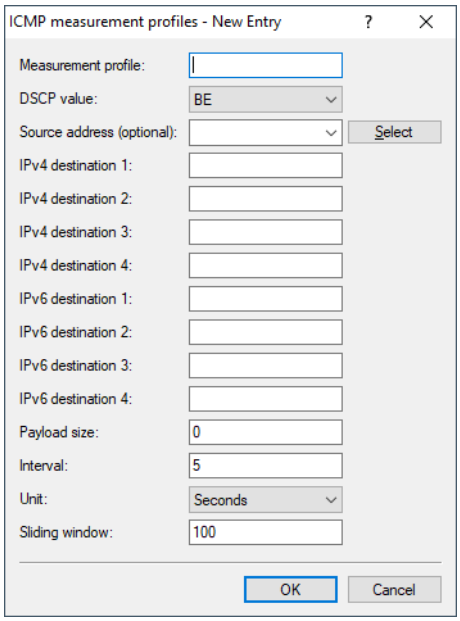
To configure dynamic path selection with LANconfig, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection**.



6.10.1.1 ICMP-Measurement-Profiles

ICMP measurement profiles specify a parameter set used by measurements that are based on ICMP pings. Interface metrics are derived from measurements to quantify the connection quality. These metrics are: Average round trip time (RTT, latency), jitter and packet loss rate.

To configure the ICMP measurement profiles, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP measurement profiles**.



Measurement-Profile

The name of the profile. This name is used to reference the profile in DPS policies.

DSCP value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Source address (optional)

References a named loopback address that is used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

IPv4 destination 1-4

Up to 4 measurement targets as valid IPv4 unicast addresses or DNS host names. With 0.0.0.0 entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

IPv6 destination 1-4

Up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Payload size

Specifies the size of the data payload that follows the ICMP header (payload size) of the pings being sent.

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

Unit

Specifies whether the ICMP measurements for the value should be in seconds or milliseconds. Possible values: Seconds (default), milliseconds.

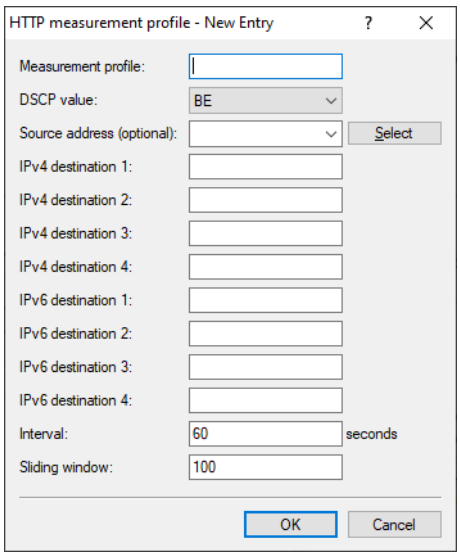
Sliding-Window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

6.10.1.2 HTTP measurement profiles

HTTP measurement profiles specify a parameter set used by measurements that are based on HTTP(S) connections. Interface metrics are derived from measurements that quantify the connection quality. These metrics are: Mean time to establish an HTTP(S) connection (latency), jitter, and connection-error rate (packet loss).

To configure the HTTP measurement profiles, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **HTTP measurement profiles**.



Measurement profile

The name of the profile. This name is used to reference the profile in DPS policies.

DSCP value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Source address (optional)

References a named loopback address that is used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

IPv4 destination 1-4

Up to 4 measurement targets as valid IPv4 unicast addresses or DNS host names. With 0.0.0.0 entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

IPv6 destination 1-4

Up to 4 measurement targets as valid IPv6 unicast addresses or DNS host names. With :: entered, the measurement target is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

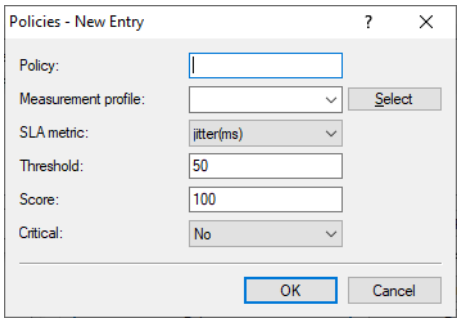
Sliding window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

6.10.1.3 Policies

To evaluate the connection quality of the interfaces used for Dynamic Path Selection, the metrics calculated from the measurement profiles are compared to threshold values, and points (as a score) are awarded. These points added up to determine which is the "best" interface. Certain thresholds can be specified as being "critical" (e.g. jitter <= 30 ms). Dynamic load balancer decisions are based on the points total in combination with the exceeded critical threshold values. A DPS policy collects the threshold values and criticality markings that are required to calculate the total points.

To configure the DPS policies, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Policies**.



Policy

The name of the DPS policy. This name is used to reference the policy in firewall rules. All of the rows in this table with the same policy name are combined into one policy. This makes it possible, for instance, to use the same metric multiple times with different thresholds in the same policy. This allows a points-based grading (e.g. 10 points with a latency <= 100, another 10 points with a latency <= 50).

Measurement profile

Either empty or the name of an ICMP measurement profile.

The field must be empty if and only if the **SLA metric** is set to "Load(%)". In all other cases, a measurement profile must be specified.

SLA metric

This is the metric generated from the measurements of the set measurement profile. The value of metric is compared to the threshold value. Possible values:

- Latency (ms)
- Jitter (ms)
- Packet loss (%)
- Load (%)

The metric "Load(%)" denotes the utilization of the interface in percent of the maximum bandwidth. As this value is not determined using separate measurements, the entry **Threshold** must be left empty.

Threshold

Threshold which the chosen SLA metric should not undershot.

Score

If a metric undershoots the chosen threshold, the points are added to the overall result of the policy.

Critical

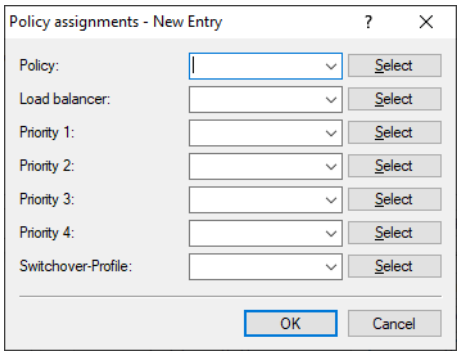
Marks whether a threshold is critical. If a threshold value marked as "critical" is not undershot, the overall result is not defined.

An interface with an undefined overall result cannot be selected by a dynamic load balancer decision.

6.10.1.4 Policy-Assignments

Here you set which DPS policy should be used with which load balancer, and what the priorities are if the overall results are equal.

To configure the policy assignments, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Policy assignments**.



Policy

The name of an existing DPS policy from *Policies* on page 443.

Load balancer

Name of a load balancer (also see *Configuring load balancing* on page 435) to be rated by this policy. Measurements are automatically started on all interfaces of this load balancer according to the measurement profiles referenced in the policy.

Measurements can be suppressed for individual interfaces of this load balancer. See also *Policy exceptions* on page 445.

Priority

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

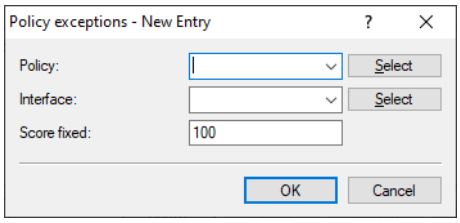
Switchover-Profile

Specify the name of the Switchover profile used for this policy. See also *Switchover-Profiles* on page 445.

6.10.1.5 Policy exceptions

One option is not to apply measurement profiles to certain interfaces, for example if they are charged by data volume.

To configure the policy exceptions, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Policy exceptions**.



Policy

The name of an existing DPS policy from *Policies* on page 443.

Interface

The name of an interface (e.g. WAN remote sites, VPN tunnels) belonging to a load balancer that is rated by the policy. The measurement profiles referenced in the policy are not used to start measurements on the interface.

Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements must be prevented by making an an exception for this interface in all of the affected policies.

Score fixed

Since no dynamic overall result can be derived without making measurements, this score for the interface is used for all decisions relating to dynamic path selection.

6.10.1.6 Switchover-Profiles

By default, Dynamic Path Selection only distributes new sessions to a better line. If you want ongoing sessions to be moved to a better line, you have to enable session switchover. A session switchover only makes sense for unmasked connections, such as VPN or SD-WAN overlays. With masked connections, the public WAN address would change during the session, so it would be rejected by servers offering SIP sessions or online banking. Two configuration steps are necessary to enable session switchover:

1. The firewall rules for Dynamic Path Selection must be enabled for session switchover.

   To do this, the **Dynamic path selection session switchover** control has to be set for IPv4 under **Firewall/QoS** > **IPv4 Rules** > **Rules** > **General** and/or for IPv6 under **Firewall/QoS** > **IPv6 Rules** > **IPv6 forwarding rules**.

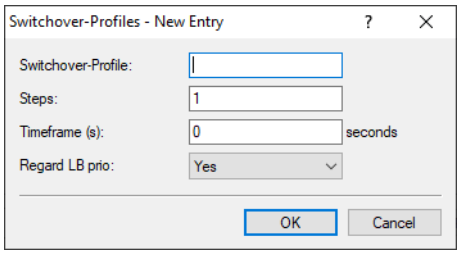
2. A switchover profile must be linked to the corresponding policy in the Policy assignments table

The switchover profile can be used to control how quickly the set of sessions is moved to the new line or interface on the same load balancer.

To prevent sessions from being concentrated on a single interface, sessions are usually moved step-by-step in groups within the configured timeframe. Before each step, a check sees whether the switchover is still necessary, because in the meantime the policy scores and thus the ranking of the interfaces may have changed. If it is no longer necessary, switchover is canceled and the sessions remain on their current interface. If it remains necessary, the sessions for the group being moved in the next step are determined at random.

If the number of steps = 1 or the overall time = 0, all sessions are moved immediately.

To configure the HTTP measurement profiles, navigate to the view **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Switchover-Profiles**.



Switchover-Profile

The name of the switchover profile. This name is used to reference the profile.

Steps

Number of steps or groups in which the set of sessions is moved to the new line.

Timeframe

Timeframe in seconds within which the set of sessions is shifted to the new line.

Regard LB prio

This parameter controls the behavior of the DPS session switchover.

If the table is reset to the default, the row “AGGRESSIVE-SWITCHOVER” is set to “Yes” and “SOFT-SWITCHOVER” is set to “No”.

Possible values:

Yes

Sessions also switch between interfaces with the same score, provided that the prioritization specified in table *Policy-Assignments* on page 444 favors one of them. Appropriately, the output tables **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv4-Preferred-Lines-Log** and **Status** > **Firewall** > **Dynamic-Path-Selection** > **IPv6-Preferred-Lines-Log** will only show the highest-priority interface as “Preferred” in such a case. This is also the interface that all sessions switch over to, with a speed and in the corresponding number of intermediate steps according to the other parameters in the corresponding switchover profile.

This setting is useful in the following scenario, an an example: LTE or 5G is used together with VDSL. In some locations, LTE/ 5G is significantly better than VDSL. For cost reasons, however, DSL should be used first instead of LTE/5G, since this should only be used as a booster. This works for example with the priorities of the load balancer. With the default behavior, however, the switchover does not switch back from the bad line to the better one.

This is the default for new entries.

No

The behavior of the DPS session switchover is that it is only performed if another line is actually better (better score) than the line currently used by the session. Not taken into account is the prioritization that can be entered into the load balancer policy assignments. For this reason there are no switch-overs between interfaces with identical policy scores.

This is the default for entries from before LCOS 10.80.

6.10.2 Show commands

- `DPS-v4-Policies <policy> <peer>`: Displays information about the IPv4 policies used by dynamic path selection for the corresponding policy and remote site.
- `DPS-v4-Score <policy> <load-balancer>`: Shows information about the score for dynamic path selection over IPv4 for the corresponding policy and load balancer.
- `DPS-v4-Score-Details <policy> <peer>`: Shows detailed information about the IPv4 dynamic path selection score for the corresponding policy and remote site.
- Extension to the ping command:

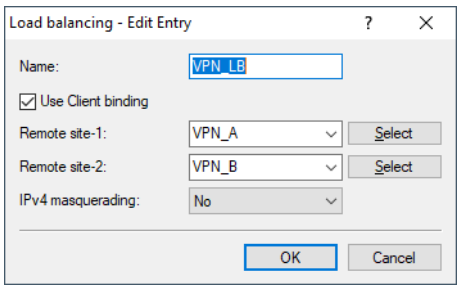
  `ping -l <policy>`: Uses the specified dynamic path selection load balancer policy to determine the outgoing interface.

6.10.3 Sample configurations

6.10.3.1 Scenario with two VPN tunnels over two different Internet connections from the branch office to the headquarters

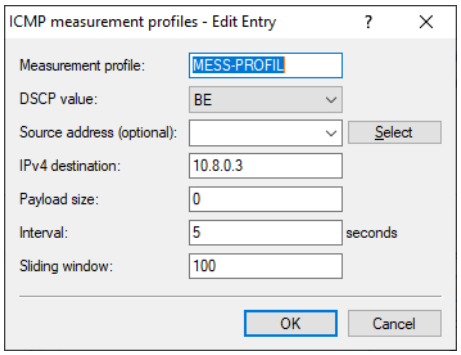
In this example, dynamic path selection should be set up for all data traffic in a scenario with two VPN tunnels over two different Internet connections from the branch office to the headquarters. The IP address for testing the line quality with ICMP test packets is the private IP address of the central-site gateway, 10.8.0.3. The goal is that only the best line or VPN tunnel should be selected according to the latency.

Dynamic path selection is activated at the branch office only. We are assuming that both of the Internet connections are available and that the two VPN tunnels VPN_A and VPN_B are already configured as a load balancer with the name VPN_LB:



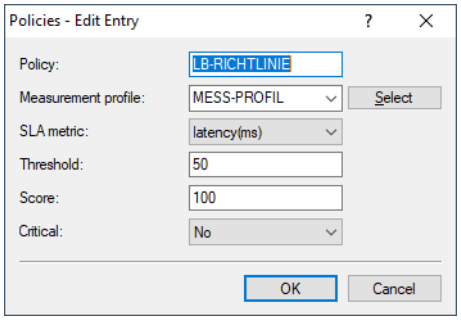
1. Add a new table row under **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **ICMP measurement profiles**.

The first step is to create a new measurement profile. The IPv4 destination is the private IP address of the central gateway, 10.8.0.3. Measurement packets used to evaluate the paths are sent over the VPN tunnels (SD-WAN overlays) every 5 seconds.



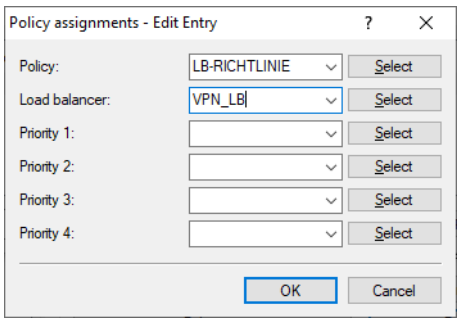
2. Add a new table row under **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Policies**.

   The next step is to create a new policy with an SLA metric "Latency" set with a threshold of 50 ms. If the corresponding VPN tunnel has a latency of less than 50 ms, the path is given a score of 100 (points). A connection that does not meet this criterion receives a score of 0, i.e. it is rated as worse. The path with the highest score is the preferred path and is therefore used for the data traffic. If both paths have an identical score of 100, load balancing is performed with both of the VPN tunnels.



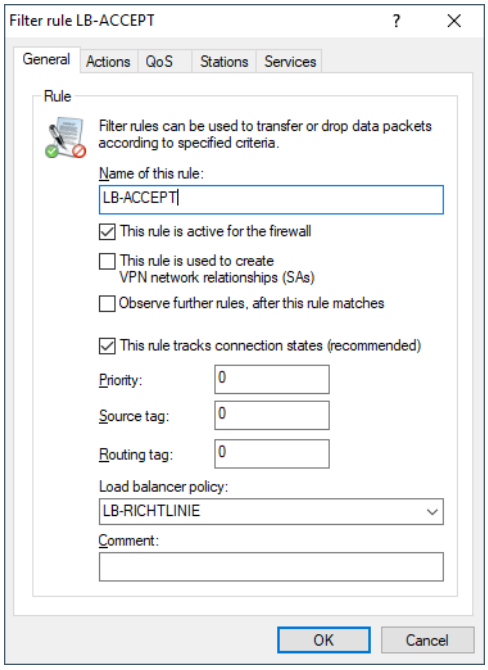
3. Add a new table row under **IP Router** > **Routing** > **SD-WAN Dynamic Path Selection** > **Policy assignments**.

   In the following, the newly created policy is linked to the VPN load balancer cluster VPN_LB. The priority fields can be left blank.



4. Add a new table row under **Firewall/QoS** > **IPv4 rules** > **Rules**.

Create a new firewall rule that accepts all traffic and that has the value “LB-RICHTLINIE” as the load balancer policy.



6.11 N:N mapping

Network Address Translation (NAT) can be used for a number of purposes:

- To make better use of the increasingly scarce IPv4 addresses
- To couple networks that use the same (private) address ranges
- To create unique addresses for network management

The first application uses N:1 NAT, also known as IP masquerading (*IP masquerading* on page 420). In this case, all addresses ("N") on the local network are mapped to a single ("1") public address. The unambiguous assignment of the data streams to the correct internal computers is generally handled by the ports used by the TCP and UDP protocols. This is why this technique is also known as NAT/PAT (Network Address Translation/Port Address Translation).

Since N:1 masquerading uses dynamic port translation, it can only be used for connections that originate inside the internal network. Exception: An internal IP address is statically exposed on a specific port, e.g. to make a server in the LAN accessible from the outside. This procedure is called "inverse masquerading” (*Port forwarding (inverse masquerading)* on page 422).

An N:N mapping is used to connect networks with the same address ranges. This translates several IP addresses ("N") from the local network explicitly into several ("N") IP addresses of any other network. This translation prevents address conflicts.

The rules for address translation are defined in a static table in the device. This involves specifying new IP addresses for individual LAN devices, for subnets or for the whole LAN, which are then used by the devices to communicate with other networks.

Some protocols (e.g. FTP) exchange parameters during the protocol negotiation, which influence the address translation undertaken by the N:N mapping. For these protocols, the relevant connection information is stored by the firewall in a dynamic table. These entries are used in combination with those in the static table to implement address translation correctly.

The address translation takes place "outbound", i.e. outgoing data packets are given a translated source address and incoming data packets are given the translated destination address, as long as the addresses are within the specified range. An “inbound” address mapping, whereby the source address is translated (instead of the destination address), needs to be implemented with an appropriate “outbound” address translation on the remote side.

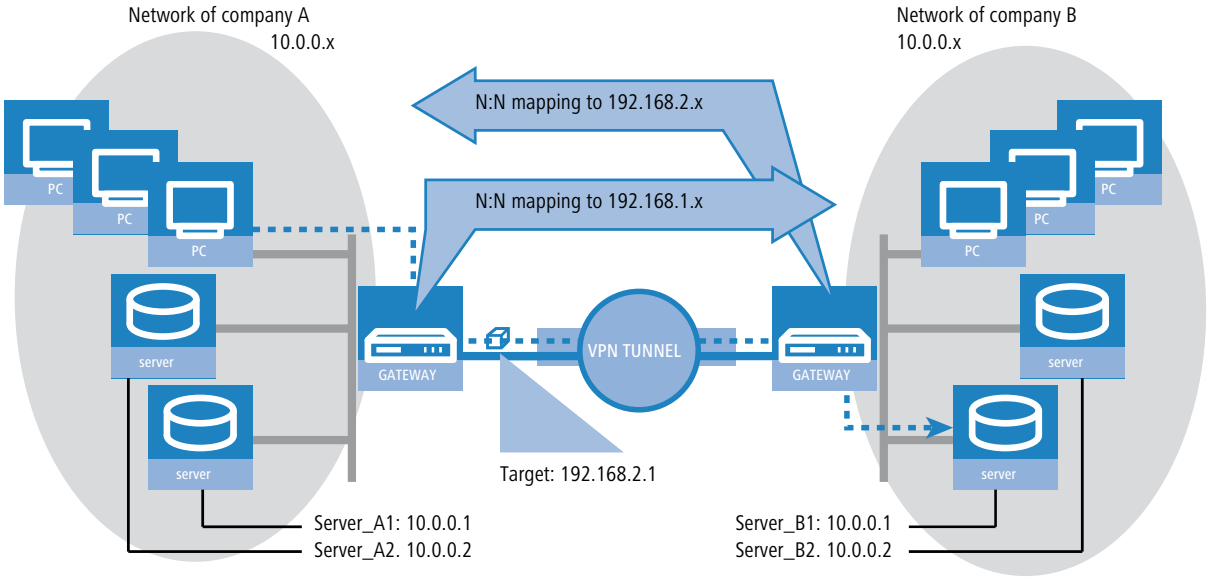
6.11.1 Example applications

This section describes the following typical applications:

- Connection of private networks that use the same address range
- Remote monitoring by service providers

6.11.1.1 Network coupling

A common scenario is the coupling of two company networks that internally use the same address range (e.g. 10.0.0.x). This usually happens when a company needs access to one (or more) server(s) at the other site:

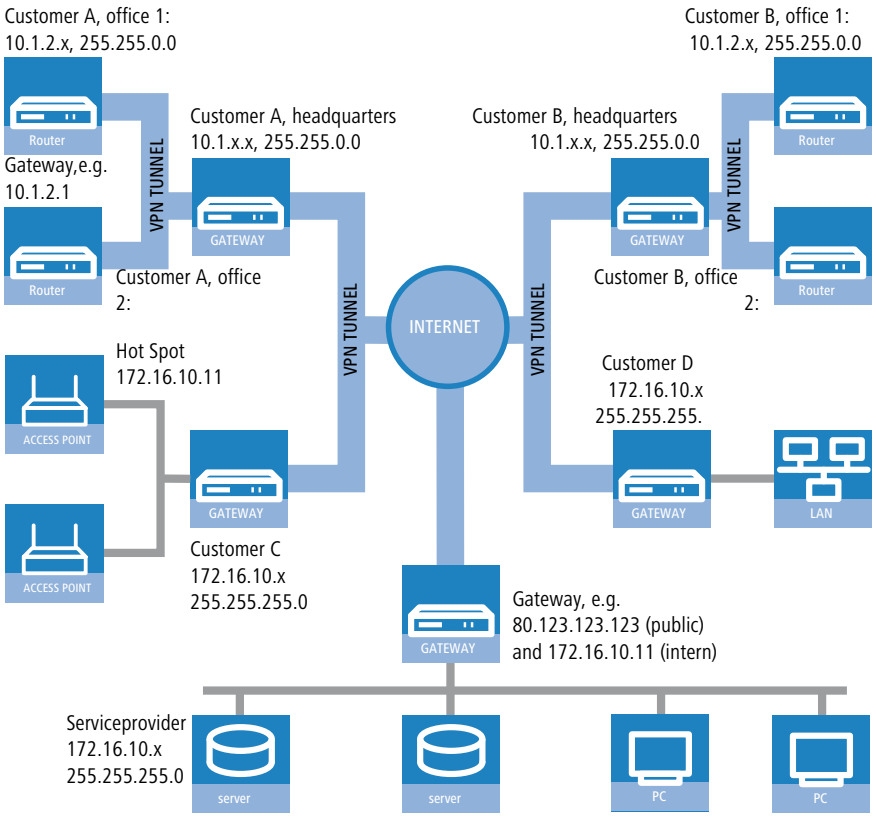


In this example, the networks of the companies A and B contain servers that want to access the other network via a VPN tunnel. All stations in the LAN should have access to the servers in the remote network. Because both networks use the same address range, it is initially not possible to access the other network with this configuration. If a station in the network of company A wants to access server 1 of company B, the addressee (with an address on the 10.0.0.x network) is searched for on its own local network. The request does not even reach the gateway.

The N:N mapping translates all addresses within the LAN into a new range of addresses for communication with the remote network. Company A's network is translated, for example, to the range 192.168.1.x, while company B's network is translated to 192.168.2.x. Each LAN is now accessible by the other at these new addresses. The station from the network of company A addresses the server 1 of company B under the address 192.168.2.1. The device being addressed is not located in the local network, so the request is forwarded to the gateway and routed to the remote network, as desired.

6.11.1.2 Remote maintenance and monitoring of networks

The remote maintenance and monitoring of networks is becoming increasingly important because of the possibilities of VPN. With the use of almost ubiquitous broadband Internet connections, administrators in these management scenarios no longer have to rely upon different data communication technologies or expensive leased lines.



In this example, a service provider monitors the networks of various customers from a central location. For this purpose, the SNMP-capable devices should automatically send the corresponding traps of important events to the SNMP trap receivers (e.g. LANmonitor) in the network of the service provider. The administrator in the service provider's LAN thus has an up-to-date overview of the status of the devices at all times.

The individual networks can be structured very differently: Customers A and B integrate their branch offices and their networks into the central LAN by means of VPN connections, customer C operates a network with several public Wi-Fi base stations as hotspots, and customer D has another router for access into their LAN.

The networks of customers A and B use different address ranges to their affiliated branch offices. These networks can thus be coupled by means of VPN.

In order to avoid operating a separate VPN tunnel to each of the customers' (A and B) subnets, the service provider establishes a VPN connection solely to the main office and uses the existing VPN lines to communicate with the branch offices.

Traps from the networks report to the service provider whether, for example, a VPN tunnel has been established or terminated, a user tried to log in three times with a wrong password, a user logged into a hotspot, or a LAN cable has been pulled out of a switch somewhere.

See the appendix to this reference manual for a complete list of all SNMP traps supported by the device.

The routing of these different networks quickly reaches its limits when two or more customers use the same address range. The problem can be compounded if customers use the same address range as the service provider themselves, which causes further address conflicts. In this example, a hotspot operated by customer C has the same address as the gateway of the service provider.

There are two different variants for resolving these address conflicts:

- In the decentralized variant, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of 1:1 mapping. The technical term for this address is a "loopback address", the method is correspondingly referred to as the "loopback method".

  The loopback addresses are only valid for communication with certain remote sites on the relevant connections. Consequently, a device is not generally accessible under this IP address.
- A more appealing solution is central mapping: Instead of configuring each individual gateway at the branch networks, the administrator sets the address translation in the gateway of the central office. In doing so, all subnetworks "behind" the main office are automatically supplied with the necessary new IP addresses.

In this example, the service-provider administrator for customer B's network sets the central address translation to 10.2.x.x., so that the two networks using the same address pools appear to the service provider's gateway to be two different networks.

For customers C and D the administrator selects the address pools 192.168.2.x and 192.168.3.x, so that these networks have different addresses from the service provider's own network.

In order for the gateway of the service provider to communicate with the networks of customers C and D, the administrator additionally sets up an address translation to 192.168.1.x for his own network.

6.11.2 Configuration

6.11.2.1 Setting up address translation

Configuring N:N mapping requires actually very little information. Since a LAN can be coupled with numerous other networks via N:N, a source IP range can be translated in different ways depending on the destination. The NAT table contains a maximum of 64 entries containing the following information:

- **Index**: Unique index for the entry
- **Source address**: IP address of the computer or network that is to receive an alternative IP address.
- **Source mask**: Netmask of the source range.
- **Destination station**: Name of the remote device that can be used to access the remote network.
- **Mapped network**: IP address or address range that should be used for the translation.

For the new network address, the same netmask is taken as used by the source address. The following applies with the assignment of source and mapping addresses:

- When translating individual addresses, source and mapping can be assigned in any way. For example, the server in the LAN with the IP address 10.1.1.99 can be assigned the mapping address 192.168.1.88.
- When entire address ranges are translated, the computer-related part of the IP address is used directly and only the network-related part of the mapping address is appended. When assigning 10.0.0.0/255.255.255.0 to 192.168.1.0, the server in the LAN with the IP address 10.1.1.99 is necessarily assigned with the mapping address 192.168.1.99.

The address range for translation must be at least as large as the source address range.

Please note that the N:N mapping function is only effective when the firewall is activated.

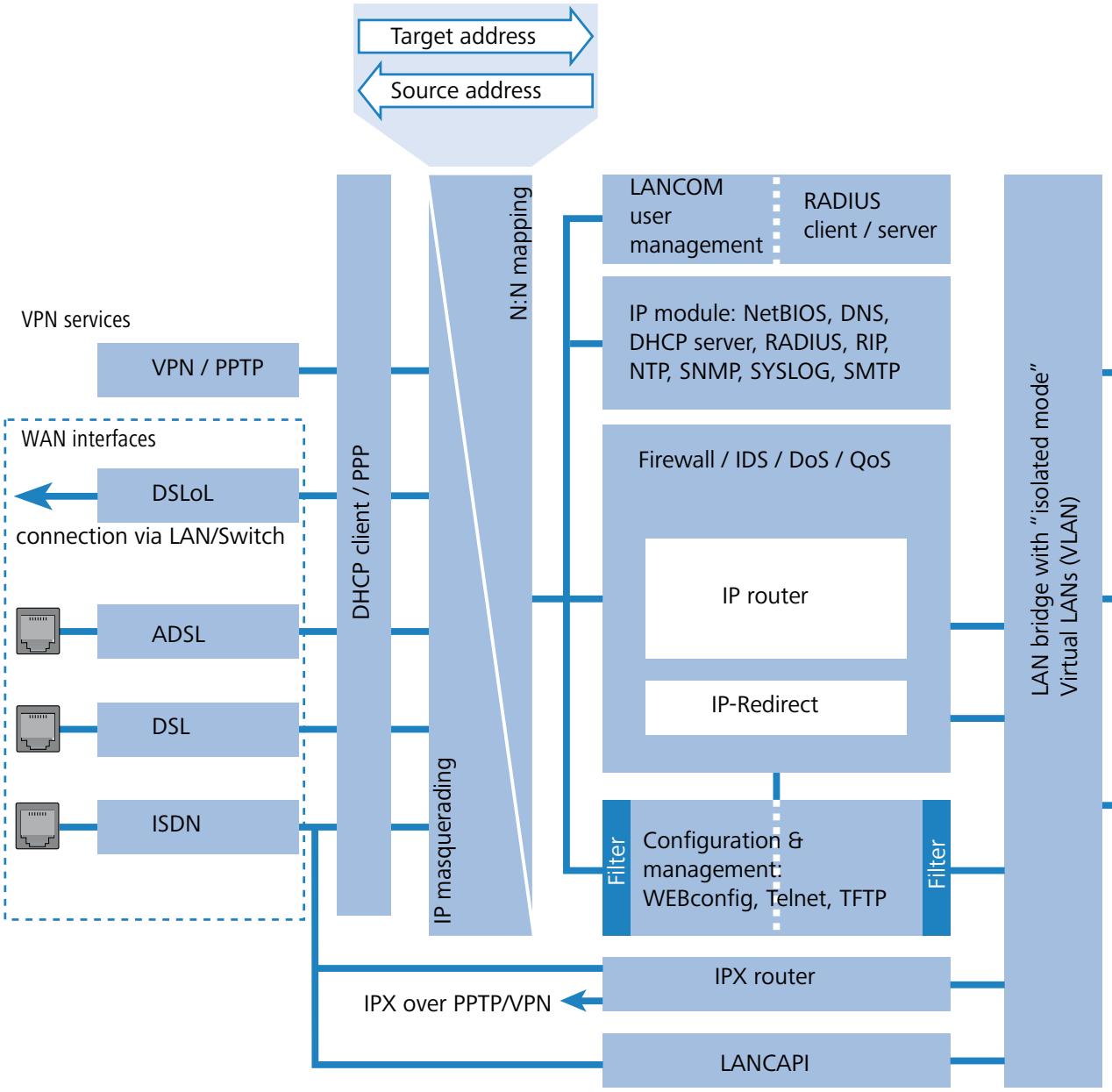
6.11.2.2 Additional configuration hints

When the address translation is set up in the NAT table, the networks and computers are initially only visible under a different address in the higher-level network. For the seamless routing of data between the networks, further settings are required:

- Entries in the routing tables, so that packets with their new addresses can find their way to the destination.
- DNS forwarding entries so that requests for specific devices in the other networks can be resolved to the mapped IP addresses.

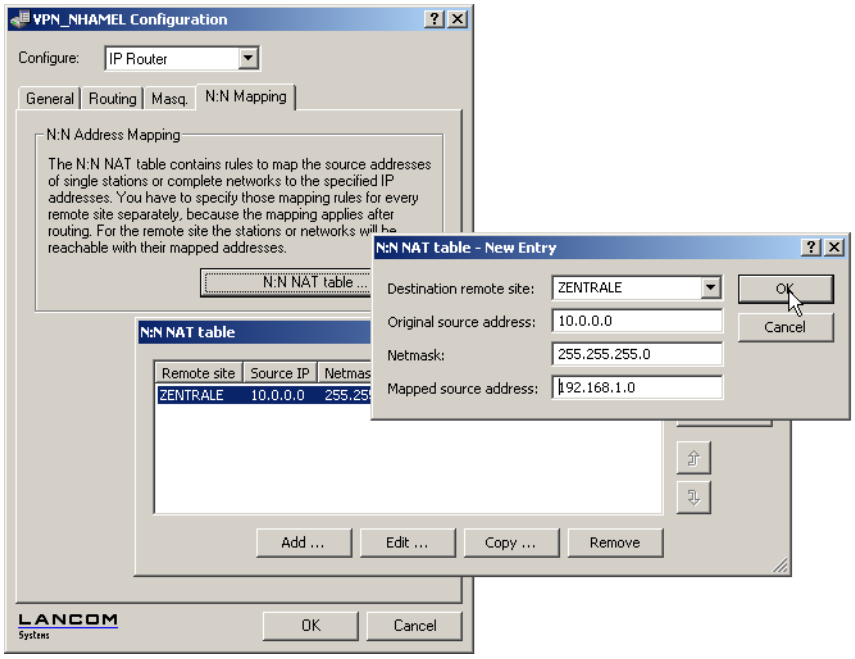
- The firewall rules in the gateways must be adapted in such a way that, if necessary, it is also possible to connect to the accessible stations or networks from the outside.
- VPN rules for loopback addresses so that the newly assigned IP addresses can also be transmitted through the corresponding VPN tunnels.

The device performs IP address translation between the firewall and IP router on the one hand and the VPN module on the other. Rules that relate to their own local network therefore use the "unmapped" original addresses. Entries for the remote network therefore use the "mapped" addresses of the remote site, which are valid on the VPN connection.



6.11.2.3 Configuration with different tools

In LANconfig, address translation is set up in **IP router** > **N:N mapping**:



Console: **Setup** > **IP-Router** > **NAT-Table**

6.12 Connection establishment with PPP

Devices from LANCOM support the point-to-point protocol (PPP). PPP is a collective term for a whole series of WAN protocols. It is widely supported and allows routers from different manufacturers to interact.

Because PPP is independent of any specific router operating mode and is of increasing significance now and for the future, we are dedicating this section to the device functions that are related to PPP.

6.12.1 The protocol

6.12.1.1 What is PPP?

The point-to-point protocol (PPP) was specifically developed for network connections on serial channels (e.g. ISDN, DSL, etc.) and has become the standard for connections between routers. It implements the following features:

- Password protection according to PAP, CHAP or MS-CHAP
- Callback functions
- Negotiating the network protocol to be used over the established connection (e.g. IP). These include parameters necessary for these protocols, such as IP addresses. This negotiation is conducted using the IPCP protocol (IP Control Protocol).
- Negotiation of connection parameters such as the MTU (Maximum Transmission Unit*Manual definition of the MTU* on page 466).
- Verification of the connection by LCP (Link Control Protocol)

PPP is the standard used for communication between routers and WAN-connection software from different manufacturers. To ensure successful data transmission wherever possible, the connection parameters are negotiated with standardized control protocols (e.g. LCP, IPCP, CCP), which are included in PPP.

6.12.1.2 What is PPP used for?

The point-to-point protocol is used in the following applications:

- For compatibility reasons, e.g. communicating with third-party routers
- Access (with the transmission of addresses)

The PPP implemented in the device can be used synchronously or asynchronously via either a transparent HDLC connection or an X.75 connection.

6.12.1.3 The phases of PPP negotiation

When establishing a connection using PPP, the initial stage is to negotiate the parameters to be used for the connection. This negotiation has four phases, and you need to be aware of these for configuration and troubleshooting.

- Establish phase

  Once a connection has been made at the data communication level, the first stage is to negotiate the connection parameters using LCP.

  This ascertains whether the remote site is also ready to use PPP, as well as the packet sizes and the authentication protocol (PAP, CHAP, MS-CHAP, or none). With this phase complete, LCP switches to the opened state.

- Authenticate phase

  If required, the passwords are exchanged. When authenticating to PAP, the password is transmitted only once. When using CHAP or MS-CHAP, an encrypted password is sent periodically at configurable intervals.

  One possibility is that this phase also negotiates a callback via CBCP (Callback Control Protocol).

- Network phase

  The IPCP protocol is implemented in the device.

  After the password was transmitted successfully, the network layer IPCP can be established.

  If the parameters were negotiated successfully, the router module can transmit IP packets on the opened (logical) line.

- Terminate phase

  In the final phase, the line is closed when the logical connections for all protocols are terminated.

6.12.1.4 PPP negotiation in the device

The PPP negotiation process is logged to the PPP statistics of the devices and, in the event of an error, you can check the protocol packets listed in detail there.

The PPP trace outputs offer a further method of analysis. The command

```
trace + ppp
```

starts the output of the PPP protocol frames exchanged during a terminal session. If this terminal session is stored to a log file, a detailed analysis can be performed once the connection has been terminated.

6.12.2 Everything OK? Checking the line with LCP

When establishing a connection via PPP, the participating devices negotiate a common behavior for the data transfer. For example, they first decide whether they should connect at all using the security method, names and passwords specified.

Once the connection is established, the reliability of the line can be constantly monitored using the LCP. This is achieved within the protocol by the LCP echo request and its associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote site along with the data. A valid response (LCP echo reply) to this request shows that the connection is reliable and stable. This request is repeated at specified intervals so that the connection can be continually monitored.

What happens when there is no reply? First a few retries will be initiated in case the disturbance is temporary. If all the retries remain unanswered, the line will be dropped and an alternative route sought.

When remotely accessing individual workstations with Windows operating systems, we recommend switching off the regular LCP requests because these operating systems do not reply to LCP echo requests and the connection would be terminated.

The LCP request behavior is configured in the PPP list for each individual connection. The intervals at which LCP requests should be made are set by the entries in the 'Time' and 'Retr.' fields, along with the number of retries that go unanswered before the line is considered faulty. LCP requests are switched off entirely by setting the time to '0' and the retries to '0'.

6.12.3 Assigning IP addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. If a remote site does not have its own IP address (such as the individual workstation of a telecommuter), the device assigns it an IP address for the duration of the connection, so enabling communications to take place.

This type of address assignment is performed during PPP negotiation and is used only for connections via WAN. In contrast, the assignment of addresses using DHCP is (usually) used within a local area network.

Assignment of an IP address is only possible if the device can identify the remote site by its call number or name when the call arrives, i.e. authentication was successful.

6.12.3.1 Examples

- Remote access

  Address assignment is made possible by a special entry in the IP routing table. Along with the entry for the IP address to be assigned to the remote site from the 'Router name' field, the net mask is entered as 255.255.255.255. In this case, the router name is the name required for the remote site to authenticate with the device.

  This configuration involves the transmission of entries from the TCP/IP module, including the IP address and the addresses of the DNS servers (Domain Name Server), including the backup server.

  In order for everything to function properly, the remote site must also be set up to obtain the IP address and the name server from the device. In Dial-Up Networking under Windows, for example, this is done with the entries in the 'TCP settings' under 'IP address' and 'DNS configuration'. The options 'IP address assigned by server' and 'Specify name server addresses' are activated here.

- Internet access

  If the device is used to provide a local area network with Internet access, the assignment of IP addresses can take place the other way around. In some configurations the device itself does not have a valid IP address on the Internet, and instead it receives one from the Internet provider for the duration of the connection. During the PPP negotiation the devices receives the IP address and information about the DNS server at the provider.

  In the local network, the device is only known by its internal intranet address. This allows all of the workstations in the local network to access the same Internet account and, for example, reach the DNS server.

Windows users are able to view the assigned addresses via LANmonitor. This also lists the name of the connected remote site, the current IP address, and the addresses of DNS servers. Options such as channel bundling or the duration of the connection are also displayed.

6.12.4 Settings in the PPP list

In the PPP list, you are able to specify you own definition of PPP negotiation for every remote site contacting your network.

You can also specify whether communications should use an IPv4 or an IPv6 connection.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MSCHAP or MSCHAPv2. The protocols here have a "hierarchy" amongst themselves, i.e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the authentication protocol used by the device is fixed, the connection may fail because no common authentication protocol can be negotiated.

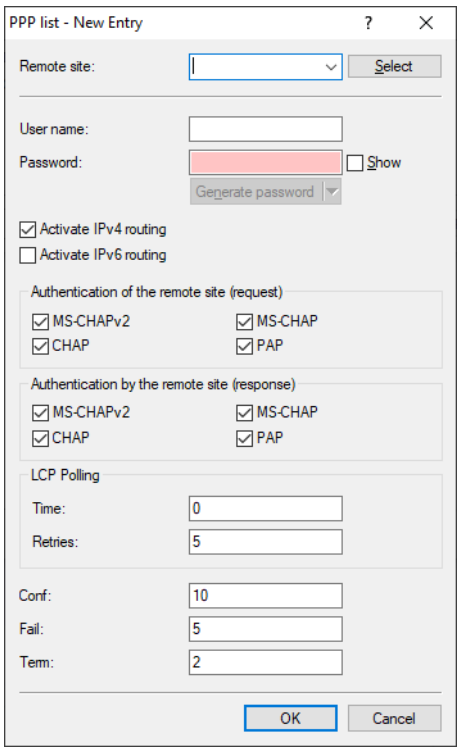
In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the device must explicitly refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the device ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the device (inbound connections) and on login of the device into other remote sites (outbound connections).

- When establishing inbound connections, the device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the device).
- When establishing outbound connections, the device offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.

LANconfig: **Communication** > **Protocols** > **PPP list**



Remote site

Enter the name of the remote site here. This name has to agree with the entry in the list of peers/remote sites. You can also select a name directly from the list of peers / remote sites.

During PPP negotiations, a remote site dialing-in to the device logs on with its name. The device can use the name to retrieve the permitted values for authentication from the PPP table. At the start of

the negotiation, the remote site occasionally cannot be identified by IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined. If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

User name

Enter the name under which the router should log in to the remote station. The router will use its own name if you leave this field blank.

Password

Enter the PPP password for this remote station.

If your router has to log in to the remote station (e.g. an Internet provider), enter the log-in password here.

If the remote station is to call your router, enter the log-in password with which the remote station will authenticate itself.

Activate IPv4 routing

Activates IPv4 routing for this remote site.

Activate IPv6 routing

Activates IPv6 routing for this remote site.

Authentication of the remote site (request)

Specify the security measures which apply to the remote site when a connection is established. At least one of the selected measures must be responded by the remote site. This is necessary e.g. on local dial in.

If the remote site is an Internet provider, select **none** of them

If more than one method is selected, a fallback to the next protocol is performed till the remote site successfully responds.

Authentication by the remote site (response)

Specify the security measures which are allowed for the local station when performing an authentication response.

If the remote site is an Internet provider, select **all** of them.

If none of the methods are selected, no local authentication is accepted from the remote site.

Time

Time between two tests of the connection with LCP (see also LCP). This time is entered in multiples of 10 seconds (e.g. 2 for 20 seconds). The value is also the time between two tests of the connection as per CHAP. This time is entered in minutes. For remote sites running the Windows operating system the time must be set to 0.

Retries

Number of retries for the test attempt. Multiple retries reduces the impact from temporary line faults. The connection is only terminated if all tries prove unsuccessful. The time between two retries is one tenth (1/10) of the time between two tests. This value is also the maximum number of "Configure Requests" that the device sends before assuming a line fault and tearing down the connection itself.

Conf

Conf corresponds to the parameter Max-Configure in *RFC 1661*. Max-Configure indicates the number of Configure-Request packets sent without receiving a valid Configure-Ack, Configure-Nak or Configure-Reject before assuming that the peer is unable to respond. Max-Configure default value is set to ten transmissions.

Fail

Fail corresponds to the parameter Max-Failure in *RFC 1661*. Max-Failure indicates the number of Configure-Nak packets sent without sending a Configure-Ack before assuming that configuration is not converging. Any further Configure-Nak packets for peer requested options are converted to Configure-Reject packets, and locally desired options are no longer appended. Max-Failure default value is set to five transmissions.

Term

Term corresponds to the parameter Max-Terminate in *RFC 1661*. Max-Terminate indicates the number of Terminate-Request packets sent without receiving a Terminate-Ack before assuming that the peer is unable to respond. Max-Terminate default value is set to two transmissions.

6.12.5 The meaning of the DEFAULT remote site

During PPP negotiations, a remote site dialing-in to the device logs on with its name. The device can use the name to retrieve the permitted values for authentication from the PPP table. At the start of the negotiation, the remote site occasionally cannot be identified by IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

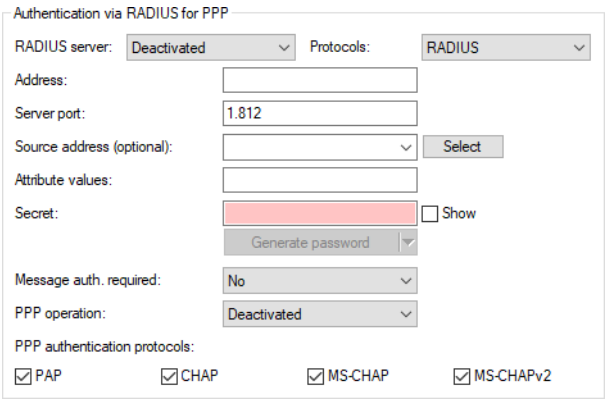
If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

6.12.6 RADIUS authentication of PPP connections

PPP connections can also be authenticated by an external RADIUS server. However, these external RADIUS servers do not necessarily support all available protocols. For this reason, the permitted protocols can also be selected in the configuration of the RADIUS authentication. LCP negotiation is restarted with the permitted protocols if the RADIUS server does not support the negotiated protocol.

6.12.6.1 WAN RADIUS table

LANconfig: **Communication** > **RADIUS**



Console: **Setup** > **WAN** > **RADIUS**

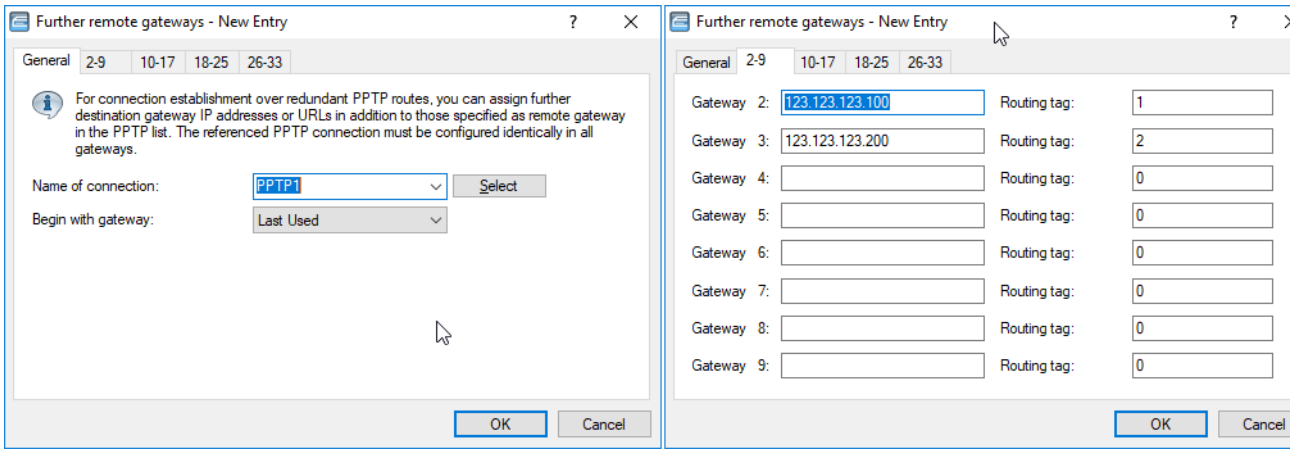
6.12.7 32 additional gateways for PPTP connections

6.12.7.1 Introduction

Up to 32 additional gateways can be configured to assure the availability of any PPTP remote site. Consequently, each PPTP remote site can use a total of up to 33 gateways.

6.12.7.2 Configuration

The additional PPTP gateways are defined in a separate list.



LANconfig: **Communication** > **Remote Sites** > **PPTP** > **Further remote gateways**

Console: **Setup** > **WAN** > **Additional PPTP gateways**

› **Name of connection**

Here you select the PPTP remote site that this entry applies to.

Possible values:

› Select from the list of defined PPTP remote sites.

Default:

› Empty.

› **Begin with**

Here you select the order in which the entries are to be tried.

Possible values:

› Last used: Selects the entry for the connection which was successfully used most recently.
› First: Selects the first of the configured remote sites.
› Random: Selects one of the configured remote sites at random. This setting provides an effective measure for load balancing between the gateways at the headquarters.

Default:

› Last used

› **Gateway 2 to 33**

Enter the IP addresses of the additional gateways to be used for this PPTP remote site.

Possible values:

› IP address or 63 alphanumerical characters.

Default:

› Empty.

› **Routing tag**

Enter the routing tag for setting the route to the relevant remote gateway.

Possible values:

› Maximum 5 characters.

Default:

› 0.

If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote site in the PPTP connection list will be taken for the associated gateway.

6.13 DSL connection establishment using PPTP

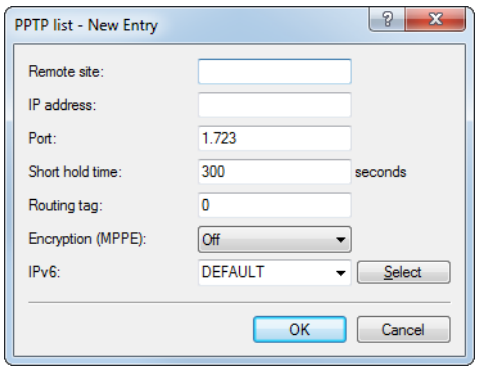
Instead of using PPPoE for dialing-in, some DSL providers instead PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). PPTP is a protocol extension of PPP and was primarily developed by Microsoft.

PPTP allows you to establish "tunnels" to a remote site via IP networks. A tunnel is a logically shielded connection that protects the transmitted data from unauthorized access by third parties. The RC4 encryption algorithm is used for this.

6.13.1 Configuring PPTP

The PPTP parameters required by the device are requested as soon as the Set up Internet Access wizard is started and you select Internet access via PPTP. Along with the usual inputs required for PPPoE access, the IP address of the PPTP gateway must also be specified. The PPTP gateway is usually the DSL modem. Precise information can be supplied to you by your DSL provider.

Any changes to the configuration are made in the PPTP list:



LANconfig: **Communication** > **Remote sites** > **PPTP** > **PPTP list**

The PPTP configuration consists of the following parameters:

Remote site

This name from the list of DSL broadband peers.

IP address

IP address of PPTP gateway, usually the address of the DSL modem.

Port

IP port used for running the PPTP protocol. According to the protocol standard, port '1,723' should always be specified.

Short hold time

This value specifies the number of seconds that pass before a connection to this remote site is terminated if no data is being transferred. Applicable values range from 0 to 3600 seconds.

With the value 9999, connections are established immediately and without a time limit.

Routing tag

Routing tag for this entry.

Encryption (MPPE)

Key length of the encryption. Also see *MPPE for PPTP tunnels* on page 832

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **WAN interfaces**.

6.14 Permanent connection for flat rates – keep-alive

The term flat rate refers to all-inclusive connection rates that are not billed according to connection times, but instead as a flat fee for fixed periods. With flat rates, there is no longer any reason to disconnect. On the contrary: New e-mails should be delivered immediately to the PC, the home office should be continuously connected to the company network, and you want to be accessible to friends and colleagues over Internet messenger services non-stop. This means it is desirable for connections to be continuously maintained.

The keep-alive function ensures that the device re-establishes the connection whenever the remote site cuts it off.

6.14.1 Configuring the keep-alive function

The keep-alive function is configured in the Remote sites list.

If the short hold time is set to 0 seconds, the connection is not actively terminated by the device. This setting thus prevents disconnection if no data is transferred over a longer period. With this setting, however, a disconnect at the remote site is not automatically re-established.

With a holding time of 9,999 seconds the connection is always re-established after any disconnection. Additionally, the connection is re-established after booting the device ('auto reconnect').

6.15 Data volumes on the WAN interface

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. The device captures the amount of data sent over each WAN interface, archives the values for up to 12 months, and can perform actions when a specified threshold is reached. The budgets also apply to VPN, PPTP, or all other kinds of connection.

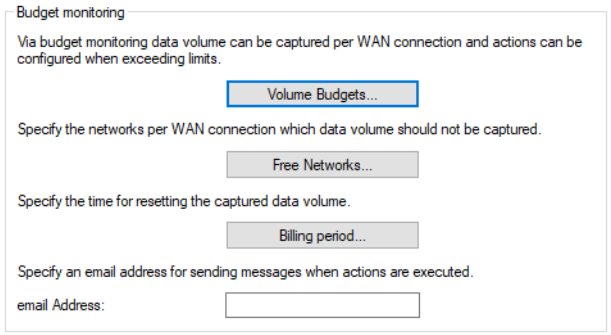
At the change of the month, the device archives the data for the previous month and resets the counter to zero for the current month. You can view the current data volume and the archived information in LANmonitor or in the WEBconfig

status menu. The archive contains data from the last 12 months. In the 13th month, the device automatically overwrites the archive data of the 1st month.

6.15.1 Configuring data volume budgets

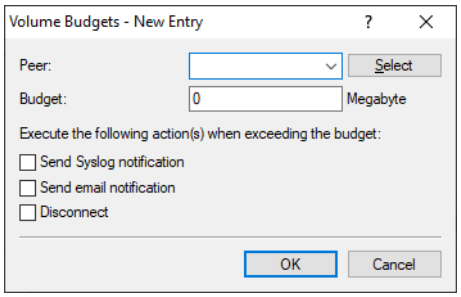
The following section describes how you can use LANconfig to manage the data volumes exchanged with remote sites.

1. Start LANconfig and open the configuration of the device for which you want track the data volumes.
2. In the configuration dialog, navigate to the item **Management** > **Budget**.



If the device should send an e-mail when your data volume is exceeded, you can enter the required address into the field **E-mail address**.

3. Click on **Volume budgets** and then on **Add**.



The item **Peer** lets you select the remote site which requires a volume budget. With **Select** you can choose from the available remote sites or manage new ones.

Specify the data volume in the **Budget** field. In most cases this value is the permitted data volume specified by the provider before the data rate is throttled.

Further, you can specify actions that the device should perform when the budget is reached:

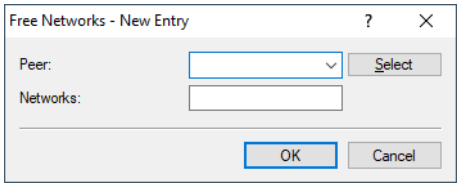
- **Send SYSLOG notification**: When the thresholds 80% and 100% of the budget are reached, the device stores a SYSLOG message (with the flag "Critical") that you can analyze with LANmonitor or a special SYSLOG client.
- **Send e-mail notification**: When the 80% and 100% thresholds are reached, the device sends a notification to the e-mail address you specified in the dialog above.
- **Disconnect**: The device disconnects from the remote site.

The **disconnect** action activates the charge limiter. The device can no longer connect to this remote until the end of the month unless you increase the volume budget for this remote site.

You can also specify that the device should perform multiple actions. If they include the action **disconnect**, the device performs this action as the last one.

4. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.

5. If data transfer to certain networks does not affect the volume budget for a remote site, you can exclude these networks from the budgeting. To do this, click on **Free networks** and then on **Add**.

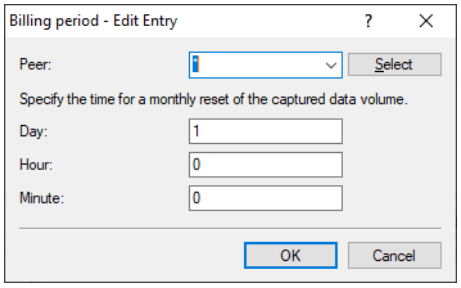


The item **Peer** lets you select the remote site which is to be excluded. With **Select** you can choose from the available remote sites or manage new ones.

You can make multiple entries for each remote by suffixing the name of the remote site with the # character and adding a number (e.g. "INTERNET", "INTERNET#1", "INTERNET#2", etc.). This is useful if you explicitly wish to define an exception that is only temporarily active. When this exception is no longer valid, you delete only the entry with the correspondingly numbered remote site.

In the **Networks** field you can specify IPv4 and IPv6 addresses and also whole networks in prefix notation (for example "192.168.1.0/24"). Separate each entry with a comma. Here too you can add the # character and a digit to the remote site name.

6. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.
7. You can set the day and time when the device should start each monthly billing period under **Billing period**.
8. If you want to change the preset values, select the line containing the peer named "*" and click on **Edit**; otherwise click on **Add**.



The item **Peer** lets you select the remote site for which you want to set the time when the period starts. With **Select** you can choose from the available remote sites or manage new ones.

You can use wildcards for the names of the remote sites. The wild card "*" in this case applies for all remote sites.

In the fields **Day**, **Hour** and **Minute** you set the day of the month and the time at which the device resets the budget for this peer.

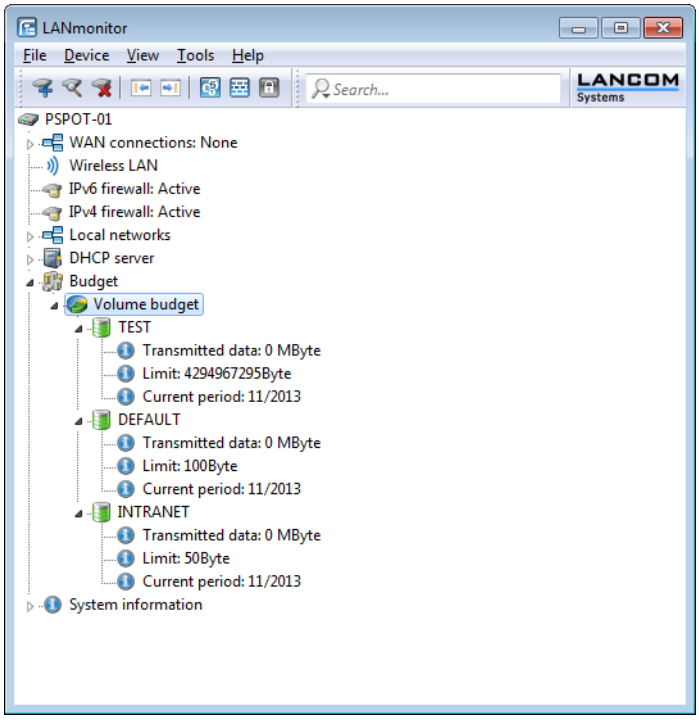
By default the device resets the budget for all peers on the first day of the month at 00:00h.

If you enter the value "31" in the field **Day**, the device does not reset the budget in months with fewer days (e.g. February or November).

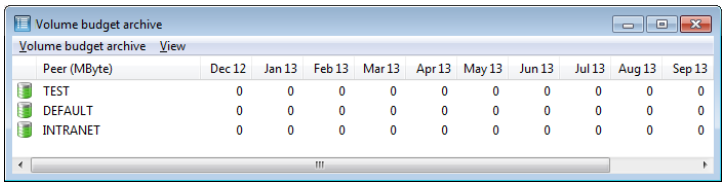
9. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.
10. Finally click on **OK** to load the configuration into the device.

6.15.2 Budget analysis

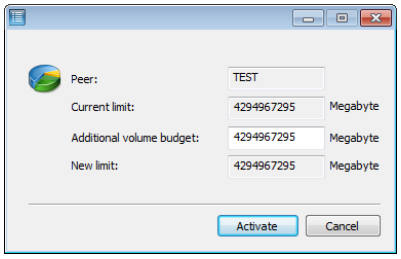
The convenient analysis and management of your configured volume budgets is available in LANmonitor under the **Budget** branch.



By clicking with the right mouse button on **Volume budget** you can reset all of the displayed volume budgets or display the volume budget archive.



By clicking with the right mouse button on a WAN interface, you can reset the budget for the corresponding interface or assign an additional volume budget.



6.16 Manual definition of the MTU

Many Internet providers operate their own backbone; however, their customers dial in to the network over the access nodes provided by third-party telecommunications providers. The “two-stage” dial-in procedure can lead to problems with the realized data rate:

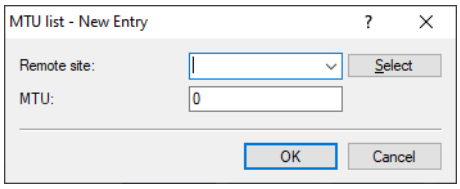
- When dialing into the nodes of Deutsche Telekom, for example, a device conducting a PPP negotiation agrees a permissible maximum transmission unit (MTU), which defines the greatest possible size of unfragmented data packet. The MTU results from the lesser of the MRU (Maximum Receive Unit) protocol parameters set on the local and remote devices. This MTU is then observed by the device.
- When the data packets are forwarded to the actual provider, an additional header is added which increases the size of the data packets again. For the data packets to meet with the permitted size, they must now be fragmented into smaller units. This additional fragmentation can cause losses in the data-transfer speeds.

This problem can be avoided by entering a fixed MTU for each remote site.

6.16.1 Configuration

LANconfig: **Communication** > **Protocols** > **MTU list**

Console: **Setup** > **WAN** > **MTU-List**



Remote Site

Enter the name of the peer here. This name must match an entry in the list of peers. You can also directly select a name from the list of peers.

You can use the wildcards “?” and “*” at any position in the peer name. “?” represents exactly one character. “*” represents any number of characters or none. The MTU list is sorted in descending order by the length of the peer name and, for names of the same length, in descending alphabetical order. This ensures that complete names always appear before names with wildcards.

MTU

MTU to be used on the connection.

6.16.2 Statistics

Under **Status** > **WAN-statistics** you will find the MTU statistics recorded for all current connections. The table is partially dynamic and begins with 16 entries. Like the MTU list under **Setup** > **WAN** it contains two columns with the remote name and the MTU.

Peer	MTU	Comment
INET	1200	The INET remote site is the Internet connection and a forced MTU of 1200 bytes.
MULTI	1492	MULTI is a PPPoE connection, for which the MTU was negotiated (and is consequently 1492 bytes).
TESTVPN	1100	TESTVPN is a VPN connection established via the Internet. An assumed overhead of 100 bytes is taken for VPN connections, and consequently the MTU here is 1100 bytes.
TESTVPN-PPTP	1060	TESTVPN-PPTP is a PPTP connection established over the VPN connection TESTVPN. The overhead for PPTP connections is 40 bytes, and consequently the MTU here is 1060 bytes.

MTU lists and MTU statistics are only available for devices with a DSL or ADSL interface.

6.17 The Rapid Spanning Tree Protocol

In networks with many switches and bridges, numerous physical connections can exist between any two stations that are connected to the network. These redundant data paths are desirable because they offer alternative paths to the desired destination in case individual network paths fail. On the other hand, these multiple connections can also lead to loops or cause network stations to receive multiple frames. Both occurrences negatively impact frictionless data traffic performance in the network.

The Spanning Tree Protocol (STP) enables an analysis of the network at the layer-2 level and, as such, offers solutions for intelligent path selection between two network stations below the routing layer. By discovering redundant paths between network stations, STP builds a unique structure in which loops and double packets can be avoided. To this end, so-called Bridge Protocol Data Units (BPDUs) are sent as a multicast to a specific MAC address. The BPDUs allow redundant paths to be discovered as well as the distance and the data rate available on this connection. Using these values, the Spanning Tree Protocol calculates a priority (also called route or path costs) with which the various connections are to be treated. The low-priority connections are disabled and are therefore no longer available for clients. Through the reduction of non-redundant connections between the clients, the protocol builds a tree which unambiguously defines all of the connections that arise from a central switch (root bridge).

The BPDUs are sent regularly in the network in order to check the availability of the connections. If a connection fails, then the network analysis is triggered again; the possible paths and the corresponding priorities are redefined.

After initialization all ports are initially in the “blocking” state, in which only BPDUs are exchanged. The ports subsequently switch to the states of "listening" and then "learning" before reaching “forwarding” which allows payload data to be exchanged via the ports.

6.17.1 Classic and rapid spanning tree

The early version of the spanning-tree protocol compliant with IEEE 802.1D, here referred to as classic spanning tree, had the problem that changes to topology after a connection failure were implemented very slowly: Depending on the complexity of the network, the classic spanning tree takes between 20 seconds and a minute to establish new routes. For many network services a failure of this length of time is unacceptable.

The spanning tree protocol was improved and published as the “Rapid Spanning Tree Protocol” (RSTP), initially as the IEE 802.1t/w standard and later as a part of the newly published IEEE 802.1D. Even though the classic spanning tree protocol was thus withdrawn, it continues to be supported by LCOS.

6.17.2 Improvements from rapid spanning tree

As mentioned above, the primary aim of RSTP is to accelerate the activation of network paths once an active connection has failed. RSTP achieves this by dispensing with the states "blocking" and "listening" to reduce the time required to update the network paths to just a few seconds. In case of a network path failure, not all of the links are blocked until the new topology has been calculated; instead, only the failed connections are unavailable for use.

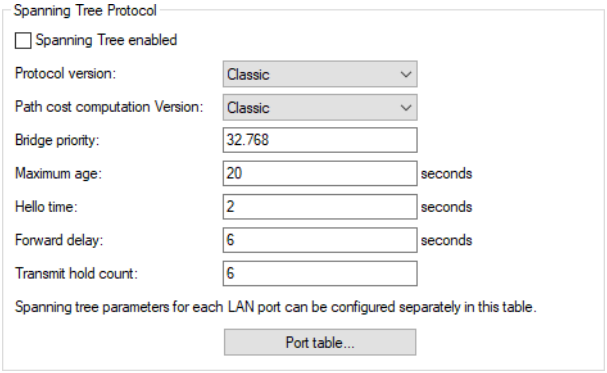
RSTP also enables the administrator to configure information on network topology.

- A bridge port can be defined as an “edge port”. An edge port is the only bridge port leading to the connected LAN segment, i.e. no other bridges are connected to the LAN segment, but workstations or servers only, for example. As these ports cannot lead to loops, they change immediately into the forwarding state without waiting for the network topology to be determined. However, RSTP continues to monitor these ports. Should BPDUs be unexpectedly received at an edge port due to another bridge being connected to the LAN, the port automatically returns to its normal state.
- A bridge port can also operate as a point-to-point link. In this case the port is directly connected with an additional bridge. Since no additional stations can occur between the two bridges, the switch into the forwarding state can take place faster.

In the ideal case, RSTP immediately resorts to familiar alternative network paths in case of connection failure.

6.17.3 Configuring the Spanning Tree Protocol

The following parameters are available for configuring RSTP or STP functionality in the device:



LANconfig: **Interfaces** > **Spanning Tree**

Console: **Setup** > **LAN-Bridge** > **Spanning-Tree**

6.17.3.1 General parameters

- Spanning tree operating

  When Spanning Tree is turned off, a device does not send any Spanning Tree packets and passes received packets along instead of processing them itself.

- Protocol version
  - Classic: Uses the classical STP to determine network topology.
  - Rapid: Uses the RSTP method to determine network topology.

  RSTP is compatible with STP. Network components which only support classical STP continue to be supported where RSTP is operational.

- Path cost computation
  - Classic: Uses the classical STP method to compute path costs.
  - Rapid: Uses the RSTP method to compute path costs.

- Bridge priority

  Defines the priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the Spanning Tree Protocol.

  So as to maintain compatibility with RSTP, this value should only be adjusted in steps of 4096 owing to the fact that RSTP uses the lower 12-bits of this 16-bit value for other purposes.

- Maximum Age

  This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as 'aged'. This parameter defines how quickly the Spanning Tree algorithm reacts to changes, for example due to failed bridges.

- Hello Time

  This parameter defines (in seconds) in which intervals a device selected to be the root bridge sends Spanning Tree information into the LAN.

- Forward delay

This time (in seconds) determines how much time must pass at a minimum before a Spanning Tree port can change the status (listening, learning, forwarding).

When using RSTP the forwarding delay often has no effect because RSTP has suitable mechanisms of its own to prompt a rapid switching into the forwarding state.

Modifying any of these three time values is only recommended for those with exact knowledge of the Spanning Tree protocol. An adjustment can be useful in order to optimize reaction times after topology changes or to achieve stable performance in networks with many 'bridge hops'.

- Transmit-hold count

  Number of BPDUs which can be transmitted by RSTP before a one second pause commences.

  When using classical STP the transmit-hold count has no effect.

6.17.3.2 Port table

The port table can be used to set the following values separately for all available ports (LAN, wireless LAN, point-to-point connections).

- Mark as edge port

  Marks the port as an edge port which is not connected to any further bridges but to workstations or servers only. Edge ports switch immediately into the forwarding state.

  Edge ports continue to be monitored by RSTP. If a port of this type receives BPDUs, then its status as an edge port is removed.

- Priority

  Defines the priority of the port. In the case of multiple network paths with identical path costs, the priority value decides which port is used. If priority values are identical then the port to be taken is the first in the list.

  So as to maintain compatibility with RSTP, this value may only be adjusted in steps of 16 owing to the fact that RSTP uses only the upper 4-bits of this 16-bit value.

- Path cost override

  This parameter controls the priority of paths with equal value. The value set here is used to make the selection instead of the computed path costs.

  - Special values: 0 switches path-cost override off.
  - Default: 0

6.17.4 Status reports via the Spanning Tree Protocol

The current STP values can be viewed via Telnet in the LAN Bridge Status.

Console: **Status** > **LAN-Bridge** > **Spanning-Tree**

6.17.4.1 General status information

- Bridge ID

  This is the ID for the device that is being used by the Spanning Tree algorithm. It is composed of the user-defined priority (upper 16 bits) and the device MAC address (lower 48 bits).

- Root bridge

  The ID for the device that is currently elected root bridge.

- Root port

The port that can be used to reach the root bridge from this device. If the device itself is the root bridge, it is displayed with the special value '255'.

- Root path cost

  The path costs of all hops added together in order to reach the root bridge from this device.

- Protocol version

  The protocol version currently set for determining network topology.

- Path cost computation

  The protocol version currently set for computing path cost.

- Bridge priority

  Current setting for bridge priority.

6.17.4.2 Information in the port table

The port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections).

- Priority

  The priority of this port taken from the port configuration

- **Status**

  The current state of the port:

  - Disabled: No packets can be sent or received through this port. This occurs when the port has either been disabled manually or when it has a negative link status.
  - Listening: Intermediate state on the way to enabling. Only Spanning Tree packets are listened to, data packets are ignored and are also not forwarded to this port.
  - Learning: Another intermediate state. As opposed to 'listening' additional MAC addresses from data packets entering this port are learned but data packets are still not forwarded.
  - Forwarding: The port is completely active, data packets are received and forwarded in both directions
  - Blocking: Spanning Tree has identified this port to be redundant and disabled it for data traffic.

- **Root**

  The ID for the root bridge that can be reached through this port.

- **Bridge**

  This is the ID for the bridge through which the root bridge can be reached.

- **Costs**

  This value defines the 'costs' for this port. The value is determined by the port technology (Ethernet, WLAN, etc.) and the bandwidth. Examples of values used are:

Transfer technology	Costs of Classic Spanning Tree	Costs of Rapid Spanning Tree
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

If path costs for a port were manually entered, then the configured value appears in this column.

6.17.4.3 Information in the RSTP port statistics

The RSTP port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections).

- **Role**

  Root or Non-root bridge

- Learning

  Port in learning state.

- Forwarding

  Port in forwarding state.

- Edge port

  Port defined as an edge port.

- Protocol version

  Classic or Rapid

- **Costs**

  Setting for this port's cost

6.18 The Action table

6.18.1 Introduction

The action table controls actions triggered when there is a change in status of WAN connections. WAN connections include direct connections to an Internet provider, and also VPN connections based on this, such as those used to connect a branch office to a main office. Every action is linked with a condition that describes the change in status of the WAN connection (establishment, termination, failure or establish failure). Actions can be any of the commands available at the Telnet terminal. Furthermore, actions can transmit messages by e-mail or SYSLOG, send an HTTP request, or transmit a DNS request. Different variables allow information such as the current IP address, the name of the device, or an error message to be integrated into the action.

6.18.2 Actions for Dynamic DNS

Systems with dynamic IP addresses can be made available for access via the WAN, for example via the Internet, by using the services of commercially available dynamic DNS servers. Servers offering these services can assign the current IP address of a device to its FQDN name (Fully Qualified Domain Name, e.g. “http://MyDevice.dynDNS.org”).

The advantage is obvious: If you wish to carry out remote maintenance via WEBconfig/HTTP, the only information you need is the dynamic DNS name. Also, a DynDNS name can be used to establish VPN connections between remote sites that have changing IP addresses.

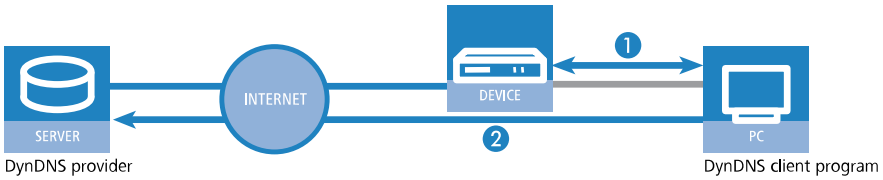
In order for the current IP address to match with the DynDNS name at all times, the IP address recorded on the DynDNS server must be constantly updated. This change is triggered by a dynamic DNS client.

- The DynDNS server, maintained by a DynDNS service provider on the Internet, is in contact with the Internet DNS servers.

› The Dynamic DNS client can run on a workstation as a separate client program. As an alternative, a dynamic DNS client is integrated into the device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP address for the DNS name translation.

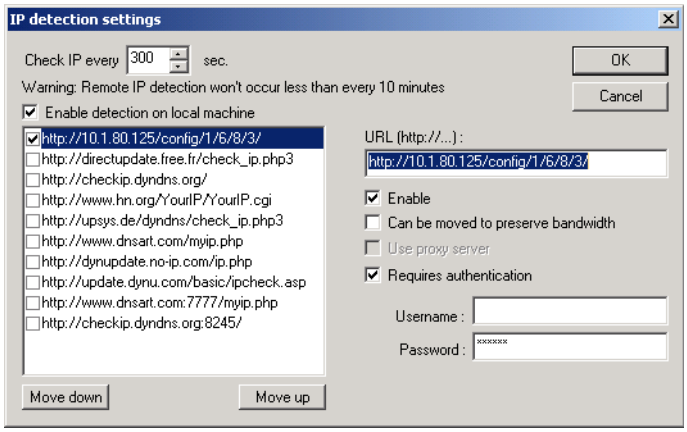
6.18.2.1 Dynamic DNS client on the workstation

Dynamic DNS providers support a range of PC client programs that use various methods to determine the IP address currently assigned to a device **1**. A change in IP address is communicated to the appropriate dynamic DNS server **2**.



The current WAN-side IP address of a device can be read from the following address and entered into a client program:

```
http://<Address of the device>/config/1/6/8/3/
```



6.18.2.2 Dynamic-DNS client in the device via HTTP

Alternatively the device can transmit the current WAN IP to the DynDNS provider directly:

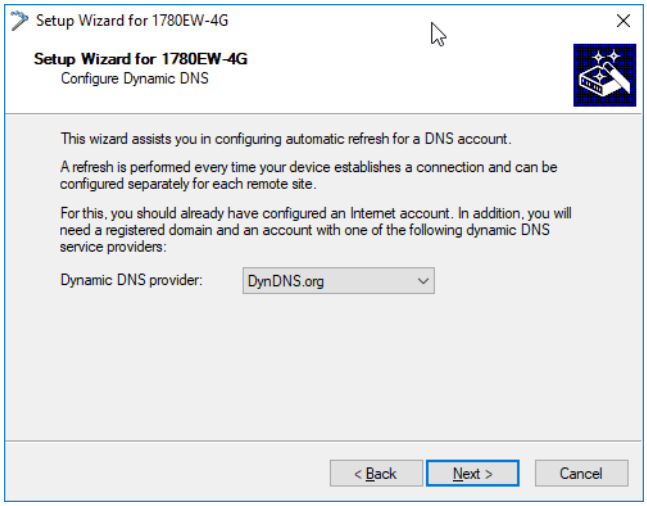


You do this by defining an action for this which, for example, automatically sends an HTTP request to the DynDNS server each time a connection is established. The necessary information is transferred via the DynDNS account, so triggering an update of the registration. An HTTP request of this type from DynDNS.org appears as follows:

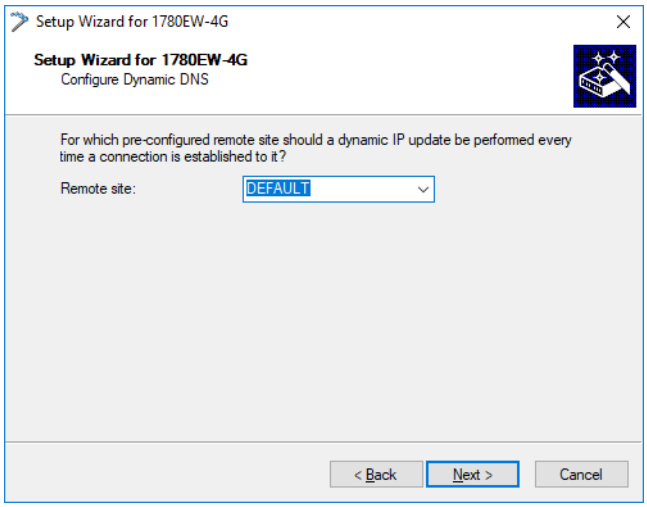
```
http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

The device sends the host name of the action along with the IP address to an account at DynDNS.org as specified by a username and password, and this updates the corresponding entry. The settings necessary for this are adjusted using the Setup Wizards in LANconfig:

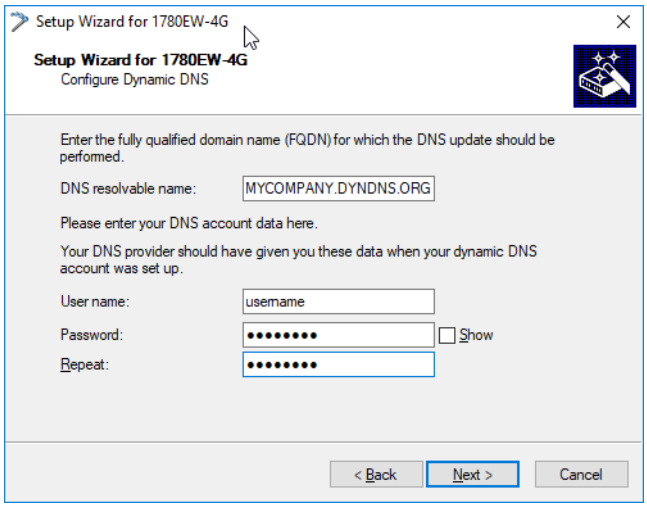
First, select the service provider you want to use from the list.



Now set the WAN remote site to which the action applies.



Then enter your login data.



The Setup Wizard supplements the basic action with further provider-specific parameters, which are not described here. Apart from that, the Setup Wizard creates additional actions that control the device in case the DynDNS provider was unable to successfully perform the update the first time.

6.18.2.3 Dynamic-DNS client in the device via GnuDIP

As an alternative to using a simple HTTP request to update DynDNS information, some services make use of the GnuDIP protocol. The GnuDIP protocol is based on a challenge-response mechanism:

1. The client opens the connection to the GnuDIP server.
2. The server responds with a random value calculated for the session.
3. The client uses the random value and the password to create a hash value, which is returned to the server.
4. The server checks this hash value and reports its result by sending a number back to the client.

The GnuDIP protocol can exchange the messages between the client and server either via a simple TCP connection (standard port 3495) or as a CGI script running on an Internet server. The version using an HTTP request from a CGI script has the advantage that no additional ports have to be opened on the GnuDIP, and also that HTTP offers protection from passive interception and offline dictionary attacks.

Requests to a GnuDIP server are triggered by the device with an action in the following form:

- gnudip://<srv>[:port][/path]?<parameter>
  - <srv> – The GnuDIP server address.
  - [:port] – Specifying the port is optional. If it is not defined, default values are taken instead (3495 for TCP, 80 or 443 for HTTP/HTTPS).
  - [/path] – Path information is only required by HTTP/HTTPS to define the location where the CGI script is stored.

  The following parameters are extensions to the request:

  - method=<tcp|http|https> – Selects the protocol to be used for the transmission between the GnuDIP server and client. Only one protocol can be selected here.
  - user=<username> – Specifies the user name for the account on the GnuDIP server.
  - pass=<password> – Specifies the password for the account on the GnuDIP server.
  - domn=<domain> – Specifies the DNS domain containing the DynDNS entry.
  - reqc=<0|1|2> – Defines the action that is triggered by the request. Action <0> sends the server a dedicated IP address that is to be used for the update. Action <1> deletes a DynDNS entry. Action <2> triggers an update, although no IP address is transmitted to the server. Instead, the server carries out the update with the IP address of the GnuDIP client.
  - addr=<address> – Specifies the IP address that an action with the parameter <0> is to use for updating the DynDNS entry. If this is unspecified in a <0> action, the request is treated as a <2> action.

  With the GnuDIP protocol, the host name that is to be registered corresponds to the user name sent to the server. If, for example, the username is "myserver" and the DNS domain is "mydomain.org", then the DNS name "myserver.mydomain.org" is registered.

  For example, the following action executed via the GnuDIP protocol updates the DynDNS entry at a DynDNS provider with the current IP address of the device (%a) as soon as a connection is established:

  - gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org &pass=password&reqc=0&addr=%a

  Use the following action to delete a DynDNS entry, for example once the connection has been terminated:

  - gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org &pass=password&reqc=1

  The line-break is for legibility only and is not to be entered into the action.

In response to the request, the GnuDIP server returns one of the following values to the GnuDIP client (assuming that the connection between server and client was established):

- 0 – The DynDNS entry was updated successfully.
- 0:address – The DynDNS entry was successfully updated with the specified address.

- 1 – Authentication at the GnuDIP server failed.
- 2 – The DynDNS entry was deleted successfully.

These responses can be processed by the device's actions to trigger further actions if necessary.

6.18.3 Further example actions

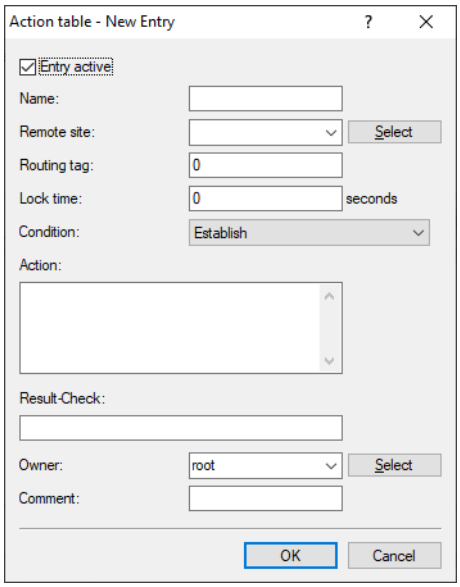
6.18.3.1 Broken connection alert as an SMS to a mobile telephone

The placeholder %t allows the current time of an event to be incorporated into a message. For example, an alert about the interruption of an important VPN connection can be sent by e-mail or as an SMS to a system administrator's mobile telephone.

The following requirements have to be met for messaging:

- The status of the VPN connection must be monitored, for example by means of “dead-peer-detection” (DPD).
- The device has to be configured as an NTP client in order to have the current system time.
- An SMTP account must be set up for transmitting e-mails.

Once these requirements are fulfilled, messaging can be set up. This is done with a new entry in the action table; e.g. with LANconfig under **Communication** > **General** > **Action table**.



Select the remote site for the relevant connection. As Condition select 'Broken' and enter the action as the transmission of an e-mail.

```
mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to Subsidiary 1 was broken.
```

If the connection is broken, this action sends an e-mail to the administrator with the time of the event in the subject line.

If the mail is sent to an appropriate Mail2SMS gateway the alert can be sent directly to a mobile telephone.

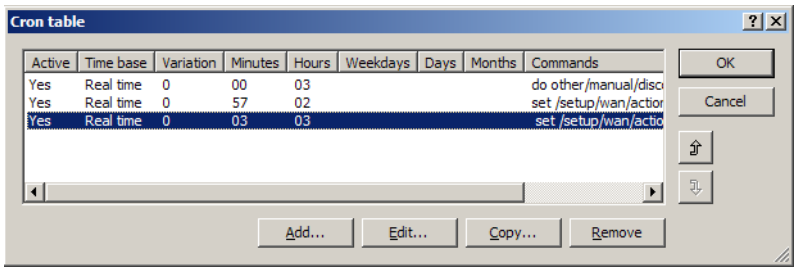
For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the device at the central device. For monitoring the central device itself, an action is entered into a device at one of the subsidiaries. In this way the administrator receives an alert even if the VPN gateway at the central location fails, which could potentially prevent any messages from being transmitted.

6.18.3.2 Example: Suppress messaging in case of re-connects with a DSL connection

Some providers interrupt the DSL connection used for the VPN connections once every 24 hours. To avoid informing the administrator of these regular interruptions, messaging can be disabled at the time when the re-connect occurs.

First of all an action is required to force the re-connect to occur at a fixed time; generally at night when the Internet connection is not in use. The entry defines, for example, 03:00h and the Internet connection is broken with the command `do other/manual/disconnect internet`.

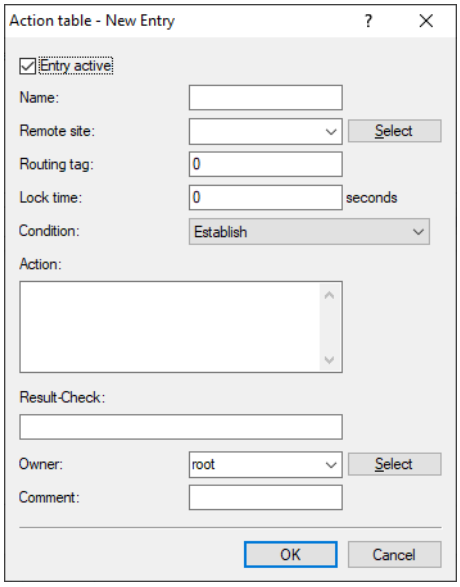
With two more cron commands `set /setup/wan/action-table/1 yes/no` the corresponding entry in the action table is switched off three minutes before 03:00h and switched on again three minutes after 03:00h. The number 1 following the path to the action table is an index that stands for the first entry in the table.



6.18.4 Configuration

With the Action table you can define actions that the device executes when the status of a WAN connection changes.

In LANconfig, the Action table is located under **Communication** > **General** > **Action table**



Entry active

Activates or deactivates this entry.

Name

Action name. This name can be referenced with the wildcard `%h` (hostname) in the fields **Action** and **Result check**.

Remote site

A change in status of this remote site triggers the action defined in this entry.

Routing tag

You can use the routing tag to specify which remote site the device uses when the action is applied. Of course, this site must be equipped with the appropriate routing tag.

Block time

Prevents this action from being repeated within the period defined here in seconds (max. 10 characters).

Condition

Various changes in WAN-connection status can be set here, and the action is triggered when this condition occurs. Possible values are:

Establish

The action triggers if the device has successfully established the connection.

Disconnect without failure

The action triggers if the device itself terminates the connection (e.g. through manual disconnection or expiry of a holding time).

End (disconnect or broken)

The action triggers as soon as the connection terminates (regardless of the reason).

Broken with failure

This action is triggered on disconnects that were not initiated or expected by the device.

Establish failure

The action triggers if connection establishment was unsuccessful.

Volume budget exhausted

This action executes when the specified volume is reached.

Volume budget released

This action occurs after a state change from "Volume exceeded" to "Volume no longer exceeded", e.g. when you reset an exceeded volume or when the device enters a new billing period. If the volume has not been exceeded at the time of the reset, no action takes place.

Action

This item describes the action to be executed by the device when there is a change in the status of the WAN connection. You can specify only one action per entry (max. 250 characters). For each of the following values, the colon (:) is part of the action value. Possible values are:

exec:

This prefix initiates any command as you would enter it at the CLI. For example, the action `exec:do /o/m/d` terminates all current connections.

dnscheck:

This prefix initiates an IPv4 DSN name resolution. For example, the action `dnscheck:myserver.dyndns.org` requests the IPv4 address of the indicated server.

dnscheck6:

This prefix initiates an IPv6 DSN name resolution. For example, the action `dnscheck6:myserver.dyndns.org` requests the IPv6 address of the indicated server.

http:

This prefix initiates an HTTP-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org:

```
http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

The meaning of the place holders `%h` and `%a` is further below.

https:

Like `http:`, except that the connection is encrypted.

gnudip:

This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:

```
gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
```

The meaning of the place holder `%a` is described below.

repeat:

This prefix together with a time in seconds repeats all actions with the condition "Establish" as soon as the connection has been established. For example, the action `repeat 300` causes all of the establish actions to be repeated every 5 minutes.

mailto:

This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator as soon as a connection is terminated: `mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to branch office 1 was broken.`

Optional variables for the actions:

%a

WAN IPv4 address of the WAN connection relating to the action.



If the string `&myip=%a` is removed from the entries in the Action table, the DynDNS provider uses the public IP address of the packet from which the request originates. This is especially useful in scenarios where an Internet connection with an IP address from a private IP address range is used.

%x

The current IPv6 LAN prefix as a string in the format “fd00:0:0:1::/64”

%{x*network name*}

For example `%{xTEST-NET}` for the current IPv6 LAN prefix of the TEST-NET network as a string in the format “fd00:0:0:1::/64”.



The variable `%x` only transmits the values of the network with the fixed name INTRANET. This can also be used to transmit the LAN network name that will be used for this variable.

%y

The current IPv6 LAN address of the device as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”.

%{y*network name*}

For example `%{yTEST-NET}` for the current IPv6 LAN address of the device in the TEST-NET network as a string in the format “fd00::1:2a0:57ff:fa1b:9d7b”.



The variable `%y` only transmits the values of the network with the fixed name INTRANET. This can also be used to transmit the LAN network name that will be used for this variable.

%z

WAN IPv6 address of the WAN connection relating to the action.

%H

Host name of the WAN connection relating to the action.

%h

Like `%h`, except the hostname is in small letters.

%c

Connection name of the WAN connection relating to the action.

%n

The device name.

%s

The device serial number.

%m

Device MAC address (as in Sysinfo)

%t

Time and date in the format "YYYY-MM-DD hh:mm:ss".

%w

Variable for IPv6. With the variable %w, together with the network name, e.g., %{wINTRANET}, a static address with a fixed host identifier can be assigned to any station in the local network.

Example: `%{wINTRANET}dd06:57b3:f1ee:201e` together with the prefix `2003:c9:1703:5b51::/64` on the INTRANET network results in: `2003:c9:1703:5b51:dd06:57b3:f1ee:20ff`

The prefix is formatted so that only the 64-bit host portion needs to be appended to form a complete 128-bit address. The prefix length "::64/" is truncated in the process.

%e

Description of the error that was reported when connection establishment failed.

Using the variable `%z` requires that you specify the IPv6 address. If you do not supply an address, the device will not execute the script.

The variable `%z` is available only for native IPv6 WAN connections and not for tunnel connections (6to4, 6in4, 6rd).

You can inspect the outcome of the actions in the field **Result check**.

Result check

You can evaluate the result of the action here to determine the number of lines to be skipped in the processing of the action table. Possible values for the actions (max. 50 characters):

contains=

This prefix checks if the result of the action contains the defined string.

isequal=

This prefix checks if the result of the action is exactly equal to the defined string.

?skipiftrue=

This suffix skips the defined number of lines in the list of actions if the result of "contains" or "isequal" is TRUE.

?skipiffalse=

This suffix skips the defined number of lines in the list of actions if the result of "contains" or "isequal" is FALSE.

The optional variables for the actions are the same as for the actions above.

Example: A DNS check queries the IP address of an address in the form "myserver.dyndns.org". The check `contains=%a?skipiftrue=2` allows you to skip the two following entries in the action table if the IP address found by the DNS check agrees with the current IP address (%a) of the device.

Owner

Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the device cannot execute the action.

Comment

Enter a descriptive comment for this entry.

6.19 Using the serial interface in the LAN

6.19.1 Introduction

In the IT field, COM-port servers (also known as serial-port servers) are devices that transport data between TCP and serial connections. There are many applications.

- Networking of devices with a serial interface but without a network interface.
- Remote maintenance of devices that can only be configured via a serial interface.
- Virtual extension of a connection between two devices with serial interfaces over a network.

Most devices feature a serial interface that can be used to carry out configurations or to connect to a modem. In some cases the interface is used for neither of these scenarios, and yet a COM port server is required somewhere in the vicinity of the device. In such cases the device can use its serial interface as a COM-port server, thus saving the investment in an external COM-port server. Where an application is to support the configuration of these devices via their serial interfaces, then some models are able to provide additional serial interfaces with the use of CardBus or USB adapters. This enables multiple instances of the COM-port server to be operated in one device.

6.19.2 Operating modes

A COM port server has two operating modes:

- Server mode: The COM port server waits for requests from a defined TCP port to establish TCP connections. The mode is used for remote maintenance, for example.
- Client mode: As soon as a device connected to the serial interface becomes active, the COM port client opens a TCP connection to a preset remote site. This operating mode is used, for example, for devices that have just one serial interface but requiring network access.

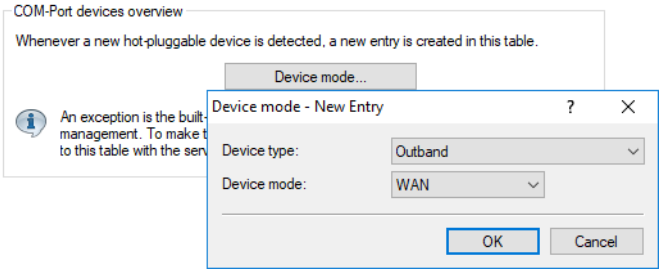
In both of these cases a transparent connection is set up between the serial interface and the TCP connection. Data packets received at the serial interface are forwarded to the TCP connection, and vice versa. A common server-mode application is to install a virtual COM port driver at the remote site which connects to the COM port server. Drivers of this type allow applications running at the remote site to use the TCP connection as if it were an additional COM port.

The IETF RFC 2217 standard sets down the Telnet WILL/DO protocol extensions, which transmit the negotiations for the serial connection (bitrate, data and stop bits, handshake) to the COM port server. The use of this protocol is optional, so practical default values can be set in the COM port server.

6.19.3 Serial interface configuration

The serial interfaces in the device can be used for various applications, for example for the COM port server or as a WAN interface. The Devices table allows individual serial devices to be assigned to certain applications. As soon as a HotPlug-capable USB adapter is detected, a new entry for the serial interface provided by this USB adapter is created automatically in this table. This automation simplifies the configuration of the serial devices. An exception is the built-in serial interface, which is used for configuration purposes as standard. Entries can be added to the Devices table manually to use this interface for the COM port server or WAN applications.

LANconfig: **Miscellaneous Services** > **COM ports** > **Device mode**



Console: **Setup** > **COM-Ports** > **Devices**

Device type

Selects a serial interface from the list of those available in the device.

Device mode

Activation of the port in the COM port server.

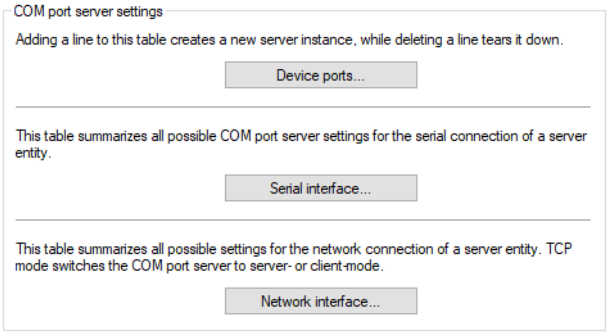
6.19.4 Configuring the COM port server

Configuring the COM port server involves three tables. What all three tables have in common is that a certain port at a serial interface is identified by the values for device type and port number. Because some serial devices such as a CardBus card have multiple ports, the port to be used must be specified explicitly. For a device with just one port, such as with the serial configuration interface, the port number is set to zero.

6.19.4.1 Operational

This table activates the COM port server at a port of a certain serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to stop the corresponding server instance. The switch Operating can be used to deactivate a server instance in the table.

When a server instance is created or activated, the other tables in the COM port configuration are searched for matching device type and port number values. If no suitable entry is found, the server instance takes workable default values.



LANconfig: **Miscellaneous Services** > **COM ports** > **Device ports**

Console: **Setup** > **COM-Ports** > **COM-Port-Server** > **Devices**

Device type

Selects a serial interface from the list of those available in the device.

Port number

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

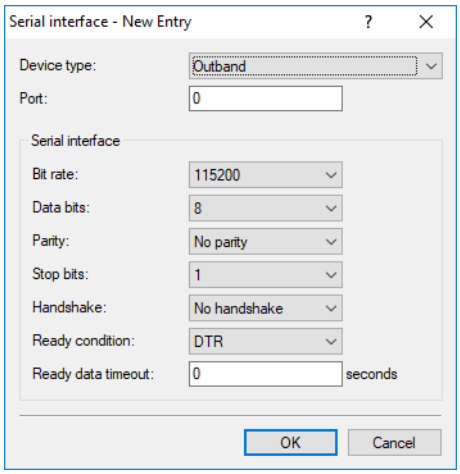
Operating

Activates the COM port server on the selected port of the selected interface.

6.19.4.2 COM-Port-Settings

This table contains the settings for data transmission over the serial interface.

Please note that all of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu.



LANconfig: **Miscellaneous Services** > **COM Ports** > **Serial interface**

Console: **Setup** > **COM-Ports** > **COM-Port-Server** > **COM-Port-Settings**

Device type

Selects a serial interface from the list of those available in the device.

Port

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

Bit rate

Bit rate used on the COM port.

Data bits

Number of data bits.

Parity

The checking method used on the COM port.

Stop bits

Number of stop bits.

Handshake

The data-flow control used on the COM port.

Ready condition

The ready condition is an important property of any serial port. The COM port server transmits no data between the serial port and the network if the status is not "ready". Apart from that, in the client mode the act of switching between the "ready" and "not-ready" states is used to establish and terminate TCP connections. The readiness of the port can be checked in two different ways. In DTR mode (default) only the DTR handshake is monitored. The serial interface is considered to be ready for as long as the DTR line is active. In data mode, the serial interface is considered to be active for as long as it receives data. If no data is received during the timeout period, the port reverts to its "not ready" status.

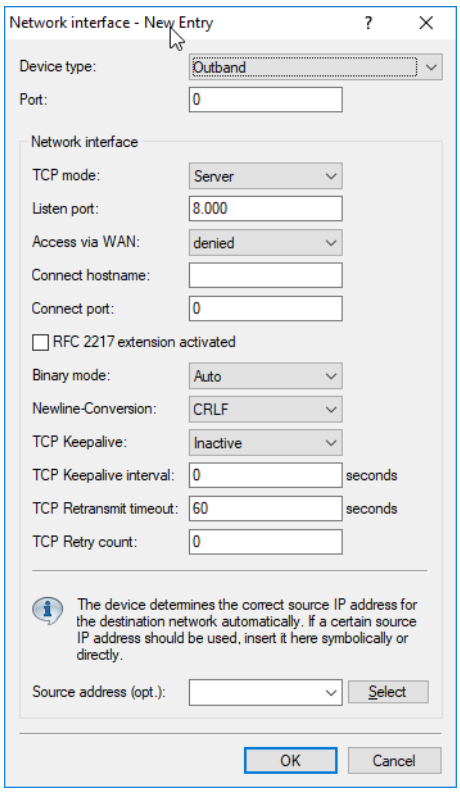
Ready data timeout

The timeout switches the port back to the not-ready status if no data is received. This function is deactivated when timeout is set to zero. In this case the port is always ready if the data mode is selected.

6.19.4.3 Network settings

This table contains all settings that define the behavior of the COM port in the network.

Please note that all of these parameters can be overwritten by the remote site if the RFC-2217 negotiation is active. Current settings can be viewed in the status menu.



LANconfig: **Miscellaneous services** > **COM ports** > **Network interface**

Command prompt: **Setup** > **COM-Ports** > **COM-Port-Server** > **Network-Settings**

Device type

Selects a serial interface from the list of those available in the device.

Port

Some serial devices such as the CardBus have more than one serial port. Enter the port number that is to be used for the COM port server on the serial interface.

TCP-Mode

Each instance of the COM port server in server mode monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused. In client mode, the instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable. In both cases a device closes any open connections when the device is restarted.

Listen port

The TCP port where the COM port in TCP server mode expects incoming connections.

Access via WAN

Access to this serial port from the WAN can be set to **allowed**. **denied** or **only via VPN**.

Connect hostname

The COM port in TCP client mode establishes a connection to this host as soon as the port is in the “Ready” state.

Connect port

The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in the "Ready" state.

RFC 2217 extension activated

The RFC2217 extension can be activated for both TCP modes. With this extension activated, the device uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extension with incompatible remote sites is not critical, although unexpected characters may be displayed at the remote site. A side effect of using the FRC2217 extension may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.

Binary mode

Serial data is forwarded in binary, i.e. there is no CR/LF (carriage return/line feed) translation.

Newline conversion

The Newline conversion setting specifies the character sequence sent to the serial port when a carriage return character is detected in non-binary mode. The default setting (CRLF) maps what was received over the TCP connection, but this is not necessarily suitable for all applications. For example, some Unix consoles interpret this sequence as an unwanted double-line return, so a single line feed (LF) or carriage return (CR) would be more appropriate. If the outband connection of another LANCOM device is connected to the serial port, both CRLF and CR will work, but not LF, because CR characters from the LANCOM device are used for the auto-bauding feature.

TCP keepalive

If activated, dummy packets are sent to the remote site at regular intervals. Although these packets have no payload, they prevent firewalls and NAT gateways from dropping the connection as it always appears to be active. In addition to RFC 1122, TCP keepalive offers three operating modes:

Inactive

No packets are sent during idle times.

Active

Packets are sent regularly, but the lack of response packets has no further impact. Connections to firewalls or NAT gateways are maintained. A complete termination of the TCP connection is not detected. This operating mode is recommended for server operation.

Proactive

The TCP stack additionally expects responses to its keepalive packets and will report a broken TCP connection if no response is received after multiple attempts. The number of attempts is the same as for the **TCP retry count**.

TCP keepalive interval

Here you specify how often the TCP stack transmits keepalive packets. A value of 0 uses the default internal value of 7200 seconds.

TCP retransmit timeout

The length of time after which a retransmission is started. Note that the time it takes for a connection to be recognized as broken includes the duration of all retransmissions.

TCP retry count

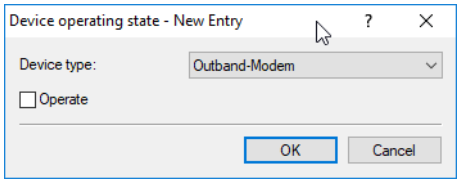
The total number of retransmissions is limited here. A repeat count of 0 specifies the default value of 5 retries.

Source address

The COM port can be reached at this address. This is its own IP address that is taken as the source address when establishing connections. This is used to define the IP route to be used for the connection.

6.19.5 WAN device configuration

The table with WAN devices is a status table only. All Hotplug devices (connected via USB or CardBus) are automatically entered into this table.



LANconfig: **Miscellaneous Services** > **COM Ports** > **Device operating state**

Console: **Setup** > **COM-Ports** > **WAN** > **Devices**

Device type

List of serial interfaces available in the device.

Operate

Status of connected device.

6.19.6 Serial connection status information

Various statistics and status values are recorded for every instance of the COM-port server. The serial port using the instance is indicated in the first two columns of the table—the values for device type and port number as entered during the configuration are displayed here.

6.19.6.1 Network status

Console: **Status** > **COM-Ports** > **COM-Port-Server** > **Network-Status**

This table contains information on current and recent TCP connections.

- Device type

  List of serial interfaces available in the device.

- Port number

  The port number used for the COM port server on the serial interface.

- Connection status

  Possible values:

  - Connected: An active connection exists (server or client mode).
  - Listening: This instance is working in server mode; no TCP connection is currently active.
  - Non-listening: In server mode, the specified TCP port could not be reserved for inbound connections, e.g. because it is already occupied by another application.
  - Blank: This instance is working in client mode and the port is not ready. No TCP connection will be established now.
  - Transfer: The port has reached the "ready" state; a connection is being established.

- Last error

In client mode this displays the reason for the last connection error. In server mode this value has no significance.

- Remote address

  Displays the IP address of the remote site for a successful TCP connection.

- Local port

  Displays the local TCP port used for a successful TCP connection.

- Remote port

  Displays the remote TCP port used for a successful TCP connection.

6.19.6.2 COM-port settings

This table displays the serial port status and the settings currently used by this port.

- Device type

  List of serial interfaces available in the device.

- Port number

  The port number used for the COM port server on the serial interface.

- Port status

  Possible values:

  - Not available: The serial port is currently not available to the COM port server, for example because the USB or CardBus adapter has been removed or because it is being used by other functions in the device.
  - Not ready: The serial port is available to the COM port server but is currently not ready for data transfer, for example because the DTR line is inactive. In the client state, no attempt is made to establish a connection as long as the port is in this state.
  - Ready: The serial port is available and ready for data transfer. In the client state, an attempt is made to establish a TCP connection as soon as the port is in this state.

  Please note that the port status is relevant in server mode, too. All TCP connection requests are accepted, although the COM port instance will only transfer data between the serial port and the network when the serial port has reached the "ready" state. The following columns display the settings that are currently in use on the serial port. These are either the values as configured or as set by the negotiations via the RFC2217 extensions.

- Bit-Rate

  Bitrate used on the COM port

- Data bits

  Number of data bits.

- Parity

  The checking method used on the COM port.

- Stop bits

  Number of stop bits.

- Handshake

  The data-flow control used on the COM port.

6.19.6.3 Byte counters

This table displays the inbound and outbound data packets at the serial port and on the network side.

These values are not reset when the connection is opened or closed.

- Device type

  List of serial interfaces available in the device.
- Port number

  The port number used for the COM port server on the serial interface.
- Serial-Tx

  Number of bytes sent over the serial interface.
- Serial-Rx

  Number of bytes received over the serial interface.
- Network Tx

  Number of bytes sent to the network.
- Network Rx

  Number of bytes received from the network.

6.19.6.4 Port errors

This table displays the serial port errors. These errors may indicate a faulty cable or errors in the configuration.

- Device type

  List of serial interfaces available in the device.
- Port number

  The port number used for the COM port server on the serial interface.
- Parity errors

  Number of errors due to a checksum mismatch.
- Framing errors

  Number of erroneous data packets.

6.19.6.5 Connections

This table displays successful and failed TCP connections in both server mode and client mode.

- Device type

  List of serial interfaces available in the device.
- Port number

  The port number used for the COM port server on the serial interface.
- Server granted

  Number of connections granted by the COM port server.
- Server rejected

  Number of connections rejected by the COM port server.
- Client succeeded

  Number of connections successfully established by the COM port client.
- Client DNS error

Number of connections that the COM port client could not establish due to DNS errors.

- Client TCP error

  Number of connections that the COM port client could not establish due to TCP errors.

- Client remote disconnects

  Number of connections where the COM port was disconnected from the remote site.

6.19.6.6 Delete values

This action deletes all values in the status tables.

6.19.7 COM-port adapters

Devices with serial interfaces can be connected to a device in the following ways:

Adapters	Devices
COM-port adapters	All those with a serial configuration interface
USB serial adapter	All those with a USB interface

The COM port adapter must be a two-way D-sub plug with the following PIN assignment:

Pin	Signal	Signal	Pin
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

6.20 IGMP / MLD snooping

6.20.1 Introduction

All devices with wireless LAN interfaces feature a “LAN bridge”, a software entity for transferring data between the Ethernet ports and the WLAN interface(s). In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets precisely to the port which the relevant user is connected to. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. This means that a switch can only deliver a packet precisely if the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being “flooded” to all ports.

This may be the correct action for broadcasts which are supposed to reach all available receivers, but this may not be the case for multicasts. Multicasts are generally aimed at a certain group of receivers within a network, but not all of them:

- For example, video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field rely on multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the device will have ports to which no multicast recipients are connected. This "unnecessary" transmission of multicasts to ports without any receivers is not an error, but it can compromise overall performance.

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines the protocol Internet Group Management Protocol (IGMP) for IPv4 and Multicast Listener Discovery (MLD) for IPv6 that allow network stations to inform their router that they wish to receive certain IP multicasts. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP and MLD makes use of Join messages and Leave messages to register and de-register respectively.

Information about which multicast groups a station can or should join are available from other protocols than IGMP/MLD.

As layer-3 protocols, IGMP and MLD only manage IP subnets according to the multicast group memberships. However, network devices such as bridges, switches or WLAN access points only forward the packets on layer 2, meaning that IGMP and MDL themselves do not help in any way to further guide multicast traffic through these structures. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for distributing multicasts. IP multicasts only need to be forwarded to an interface where a router is located that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets. This method is referred to as IGMP snooping with IPv4 and MLD snooping with IPv6. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

To continue describing the functions of IGMP/MLD snooping in LCOS, we have to differentiate between two important terms:

- A port is "member of a multicast group" if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP or MLD snooping or configured manually.
- A port is a "router port" if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

6.20.2 IGMP/MLD snooping operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the receiver.

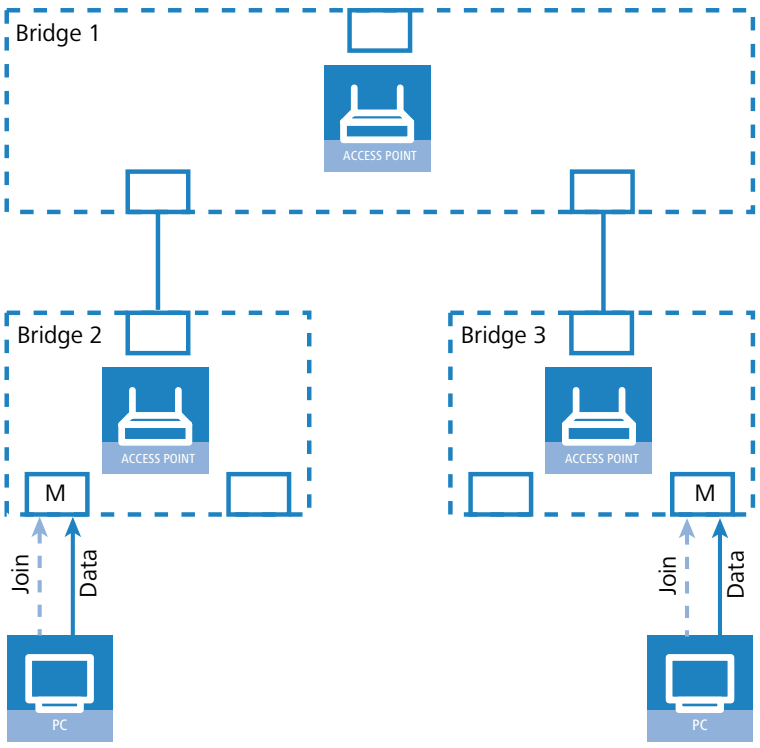
Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are dropped entirely):

- IGMP/MLD messages are handled in different ways depending on their content:
  - A Join message results in the incoming port becoming member of the respective multicast group. This message is forwarded to router ports only.
  - Leave messages are ignored as the IGMP/MLD snooping in LCOS is passive. This means that Joins only disappear from the table by aging.
  - An incoming IGMP/MLD query results in the port being marked as a router port. These messages are flooded to all interfaces.
  - All other IGMP/MLD messages are flooded to all interfaces—no ports experience a change of state.

- If an IP multicast packet does not contain an IGMP/MLD message, the IP destination address is examined. Packets for the destination address "224.0.0.x" (IPv4) or "FF02::1" (IPv6) are flooded to all ports because this "reserved" range is used by protocols without proper IGMP/MLD registration. For all other packets the destination address is looked up in the IGMP/ MLD membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be dropped, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

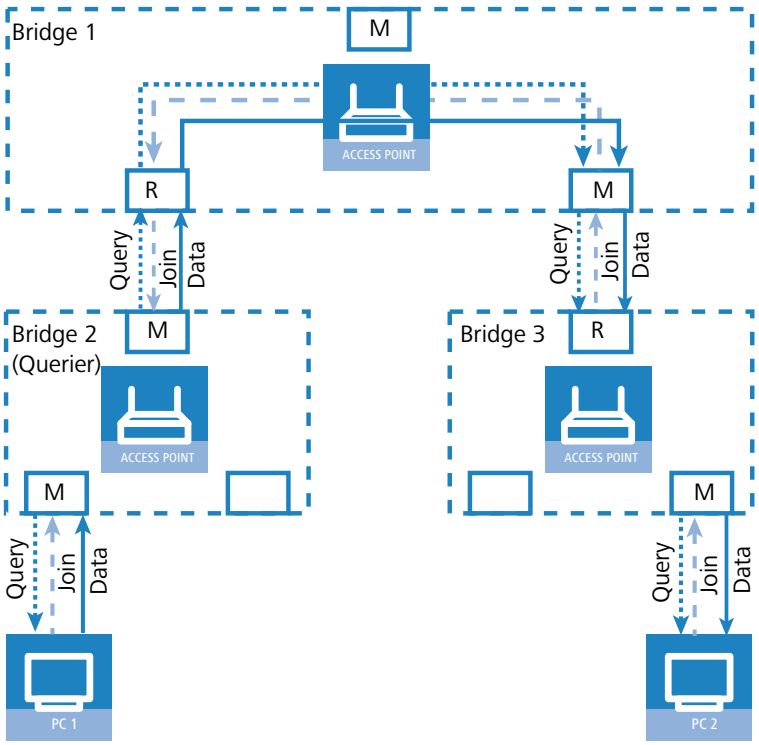
6.20.3 IGMP/MLD snooping through multiple bridges

As described, IGMP/MLD snooping only forwards incoming Join or Leave messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this phase, so the Join messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.



Consequently, bridges must have router ports in order for membership information to be propagated. Since the ports of a bridge only become router ports in the case of IGMP/MLD queries, one of the multicast-capable routers in the network must take over the task of distributing the necessary IGMP/MLD queries throughout the network. This router is referred to as the IGMP/MLD querier. If the network does not contain a multicast router, the access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP/MLD information by the querier can be explained with the following example:

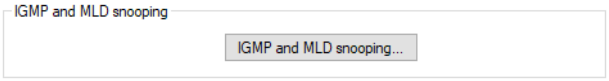
1. The querier (Bridge 2 in this example) regularly sends out IGMP/MLD queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).
2. In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).
3. The station (PC2) connected to Bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).
4. Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.
5. In the final step, Bridge1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.

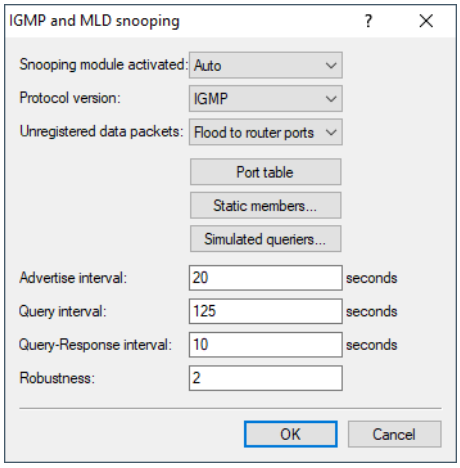


If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

6.20.4 Configuration

In LANconfig, IGMP/MLD snooping are configured under **Interfaces** > **Snooping** > **IGMP and MLD snooping**





Snooping module activated

Activates or deactivates IGMP/MLD snooping in the device and all of the defined querier instances. Without IGMP/MLD snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

Possible values:

- On
- Off
- Automatic

Default:

- Automatic

In the setting **automatic** the bridge enables IGMP/MLD snooping only if there are queriers in the network.

If this function is deactivated, the bridge sends all IP multicast packets on all ports. With a change of the operating mode, the bridge completely resets the IGMP/MLD snooping function, i.e. it deletes all dynamically learned values (memberships, router-port properties).

Protocol version

Specify the supported protocols: IGMP, MLD, or both.

Unregistered data packets

This setting defines the handling of multicast data packets with a destination address outside of the reserved ranges “224.0.0.x” (IPv4) and “FF02::1” (IPv6), for which neither static memberships were defined nor were dynamic memberships learned.

Possible values:

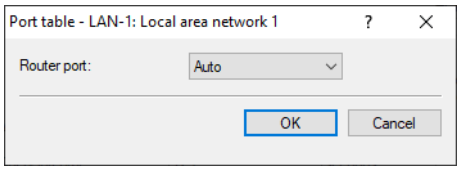
- Flood to router ports only: Sends these packets to all router ports.
- Flood to all ports: Sends these packets to all ports.
- Discard: Discards these packets.

Default:

- Router-Ports-only

Port table

This table is used to define the port-related settings for IGMP/MLD snooping.



Port

The port for which the settings apply.

Possible values:

- Selects a port from the list of those available in the device.

Default:

- N/A

Router port

This option defines the port's behavior.

Possible values:

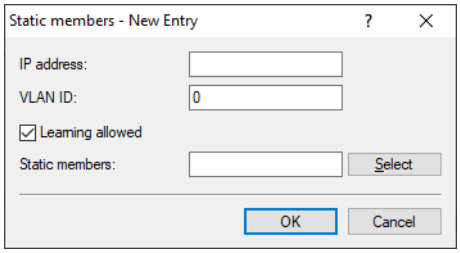
- Yes: This port will always work as a router port, irrespective of IGMP queries or router messages that the bridge receives on this port.
- No: This port will never work as a router port, irrespective of IGMP queries or router messages that the bridge receives on this port.
- Automatic: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if the bridge receives no packets on this port for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

Default:

- Automatic

Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



IP address

The IP address of the manually defined multicast group.

Possible values:

- Valid IP multicast address.

VLAN ID

The VLAN ID used by the bridge to apply this static membership. For each IP multicast address you can make multiple entries with different VLAN IDs.

Possible values:

- 0 to 4096.

Default:

- 0

Special values:

- If "0" is selected as VLAN, the IGMP/MLD queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Learning allowed

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, packets can only be sent via the ports which have been manually defined for the multicast group.

Static members

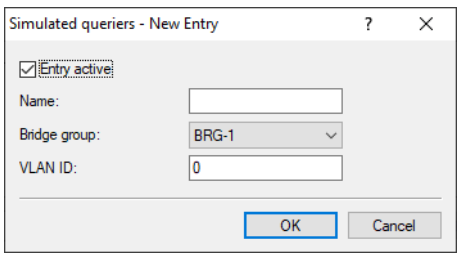
The bridge always delivers the packets with the corresponding IP multicast address to these ports, irrespective of any Join messages received.

Possible values:

- Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP/MLD snooping functions are required but there is no multicast router in the network. The querier can be restricted to certain bridge groups or VLANs if you define multiple independent queriers which support the corresponding VLAN IDs.



Entry active

Activates or deactivates the querier instance

Name

Name of the querier instance

Possible values:

- 8 alphanumerical characters.

Bridge group

Limits the querier instance to a certain bridge group.

Possible values:

- Select from the list of available bridge groups.
- None

Default:

- BRG-1

Special values:

- If the bridge group is set to “none”, the bridge outputs the IGMP/MLD queries to all bridge groups.

VLAN ID

Limits the querier instance to a certain VLAN.

Possible values:

- 0 to 4096

Default:

- 0

Special values:

- If “0” is selected as the VLAN ID, the bridge outputs IGMP/MLD queries without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Advertise interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP/MLD snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP/MLD queries.

Possible values:

- 4 to 180 seconds

Default:

- 20 seconds

Query interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP/MLD queries to the multicast address `224.0.0.1` (IPv4) “or FF02::1” (IPv6), so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which memberships “age”, expire, and are deleted.

- After the startup phase, the querier sends IGMP/MLD queries in this interval.
- A querier returns to the querier status after a time equal to “Robustness*Query-Interval+(Query-Response-Interval/2)”.
- A port loses its router-port status after a time equal to “Robustness*Query-Interval+(Query-Response-Interval/2)”.

Possible values:

- 10-figure number greater than 0.

Default:

- 125

The query interval must be greater than the query response interval.

Query-Response-Interval

Interval in seconds influencing the timing between IGMP/MLD queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP/MLD queries. These regular queries influence the time in which memberships "age", expire, and are then deleted.

Possible values:

- 10-figure number greater than 0.

Default:

- 10

The query response interval must be less than the query interval.

Robustness

This value defined the robustness of the IGMP/MLD protocol. This option tolerates packet losses of IGMP/MLD queries with respect to Join messages.

Possible values:

- 10-figure number greater than 0.

Default:

- 2

6.20.5 IGMP/MLD status

6.20.5.1 General statistics

The status messages for IGMP/MLD snooping are available here:

Command prompt: **Status** > **LAN-Bridge** > **IGMP-Snooping**

- Operating

  Indicates whether IGMP/MLD snooping is activated or deactivated.

- IPv4 packets

  Shows the number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.

- IPv6 packets

  Shows the number of IPv6 multicast packets received at all ports, whether they were MLD packets or not.

- Data packets

  Shows the number IP multicast packets received at all ports and which were not IGMP/MLD packets.

- Control packets

  Shows the number of intact IGMP/MLD packets received at all ports.

- Bad packets

  Shows the number of damaged data or IGMP/MLD packets received at all ports. Possible causes for damage to packets may be IP checksum errors or truncated packets.

For performance reasons, IP checksums are evaluated for IGMP/MLD packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- Delete values

  This action deletes all statistical entries.

6.20.5.2 Port status

This table shows all port-related statistics.

Command prompt: **Status** > **LAN-Bridge** > **IGMP-Snooping** > **Port-Status**

- Router port

  Shows whether the port is currently in use as a router port or not, irrespective of whether this status was configured statically or learned dynamically.

- IPv4 packets

  Shows the number of IPv4 multicast packets received on this port, whether they were IGMP packets or not.

- IPv6 packets

  Shows the number of IPv6 multicast packets received on this port, whether they were MLD packets or not.

- Data packets

  Shows the number IP multicast packets received on this port and which were not IGMP/MLD packets.

- Control packets

  Shows the number of intact IGMP/MLD packets received on this port.

- Bad packets

  Shows the number of damaged data or IGMP/MLD packets received on this port. Possible causes for damage to packets may be IP checksum errors or truncated packets.

For performance reasons, IP checksums are evaluated for IGMP/MLD packets only and not for the data portion of multicast packets. This is why packets with a faulty checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

6.20.5.3 Groups

This table displays all the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries.

Command prompt: **Status** > **LAN-Bridge** > **IGMP-Snooping** > **Groups**

- Address

  Shows the group's IP multicast address.

- VLAN-ID

  Shows the VLAN ID that this entry applies to.

- Allow-Learning

  Shows whether new memberships for this group can be learned dynamically or not.

- Static members

  Shows the list of statically defined members for this group.

- Dynamic members

Shows the list of dynamically learned members for this group.

6.20.5.4 Simulated queriers

This table shows the status of all defined and active IGMP / MLD querier instances.

- Name

  Shows the name of the multicast group.

- Bridge group

  Shows the bridge group that this entry applies to.

- VLAN-ID

  Shows the VLAN that this entry applies to.

- Status

  Shows the current status of the entry.

  - Initial: The querier instance has just started and is sending IGMP/MLD queries in short intervals (four-times faster than the query interval defined).
  - Querier: The querier instance considers itself to be the active querier and is sending IGMP/MLD queries in the defined query interval.
  - Non-querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP/MLD queries.

6.21 eSIM

To gain access to mobile networks, mobile network operators (MNOs) issue so-called SIM cards (Subscriber Identity Module Cards) to their customers. Each MNO issues its own SIM cards per customer. SIM cards consist of a plastic carrier and a security chip with security keys that grant access to the mobile network. If a customer wanted to change operators, the old SIM card had to be replaced with a new SIM card from the new MNO in the device. SIM cards are usually sent by the MNO via postal mail, which the customer receives a few days after signing the contract.

An eSIM is, simply put, the digital version of the classic SIM card. It consists of a chip (e.g., in the M2FF form factor) that is permanently installed in the mobile phone or router, and a solution for managing mobile profiles, referred to as eUICC (embedded Universal Integrated Circuit Card). eUICC functionality can be provided in different form factors. In the following, the terms eSIM and eUICC are used synonymously for simplicity.

Basically, three different types or solution architectures of eSIMs exist:

1. M2M eSIM: Machine-to-Machine (M2M) eSIMs are designed for machines and device types without a user interface or user interaction on the device. M2M eSIMs are centrally managed by a management portal or provisioning system and can be transferred to the end device over-the-air (OTA) via SMS. Typically, these are closed systems provided by solution vendors for customers with many end devices. M2M eSIMs are specified according to the SGP.02 standard.
2. Consumer eSIMs: Consumer eSIMs are issued by MNOs and are used in mobile phones, smartwatches, or routers. Typically, the MNO supplies a QR code or activation code that the customer can use to install the eSIM or profile on the device. Closed or proprietary provisioning systems also exist from certain smartphone manufacturers, enabling the MNO to notify the customer that the eSIM is ready for download. Unlike the M2M eSIM, the end customer must initiate the installation of the eSIM. End devices have software called the Local Profile Assistant (LPA), which establishes encrypted communication between the embedded eSIM/mobile chip and the MNO's system. Downloading the eSIM profile always requires an existing internet connection, e.g., through the phone's integrated WLAN. Consumer eSIMs are defined in the SGP.22 standard.

3. IoT eSIM: IoT eSIMs are designed for a large number of IoT devices and combine part of the LPA functionality on the device with a server for managing the eSIMs. IoT eSIMs are defined in the SGP.32 standard and are the newest of the solution architectures.

LANCOM routers include an eSIM chip in the M2FF form factor with eUICC functionality. This is a consumer eSIM according to the SGP.22 standard. This solution is compatible with common eSIMs issued by MNOs for mobile phones. The eSIM can be used with all mobile profiles for consumer eSIMs according to the SGP.22 standard and is not technically restricted. In principle, eSIMs must be supported by the MNO and must not be limited to specific devices or device types.

As of LCOS 10.94, LANCOM routers support, in addition to classic plastic SIM cards, an eSIM solution in cellular routers. Several prerequisites are required:

1. At least LCOS 10.94 firmware
2. Cellular router with integrated on-board eSIM chip
3. Possibly an update of the WWAN firmware to the minimum version supporting eSIM functionality

The general process of installing an eSIM on a LANCOM router is as follows:

1. Sign a mobile contract with an MNO.
2. The MNO supplies a QR code or activation code (both contain the same information, just in different formats) for the eSIM.
3. The activation code is entered via WEBconfig or the router's command line. The router then downloads the corresponding profile from the MNO's server via an existing internet connection (e.g., DSL or fiber) to the integrated chip. The profile is stored permanently in the chip. The activation code contains both the server URL and a code for retrieving the eSIM.
4. The successfully downloaded eSIM is configured in the router's WWAN profile table for use.

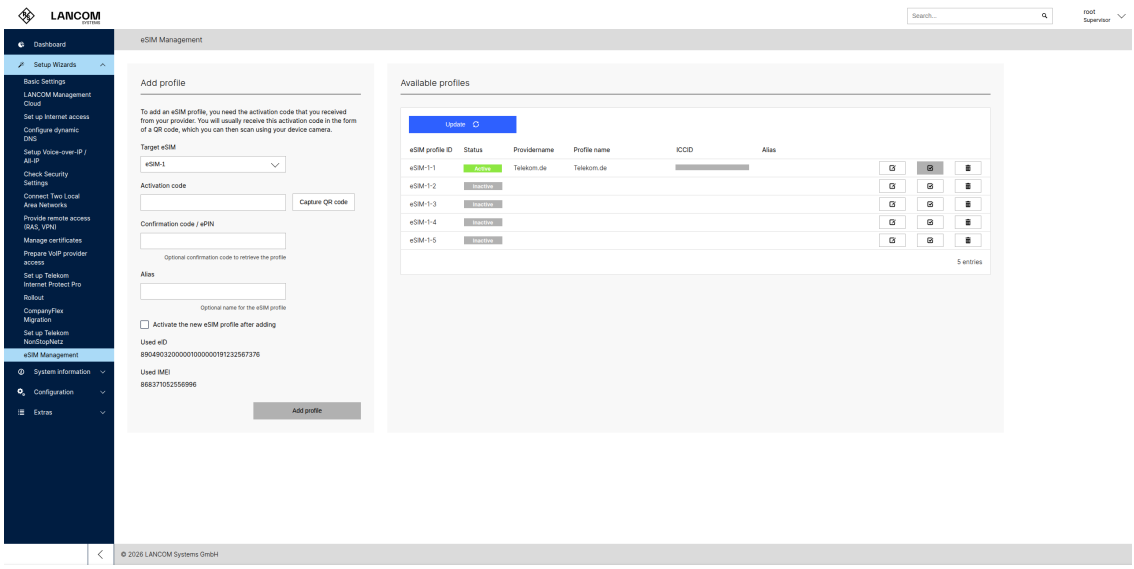
To download the eSIM, the router requires an existing internet connection, e.g., via DSL or fiber, similar to a mobile phone that requires a WLAN connection. It is technically not possible to download the eSIM via the same device's WWAN modem, as the eSIM installation process is an exclusive, continuous operation in the mobile chip and the router must switch access from the physical SIM card to the eSIM during this process.

Further notes on usage:

- Up to eight eSIM profiles can be stored on the integrated eSIM
- eSIMs can be installed and managed via WEBconfig or CLI commands
- An optional GSMA test profile, if present on the eSIM, can be safely deleted and serves to simplify testing for MNOs, developers, or certification/test procedures
- The eSIM is implemented as a "virtual SIM slot" that can hold up to eight profiles
- Only the active eSIM profile is used when the eSIM is referenced as "eSIM-1" in the SIM slot configuration
- If the internal cellular modem is unavailable, the eSIM management cannot be accessed
- A device reset is not a secure method for deleting eSIM profiles, as it cannot be guaranteed that the modem has access to the eSIM at that moment
- To securely delete eSIMs, the profiles must be manually removed via eSIM management. If this is not possible, the corresponding eSIM profile can, as a last resort, be disabled by the MNO, as is already the case with physical SIM cards
- eSIMs can generally only be downloaded once and cannot be re-downloaded. eSIMs must explicitly be re-enabled by the MNO for download.
- Downloaded eSIMs are permanently tied to the embedded chip and cannot be transferred between different devices.

6.21.1 Configuration

In the device's WEBconfig, open the section **Add profile** under **Setup Wizards** > **eSIM Management**.



Target eSIM

Select the desired target eSIM, e.g., eSIM-1.

Activation code

Insert here the eSIM activation code provided by your mobile network operator (MNO), e.g., `LPA:1$prov.example.com$ABCDEFGH12345`.

This is the so-called LPA string ("Local Profile Assistant" string). It is a character string that contains the address of the SM-DP+ server (Server for Profile Management) and an activation code to manually install an eSIM profile on a device. It is identical to the content of the QR code. The string follows the format LPA:1$SM-DP+address$activation-code and is used by the LPA in the device to download and install the eSIM profile from the SM-DP+ server over an existing Internet connection.

The activation code can either be entered as text or scanned from a QR code if the device has a camera.

Confirmation code / ePIN

Optional confirmation code that is entered together with the activation code. Some MNOs refer to this as an ePIN. The code is provided by your mobile network operator along with the QR code/activation code.

Alias

The alias is an optional label for the eSIM profile. It allows easier identification of the profile in the profile table.

Used eID

Displays the eID (Embedded Identity Document). The eID is the globally unique identifier of the eSIM installed in the device. This information is for reference only.

Used IMEI

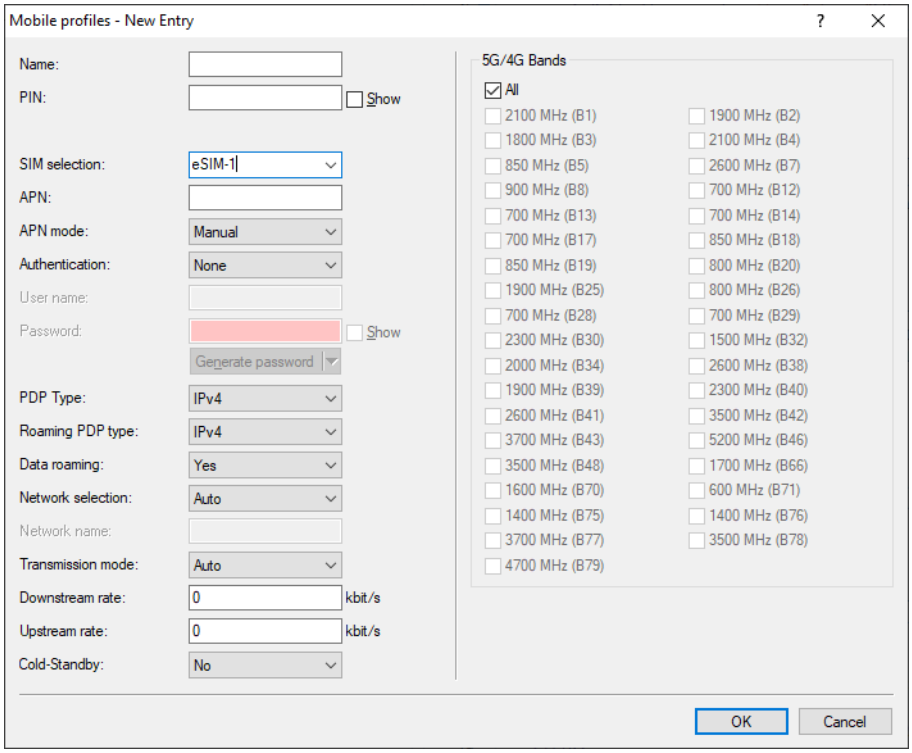
Displays the IMEI (International Mobile Equipment Identity). The IMEI is a 15-digit number assigned to your LANCOM cellular router that uniquely identifies it worldwide. This information is for reference only.

Section “Available profiles”

This area displays the eSIM profiles stored on the local device. In principle, only one eSIM profile out of a maximum of eight profiles can be active at any one time. The active profile can be used as “eSIM-1” in the SIM selection of the WWAN profile configuration. The three icons on the right-hand side allow the actions “Edit profile”, “Activate profile”, and “Delete profile”.

Assign WWAN profile in LANconfig

In LANconfig, open **Interfaces** > **WAN** > **Mobile settings** > **Mobile profiles**.



SIM selection

Defines the SIM slot or eSIM of the device to be used. Possible values (depending on the device):

- SIM-1 (Default): first SIM slot in the device
- SIM-2: second SIM slot in the device
- eSIM-1: embedded eSIM in the device. The currently active profile configured in WEBconfig is used.
- Iccid:<iccid of the SIM card or eSIM profile>: With this value, the SIM card or eSIM profile can be explicitly selected via the unique ICCID (Integrated Circuit Card Identifier). The ICCID of the installed eSIM profiles can be found in the eSIM management section of WEBconfig.

6.21.2 CLI Configuration

In addition to management via WEBconfig, eSIMs can also be managed via the command line. This allows eSIM profiles to be downloaded or deleted.

Under **Status** > **Modem-Mobile** > **eSIM** you will find the status table **eSIM Profiles**, which displays the currently installed eSIMs.

You will also find the actions Change-Alias, Enable-Profile, Disable-ProfileDelete-Profile, and Download-Profile here.

Change-Alias

This command allows you to change the alias or user-defined label of the eSIM.

Usage: do Change-Alias "<eSIM Profile ID>" "<New alias>"

Enable-profile

Use this command to enable the profile.

Usage: do Enable-Profile "<eSIM Profile ID>"

Disable-profile

Use this command to disable the profile.

Usage: do Disable-Profile "<eSIM Profile ID>"

Delete-Profile

This command allows you to delete an eSIM profile.

Usage: do Delete-Profile <eSIM Profile ID>

Download-Profile

This command allows you to download an eSIM profile.

Usage: do Download-Profile [Option]... "<eSIM activation code>"

Options:

- -a "<Alias>" – Set alias for the profile after download
- -c "<Confirmation code>" – Provide confirmation code
- -s "<Target SIM>" – Set target SIM (Default: eSIM-1)

6.22 Configuring WWAN access

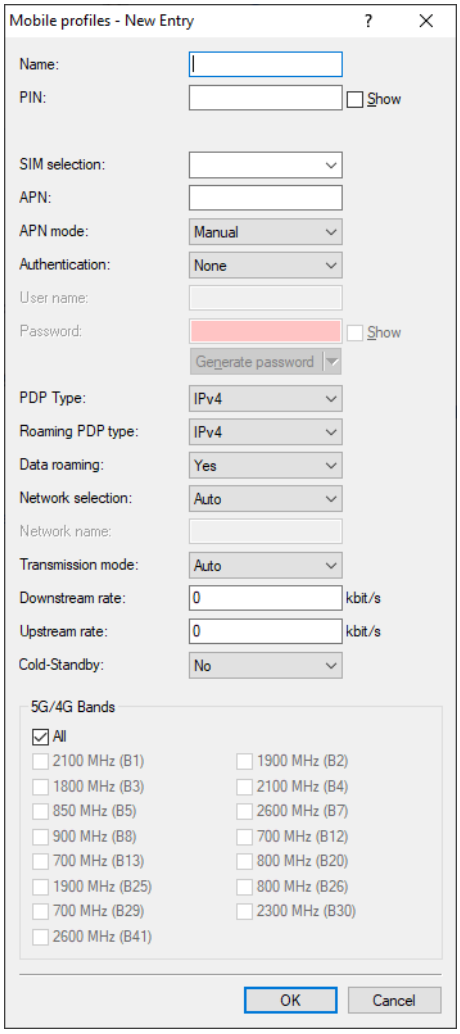
The following tutorial shows how you manually configure devices with an internal cellular modem to use access via mobile networks (WWAN). First you either create a mobile profile for your provider or edit an existing profile, and then you assign this profile to the WAN interface of the device.

Alternatively, a simpler and faster way of configuration is available with a Setup Wizard (**Set up Internet access**).

This also provides the option for you to specify the generation descriptions for the cellular standards, and have them displayed.

1. In LANconfig, open the configuration dialog for your device and navigate to the section **Interfaces** > **WAN**.
2. Select an existing profile to be edited or add a new profile for your provider in the **Mobile profiles** table.

In the interests of completeness this tutorial explains the creation of a new profile.



3. Under **Name**, enter the same name as the remote station for the mobile profile.
4. Under **PIN** enter the 4-digit PIN of the mobile phone SIM card. The device needs this information to operate the mobile modem.

   The SIM card logs every failed attempt with an incorrect PIN. The number of failed attempts remains stored even when the device is temporarily disconnected from the mains. After 3 failed attempts, the SIM card is locked from further access attempts. If this occurs, you usually need the 8-digit PUK or SuperPIN to unlock it.

5. If your device accommodates several SIM cards, use **SIM slot** to select the SIM card that you want to associate with this profile.

   The item **Profile disabled** switches this mobile profile off. This option is useful if you wish to create a profile template only and complete the mobile setup at a later time.

   Only enabled profiles are visible for selection in LANmonitor.

6. Under **APN**, enter the name of the access server for the data services of your mobile provider.
   The APN (access point name) is specific to each mobile phone provider. You will usually find this information in the documentation provided with your mobile phone contract.
7. Specify under **Authentication** whether authentication is required for logging in to the APN. Possible values: None, PAP, CHAP.

8. If necessary, enter the APN login credentials under **User name** and **Password**.
9. Under **PDP type** you specify the type of the PDP context for the mobile profile.
   The PDP context describes the support of the address spaces which the backbone of the corresponding cellular network provider offers for connections from the cellular network to the Internet. This can be either IPv4 or IPv6 alone, or can include support for both address spaces (dual stack). Clients that want to use the corresponding cellular network provider must support at least one of the specified address spaces.
10. Set the preferred **Network selection** mode:

Automatic

The cellular modem automatically logs into the mobile network that it last used successfully. If the device fails to login, the mobile interface automatically logs in to the home network (HPLMN) stored on the SIM card.

If the cellular modem is also unable to login to the home network stored on the SIM card, a PLMN list of preferred roaming partners on the SIM card is processed in sequence with attempted logins. The mobile interface then connects to the first available cellular network, regardless of the signal quality.

If none of the above networks is available, one of the available PLMN networks with a "good" signal quality is selected at random: Failing this, the PLMN networks with a sufficient signal quality are processed, in the descending order of signal quality.

As soon as the login process succeeds, the network will be used. There is no change of network unless a loss of connection occurs. The provider can however trigger a change of the cell and the access mode, if it considers this to be appropriate.

Manual

The cellular modem connects to the mobile phone network specified under **Network name** only.

Manual mobile network selection is especially suitable when the device is in stationary operation and you wish to prevent it from connecting to another undesirable or more expensive mobile phone network.

If the manually set mobile network is not available, no connection will be established because the cellular modem only ever logs in to the manually specified network.

With the setting **Manual** and the field **Network name** empty, following a scan, the CLI command

```
do /Status/Modem-Mobile/Scan-Networks -s
```

enters the best network found into the field **Network Name**.

Semi automatic

With this method, the cellular modem initially logs in to the mobile network that is entered into the field **Network Name**. If the device fails to login, the cellular modem logs on to the home network (HPLMN) stored on the SIM card.

If the HPLMN is not available, then a method analogous to automatic network selection is used, whereby the device attempts to connect to the "operator controlled PLMN selector" (roaming partner), a randomly chosen good network, or the best weak network (in that order).

By quality

Using a scan manually initiated in LANmonitor or from the command line, the cellular modem searches for all available cellular networks and logs into the one with the best signal quality. If this login process fails, the cellular interface uses the **semi-automatic** network selection.

CLI commands

`do /Status/Modem-Mobile/Scan-Networks -s -f`

This command initially disconnects any existing cellular WAN connection, it then performs an extended scan and the best network is selected and stored to the configuration.

This command is available in combination with **semi-automatic** and **manual** network selection. The stored network is also valid after restarting the device (cold/warm boot) until "Scan-Networks -s / -e" is executed, for all modes except **automatic**. The results of the scan can be viewed under **Status** > **Modem-Mobile** > **Network-List**.

`do /Status/Modem-Mobile/Scan-Networks -e -f`

This command initially disconnects any existing cellular WAN connection and it then performs an extended scan. The parameter -e ensures that the best network found is used, but it is not entered into the configuration. However, the entry is made in the status tree.

`do /Status/Modem-Mobile/Scan-Networks -s`

This command performs a network scan only when the WWAN connection is inactive.



A manual scan can be performed on a regular basis and automatically by making an entry in the cron table on the LANCOM router. Enter the command

`do /Status/Modem-Mobile/Scan-Networks -s -f`

into the configuration dialog.

LANmonitor

In LANmonitor, you perform the scans mentioned above by right-clicking with the mouse on the Network list and selecting the desired operation from the context menu. The scanning method **Disconnect and use best network** is the most effective.

11. If you have selected manual network selection, enter the exact name of your desired network under **Network name**.
12. Specify the preferred transfer mode within the mobile network under **Transmission mode**:

Automatic

Automatic selection of transmission mode

LTE(4G)+UMTS(3G)

Combined LTE-UMTS operation

LTE(4G)+GPRS(2G)

Combined LTE-GPRS operation

LTE(4G)

LTE operation only

UMTS(3G)+GPRS(2G)

Combined UMTS-GPRS operation

UMTS(3G)

UMTS operation only

GPRS(2G)

GPRS operation only

13. Under **Downstream rate** and **Upstream rate** you specify the transfer rates for the mobile phone connection. This is important for the QoS (quality-of-service) feature and the functioning of the firewall.
    If the value is set to `0`, the mobile interface in the corresponding direction is considered to be unlimited and the QoS mechanisms will not take effect.
14. Under **Cold-Standby**, specify whether the cellular modem should be logged into the cellular network in the non-backup case. If "Yes" is selected, the cellular modem is not logged into the cellular network in the non-backup case. In the backup case, it takes correspondingly longer for the module to establish a complete backup connection. This function is only supported in connection with the use of the backup table. This function has no effect or is not possible when using administrative distances, because there the WWAN modem has always established an active data connection. Default: No.
15. If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result. The selection under **LTE bands** allows you to control which frequency bands are used by the mobile modem.

    All

    All frequency bands are enabled.

    2100 MHz (B1)

    2.1GHz band is enabled.

    1800 MHz (B3)

    1.8GHz band is enabled.

    2600 MHz (B7)

    2.6GHz band is enabled.

    900 MHz (B8)

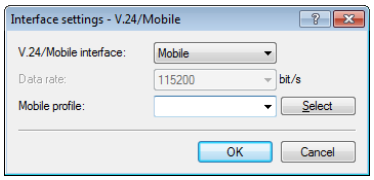
    900MHz band is enabled.

    800 MHz (B20)

    800MHz band is enabled.

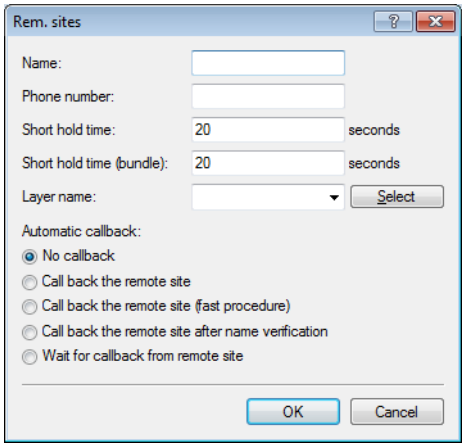
    This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

16. Click **OK** to save the settings.
17. In the dialog **Interfaces** > **WAN**, click **Interface settings** and select **V.24/Mobile**.
18. Set the **V.24/Mobile interface** to **Mobile**.
19. Under **Mobile profiles**, select the profile you created earlier for your mobile phone provider.



20. Click **OK** to save the settings.

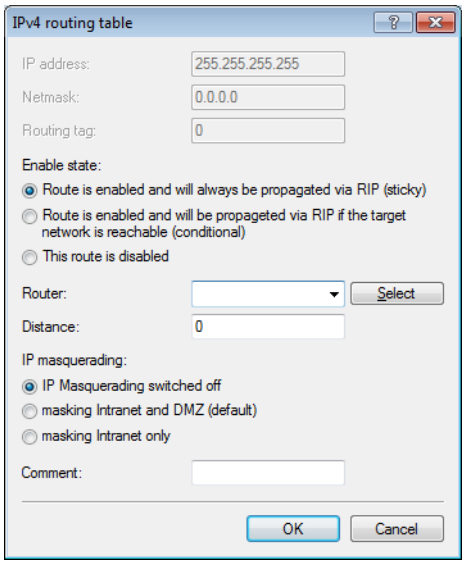
21. In the view **Communication** > **Remote sites**, click **Rem. (Mobile /...)** and add a new profile.



22. Under **Name**, enter the same name as the mobile profile.
23. Under **Phone number**, enter the dial-in number of your mobile phone provider. If your provider has not given you a dial-in phone number, enter `*99#`.
24. Under **Short hold time**, enter the time after which the device disconnects from the remote site if no packets are transmitted

    Enter a value in seconds to find a balance between the costs arising from idle time those of connection establishment, for example `300`. A value of `0` causes the device to stay connected until it is broken and terminated. With a value of `9999` the device automatically reconnects every time.

25. For **Layer name** select the presetting `WWAN`.
26. Click **OK** to save the settings.
27. In the view **IP Router** > **Routing**, click **IPv4 routing table** and add the **Default route** (`255.255.255.255`).



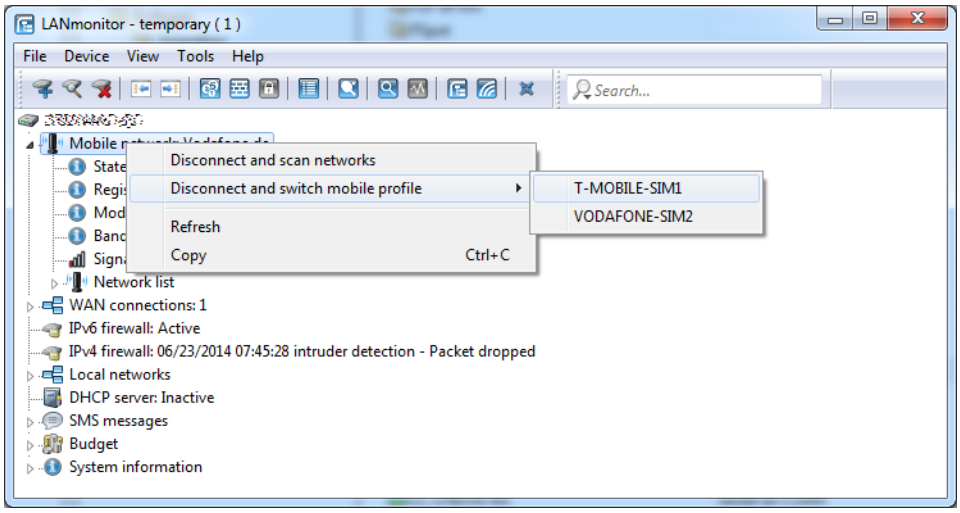
28. Under **Router**, select the profile created earlier under **Rem. sites (Mobile /...)**.
29. Set the **IP masquerading** to **Masking intranet and DMZ (default)**.
30. Click **OK** to save the settings.
31. Write the changes back to the device.

This concludes the configuration of the WWLAN access.

6.23 Switching between mobile profiles or SIM cards

If you have created different mobile profiles for a SIM card or one mobile profile for several SIM cards, LANmonitor allows you to toggle between these profiles or SIM cards. The following steps show you how to select an alternate profile or an alternate SIM card.

1. Select your device in LANmonitor.
2. On the entry **Mobile network**, open the context menu and select the option **Disconnect and switch mobile profile**.



3. Select the mobile profile that you want to switch to.

The device then disconnects from the mobile network and reconnects using the selected mobile profile.

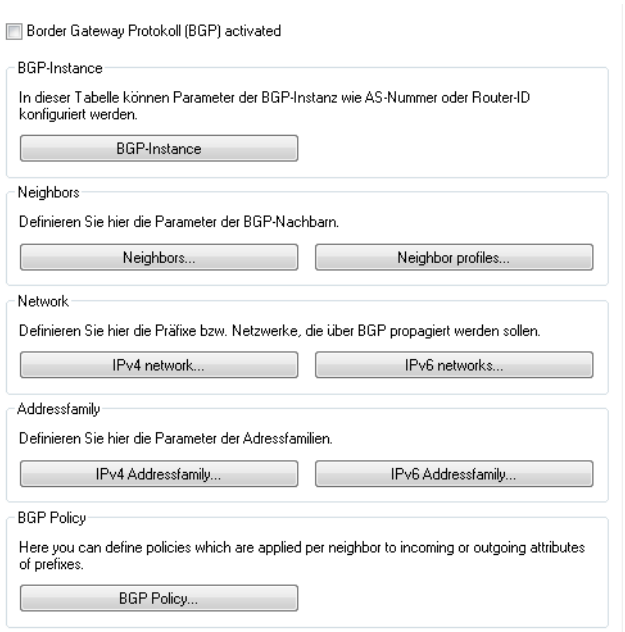
6.24 BGPv4

6.24.1 Border Gateway Protocol version 4 (BGPv4)

The network of a network provider is also referred to as an "autonomous system" (AS). The Border Gateway Protocol version 4 (BGPv4) is used to exchange routing information between autonomous systems (eBGP: external BGP) and to re-distribute this information to the routers of your own AS (iBGP: internal BGP).

6.24.1.1 Configuring BGPv4 with LANconfig

In order to configure BGPv4 with LANconfig, navigate to the **Routing protocols** > **BGP** menu.



Enabling BGP

To activate the BGP function, set a check mark for **Border Gateway Protocol (BGP) active**.

BGP instance

LCOS associates the BGP configuration of the BGP router with what is known as a **BGP instance**. This BGP instance contains the AS number and the router ID, among other things.

Currently LCOS supports only one BGP instance at a time.

Neighbors

The term **Neighbors** refers to the BGP gateways of other autonomous systems. These autonomous systems do not have to be immediate neighbors, although they must be known to at least one neighboring BGP gateway.

Neighbor profiles offer a convenient way to configure the BGP neighbors.

Networks

The BGP router propagates its managed networks to the BGP neighbors.

Address families

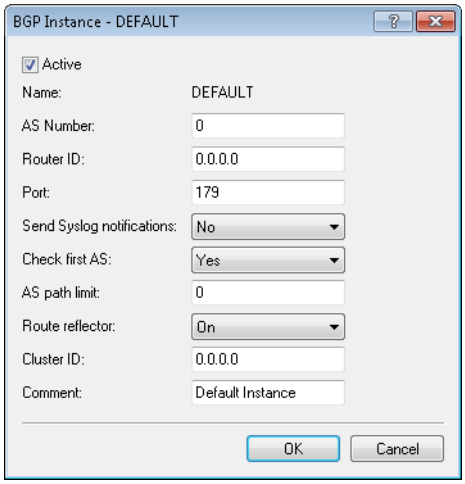
The BGP router organizes the BGP neighbors into address families as a convenient way to manage the communications with these neighbors.

BGP policy

Filter policies allow the BGP router to decide how to handle the inbound and outbound BGP messages.

BGP instance

You configure the BGP instance of the device under **BGP instance**.



Active

Activates or deactivates this BGP instance

This setting only takes effect if BGP is activated on the device.

Name

Contains the name of the BGP instance.

Since the device only supports one BGP instance at a time, this table contains one entry only, "DEFAULT".

AS number

The AS number assigned to this BGP instance.

It is only possible to connect to a BGP router that does not support 32-bit AS numbers if you enter a 16-bit AS number here (less than 65536).

Router ID

The router ID (IPv4 address) of this particular BGP instance.

The router ID must be unique among the neighbors of a BGP router.

When using IPv6 connections, you enter a fictional IPv4 address or any IPv4 address for the router here.

Port

Contains the port used by the BGP instance to listen to inbound connections from neighbors.

Send SYSLOG message

The device is able to store events, such as disconnects of neighbors associated with this BGP instance, to the SYSLOG. Use this option to enable or disable this feature.

Check-First-AS

Checks whether the first AS number in the AS path of received Update messages corresponds to the AS number of the neighbor. If this is not the case, this route is discarded.

This check must be disabled if the router is connected with a BGP route server which, although it distributes routes, is not itself in the routing path and/or inserts its own AS into the AS path.

AS-Path-Limit

Maximum number of permitted AS numbers in the AS path of received Update messages. If the limit is exceeded, the device discards the route. An AS-Path-Limit provides protection against messages from incorrectly configured routers that advertise AS paths that are too long.

Route-Reflector

This specifies whether the router assumes the function of a route reflector.

When operating iBGP, all of the BGP routers usually need to be fully meshed, i.e. each BGP router must have established a BGP connection to every other BGP router. A route reflector negates this requirement and enables iBGP routers to form, for example, a star-shaped topology. A route reflector forwards the iBGP routes to all of the route-reflector clients.

A route reflector is able to serve route-reflector clients as well as normal BGP clients. In both cases no special configuration of the client is necessary.

Cluster-ID

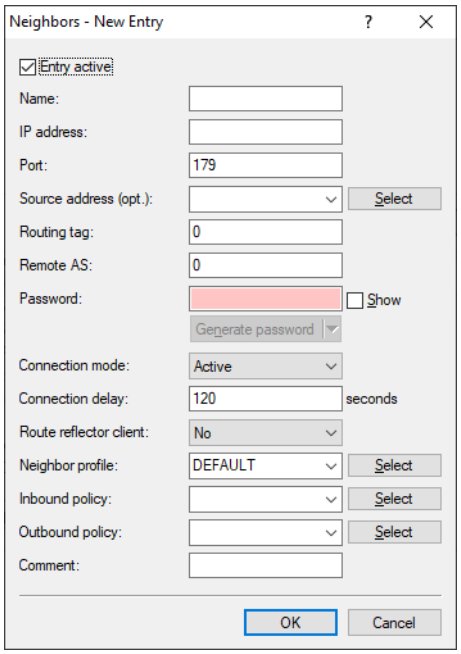
Cluster-ID of the router in case it is configured as a route reflector. This is entered as an IPv4 address.

Comment

Comment about this BGP instance.

Neighbors

You configure the BGP neighbors of the device under **Neighbors**.



Entry active

Activates or deactivates the entry for this BGP neighbor.

The activation of the BGP neighbor triggers the establishment of a BGP connection, if applicable.

It is not possible to connect to disabled BGP neighbors.

Name

Contains the name of the BGP neighbor.

IP address

Specifies this BGP neighbor's IP address (IPv4 or IPv6) as used by the device to establish a BGP connection in the “active” or “delayed” connection mode. When using a link-local IPv6 address, it must be specified with % and the name of the logical interface, e.g. “fe80::1%INTRANET”.

Alternatively, you have the option to configure an entire IPv4 subnet, e.g. 192.168.1.0/24. In this case, the router accepts BGP connections from other routers on the subnet 192.168.1.0 with a subnet mask of 255.255.255.0. For this it is necessary to define the connection mode as "Passive".

IPv6 subnets are not supported.

This entry must match the IP address (e.g. physical interface address, loopback address) reported by this neighbor in an incoming connection.

Port

Shows the port on which the BGP neighbor expects inbound BGP messages and, correspondingly, the port used by the device for outbound connections of the connection type “active” or “delayed”.

The device accepts incoming connections from any source port used by the sender.

Source address (optional)

Contains the sender address (IPv4 or IPv6) that the device communicated to the BGP neighbor when connecting.

Entry is optional and is only relevant for the connection modes “active” and “delayed”.

Routing tag

Contains the routing tag. The device denies the connection if the routing tag does not match with the incoming connection.

Remote AS

Contains the AS number of the BGP neighbor.

If the AS number of the BGP neighbor is identical to the AS number of the device's own BGP instance, then this neighbor is an iBGP peer (internal BGP) in its own AS.

Password

The device and the BGP neighbor authenticate themselves by exchanging this password in the form of an MD5 signature in the TCP packets.

Authentication is not used if no password is set.

Connection mode

Sets the mode in which the connection is established from the device to this BGP neighbor. The following modes are available:

- **Active**: In this mode the device attempts to connect to the BGP neighbor as soon as, among other things, one of the following conditions is met:
  - The BGP neighbor is configured completely.

- Using WEBconfig or via the CLI, you execute the action **Manual start**.
- You start the device.
- The BGP instance is enabled under **Routing protocols** > **BGP** > **BGP instance**.
- You enable this BGP neighbor under **Entry active**.

If the active connection setup does not succeed, a new attempt is made after 120 seconds.

- **Passive**: In this mode the device does not actively connect to the BGP neighbor; instead, it waits for a connection request from the BGP neighbor.
- **Delayed**: In this mode the device waits for a timeout before it tries to connect to the BGP neighbor. The conditions for establishing a connection are the same as for the "Active" mode.

Connection delay

Specifies the wait time in seconds before the device in the "Delayed" connection mode establishes a connection to this BGP neighbor.

Route reflector client

Specifies whether this neighbor is treated as a route-reflector client, in which case the device reflects iBGP routes to it.

This switch is valid only if

- The device has been configured as a route reflector in the BGP instance, i.e. it is a route reflector itself, and
- The remote AS number matches its own AS number (iBGP).

Neighbor profile

Contains the name of the BGP neighbor profile from **Routing protocols** > **BGP** > **Neighbor profiles**.

If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

Inbound policy

Specifies the policy used by the device to filter the inbound connections from this BGP neighbor.

The policy is configured under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.

If you leave this field empty, the device filters the inbound connections according to the default policy under **Routing protocols** > **BGP** > **BGP policy** > **Standard**.

Outbound policy

Specifies the policy used by the device to filter the outbound connections from this BGP neighbor.

The policy is configured under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.

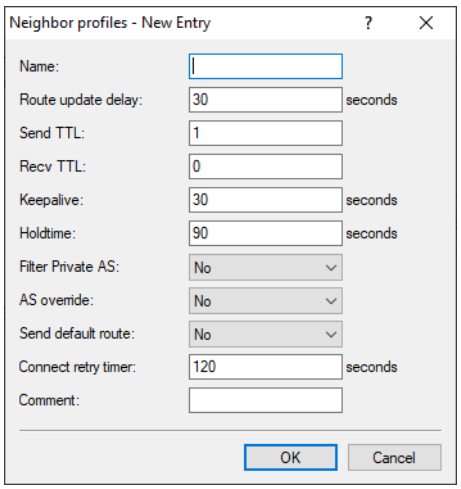
If you leave this field empty, the device filters the inbound connections according to the default policy under **Routing protocols** > **BGP** > **BGP policy** > **Standard**.

Comment

Contains a comment about this BGP neighbor.

Neighbor profiles

You configure the profiles of the BGP neighbors of the device under **Neighbor profiles**.



Name

Contains the name of the profile.

This name is used in the following tables, among other things:

- **Neighbor profile** under **Routing protocols** > **BGP** > **Neighbors**
- **Neighbor profile** under **Routing protocols** > **BGP** > **IPv4 address family**
- **Neighbor profile** under **Setup** > **Routing protocols** > **BGP** > **IPv6 address family**

Route update delay

This is the minimum delay in seconds between BGP advertisements sent by the device to neighbors using this profile.

Send TTL

Specifies the TTL (time to live) that the device adds to TCP packets sent to the BGP neighbors that use this profile.

For directly connected neighbors, this value is set to "1". For eBGP environments, you can increase this value by 1 per hop.

For iBGP sessions, the device ignores this value and defaults to the maximum TTL value.

This value must be "0" if **Recv TTL** is set to a value other than "0". The device automatically uses the value "1" if both **Send TTL** and **Recv TTL** are set to "0".

Recv TTL

Specifies the minimum TTL (time to live) required of inbound TCP packets from BGP neighbors that use this profile. Inbound TCP packets must have a TTL greater than or equal to this value in order to be accepted.

The device ignores this value in iBGP sessions.

If this value is not equal to "0", the device sets the internal value for **Send TTL** to "255".

This value must be "0" if **Send TTL** is set to a value other than "0".

Keepalive

Specifies the time in seconds for the keepalive timer. After this time has elapsed, the device sends a keepalive message to the neighbors using this profile in order to keep the BGP connection intact.

The device must send at least three keepalive messages per unit of holdtime. For this reason the value should be max. one third of the holdtime. If the value is set higher than this or equal to "0", the LCOS automatically sets an internal value that is one-third of the holdtime.

Short hold time

If the router does not receive regular BGP keepalive, update or notification messages within the configured BGP short-hold time, the router will terminate the BGP session and send a notification with the error code "Hold Timer Expired".

The device negotiates this value with the BGP neighbors during connection establishment. The lower of the two values is considered to be valid.

If negotiation results in a value of "0", the device considers the connection to be valid until it receives a connection error or the connection breaks. No keepalive messages are sent to the BGP neighbors during this period, even if the keepalive timer is set with a value.

In accordance with the RFC, the values "1" and "2" are not permitted.

Filter private AS

Controls the removal/replacement of private AS entries (64512 – 65535, 4200000000 – 4294967294) from the `AS_PATH` list of outbound Network Layer Reachability Information (NLRI) messages of BGP neighbors that use this profile.

This option has no function for iBGP connections.

AS override

Enables or disables the overriding of AS numbers in the `AS_PATH` outbound Network Layer Reachability Information (NLRI).

With this option enabled, the device replaces all of the AS numbers of the BGP neighbors with its own AS number.

Send default route

This switch determines the behavior of the propagation of default routes. Possible values:

Yes

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table (*IPv4 networks* on page 518 or *IPv6 networks* on page 518).

Connect retry timer

Specifies the time in seconds that the router waits until the next connection attempt following a failed BGP connection attempt. Generally speaking, this option is only necessary to speed things up when the remote site is in the "passive" connection mode. Default: 120 seconds

Comment

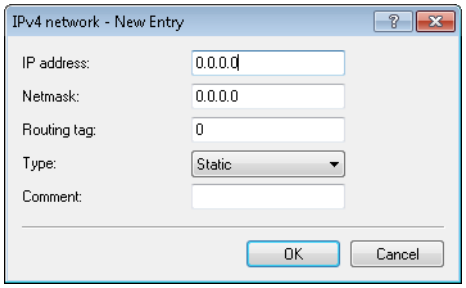
Comment on this entry.

IPv4 networks

Use this table to configure the IPv4 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Routing protocols** > **BGP** > **IPv4 address family**.

The minimum specification for a valid new entry is one **IP address**.



IP address

Contains the IPv4 address or the prefix of the network.

Netmask

Includes the IPv4 netmask of the network.

The route is the default route for this address family if this entry contains the default setting `0.0.0.0`.

Routing tag

Contains the routing tag for this network.

The table under **Routing protocols** > **BGP** > **IPv4 address family** uses this entry to filter the communication with BGP neighbors.

Type

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

- In the "Static" setting the network is always selected for advertisement.
- In the "Dynamic" setting, the network is only selected for advertisement if it appears in the active routing table.

Comment

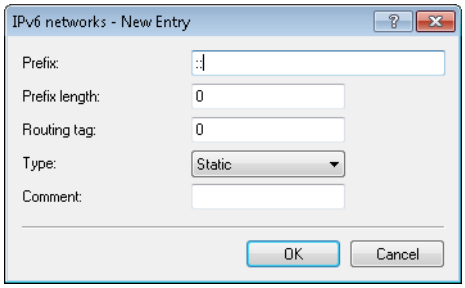
Comment on this entry.

IPv6 networks

Use this table to configure the IPv6 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Routing protocols** > **BGP** > **IPv6 address family**.

The minimum specification for a valid new entry is one **Prefix**.



Prefix

Contains the prefix (IPv6 address portion) of the network.

Prefix length

Contains the prefix length of the IPv6 network.

The route is the default route for this address family if this entry contains the default setting `0`.

Routing tag

Contains the routing tag for this network.

The table under **Routing protocols** > **BGP** > **IPv6 address family** uses this entry to filter the communication with BGP neighbors.

Type

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

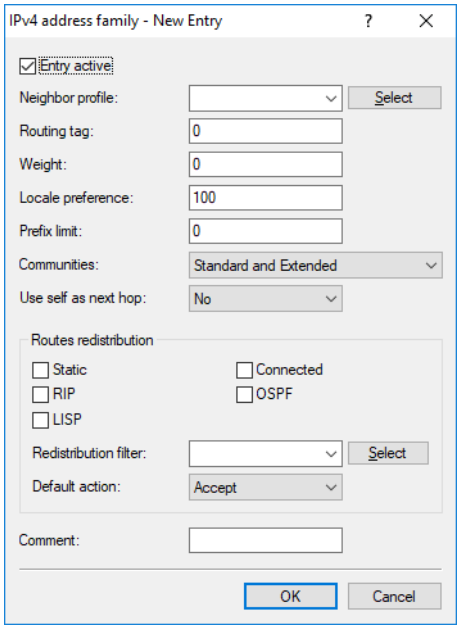
- In the "Static" setting the network is always selected for advertisement.
- In the "Dynamic" setting, the network is only selected for advertisement if it appears in the active routing table.

Comment

Comment on this entry.

IPv4 address family

Use this table to configure the settings for the IPv4 parameters that apply to all of the devices of a BGP neighbor profile.



Entry active

Enables or disables the distribution of IPv4 NLRI of this address family to the BGP neighbors that use this neighbor profile.

Neighbor profile

Contains the name of the corresponding neighbor profile as saved under **Routing protocols** > **BGP** > **Neighbor profiles**.

Routing tag

Specifies that the device only re-distributes routes if they use the routing tag as configured in the routing table. The routes received from the neighbors for this routing tag are stored by the device in the routing table.

Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

Local preference

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference. This value does not override the local preference for prefixes that already have a LOCAL_PREF attribute (for example, with iBGP). The preference of these prefixes has to be modified by a corresponding rule in the BGP policy.

"Local preference" is a BGP standard attribute (`LOCAL_PREF`) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

Prefix limit

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options “Standard” and “Extended” are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

Use own IP address as next hop

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

Possible values:

Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

No

Leaves the IP address of the next hop in the NLRI unchanged.

Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

- Static: The device distributes static routes from the routing table to the BGP neighbors.
- Connected: The device redistributes routes from the networks that it is directly connected to the BGP neighbors.
- RIP: The device distributes RIP routes from the routing table to the BGP neighbors.
- OSPF: The device distributes OSPF routes from the routing table to the BGP neighbors.
- LISP: The device distributes LISP routes from the routing table to the BGP neighbors.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

Redistribution filter

Name of the prefix-filter list from *Prefix lists* on page 382.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

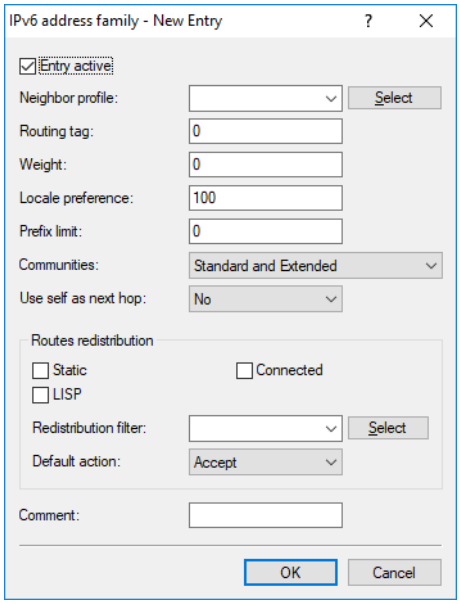
Deny

Comment

Comment on this entry.

IPv6 address family

Use this table to configure the settings for the IPv6 parameters that apply to all of the devices of a BGP neighbor profile.



Entry active

Enables or disables the distribution of IPv6 NLRI of this address family to the BGP neighbors that use this neighbor profile.

Neighbor profile

Contains the name of the corresponding neighbor profile as saved under **Routing protocols** > **BGP** > **Neighbor profiles**.

Routing tag

Specifies that the device only re-distributes routes if they use the routing tag as configured in the routing table. The routes received from the neighbors for this routing tag are stored by the device in the routing table.

Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

Local preference

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference. This value does not override the local preference for prefixes that already have a LOCAL_PREF attribute (for example, with iBGP). The preference of these prefixes has to be modified by a corresponding rule in the BGP policy.

"Local preference" is a BGP standard attribute (`LOCAL_PREF`) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

Prefix limit

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options “Standard” and “Extended” are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

Use own IP address as next hop

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

Possible values:

Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

No

Leaves the IP address of the next hop in the NLRI unchanged.

Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

- Static: The device distributes static routes from the routing table to the BGP neighbors.
- Connected: The device redistributes routes from the networks that it is directly connected to the BGP neighbors.
- LISP: The device distributes LISP routes from the routing table to the BGP neighbors.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

Redistribution filter

Name of the prefix-filter list from *Prefix lists* on page 382.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

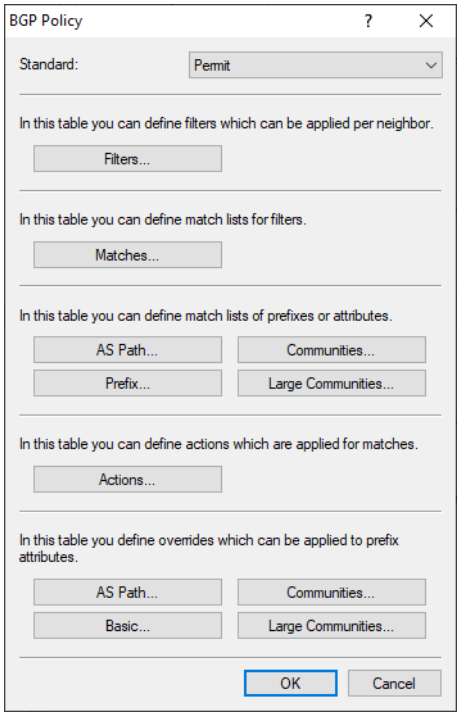
Deny

Comment

Comment on this entry.

BGP policy

Use this section to configure the filter settings for outbound and inbound NLRIs.



Default

The device applies this default policy for a BGP neighbor if it is unclear whether it should accept its prefix or not. The cause for this may be:

- There is no policy configured for this BGP neighbor.
- The specified filter does not exist.
- None of the filters under **Filters** match.

Filters

Here you specify the filters, which should be available for each neighbor.

Matches

Specify the match lists for the filters here.

Prefix and attribute lists

Here you specify the lists of prefixes and attributes for the device to recognize as a match.

Actions

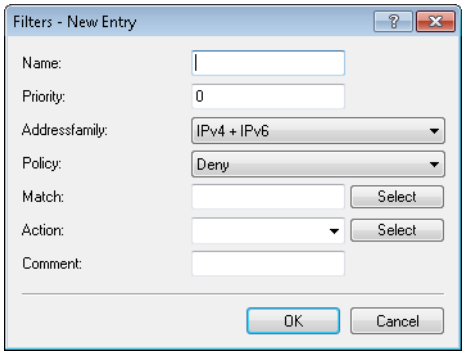
Here you specify the actions that are executed by the device in case of a match.

Overrides

Here you specify the overrides used by the device to modify prefix attributes.

Filter

This table contains filters that an NLRI to or from a BGP neighbor must pass through if the neighbor is configured with a corresponding policy.



Name

Contains the name of this entry.

For multiple filter entries with the same name, the device processes the filters according to the configured priority, until a filter matches the NLRI. The device then stops the filter pass.

Priority

Sets the priority of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value. A higher value means a higher priority.

Address families

Specifies the address family for which this filter applies.

If no option is selected, the entry is disabled.

Policy

Specifies whether the device should further process the filtered NLRI in the case that the filter is valid for the NLRI.

- Deny: No further processing.
- Permit: The device processes the NLRI further.

Matches

Specifies the name of an entry from the table **Matches**.

The device applies this filter if the NLRI matches the criteria.

If this field indicates an invalid name, the device denies the NLRI and performs no further filters in the current filter chain.

Action

Specifies which of the actions from the **Actions** table is applied by the device to the NLRI.

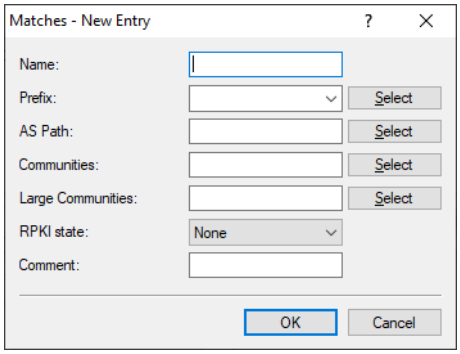
If this field is empty or refers to an invalid name, the device performs no action.

Comment

Comment on this entry.

Matches

This table combines lists of prefixes and attributes in order to compare multiple list entries for matches with the NLRI.



Name

Contains the name of this entry.

Prefix

Contains the corresponding item in the list under **Prefix**.

AS-Path

Contains the corresponding item in the list under **AS path** in the section “Prefix and attribute lists”.

Communities

Contains the corresponding item in the list under **Communities** in the section “Prefix and attribute lists”.

Large Communities

Contains the corresponding item in the list under **Large Communities** in the section “Prefix and attribute lists”.

RPKI state

The Resource Public Key Infrastructure (RPKI) status of prefixes can be used in a BGP policy, so rules can apply it to a BGP prefix. The rejection of invalid prefixes is not recommended; instead, they should be given a lower preference. In this case, a BGP rule is defined that matches to the RPKI status “Invalid”. The action sets the preference of this prefix to the value 10, for example. Once a prefix has been rejected, it is not saved and is no longer available unless the prefix is retransmitted and reevaluated by the BGP neighbor.

None

The RPKI state is not processed.

Not found

The entry matches if the PRKI state of the prefix is set to “Not-found”.

Invalid

The entry matches if the PRKI state of the prefix is set to “Invalid”.

Valid

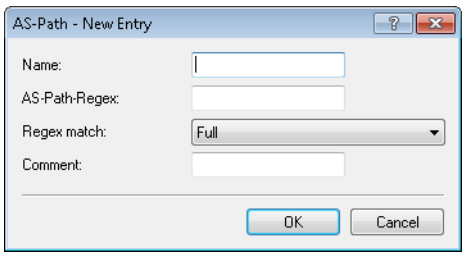
The entry matches if the PRKI state of the prefix is set to “Valid”.

Comment

Comment on this entry.

AS Path (attribute list)

This table contains AS-path lists in order to identify NLRIs by their `AS_PATH` attributes.



Name

Contains the name of this entry.

AS Path Regex

Contains a regular expression that checks the `AS_PATH` of the NLRI. Examples:

- `.*_100`: filters all NLRIs originating from "AS100".
- `.*_(100|200)`: filters all NLRIs originating from "AS100" or "AS200".
- `100_(.*_)?(500|400)_.*`: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which were also previously routed via networks with the AS numbers "AS500" or "AS400" (or both).
- `100_(500|400|123)_.*`: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand directly from BGP neighbors with the AS numbers "AS500", "AS400" or "AS123".
- `100_(100_)*(300_)*300`: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand from the BGP neighbor with the AS number "AS300". This expression also allows for AS prepend paths.
- `100_ 200`: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which originated from the network with the AS number "AS200". The route taken by the NLRIs from "AS200" to "AS100" is unimportant.

Regex-Match

Determines how closely the regular expression under **AS-Path-Regex** needs to match the `AS_PATH` attribute of the NLRI in order for the list entry to apply.

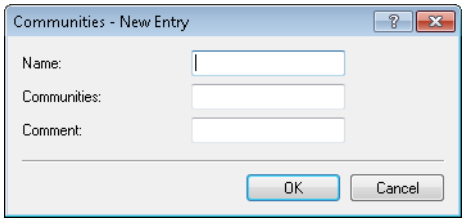
- Full: The regular expression fully describes the `AS_PATH` attribute of the NLRI.
- Partial: The regular expression only describes parts of the `AS_PATH` attribute.

Comment

Comment on this entry.

Communities (attribute list)

This table contains community lists in order to identify NLRIs by their community attributes.



Name

Contains the name of this entry.

Communities

Contains communities that the community attribute of the NLRI must match with.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

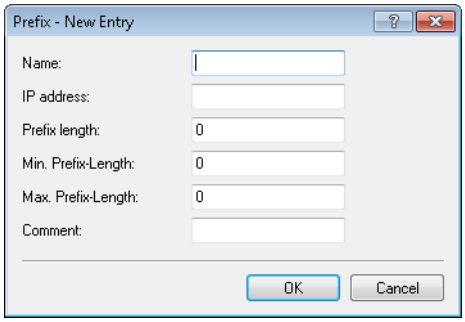
Comment

Comment on this entry.

Prefix (attribute list)

This table contains prefix lists that are used to identify NLRIs based on their network (prefix) and netmask (prefix length).

An entry can contain several prefixes.



Name

Contains the name of this entry.

IP address

Contains the IPv4 or IPv6 address of the network.

Prefix length

Contains the netmask or prefix length of the network.

This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address.

The prefix length of the NLRI must exactly match this value unless “Min. prefix length” and “Max. prefix length” are set to values not equal to zero.

If the value is “0”, the network of the NLRI matches when it comes from same IP address family as that specified under “IP address”.

Min. prefix length

Specifies the minimum prefix length value that the network of the NLRI needs in order to match.

Max. prefix length

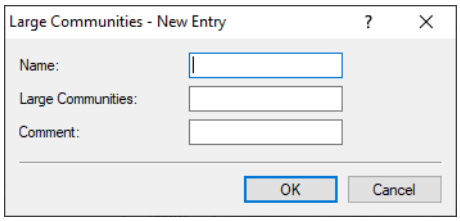
Specifies the maximum prefix length value that the network of the NLRI needs in order to match.

Comment

Comment on this entry.

Large Communities (Attributes list)

This table contains large-community lists in order to identify NLRIs by their community attributes.



Name

Contains the name of this entry.

Large Communities

Contains large communities that the large-community attribute of the NLRI must match with.

The communities are specified in a comma-separated list.

Structure of a large community: `<Global administrator or ASN>:<Local data part 1>:<Local data part 2>`

Example of a single large community: `64496:4294967295:2`

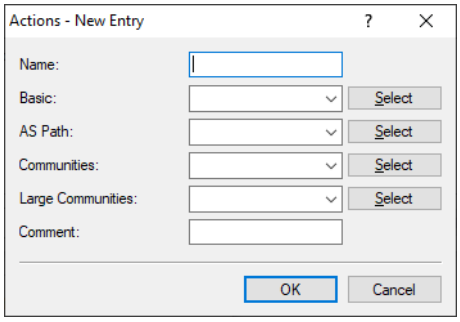
Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Comment

Comment on this entry.

Actions

This table combines override lists in order to perform multiple modifications of an NLRI by means of a single action.



Name

Contains the name of this entry.

Basic

Contains the name of an override of basic entries in the NLRI.

This entry refers to the entries in the override table under **Basic**.

AS-Path

Contains the name of an override of `AS_PATH` attributes in the NLRI.

This entry refers to the entries in the override table under **AS Path**.

Communities

Contains the name of an override of Community entries in the NLRI.

This entry refers to the entries in the override table under *Communities (override list)* on page 531.

Large Communities

Contains the name of an override of large-community entries in the NLRI.

This entry refers to the entries in the override table under *Large Communities (Overrides list)* on page 534.

Comment

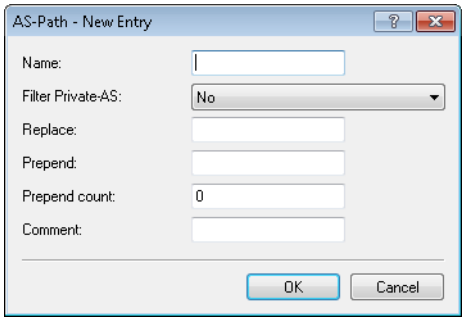
Comment on this entry.

AS Path (override list)

This table contains overrides that manipulate the `AS_PATH` attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. "Filter private AS"
2. "Replace"
3. Together "Prepend count" and "Prepend"



Name

Contains the name of this entry.

Filter private AS

If configured, this entry causes the device to modify the specification of the private AS numbers in the `AS_PATH` attribute of an NLRI in accordance with this setting.

› No: The device retains the existing private AS numbers of the NLRI.

- Remove: The device removes all private AS numbers.
- Replace: The device replaces the existing private AS numbers with the AS number of the current BGP instance.

Replace

If configured, this entry causes the device to change the `AS_PATH` attribute of the NLRI to the value specified here.

Prepend

If configured, this entry causes the device to prepend the `AS_PATH` attribute of the NLRI with the value entered here as often as is specified under "Prepend count". Special values:

- `self`: The device prepends the `AS_PATH` attribute of the NLRI with its own AS number.
- `last`: The device prepends the `AS_PATH` attribute of the NLRI with the most recently used AS number.

Prepend count

Determines how often the device prepends the `AS_PATH` attribute of the NLRI with an AS number.

Comment

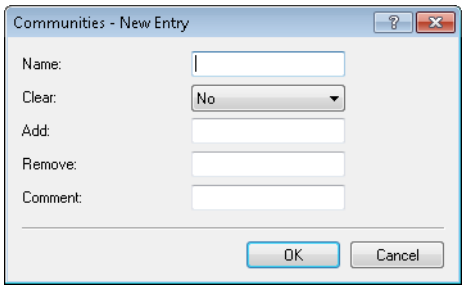
Comment on this entry.

Communities (override list)

This table contains overrides that manipulate the Communities attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. "Clear"
2. "Add"
3. "Remove"



Name

Contains the name of this entry.

Clear

Determines whether the device deletes unknown communities from the NLRI.

Known communities remain in place even if this option to set to "Yes".

Known communities are:

- `no-peer`

- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

For more information, see *RFC 1997* and *RFC 3765*.

Add

Specifies which communities the device adds to an NLRI.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

Remove

Specifies which communities the device removes from an NLRI.

Communities are specified by means of a comma-separated list (`<AS-number1>:<Value1>,<AS-number2>:<Value2>,<AS-number3>:<Value3>`).

Known communities are not removed from NLRI. Known communities are:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`
- `graceful-shutdown`

The following input formats are available for communities:

Input format	Community
1:2	Standard community
1.2.3.4:1	IPv4-specific extended community
roc:1.2.3.4:1	IPv4-specific route origin extended community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4-specific route target extended community
ext2:1:2	Two-byte AS extended community
ext4:1:2	Four-byte AS extended community
roc:1:2	Two-byte AS route origin extended community (Site-of-Origin (SoO))
rtc:1:2	Two-byte AS route origin extended community
roc:ext4:1:2	Four-byte AS route origin extended community (Site-of-Origin (SoO))

Comment

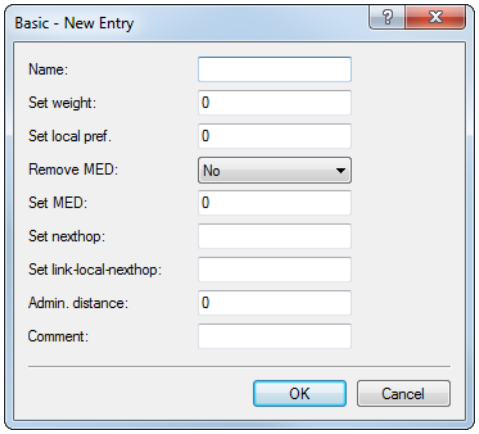
Comment on this entry.

Basic (override list)

This table contains overrides that manipulate the basic attributes of NLRIs.

If an action applies a row of this table, all of the manipulations that this row implements are processed.

The specification of basic attributes is optional. If you want the action to change just one basic attribute, enter the desired value at the appropriate place and leave the remaining attributes in their default setting.



Name

Contains the name of this entry.

Set weight

The device modifies the weighting of an NLRI to the value specified here.

Local preference

The device modifies the local preference value of an NLRI to the value specified here.

Remove MED

If set to "Yes", the device deletes the multi-exit discriminator (MED) of an NLRI before it processes the setting under "Set MED".

Set MED

The device modifies the multi-exit discriminator (MED) of an NLRI to the value specified here. If the NLRI contains no MED, the device creates this attribute.

Set nexthop

The device modifies the next-hop IP of an NLRI to the value specified here. Possible values are an IPv4 address or a global IPv6 address.

Set link-local-nexthop

The device modifies the IPv6 link-local-nexthop of an NLRI to the value specified here. This only effects IPv6 prefixes.

Administrative distance

Specifies the "administrative distance" given to prefixes received in the BGP when they are entered into the routing table. The list of fixed "administrative distances" for the various system services and routing protocols can be displayed on the command line by `show admin-distance`.

Comment

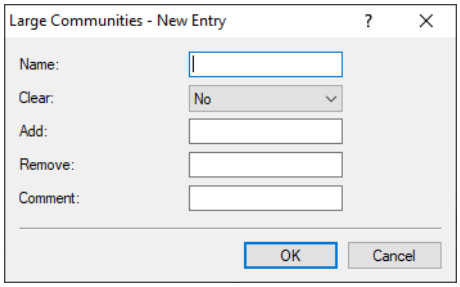
Comment on this entry.

Large Communities (Overrides list)

This table contains overrides that manipulate the large community attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Clear**
2. **Add**
3. **Remove**



Name

Contains the name of this entry.

Clear

Determines whether the device deletes unknown large communities from the NLRI.

Add

Specifies which large communities the device adds to an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global administrator or ASN>:<Local data part 1>:<Local data part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Remove

Specifies which large communities the device removes from an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global administrator or ASN>:<Local data part 1>:<Local data part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Comment

Comment on this entry.

6.24.2 Best-path selection algorithm

The following algorithm is applied for the selection of the best path:

1. The next hop in the BGP update message is available.

2. The device's own AS is not in the `AS-Path`.
3. The next hop is not the device's own address.
4. Highest weight
5. Highest local preference
6. Shortest `AS_PATH` (`AS_SET` counts as length 1)
7. Lowest origin (IGP < EGP < Incomplete)
8. Lowest MED

   This applies only if the compared routes are from the same neighbor AS.

9. eBGP is preferred before iBGP.
10. Lowest router ID
11. Neighbor with lowest IP address
12. Neighbor with lowest RTG tag
13. The oldest path is preferred over a newly learned path.

6.24.2.1 Influencing the routing algorithm with attributes

You have the option to influence the selection of the best path to a destination by means of the following attributes:

Weight

Weight is a proprietary attribute, which is not propagated to neighbors by means of BGP update messages. "Weight" is valid on the local router only. You can set the attribute locally either by means of the address family or with filter policies.

Local preference

Local preference is a BGP standard attribute (`LOCAL_PREF`) and is propagated to neighbors via iBGP. All paths have a local preference of 100 by default. This attribute can be used to favor certain prefixes. The attribute can be set by address family or by filter policies.

AS_PATH

The AS-Path contains details of the path taken by a route. Filter policies can be used to manipulate the AS path, for example by prepending the device's own AS number multiple times. This makes the AS path appear longer to a neighbor.

Origin

Origin is a default BGP attribute, which is propagated to all neighbors. This attribute indicates where a route originated. This could be an Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP, RFC 904), or "Incomplete". Here, "Incomplete" indicates a redistribution by a different routing protocol. The **origin** attribute is set automatically by the router. The origin of a route is set to IGP if it was added to BGP by means of an entry in the IPv4 / IPv6 network table. The origin for a route is set to "Incomplete" if it was configured for re-distribution in the address families.

MED

MED (`MULTI_EXIT_DISC`) is an optional BGP attribute used to distinguish between multiple inputs or outputs to the same neighbor AS. The attribute can be set by filter policies.

Router ID

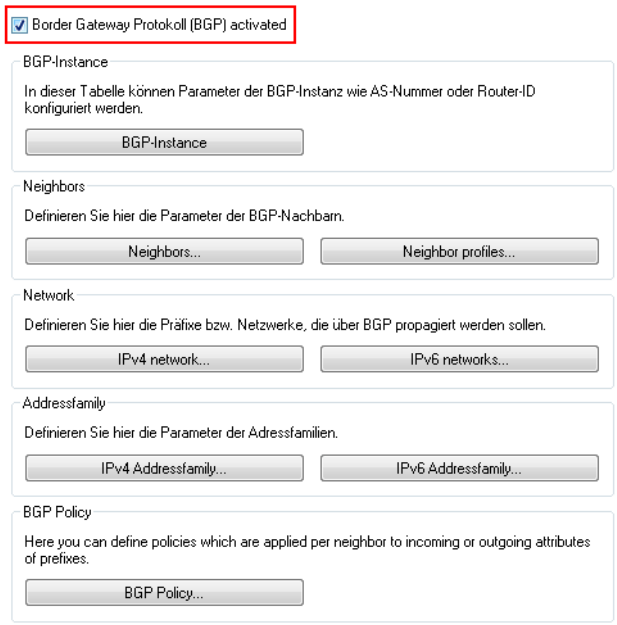
The router ID, also known as the BGP identifier, is the unique identifier of a router. It consists of the IPv4 address of the router. You can manually configure the router ID under **BGP instance** > **Router ID**.

6.24.3 Tutorial: Setting up BGPv4 under LANconfig

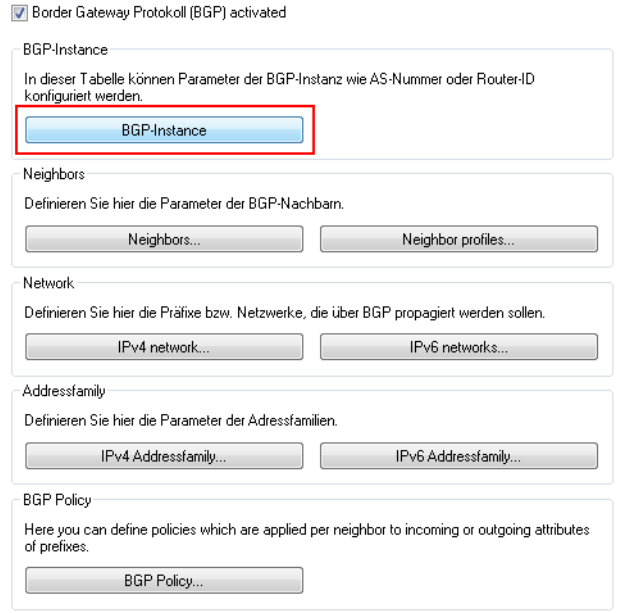
Two LANCOM routers are inter-connected over a WAN link and they are to be configured to use BGP to propagate certain IPv4 networks. The routers are a LANCOM 1800VAW at the main office and a LANCOM 1800VA-4G at the branch office.

We assume that a WAN connection exists between the two devices.

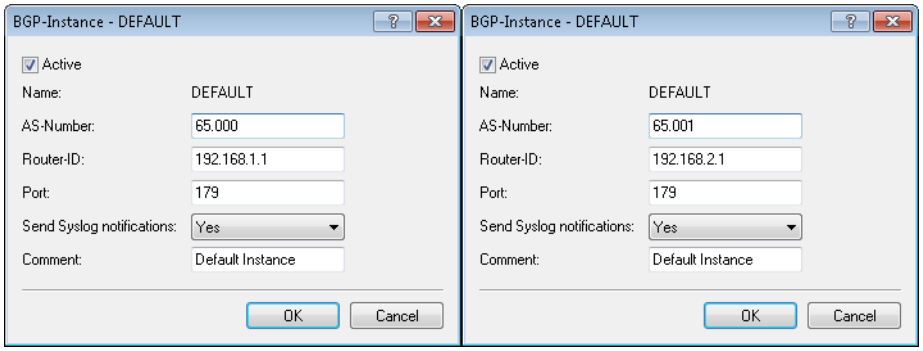
1. **Enabling BGP**: Open the menu item **Routing protocols** > **BGP** in the configuration of both routers and activate the **Border Gateway Protocol (BGP) active** check box. This enables BGP on that specific device. In the next steps you configure each BGP instance, the associated neighbors, and the networks that are to be propagated.



2. **Configuring individual BGP instances**: To configure the BGP instance of each router, click the **BGP instance** button.



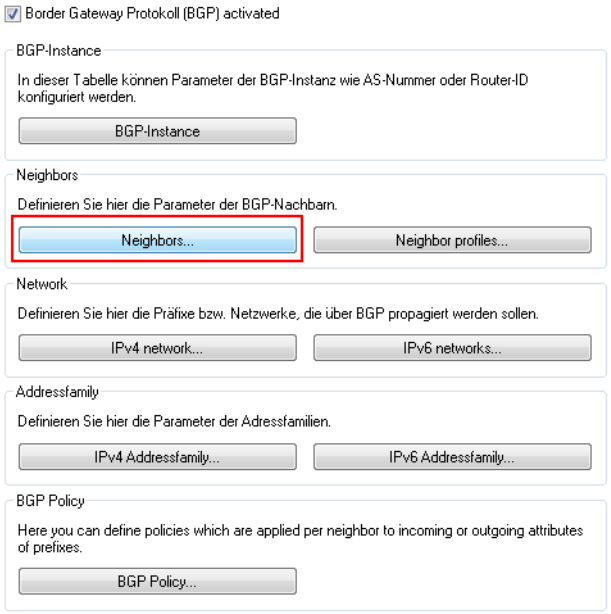
3. Use the configuration window to specify the general information about the BGP instance for each router. The screenshots below show the configurations for both devices for direct comparison side by side.



The left half of the images shows the LANCOM 1800VAW, and the right half shows the parameters of the LANCOM 1800VA-4G.

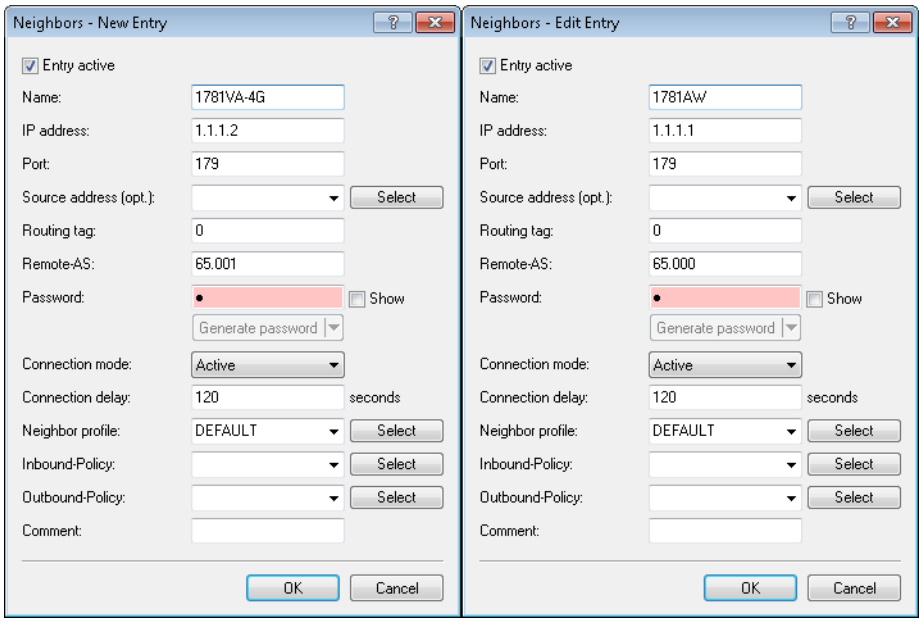
Parameter	Description
Checkbox **Active**	Enable the BGP instance of the router. This is necessary to enable communication between the two routers.
AS number	The AS number (**A**utonomous **S**ystem number) collects routers into the same administration unit. Entering different numbers here specifies the eBGP peers. Identical numbers indicate peers that share the same AS (iBGP). Learn which entries are valid by visiting *http://www.iana.org/assignments/as-numbers/as-numbers.xhtml*.
Router ID	Specify an IP address for the router. Enter `0.0.0.0` if you want the IP address to be set automatically. The router ID must be unique among the neighbors of a BGP router. Different entries are required here.
Port	Configure the TCP-IP port that the router uses for inbound BGP connections. The default value is 179.
Send Syslog notifications	Specify whether the device is to generate SYSLOG messages. Use WEBconfig to view these.
Comment	Enter a comment to make it easier to understand the configuration later.

4. **Configuring the BGP neighbors**: Once the configuration of the BGP instance is complete, the next step is to define the associated neighbors for exchanging information about the propagated networks. Click on the **Neighbors** button.



5. Click on the **Add** button to configure a new BGP neighbor. Use the configuration window to specify the information about the BGP neighbors for each router.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

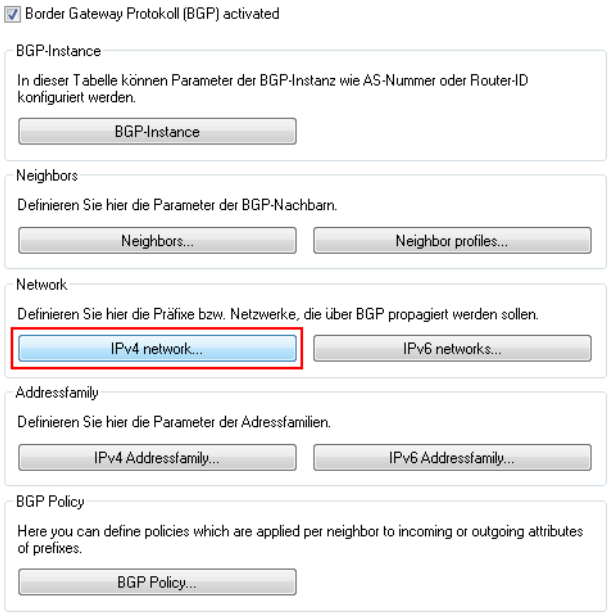


The left half of the images shows the LANCOM 1800VAW, and the right half shows the parameters of the LANCOM 1800VA-4G.

Parameter	Description
Entry active	Activate the entry for the corresponding neighbor.

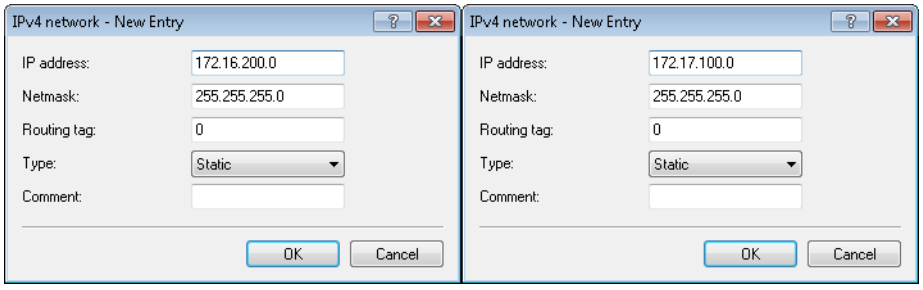
Parameter	Description
Name	Set the name for the neighbor. This example uses an abbreviated version of the device name for easy identification in the configuration.
IP address	Enter the IP address where the neighbor is to be reached. In this example, the WAN address of 1800VAW is `1.1.1.1` and that of 1800VA-4G is `1.1.1.2`.
Remote AS	Enter the AS numbers of the corresponding neighbors as specified in **step 2**.
Password	Enter a password, which is used to obscure communications between the two BGP neighbors by means of an MD5 hash. The password must be identical at both ends.

6. **Configuring the IPv4 networks to be propagated**: Configure the networks that are to be propagated by the individual BGP instances. Click on the **IPv4 networks** button.



7. Click the **Add** button to define a new IPv4 network, which is to be propagated.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



The left half of the images shows the LANCOM 1800VAW, and the right half shows the parameters of the LANCOM 1800VA-4G.

Parameter	Description
IP address	The IPv4 address range of the network to be propagated.

Parameter	Description
Netmask	The netmask corresponding to the defined network.
Type	The type of propagation to be used. This example is static for ease of configuration.

8. Write the respective configurations back to the two devices.
9. The BGP connection is easily checked via the command line. The command `show bgp-neighbor` displays all active neighbors and their status.

```
> show bgp-neighbor
BGP-Neighbors:

1.1.1.2, Rtg-Tag 0
 BGP-State: ESTABLISHED, up for 00:09:23
 remote AS 65001, remote router id 192.168.1.161, eBGP
 Neighbor capabilities:
  Four-octets ASN capability: advertised and received
  Address family IPv4 NLRI used for unicast forwarding: advertised and received
> _
```

6.24.4 Tutorial: Setting preferences for prefixes

"Preference" is an optional BGP attribute used to set preferred paths to certain prefixes. The device prefers a path with a higher preference over a path with a lower preference.

Within an AS, the iBGP neighbors exchange the BGP attribute `LOCAL_PREFERENCE`. The eBGP neighbors in neighboring ASs do not transmit this attribute.

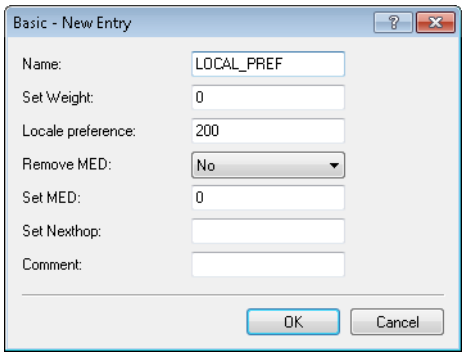
There are two ways to configure preferences:

- By address family
- By policy

This example explains how to configure the prioritization of the prefix from a BGP neighbor with the preference "200" over the prefix from another BGP neighbor with the preference "100".

The default setting for preferences is "100". In this case all you have to do is configure the neighbor that requires preferential treatment with the preference "200".

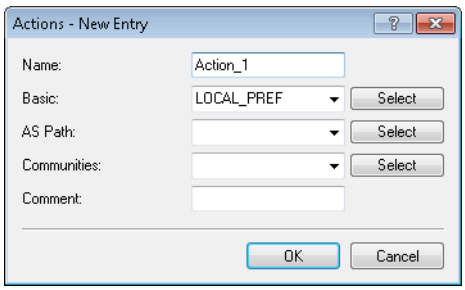
1. Navigate to **Routing protocols** > **BGP** > **BGP policy** > **Basic** and add a new entry to the manipulation of basic attributes of the NLRI (in this case the basic attribute `LOCAL_PREFERENCE`).



Give the entry a descriptive name.

Under **Set local preference** enter the value "200" for the new local preference.

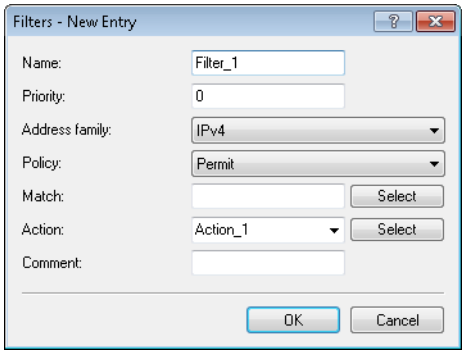
2. Under **Routing protocols** > **BGP** > **Actions** add a new action.



Give the action a descriptive name.

Under **Basic** you select the basic entry you created previously.

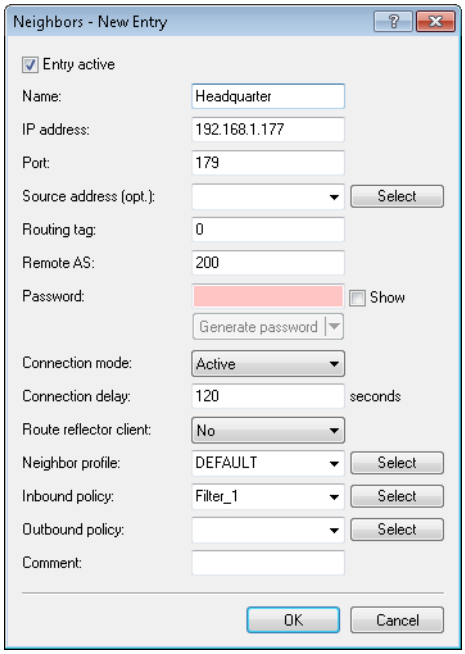
3. Add a new filter under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.



Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting "Permit" in the field **Policy** you specify that the device should modify the outbound NLRI. Under **Action** you select the action you created previously.

4. Under **Routing protocols** > **BGP** > **Neighbors** you add a new entry for a BGP neighbor.



Give the neighbor a descriptive name and configure its IP address along with the number of the remote AS where it is located.

If you have not created a dedicated neighbor profile for this BGP neighbor, use the "Default" profile.

Under **Inbound policy** you select the filter you created previously.

5. To check the configuration, open a terminal connection to the device.

   The command `show bgp-policy Filter_1` displays the current setting for the policy "Filter_1".

```
> show bgp-policy Filter_1
Traverse chain "Filter_1"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Action_1"
         No AS-path override configured
         Apply basic override "LOCAL_PREF"
            Set local preference to 200
         No community override configured
      Permit route
> _
```

   The command `show bgp-v4-adj-rib-in` displays the routing information base (RIB).

```
> show bgp-v4-adj-rib-in
IPv4 Unicast Adj-RIB-In

 192.168.1.177, Rtg-Tag 0

  Prefix            Next Hop       Local-Pref  Weight  MED AS Path
  ------------------------------------------------------------------
  192.168.210.0/24  192.168.1.177         200       0    0 AS sequence: 200
  192.168.211.0/24  192.168.1.177         200       0    0 AS sequence: 200

> _
```

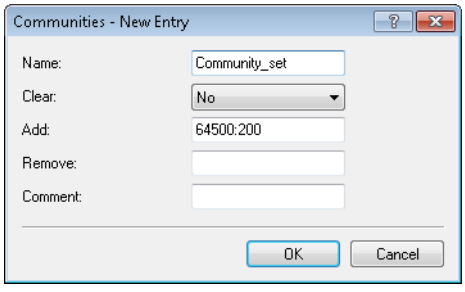
6.24.5 Tutorial: Setting the Community attribute

"Community" is an optional BGP attribute that can be used to identify prefixes and collect them into logical groups. Inbound and outbound policies can be applied to these groups. It is possible to specify multiple communities for a single prefix.

In addition to the well-known communities `NO-ADVERTISE`, `GRACEFUL-SHUTDOWN` or `NO-EXPORT`, the meaning of a community can be freely defined by the provider. So for example, the provider of AS "64500" specifies that customer routes with the community "64500:200" are to be treated with preference "200", and routes with the community "64500:90" are to be treated with the preference "90".

The following example shows how the community "64500:200" is added to all outbound routes.

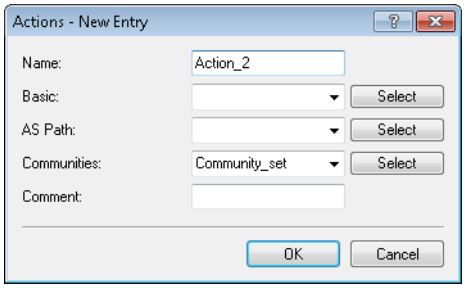
1. Add a new community under **Routing protocols** > **BGP** > **BGP policy** > **Communities (overrides)**.



   Give the community a descriptive name.

   Under **Add** enter the value "64500:200" for the community attribute. This value adds the device to the community attribute of the outbound NLRI.

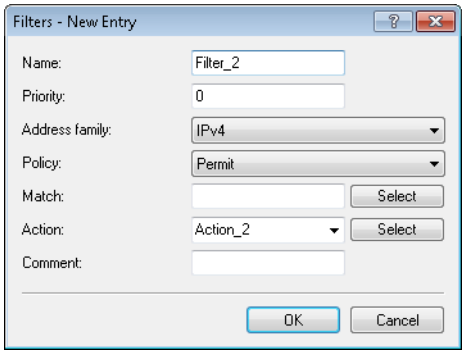
2. Under **Routing protocols** > **BGP** > **Actions** add a new action.



Give the action a descriptive name.

Under **Communities** you select the community you created previously.

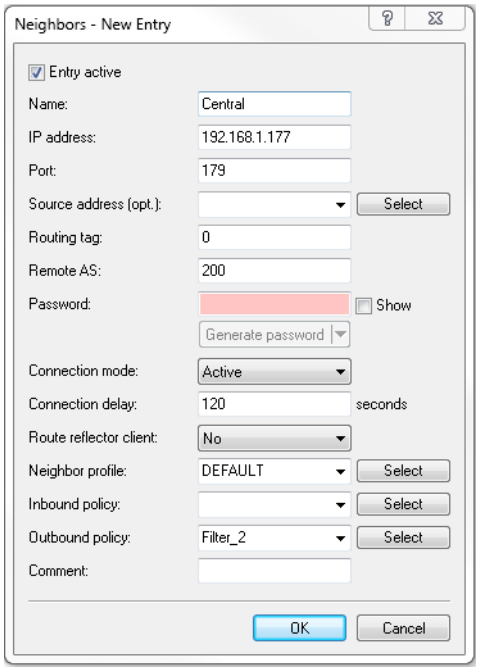
3. Add a new filter under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.



Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting "Permit" in the field **Policy** you specify that the device should modify the outbound NLRI. Under **Action** you select the action you created previously.

4. Under **Routing protocols** > **BGP** > **Neighbors** you add a new entry for a BGP neighbor.



Give the neighbor a descriptive name and configure its IP address along with the number of the remote AS where it is located.

If you have not created a dedicated neighbor profile for this BGP neighbor, use the "Default" profile.

Under **Outbound policy** you select the filter you created previously.

5. To check the configuration, open a terminal connection to the device.

The command `show bgp-policy Filter_2` displays the current setting for the policy "Filter_2".

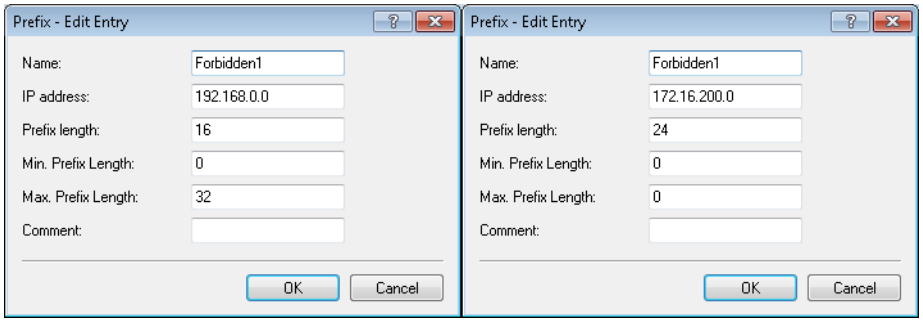
```
> show bgp-policy Filter_2
Traverse chain "Filter_2"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Action_2"
         No AS-path override configured
         No basic override configured
         Apply community override "Community_set"
            Add community 64500:200
      Permit route
> _
```

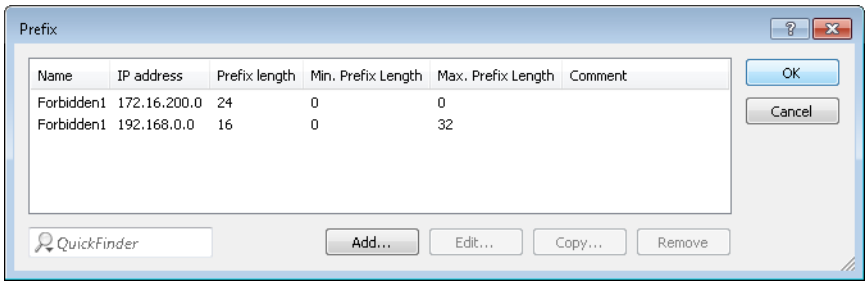
6.24.6 Tutorial: Filtering received prefixes

This example explains the configuration steps required to filter out the following inbound prefixes from a BGP neighbor:

- All prefixes in the range "192.168.0.0/16"
- The individual prefix "172.16.200.0/24"

1. Create two new entries for the prefixes to be filtered under **Routing protocols** > **BGP** > **BGP policy** > **Prefix**.



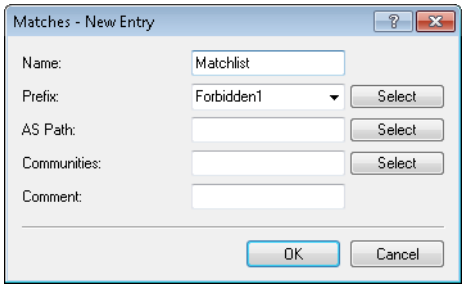


Give each entry a descriptive name.

Add an entry for each prefix to be filtered, but give each entry the same name.

For each entry specify the IP address and the prefix length.

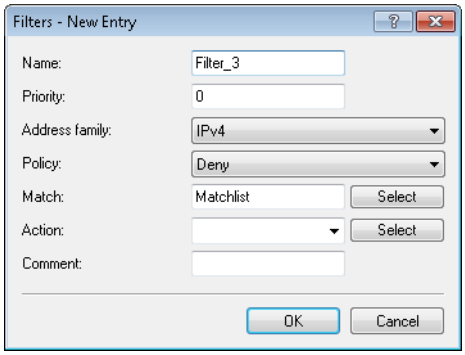
2. Specify a match for the previously created prefix entries under **Routing protocols** > **BGP** > **BGP policy** > **Matches**.



Give the entry a descriptive name.

Under **Prefix** you select the name of the prefix you added previously.

3. Add a new filter under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.



Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting “Deny” in the field **Policy** you instruct the device to filter out the inbound prefixes. Under **Match** you select the match you created previously.

4. To check the configuration, open a terminal connection to the device.

   The command `show bgp-policy Filter_3` displays the current setting for the policy “Filter_3”.

```
> show bgp-policy Filter_3
Traverse chain "Filter_3"
   Inspect filter of priority 0
      Match IPv4 routes
      Assess match "Matchlist"
         Evaluate prefix list "Prohibited1"
            Analyze prefix 172.16.200.0
               Match IPv4 routes
               Match route's 24 MSB
               Match route prefix length in [24, 24]
            Analyze prefix 172.168.0.0
               Match IPv4 routes
               Match route's 16 MSB
               Match route prefix length in [16, 32]
         No AS-path list configured
         No community list configured
      Deny route
> _
```

6.25 OSPF

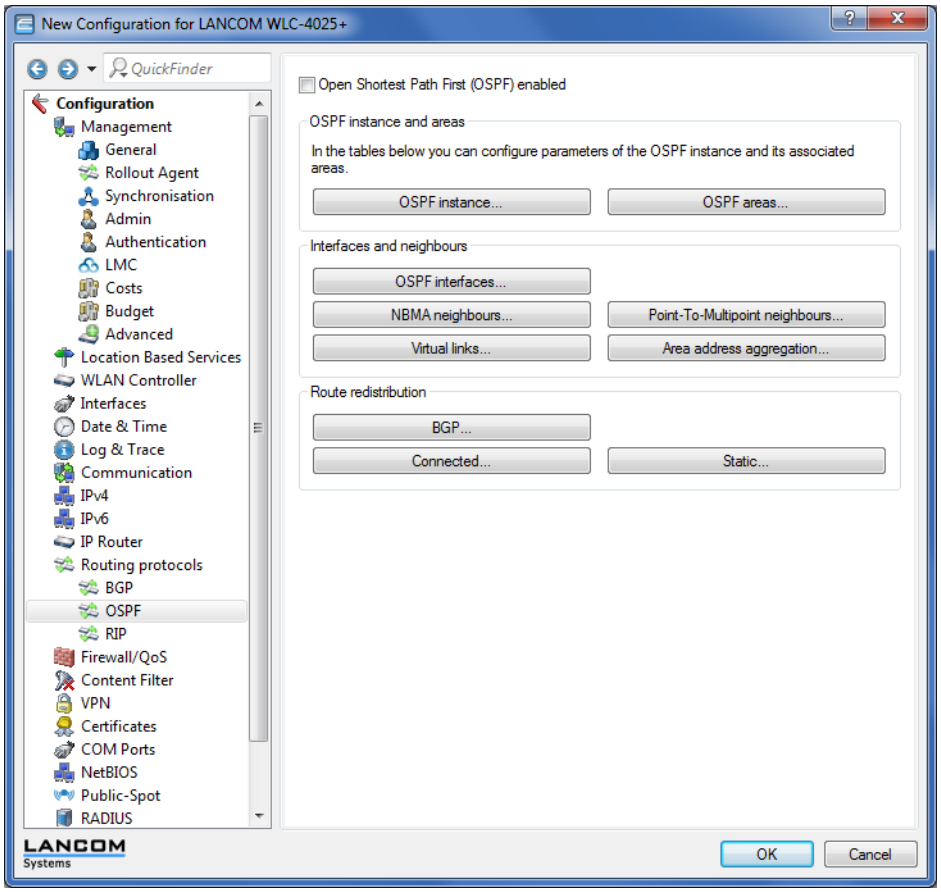
Open Shortest Path First (OSPF) is a link-state routing protocol as per RFC 2328. It belongs to the category **Interior Gateway Protocols** (IGP). This involves routers regularly exchanging link-status information via link-state advertisements (LSA). The routers use multicast to automatically discover one another on the local network. OSPF is generally used for the exchange of internal routing information in large networks (LANs).

Each router has an identical copy of the database (link state database, LSDB), which routers use to determine the best routes (Shortest Path First, SPF) using the Dijkstra algorithm.

In contrast, BGP is one of the **Exterior Gateway Protocols** (EGP) and is typically used to route between autonomous systems or within VPNs.

6.25.1 Setting up OSPF with LANconfig

In order to configure OSPF with LANconfig, navigate to the **Routing protocols** > **OSPF** menu.



Open Shortest Path First (OSPF) enabled

To activate the OSPF function, set a check mark for **Open Shortest Path First (OSPF) enabled**.

OSPF instance

The table **OSPF instance** defines the OSPF instances on this device. It is possible for a device to operate multiple OSPF instances in parallel. Each instance corresponds to an autonomous system or an OSPF domain.

OSPF areas

The table **OSPF areas** is used to define the parameters of the OSPF areas.

OSPF interfaces

This table specifies the interfaces on which OSPF is to operate.

NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. If no default router is selected, multicast is used for communications instead.

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at the borders transitioning from the backbone area to non-backbone areas. The corresponding subnet is advertised as a summary LSA.

BGP

Routes learned dynamically from BGP sources or protocols can be distributed by OSPF.

Connected

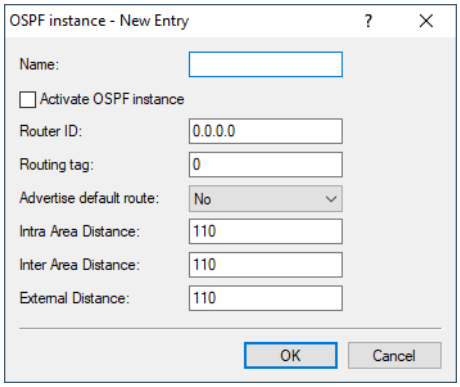
Connected routes, i.e. routes that the operating system automatically enters into the routing table, can be redistributed by OSPF.

Static

Static routes, i.e. routes that the user manually enters into the routing table, can be redistributed by OSPF.

6.25.1.1 OSPF instance

You configure the OSPF instance of the device under **OSPF instance**.



Name

Contains the name of the OSPF instance.

Activate OSPF instance

Activates or deactivates this OSPF instance

Router ID

Contains the 32-bit router ID (represented as an IPv4 address) of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

Routing tag

Contains the routing tag assigned to this instance.

Advertise default route

Specifies whether this router should advertise or propagate the default route in this instance.

Possible values:

No (Default)

The router does not advertise a default route.

Yes

The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

Intra Area Distance

Defines the administrative distance with which OSPF inserts incoming intra-area routes into the routing table.

Inter Area Distance

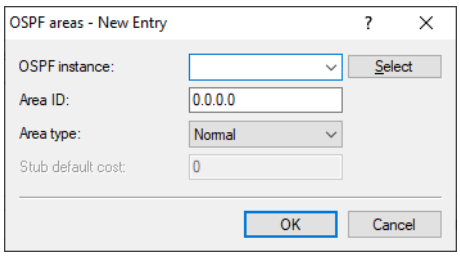
Defines the administrative distance with which OSPF inserts incoming inter-area routes into the routing table.

External distance

Defines the administrative distance with which OSPF inserts incoming external routes into the routing table.

6.25.1.2 OSPF areas

The parameters for the OSPF area are configured under **OSPF areas ...**.



OSPF instance

Contains the name of the OSPF instance.

Area ID

The area ID (displayed as an IPv4 address) identifies the area.

If this instance is to be the backbone area, the value to be used is 0.0.0.0.

Area type

Specifies the type of the area.

Possible values:

Normal (default)

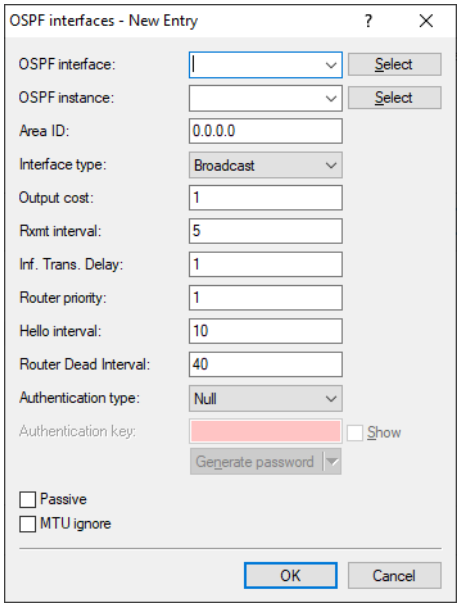
Stub

Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

6.25.1.3 OSPF interfaces

Defines the interfaces on which OSPF should be operated.



OSPF interface

Contains the interface (IPv4 network or WAN remote site) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

Port type

Defines the interface type.

Possible values:

Broadcast

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

Non-Broadcast Multi- Access (NBMA)

Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication; the neighbors are configured manually.

Output cost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

The value must always be greater than zero.

Retransmit interval

Contains the number of seconds between retransmissions.

Transmit delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

Router priority

Defines the priority of this router on this interface when set as the designated router (DR). The router with the highest priority is set as the default router.

The value 0 prevents the router from becoming default router on this interface.

Hello interval

Contains the interval in seconds in which the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

Null

Simple password

Cryptographic MD5

Authentication key

Contains the authentication key for this network.

In this case the authentication type **Null** may not be selected.

Passive

Defines whether OSPF should work actively or passively on this interface.

Possible values:

Yes

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

No (Default)

MTU ignore

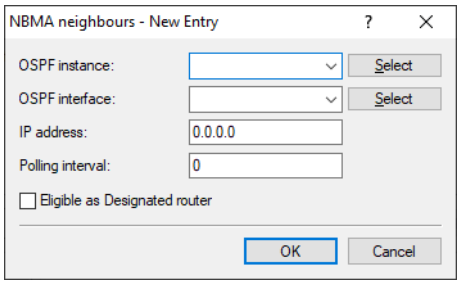
Disables the MTU value check in database description packets.

This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

6.25.1.4 NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. Initially, a default router is selected for this purpose.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.



OSPF instance

Contains the name of the OSPF instance.

OSPF interface

Contains the interface (IPv4 network or WAN remote site) on which OSPF is to be activated.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

Poll interval

Contains the interval in which Hello messages are sent to this router.

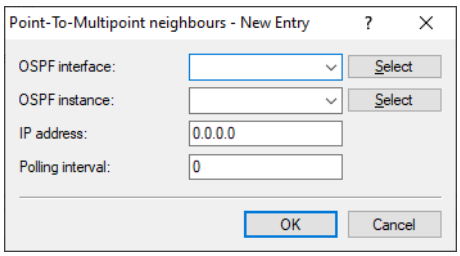
The value zero disables the transmission of Hello messages.

Eligible as default router

Specifies whether the local device itself is selectable as default router.

6.25.1.5 Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. No default router is selected and multicast is used for communications.



OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

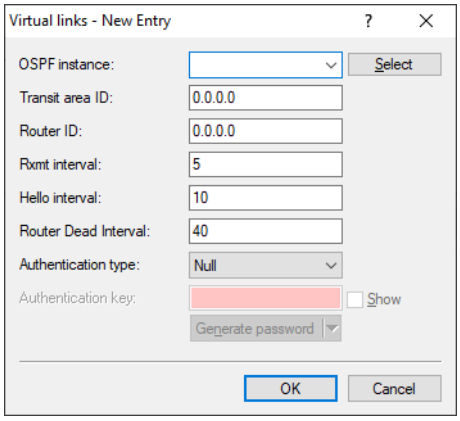
Polling interval

Contains the interval in which Hello messages are sent to this router.

The value zero disables the transmission of Hello messages.

6.25.1.6 Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.



OSPF instance

Contains the name of the OSPF instance.

Transit area ID

Contains the area ID, defined as an IPv4 address

Router ID

Contains the router ID of the router at the remote end of the virtual link as an IPv4 address.

Retransmit interval

Contains the number of seconds between retransmissions.

Hello interval

Specifies the interval in seconds that the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

Null

Simple password

Cryptographic MD5

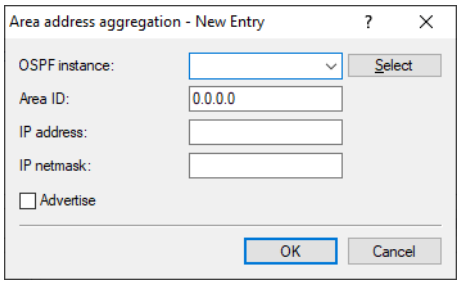
Authentication key

Contains the authentication key for this network.

In this case the authentication type **Null** may not be selected.

6.25.1.7 Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at the borders transitioning from the backbone area to non-backbone areas. The corresponding subnet is advertised as a summary LSA.



OSPF instance

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

If this instance is to be the backbone area, the value to be used is 0.0.0.0.

IP address

Contains the IPv4 address.

IP netmask

Contains the IPv4 subnet mask.

Advertise

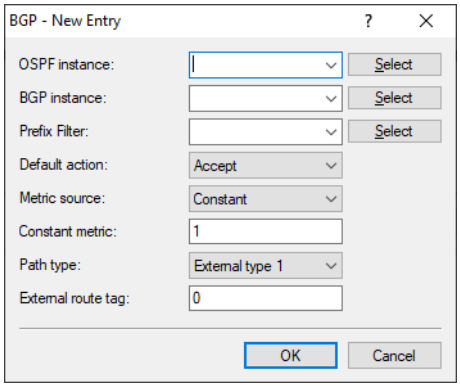
Enables or disables the advertisement of this address aggregation.

6.25.1.8 Route redistribution

Routes can be redistributed from other route sources or protocols by means of OSPF. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by OSPF.

6.25.1.9 BGP

The distribution of routes learned dynamically from the Border Gateway Protocol is configured under **BGP**.



OSPF instance

Contains the name of the OSPF instance.

BGP instance

Contains the name of the BGP instance.

Prefix filter

Name of the prefix-filter list from *Prefix lists* on page 382.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The "Local preference" value of the BGP prefix is used or imported.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

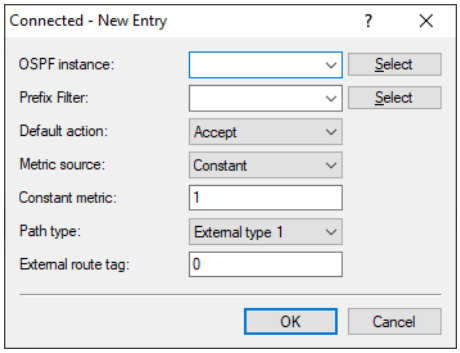
External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

6.25.1.10 Connected

The redistribution of routes that are automatically entered into the Routing table by the operating system is configured under **Connected**.



OSPF instance

Contains the name of the OSPF instance.

Prefix filter

Name of the prefix-filter list from *Prefix lists* on page 382.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

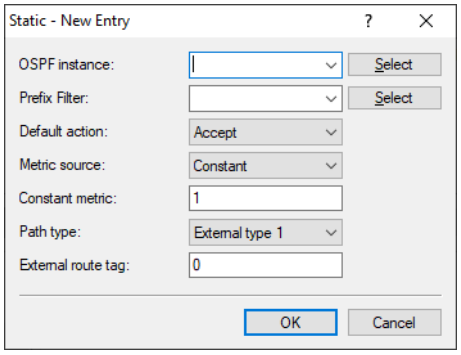
External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

6.25.1.11 Static

The redistribution of static routes, i.e. routes that the user manually enters into the routing table, is configured under **Static**.



OSPF instance

Contains the name of the OSPF instance.

Prefix filter

Name of the prefix-filter list from *Prefix lists* on page 382.

Default action

Defines the default handling of prefixes that are configured in the prefix list. Possible values:

Accept

Deny

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

6.25.2 Show commands via CLI

The available show commands are listed in the following:

- **show ospf-config**

  Displays a summary of the configured OSPF instances.

- **show ospf-database**

  Displays the OSPF database.

- **show ospf-graph**

  Displays the OSPF areas as a graphical representation in Graphviz format.

- **show ospf-neighbor**

  Displays information about OSPF neighbors.

- **show ospf-rib**

Displays information about the OSPF Routing Information Base.

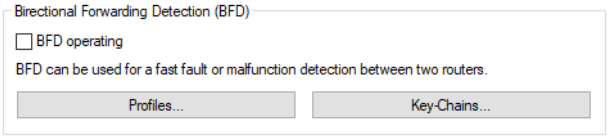
6.26 Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection according to *RFC 5880* is a simple Hello protocol to detect the loss of a connection between two routers. Hello packets are sent by both routers at a set interval. If these Hello packets are not received within a certain interval, the connection is assumed to be broken. In combination with BGP, BFD allows broken connections to be detected more quickly, since the BFD timers can be significantly shorter than the BGP timers.

Adjusting the timer interval allows lost connections to be detected faster or slower. The lower the timer interval, the faster connection losses are detected.

- BFD supports IPv4 and IPv6.
- There is no echo mode.
- BFD is a protocol that requires significant system resources, CPU time and bandwidth. BFD is processed exclusively in software. Hardware processing is not supported for BFD.
- Setting the Hello to a very short interval may result in BFD flapping or the detection of false positives. If false positives occur, you should increase the Hello interval.
- We do not recommend setting the Hello interval at less than 250ms.

In LANconfig you configure BFD under **Routing protocols** > **General** > **Bidirectional Forwarding Detection (BFD)**.

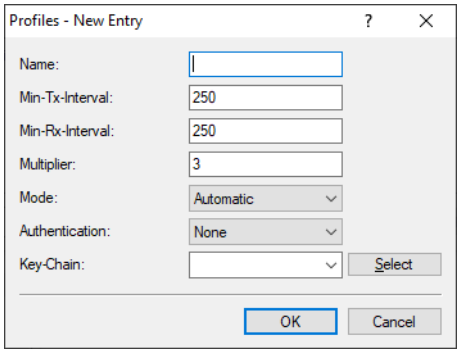


BFD operating

Activates or deactivates BFD globally

6.26.1 Profiles

To configure the BFD profiles switch to the view **IP Router** > **General** > **Bidirectional Forwarding Detection (BFD)** > **Profiles** .



Name

Enter a descriptive name for this BFD profile. If BFD is used in combination with BGP, this name is linked to the corresponding BGP neighbor.

Min-Tx-Interval

Minimum interval in milliseconds between sent BFD control messages. (Value range 1-9999 milliseconds, default 250)

Min-Rx-Interval

Minimum interval in milliseconds between received BFD control messages. (Value range 1-9999 milliseconds, default 250)

Multiplier

Number of packets not received for an interface to be declared as down. The multiplier and the interval together produce the time until a connection is declared as down. (Value range 1-255, default 3)

Mode

Specifies whether the BFD neighbor is single-hop or multi-hop connected. In single-hop mode, the UDP destination port 3784 and time-to-live of 1 are used in the IP header. Multi-hop mode uses UDP port 4784. In Automatic, single-hop mode is used if the route to the neighbor is of the type Connected LAN or WAN, otherwise multi-hop is used. By default, eBGP sessions are single-hop. iBGP sessions can be multi-hop. Possible values:

- Automatic
- Single-Hop
- Multi-Hop

Default: Automatic

Authentication

Specifies the type of authentication used for the BFD messages. Possible values:

- None
- Password
- MD5
- MD5-Meticulous
- SHA1
- SHA1-Meticulous

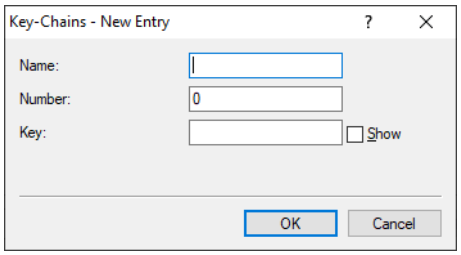
Default: None

Key-Chain

Name of the key chain from the table *Key-Chains*. Defines the key used for the BFD messages. For the parameter **Authentication**, a value must be configured that is other than "None".

6.26.2 Key-Chains

To configure the key chains, switch to the view **IP Router** > **General** > **Bidirectional Forwarding Detection (BFD)** > **Key-Chains**.



Name

Enter a descriptive name for this key chain. This name is used in the *BFD profiles* to reference this key chain.

Number

Key chain number.

Key

Key or password for this key chain.

6.26.3 Show commands via CLI

The available show commands are listed in the following:

- **show BFD-v4-details**

  Displays details about the IPv4 BFD connections.

- **show BFD-v6-details**

  Displays details about the IPv6 BFD connections.

- **show BFD-v4-status**

  Displays the status of the IPv4 BFD connections.

- **show BFD-v6-status**

  Displays the status of the IPv6 BFD connections.

6.27 BGP RPKI-RTR

The Border Gateway Protocol (BGP) is susceptible to route hijacking, i.e. unauthorized routers can advertise routes and thus redirect data traffic from the actual destination to itself. This situation can be caused by erroneous configurations and by explicit attacks.

Resource Public Key Infrastructure (RPKI) is a cryptographic method for signing and validating routing data records, which consist of a prefix and an autonomous system (AS). This record is called the Route Origin Authorization (ROA). More information on RPKI can be found in *RFC 6480*.

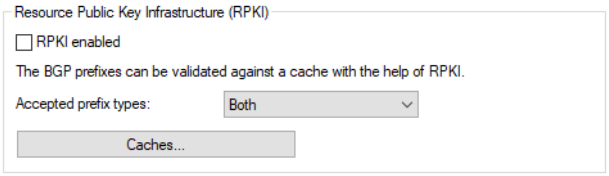
LCOS supports the Resource Public Key Infrastructure to Router Protocol (RTR) as per *RFC 8210*, with which a validator or cache supplies the router with information about validated routes and the associated AS number. This information is used by the BGP process to check whether a prefix or route was sent from the correct origin AS. Also checked is whether the prefix length corresponds to the information from the ROA data set.

This cache either runs on its own server for its own prefixes, or a public validator is used.

Public RPKI caches contain a large number of ROA entries. The recommendation is to operate RPKI only on devices with sufficient main memory to meet requirements (i.e. more than 2 GB), meaning that central-site devices or the vRouter need a correspondingly large main memory.

6.27.1 Configuring RPKI

RPKI can be found in LANconfig under **Routing protocols** > **General** > **Resource Public Key Infrastructure (RPKI)**. With the help of RPKI, BGP prefixes can be validated against a cache. To do this, the **Matches** table of the BGP policy provides an option for selecting the RPKI state of the relevant prefix. See *Matches* on page 526.



RPKI enabled

Activates or deactivates RPKI

Accepted prefix types

Specifies which ROA prefix types (IPv4 or IPv6) should be stored. To optimize the main memory, the prefix type is recommended to be restricted to the address family (IPv4, IPv6) that is actually operated.

Possible values:

Both

Both IPv4 and IPv6 RPKI records are stored on the device (default).

IPv4

Only IPv4 RPKI records are stored on the device.

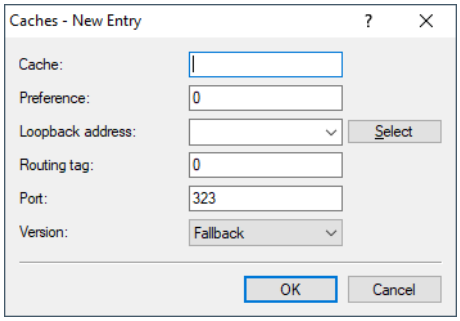
IPv6

Only IPv6 RPKI records are stored on the device

6.27.1.1 RPKI caches

This table is used to configure the RPKI validator or RPKI cache. The supported transport protocol is TCP.

The settings for the RPKI caches in LANconfig are located under **Routing protocols** > **General** > **Resource Public Key Infrastructure (RPKI)** > **Caches**.



Cache

IPv4, IPv6 address, or hostname where the RPKI cache is reached.

Preference

Preferred cache where multiple caches are used. Lower values result in a higher preference. Default: 0

Loopback address

You can optionally specify a source address that the RPKI client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

Routing tag

Enter the routing tag for setting the route to the cache. Default: 0

Port

The port of the RPKI cache. Default: 323

Version

Protocol version of the PRKI-RTR protocol operated. Possible values:

Fallback

Communication with the cache starts with version 1 and falls back to version 0 if necessary.

Zero

Protocol version 0 is used to communicate with the cache.

One

Protocol version 1 is used to communicate with the cache.

6.27.2 The CLI show commands

The available show commands are listed in the following:

- **show rpki-v4-cache**

  Displays all currently stored IPv4 ROAs received from the cache.

- **show rpki-v6-cache**

  Displays all currently stored IPv6 ROAs received from the cache.

- **show rpki-status**

  Displays the current status of the RPKI clients.

- **show bgp-prefix <prefix>**

  Along with the BGP prefix information, the show command also displays the RPKI state of the respective prefix (`Not found`, `Valid`, `Invalid`, `Not available`). The following RPKI state is possible for a BGP prefix:

  - `Not found`: The validator did not return any information about this prefix and the associated AS. It cannot be determined whether the entry is valid or invalid.
  - `Valid`: The validator returned information matching the prefix and AS in the BGP. The entry is therefore valid.
  - `Not valid`: The validator returned information that does not match the prefix and AS. Either the origin AS is incorrect or the prefix length does not match the data in the validator.
  - `Not available`: No data is available from the validator to perform a check. RPKI is either not enabled or the device has not yet retrieved data from the validator. The prefix is already in the BGP before information is available from the validator.

- **show bgp-v4-rib**

  Added the ROA-AS column, which contains the AS used for the RPKI check. The same applies to the ROA flag column, which contains the result of the ROA check.

- **show bgp-v6-rib**

  Added the ROA-AS column, which contains the AS used for the RPKI check. The same applies to the ROA flag column, which contains the result of the ROA check.

6.28 Locator / ID Separation Protocol (LISP)

The Locator/ID Separation Protocol (LISP) as per RFC 6830 is a new routing architecture that splits an IP address into two entities: The routing locator (RLOC) and the endpoint identifier (EID). The goal is to achieve a highly scalable routing architecture with integrated routing, tunneling and overlay protocols.

Conventional routing protocols such as RIP, OSPF or BGP work according to the "push principle" and proactively distribute their best routes to their neighbors. This architecture is of limited scalability, as the ever larger BGP tables and routing tables increasingly become a challenge.

LISP works according to the "pull principle" and works much like the Domain Name System (DNS). LISP routers register their networks, referred to as endpoint identifiers (EIDs), at a central instance called a map server or map resolver. Along with the EID, they also register their global (WAN) address, called the routing locator (RLOC). This keeps the information about the location (locator) separate from the identity (ID).

If a router wants to transfer data to a remote LISP network, first the LISP map resolver is queried for the mappings between the requested EID prefix and the routing locator. In the next step, a data tunnel is established between the two LISP routers.

LISP currently does not provide encryption of the data tunnel and, when used in insecure networks such as the Internet, it is typically combined with VPN. Application scenarios for LISP are multi-VPNs.

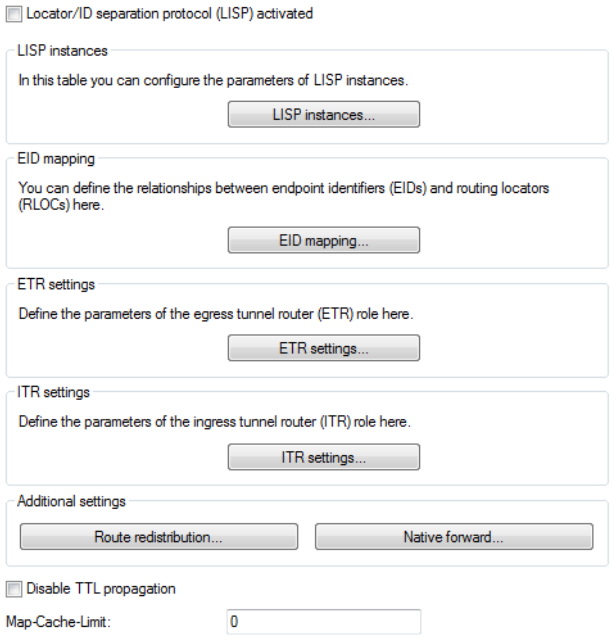
LCOS as of LCOS version 10.20 supports the following roles:

- Ingress tunnel router (ITR)
- Egress tunnel router (ETR)

The role of the map server/map resolver is currently not supported.

6.28.1 Configuration

LISP routing is configured in LANconfig under **Routing protocols** > **LISP**. The switch **Locator/ID separation protocol (LISP) activated** is used to switch this routing protocol on or off.



Disable TTL propagation

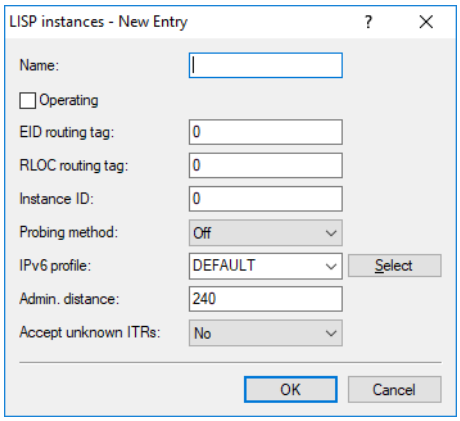
When enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

LISP instances

This table contains the global configuration of the LISP instances on the device.



Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

Entry active

Activates or deactivates this LISP instance.

EID routing tag

Routing tag of the endpoint identifier (EID) of this instance.

RLOC routing tag

Routing tag of the routing locator (RLOC) of this instance.

Instance ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

Probing method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries. Available methods:

- Off: The availability of the RLOCs is not checked periodically.
- RLOC probing: The availability of the RLOCs is periodically checked by LISP RLOC messages.

IPv6 profile

Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

Administrative distance

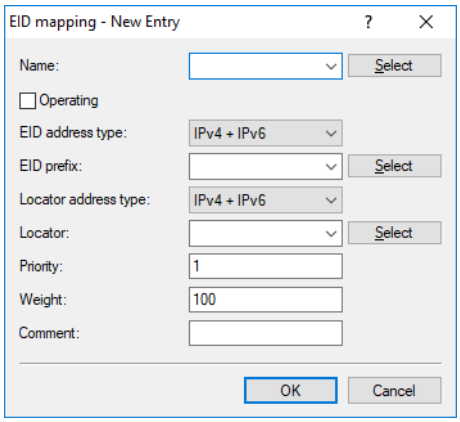
The administrative distance of this LISP instance.

Accept unknown ITRs

Specifies whether the router should accept LISP data packets from unknown ITRs with no map cache entry. This function is necessary especially for scenarios where the PITR and PETR are operated on different servers or IP addresses.

EID mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.



Name

References the name of the LISP instance.

Operating

Activates or deactivates this EID mapping.

EID address type

Protocol version of the EID prefix when referencing the EID prefix via an interface or network name. Possible values:

- **IPv4**: Only the IPv4 prefix of the referenced interface is used.
- **IPv6**: Only the IPv6 prefix of the referenced interface is used.
- **IPv4+IPv6**: Both the IPv4 prefix and the IPv6 prefix of the referenced interface are used.

EID prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority of the EID mapping. Default: 1.

Weight

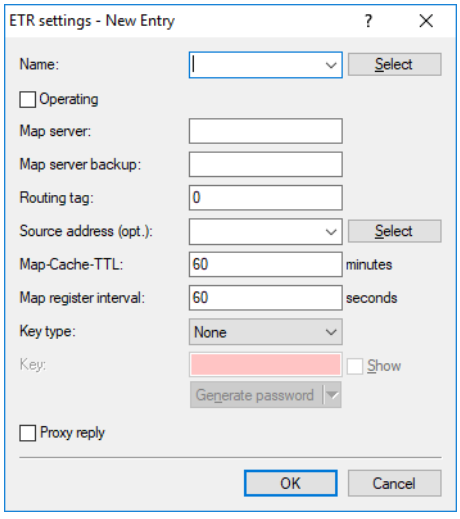
The weight of the EID mapping. Default: 100.

Comment

Enter a descriptive comment for this entry.

ETR settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).



Name

References the name of the LISP instance.

Operating

Activates or deactivates these ETR settings.

Map-Server

IPv4 or IPv6 address of the LISP map server

Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

Routing tag

Routing tag to be used to access the map server.

Source address (opt.)

Contains the sender address as the named interface that is used with the map server in LISP communication.

Map-Cache-TTL

Time-to-live of the EID mappings in minutes registered with the map server.

Map register interval

Registration interval in seconds in which map registrations are sent to the map server.

Key type

Algorithm used for authentication at the map server. Possible values:

- None
- HMAC-SHA-1-96
- HMAC-SHA-256-128

Key

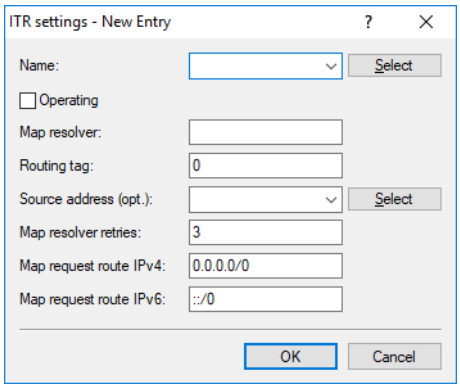
Key or password used to register the EID mapping on the map server.

Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

ITR settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).



Name

References the name of the LISP instance.

Operating

Activates or deactivates these ITR settings.

Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

Routing tag

Routing tag used to access the map resolver.

Source address (opt.)

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

Map-Resolver-Retries

Number of retries for map requests to the map resolver. Default: 3

Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

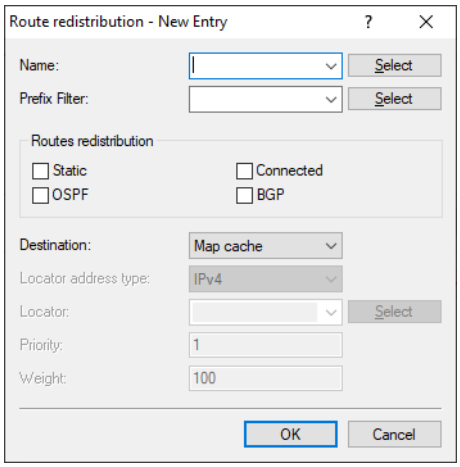
Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

Route redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.



Name

References the name of the LISP instance.

Prefix filter

Name of the prefix-filter list from *Prefix lists* on page 382. Route redistribution is allowed for prefixes in this list.

Route redistribute

Specifies the route sources of the imported routes.

- **Static**: The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

- **Connected**: From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **OSPF**: The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **BGP**: The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

Destination

Specifies the destination of routes imported to LISP. Possible values:

- **Map cache**: Imports the routes into the map cache. LISP performs map requests for these routes.
- **EID table**: Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority. Default: 1

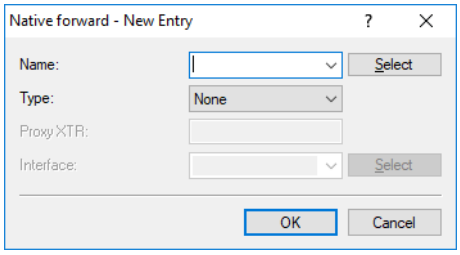
Weight

The weight. Default: 100

Native forward

If LISP networks are to communicate with non-LISP networks, proxy routers can be used. These roles are referred to as proxy ingress tunnel routers (proxy ITRs) and proxy egress tunnel routers (proxy ETRs).

If a LISP router receives a negative response from the map resolver, i.e. there is no mapping between the requested EID and an RLOC, the LISP router can either send the associated packets to a proxy xTR (packet with LISP header) or send it via another local interface (packet without LISP header).



Name

References the name of the LISP instance.

Type

Defines how to send packets to non-LISP networks.

- **None**: Packets to non-LISP networks are not forwarded but dropped
- **Proxy xTR**: Packets to non-LISP networks are sent to a proxy xTR

› **Interface**: Packets to non-LISP networks are sent via a local interface

Proxy xTR

IPv4 or IPv6 address of the proxy xTR used to send packets to LISP networks.

Interface

Name of the interface used to send packets to non-LISP networks.

6.28.2 LISP tutorial

In this tutorial we will configure a LISP network on the basis of an ARF network that is named INTRANET and uses tag 1. This involves registering the network prefix as an EID prefix with the MAP server 1.1.1.1. Registration is performed via the WAN remote site INTERNET (default route), which uses tag 0. The IP address of the INTERNET remote site can be dynamic or static. This address is registered as an RLOC address with the MAP server.

Data from the INTRANET should be sent to the LISP tunnel. For this purpose, the router requesting an unknown destination sends a map request to the MAP resolver 1.1.1.1.

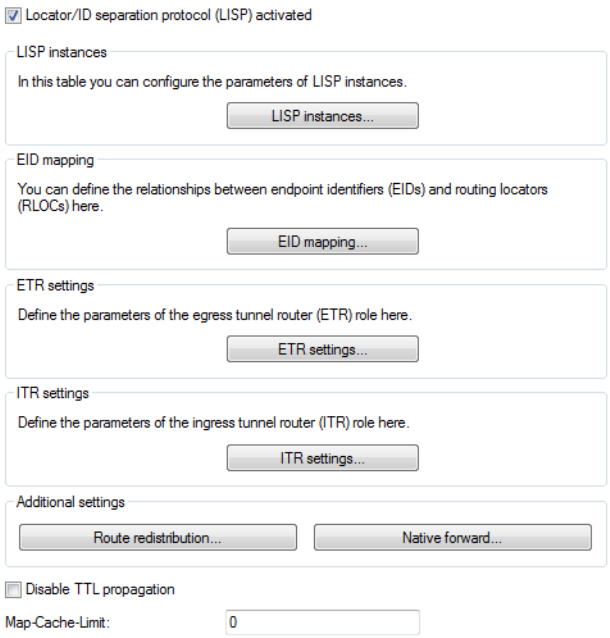
If the map resolver returns a positive mapping, LISP automatically establishes a dynamic tunnel to the remote LISP router and enters the corresponding routes into the routing table.

If the map resolver returns a negative mapping, i.e. the destination prefix is unknown or is not registered on the map server/resolver, then the packet can optionally be sent directly over the INTERNET remote site, without using a tunnel (native forward).

LISP routes do not have to be configured manually. LISP automatically creates routes and later deletes them.

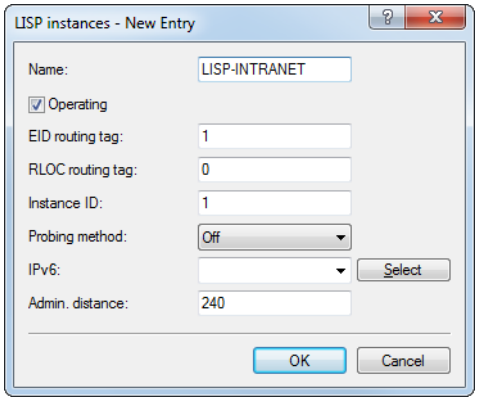
As a matter of principle, entries for the routing tags have to be created manually in the WAN tag table.

1. First, enable the LISP protocol under **Routing protocols** > **LISP** > **Locator/ID separation protocol (LISP) activated**.

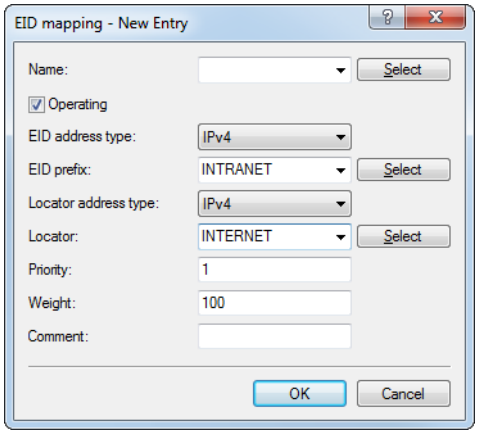


2. Create a new entry in the table of LISP instances. Do this by navigating to **Routing protocols** > **LISP** > **LISP instances** and then click on **Add**.
   a) Give this LISP instance a **Name**, e.g. LISP-INTRANET.
   b) Enable the entry **Operating**.

c) Set the **EID routing tag** to 1.
d) Set the **RLOC routing tag** to the value of the tag of the WAN remote site INTERNET, in this case 0.
e) Set the **Instance ID** to the value created on the LISP map server, in this case 1 like the tag of the INTRANET.
f) Under **IPv6** you can remove the entry **DEFAULT**, as we are only considering IPv4 here.

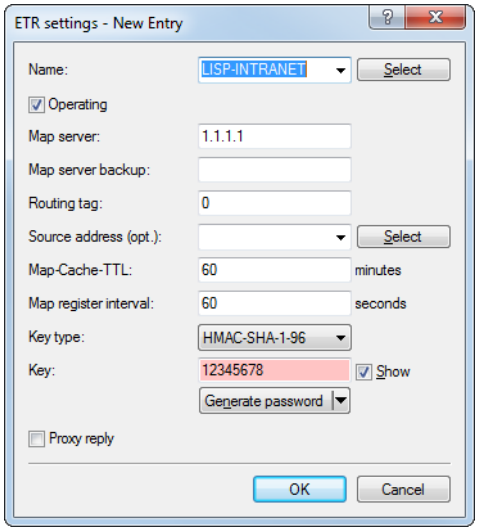


3. Create a new entry in the EID mapping table, which is used to link the EID prefix and the locator. Do this by navigating to **Routing protocols** > **LISP** > **EID mapping** and then click on **Add**.
a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
b) Enable the entry **Operating**.
c) Set both the **EID address type** and the **Locator address type** to IPv4.
d) Set the **EID prefix** to INTRANET.
e) Set the **Locator** to INTERNET.



4. In the ETR settings table, create a new entry containing the parameters for communication with the map server. Do this by navigating to **Routing protocols** > **LISP** > **ETR settings** and then click on **Add**.
a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
b) Enable the entry **Operating**.
c) Set the **Map server** to 1.1.1.1.
d) Set the **Routing tag** to 0.

e) Set the **Key type** and the **Key** for connecting to the map server. These must match the type and password configured on the map server. In this example we take HMAC-SHA-1-96 and 12345678.



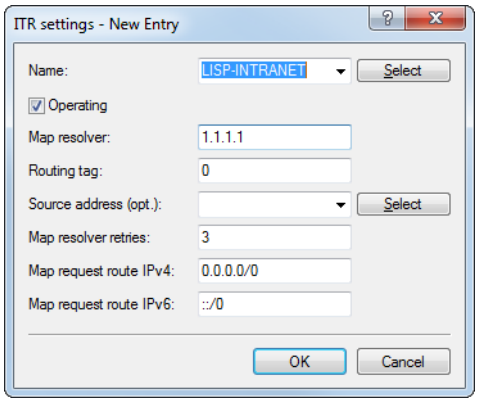
5. In the ITR settings table, create a new entry containing the parameters for communications with the map resolver. Do this by navigating to **Routing protocols** > **LISP** > **ITR settings** and then click on **Add**.

   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.

   b) Enable the entry **Operating**.

   c) Set the **Map resolver** to 1.1.1.1.

   d) Set the **Routing tag** to 0.

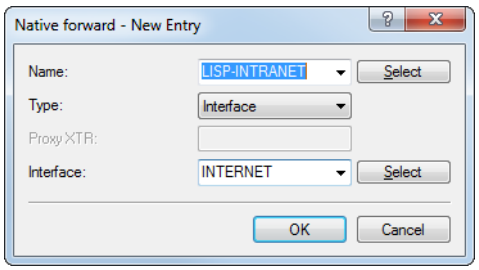


6. Optional: Packets to destinations that are not LISP networks can be sent directly via a local interface, i.e. without using the LISP tunnel. In our example, the interface to be used is INTERNET. Create a new entry in the Native forward table. Do this by navigating to **Routing protocols** > **LISP** > **Native forward** and then click on **Add**.

   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.

   b) Set the **Type** to **Interface**.

c) Set the **Interface** to INTERNET.



7. Navigate to **Communication** > **Remote sites** > **WAN tag table**, click on **Add** and create an entry for the LISP instance with the instance ID of 1 that you just created.

   For each LISP instance, an entry with the corresponding interface tag for the EID/ARF network must be created in the WAN tag table.

   Do this by creating each entry with the name for the remote site set to LISP-<LISP instance ID>*. The name of each remote site is formed from the keyword LISP supplemented by the corresponding LISP instance ID (in hexadecimal form) and the wildcard *. This unequivocally assigns the incoming traffic from the LISP tunnel to the EID/ARF network.

   The instance ID must be specified in hexadecimal without a leading 0x.

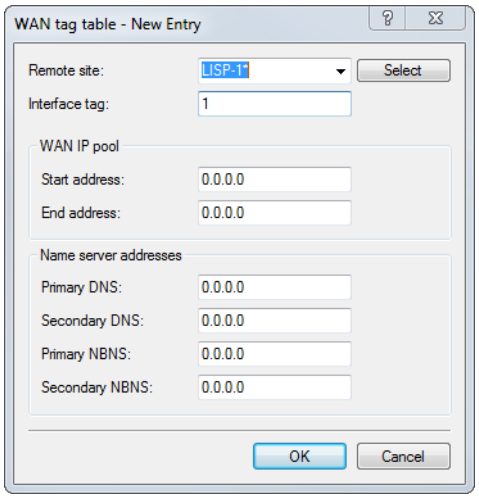
   Representation: LISP-<LISP instance ID>*

   Examples:

   - For LISP instance 1: LISP-1*
   - For LISP instance 15: LISP-F*

   a) Fill out the **Remote site** field as described above, i.e. the LISP instance with instance ID 1 takes the value "LISP-1*".

   b) Set the **Interface tag** to 1.



That's it!

6.29 Route monitor

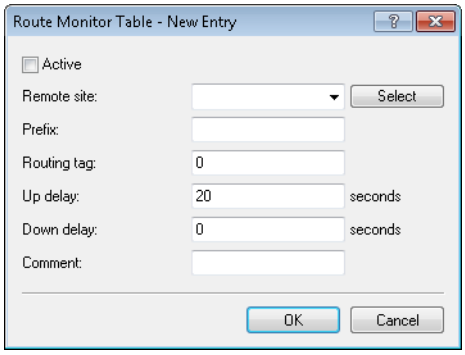
The route monitor observes the connections to the networks of different providers and establishes a backup connection in case of failure. The monitoring makes use of a trigger prefix, which providers supply in their routing protocol, for

example with the Border Gateway Protocol (BGP). As soon as a route to a provider's network becomes unavailable, the route monitor declares the relevant trigger prefix to be invalid for its network and opens a backup connection to the provider's network.

6.29.1 Configuring the route monitor with LANconfig

To activate the route monitor, switch to the view **Communication** > **Backup** and check the option **Route monitor active**.

To configure the route monitor, open the **Route monitor table**.



Active

Specifies whether this backup connection is enabled.

Remote site

Contains the name of the backup remote site.

Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

Routing tag

Contains the routing tag of the prefix being monitored.

Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

The value "0" causes the device to disconnect from the backup peer immediately after the prefix arrives (no delay).

Comment

Comment on this entry.

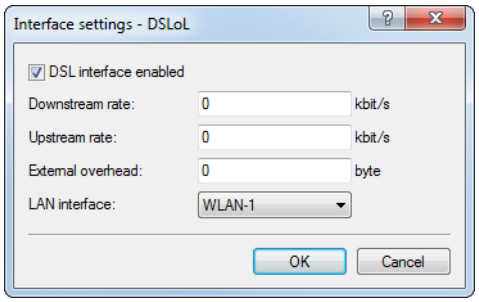
6.30 DSLoL for WLAN routers

IPv4 addresses can only be masked ("NAT") on WAN connections. If you want to masquerade in the direction of a LAN or WLAN interface, then the corresponding LAN or WLAN interface must be declared as a DSL port in order for it to establish a WAN connection (typically by IPoE or DHCPoE).

Until LCOS10.12, this was only possible for access points. From LCOS10.20, DSLoL is also available for WLAN routers.

An example scenario for DSLoL:

A WLAN router should be used to connect to the Internet primarily over WLAN. This is done using the WLAN client mode. If the WLAN is not available, the Internet connection should instead be established via LTE/4G as a backup. For this purpose, an LTE/4G connection is configured as usual, and the other WLAN-based Internet connection is set up by operating DSLoL on the WLAN interface. This is done in LANconfig under **Interfaces** > **WAN** > **Interface settings** > **DSLoL** by selecting the option **DSL interface enabled** and then setting the **LAN interface** to the WLAN that was earlier set up as the WLAN client.



The LTE/4G connection is now configured as a backup for the WLAN/DSLoL Internet connection.

6.31 WWAN bridge mode

The cellular modem integrated into the router can be used in two operating modes: Router mode and Bridge mode. In router mode, the router establishes the mobile connection itself and receives an IP address on its WWAN connection (e.g., IPv4 address and/or IPv6 address/prefix), allowing a downstream network to access the Internet via Network Address Translation (NAT). The IP address assigned by the provider is shared with multiple LAN clients in this case.

In bridge mode, the router acts as a simple network bridge and forwards all IP packets from the mobile network to exactly one downstream device. This device therefore receives the IP address assigned by the provider directly and must establish the WAN connection (via DHCP) to the provider and handle NAT and routing for the internal network.

Bridge mode is useful when the device is intended to operate purely as a modem, for example, to avoid double NAT in a router cascade. The WWAN bridge mode is conceptually comparable to the bridge mode of DSL modems.

The device providing bridge mode itself does not have an IP address on the WWAN interface and therefore cannot establish a direct connection to the mobile network, as data packets are transparently forwarded. If the device is to be managed via the LMC, for example, Internet access must be established through an alternative route.

Only the first client that connects to the device in bridge mode receives the IP address assigned by the mobile network. Packets from the cellular modem are passed on without VLAN tagging.

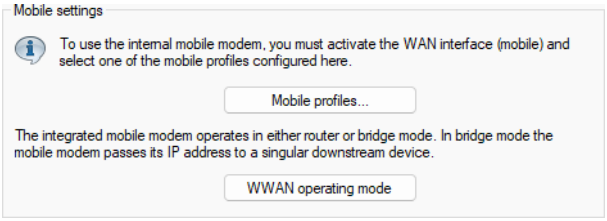
It is recommended to configure ICMP polling on the WAN connection of the downstream device, as it is not possible by design for the modem to notify the downstream device of a connection loss or address change. ICMP polling allows the downstream device to detect an interruption in the mobile connection.

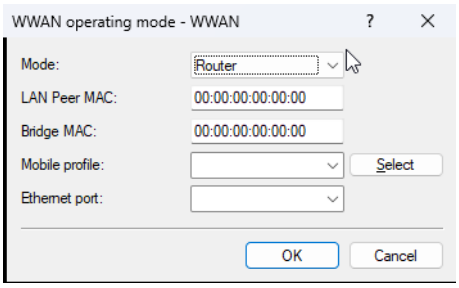
Configuration of the WWAN bridge mode is generally performed in the following steps:

1. The operating mode of the WWAN modem is set to “Bridge”, and an appropriate WWAN profile for the cellular parameters must also be specified.
2. The “WWAN” interface is configured together with a LAN interface (e.g., LAN-2) in a common bridge group. The corresponding LAN interface is assigned to an ETH port.

6.31.1 Configuration

You can find the configuration of the WWAN Bridge Mode in LANconfig under **Interfaces** > **WAN** > **Mobile settings** > **WWAN operating mode**.





Mode

Defines the operating mode of the device's internal mobile interface. Possible values:

Router

In Router Mode, the device establishes the cellular connection itself and obtains an IP address on its WWAN interface. A downstream network gains Internet access via Network Address Translation (NAT).

Bridge

In Bridge Mode, the device acts as a transparent network bridge and forwards all IP packets from the mobile network to exactly one downstream device. Detailed bridge configuration is performed in the LAN Bridge settings.

LAN Peer MAC

MAC address of the device or client in the LAN that should receive the IP address directly from the mobile network. If the MAC address is 0, the MAC address learned from received packets is used automatically.

Bridge MAC

MAC address to be used as the sender address. If the MAC address is 0, a "locally administered" address derived automatically from the device's MAC address is used.

Mobile profile

Defines the WWAN profile to be used.

Ethernet port

Defines the Ethernet port, e.g. ETH-1, on which the device signals in WWAN bridge mode by briefly bringing the Ethernet port up and down that the WWAN connection has been interrupted or re-established.

In bridge mode, the WWAN router acts solely as a modem and transparently forwards the cellular connection (WWAN) to the downstream router. The downstream router then assumes all routing functionality (NAT, DHCP, firewall, etc.). In this case, the WWAN router is not responsible for address assignment or routing.

If the WWAN connection is disconnected or re-established while the router is operating in bridge mode, the following problems may occur: The downstream router may incorrectly assume that the WWAN connection is still active and therefore display incorrect status information and attempt to send data over this connection.

For WWAN connections with a dynamic IP address, the router uses the old, no longer valid IP address while in the error state.

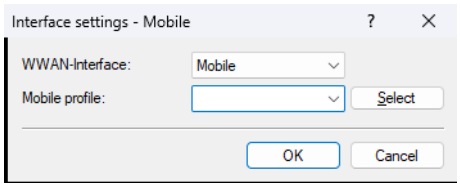
To avoid these problems, the WWAN bridge router must send an “Ethernet Port Down / Port Up” signal to the Ethernet port that is connected to the downstream router in the event of a connection failure. When the cellular modem changes state (disconnecting and establishing the cellular connection), the WWAN router physically switches off the Ethernet port for a few seconds.

This mechanism reliably informs the downstream router that the connection has been interrupted, allowing it to delete the default route, restart the DHCP client or mark the old IP address as no longer valid, and signal the failure of the cellular connection to the user.

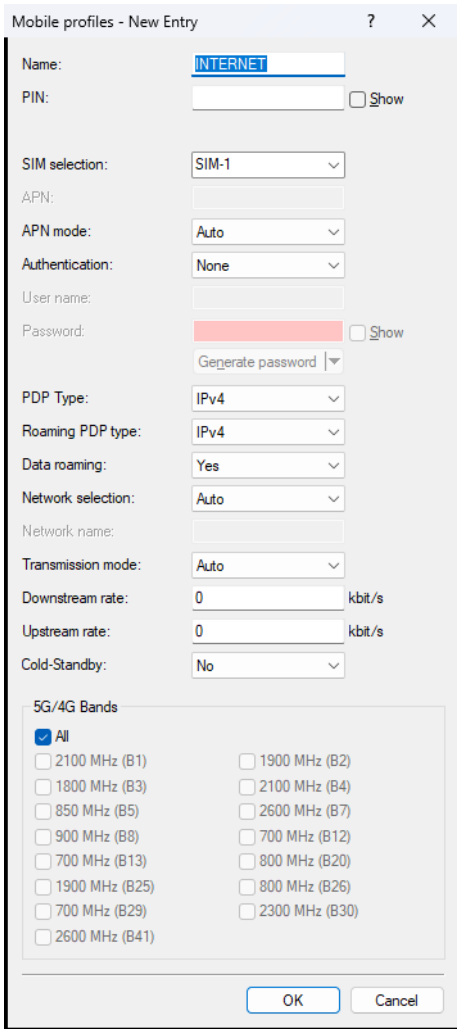
Ideally, the WWAN bridge device should be connected directly to the downstream router via an Ethernet cable so that the downstream router reliably detects the state change. If this type of installation is not possible, the downstream router should perform IP polling to actively monitor the logical Internet connection.

6.31.2 WWAN Bridge Mode Tutorial

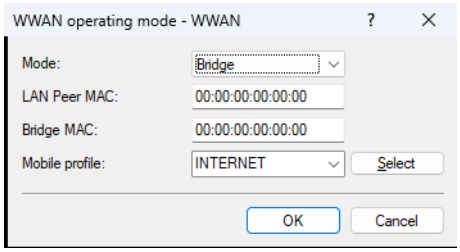
1. Open the configuration in LANconfig under **Interfaces** > **WAN** > **Interface Settings** > **Interface Settings** > **Mobile**. Set **Mobile Profile** to “empty”.



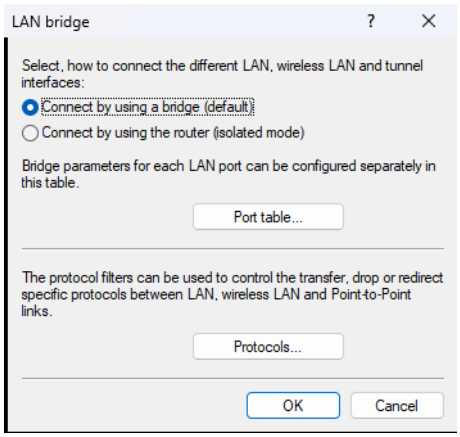
2. Open the configuration under **Interfaces** > **WAN** > **Mobile Settings** > **Mobile Profiles**. Configure the required settings for your mobile provider here.



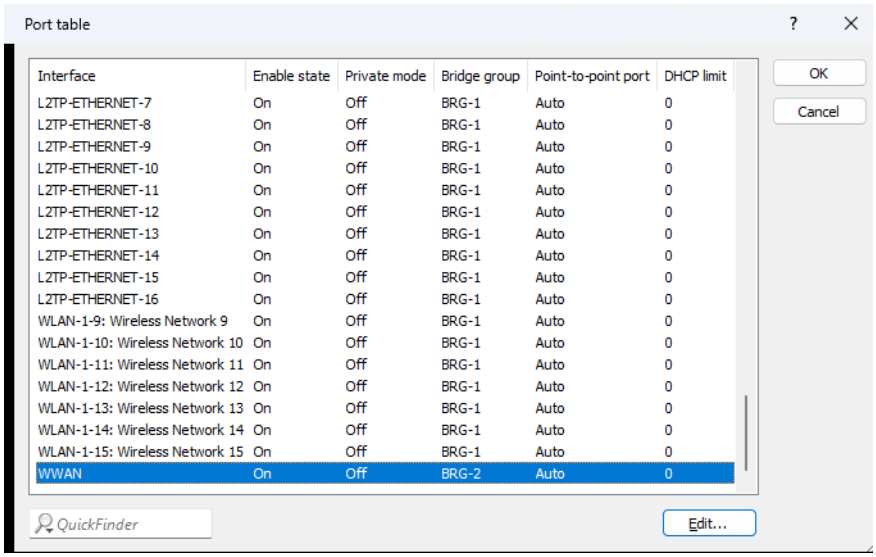
3. Open the configuration under **Interfaces** > **WAN** > **Mobile Settings** > **WWAN Operating Mode**. Set the **Mode** to "Bridge", set **LAN Peer MAC** and **Bridge MAC** to "00:00:00:00:00:00", and select the **Mobile Profile** created in step 2.



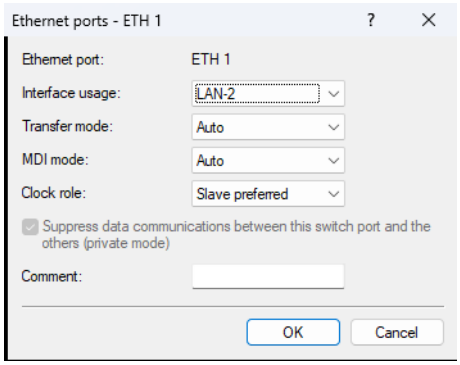
4. Enable the LAN bridge under **Interfaces** > **LAN** > **LAN Bridge Settings** > **LAN Bridge**.



5. Open the **Port Table** . To forward traffic from the mobile modem to an Ethernet port, the WWAN interface and a corresponding LAN interface must be configured together in a common bridge group. In this example, LAN-2 and WWAN are configured in bridge group BRG-2. Use a different bridge group if BRG-2 is already in use for WLAN or other functions.



6. Open **Interfaces** > **LAN** > **Ethernet Switch Settings** > **Ethernet Ports**. Configure one Ethernet port to use the LAN interface that belongs to the shared bridge group with the WWAN interface. In this example, LAN-2 is bound to Ethernet port ETH-1, which is grouped together with WWAN in bridge group BRG-2.



Please observe the following:

- No route or WWAN peer configuration is required for a WWAN device in bridge mode, because the device does not operate as a router and only requires a bridge configuration. It is recommended to delete any existing WWAN peer configurations (including the default WWAN zero-touch peer) to avoid configuration issues and unnecessary error messages caused by failed peer connection attempts.
- The router cannot reach the Internet itself via the mobile modem when operating in bridge mode.
- Ensure that only a single endpoint device is connected to the Ethernet port used for bridge mode, because only one device can obtain an IP address from the mobile network. The LAN Peer MAC address configuration ensures that only one fixed MAC address receives the IP address.
- No internal or external DHCP server may be active in the WWAN bridge group.

7 IPv6

7.1 IPv6 basics

IPv4 (Internet Protocol version 4) is a protocol for unique addressing of nodes in a network and, at the time of writing, it has defined all of the IP addresses assigned globally. The limited availability of address space required the development of IPv6 (Internet Protocol version 6), which is to replace the former standard. With a different IP-address structure, IPv6 provides for a greater range of IP addresses and thus increases the possible number of participants in networks worldwide.

7.1.1 Why use IPv6-standard IP addresses?

The new IPv6 standard was developed for the following reasons:

- IPv4 address space allows for approximately four billion IP addresses for unique identities in networks. When the IPv4 standard was implemented in the 1980s this address space was considered to be sufficient. Due to the enormous growth of the World Wide Web and the unexpectedly large number of computers and network devices, an address shortage has arisen that the IPv6 standard should solve.
- The increase in address space with IPv6 hampers the scanning of IP addresses by viruses and Trojans. The broader spectrum provides greater protection against attacks.
- IPv6 has been implemented with a view to the security requirements. For this reason it uses the security protocol IPSec (IP Security). This provides secure network communications on layer 3 whereas many of IPv4 security mechanisms only operate on higher layers.
- Simplified, fixed descriptors for data packets save on router processing power and thus accelerate the available throughput.
- IPv6 allows for easier and faster transmission of data in real time, making it suitable for multimedia applications such as Internet telephony and Internet TV.
- So-called mobile IPs allow you to use a fixed IP address to login to different networks. This allows you to log on with your laptop using the same IP address, whether you are in your home network, in a café or at work.

7.1.2 IP address structure according to the IPv6 standard

IPv6 addresses are 128 bits long and the range of possible addresses can cater for about 340 sextillion network participants. IPv6 addresses consist of eight blocks of 16 bits and are written as hexadecimal numbers. The following is an example of a possible IPv6 address:

"2001:0db8:0000:0000:0000:54f3:dd6b:0001/64"

To improve the legibility of these IP addresses, zeros at the beginning of a block of numbers are omitted. It is also possible to omit one group of blocks that consist entirely of zeros. For the above example, one possible representation would be as follows:

"2001:db8::54f3:dd6b:1/64"

An IPv6 address consists of two parts; a prefix and an interface identifier. The prefix denotes the membership of the IP address to a network, while the interface identifier (e.g. in the case of auto-configuration) is generated from a link-layer address, and thus belongs to a particular network card. The device can also generate interface identifiers from random numbers. This improves security. In this way, multiple IPv6 addresses can be assigned to a single component.

The prefix describes the first part of the IP address. The length of the prefix is shown as a decimal number after a slash. For the example given here the prefix is:

"2001:db8::/64"

The remainder of the IP address is the interface identifier. In our example, this is:

"::54f3:ddb6:1"

Compared with the IP addresses for the IPv4 standard, a number of changes have resulted in the structure of the new IPv6 addresses:

- While IPv4 addresses cater for an address space of 32 bits, the new length of 128 bits results in a significantly larger address space with IPv6. IPv6 addresses are four times longer than IPv4 addresses.
- An interface can have multiple IPv6 addresses due to the potential assignment of multiple prefixes to a single interface identifier. With the IPv4 standard, an interface has only one IP address.
- The automatic assignment of IPv4 addresses always takes place via a DHCP server. However, IPv6 can operate an auto-configuration, which makes the use of a DHCP server unnecessary. However, the option of using a DHCP server is still open to you, as is the static configuration of the IP address.

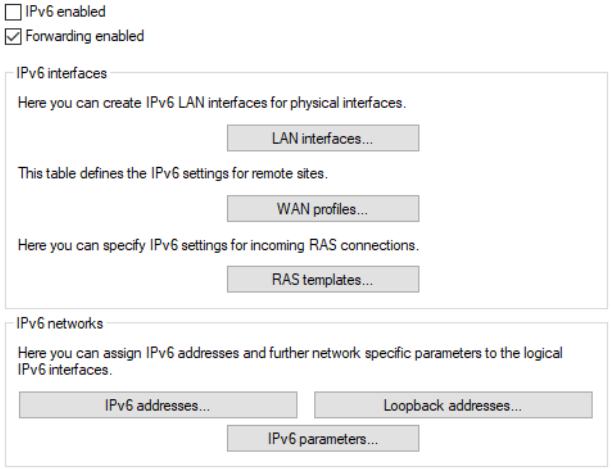
7.1.3 Stages of migration

IPv6 is available to networks in a variety of ways. We make a distinction between environments with native IPv6 and those which provide IPv6 through a tunnel.

- **Native IPv6:** Native IPv6 describes a network that communicates to the outside via IPv6. Users with IPv4 Internet access can only access this network if the router uses one of the tunnel technologies described below.
- **IPv6 via dual stack:** Dual stack refers to the parallel operation of IPv4 and IPv6 in a network.
- **IPv6 tunneling:** If a router does not have native IPv6 Internet access, a tunnel can be used for accessing IPv6 networks.

7.2 Basic settings

Use the configuration page **IPv6** > **General** to make the basic settings.



IPv6 enabled

This is where you can enable or disable IPv6 for the device.

Forwarding enabled

Forwarding is used for packet forwarding between IPv6 interfaces. This option is activated by default.

IPv6 interfaces

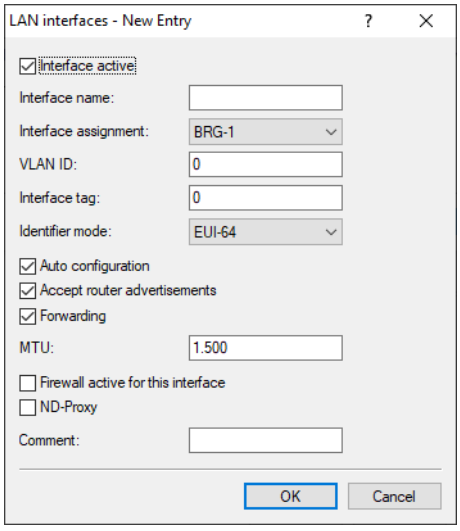
The buttons **LAN interfaces**, **WAN profiles** and **RAS templates** access the tables where you can add new interfaces, configure existing interfaces, or delete them.

IPv6 networks

The buttons **IPv6 addresses** and **IPv6 parameters** are used to assign IPv6 addresses to interfaces and to configure the interface parameters (gateway address, primary and secondary DNS). Using the **Loopback addresses** button, you can define IPv6 loopback addresses which the device considers to be additional sender addresses.

7.2.1 LAN interfaces

For each existing IPv4 network, you must create an equivalent IPv6 network under **LAN interfaces**. Here, the settings for interface binding, routing tag, and VLAN ID must match the settings of the corresponding IPv4 network settings. Because a device can have multiple IPv6 addresses, you must add statically configured IPv6 addresses under **IPv6 addresses**.



Entries in the **LAN interfaces** table have the following meaning:

Interface active

Activates or deactivates this LAN interface.

Interface name

Enter a name for the logical IPv6 interface which is to apply to the physical interface (interface assignment) and the VLAN ID.

Interface assignment

Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface. With IPv6, the mapping “any” used with IPv4 is no longer possible.

VLAN-ID

Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.

Interface tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Identifier mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Auto configuration

Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.

If the device itself sends router advertisements from this interface, it does not produce IPv6 addresses from received router advertisements from other routers, even when auto-configuration is enabled.

Accept router advertisements

Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

Forwarding

Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.

MTU

Here you set the valid MTU for the corresponding link.

Firewall active for this interface

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.

ND-Proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

Possible scenarios:

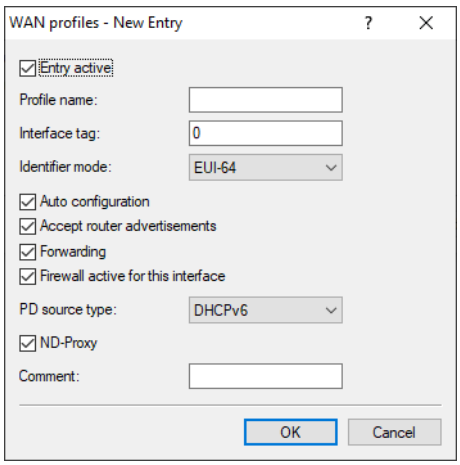
- An upstream router does not support DHCPv6 prefix delegation. The downstream router enables the ND proxy and uses the same /64 prefix on its LAN and WAN interfaces. The LAN prefix is generated from the router advertisement of the upstream router of the WAN interface. This enables communication between LAN stations and WAN stations that use the same /64 prefix.
- A VPN gateway assigns dial-up clients an IPv6 address from the same prefix that is already configured on a local interface. This router must enable the ND proxy to allow communication between dial-in clients and stations on the local LAN with the same IPv6 prefix. This scenario is analogous to the ARP proxy for IPv4.

Comment

Enter a descriptive comment for this entry.

7.2.2 WAN profiles

For each remote site with which you want to communicate using IPv6, you must additionally create an equivalent logical IPv6 WAN interface under **WAN profiles**. This profile is then selected at the remote site.



Entries in the **WAN profiles** table have the following meaning:

Entry active

Enables or disables this profile on a logical IPv6 WAN interface.

Profile name

Give the profile of the logical IPv6 interface a name. This name can be used to select the profile at the corresponding IPv6 remote site. The default is always the profile "DEFAULT". If an empty entry is selected as an IPv6 remote station, then IPv6 is not active for this remote site.

A profile in the WAN interfaces table can be referenced multiple times by remote sites.

Interface tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Identifier mode

Defines how automatically generated IPv6 addresses are created on the respective interface of the device.

EUI-64

Automatically generated IPv6 addresses on the configured interface are generated according to the EUI-64 principle, i.e., the MAC address is used as the basis for the host portion of the IPv6 address.

Stable privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Auto configuration

Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.

Accept router advertisements

Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

Forwarding

Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.

Firewall active for this interface

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here. To globally enable the firewall for all interfaces, navigate to **Firewall/QoS** > **General** and check the option **IPv6 firewall/QoS enabled**.

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

PD source type

This option allows you to set the way the router performs the prefix delegation:

DHCPv6

Prefix delegation is performed via DHCPv6.

Router-Advertisement

Prefix delegation is performed via router advertisement and the DHCPv6 client does not start.

Cellular networks that support IPv6 only support DHCPv6 prefix delegation as of 3GPP Release 10. Consequently, a terminal device in a mobile network older than Release 10 can only be assigned one /64 prefix, for example by means of router advertisements. IPv6 support is easy to implement for smartphones or laptops using this method. However, an IPv6 router needs at least one more prefix that it can propagate to clients on the LAN.

IPv6 prefix delegation from the WWAN to the LAN allows clients to work on the LAN with a /64 prefix that is assigned from the WAN. A consequence of this is that a router is able to operate in an IPv6 cellular network without DHCPv6 prefix delegation and neighbor discovery proxy (ND proxy). The router announces the retrieved /64 prefix on the LAN by router advertisement, instead of adding it at the WAN interface. Clients generate an address from this prefix and use it for their IPv6 communications.

The following restrictions apply:

- You can only use the feature on point-to-point connections (e.g. PPP or cellular interfaces), whereby the remote station automatically sends all data traffic to the router, unless the ND proxy is also activated.
- You can only create one IPv6 network on the LAN since only one /64 prefix is available.

ND proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

Example scenarios:

- An upstream router does not support DHCPv6 prefix delegation. The downstream router enables the ND proxy and uses the same /64 prefix on its LAN and WAN interfaces. The LAN prefix is generated from the router advertisement of the upstream router of the WAN interface. This enables communication between LAN stations and WAN stations that use the same /64 prefix.
- A VPN gateway assigns dial-up clients an IPv6 address from the same prefix that is already configured on a local interface. This router must enable the ND proxy to allow communication between dial-in clients and stations on the local LAN with the same IPv6 prefix. This scenario is analogous to the ARP proxy for IPv4.

Comment

Enter a descriptive comment for this entry.

7.2.3 RAS templates

There are basically two ways to manage the configuration of RAS remote stations:

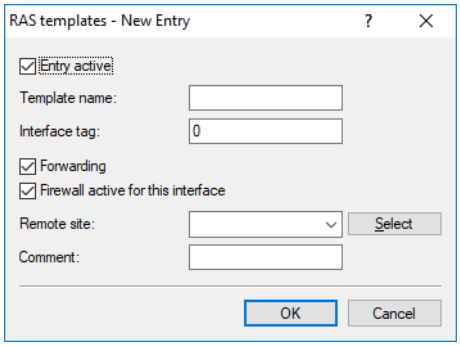
The user data or the configurations are locally stored on the device.

The advantage of this alternative is that a RADIUS server is not necessary, which reduces the management and cost of the network infrastructure.

The user data or the configurations are stored on an external RADIUS server.

The advantage of this alternative is the centralized user management for extensive distributed network scenarios.

For RAS access via IPv6, you must also set up the corresponding **RAS templates**.



Entries in the **RAS templates** table have the following meaning:

Entry active

Enable or disable this RAS template here.

Template name

Here you define the name of the RAS interface that the IPv6 remote sites use for access.

Interface tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Forwarding

Enables or disables the forwarding of data packets to other interfaces.

Firewall active for this interface

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, navigate to **Firewall/QoS** > **General** and check the option **IPv6 firewall/QoS enabled**.

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

Remote site

Specify the remote site or a list of remote sites for RAS dial-in users.

The following values are possible:

- A single remote station from the tables under **Setup** > **WAN** > **PPTP-Peers**, **Setup** > **WAN** > **L2TP-Peers** or **Setup** > **PPPoE-Server** > **Name-list**.
- The wildcard "*" makes the interface valid for all PPTP, PPPoE and L2TP peers.
- The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL" .

Using the wildcards you can create several peers for IPv6 RAS services based on so-called template interfaces These template interfaces can be used as normal interfaces for IPv6 services such as DHCPv6 server or router advertisements. For example, using these, a group of RAS interfaces can be provided from an IPv6 prefix pool.

Comment

Enter a descriptive comment for this entry.

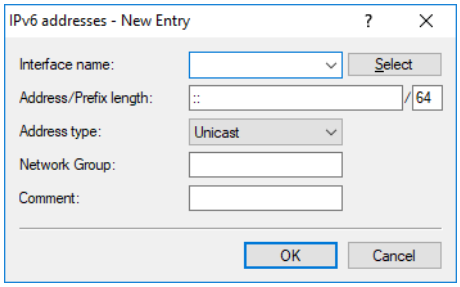
Information on RADIUS attributes for IPv6 RAS services can be found under *RADIUS attribute extensions for IPv6 RAS services* on page 1555.

If RAS clients are to be delegated to an IPv6 DNS server or are to receive their prefixes by prefix delegation, you must create a corresponding entry in the table **DHCPv6 networks** under **IPv6** > **DHCPv6**.

If you wish to authenticate a user by PPP list, you navigate to **Communication** > **Protocols** > **PPP list** and enable the option **Activate IPv6 routing** for that user.

7.2.4 IPv6 addresses

The **IPv6 addresses** table is used to create IPv6 addresses for LAN and WAN interfaces.



Entries in the **IPv6 addresses** table have the following meaning:

Interface name

Give a name to the interface that you want to assign the IPv6 network.

Address / prefix length

Specify an IPv6 address including the prefix length for this interface.

The default prefix length is 64 bits ("/64"). If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device (e.g. auto configuration) are designed for a maximum length of 64 bits.

Example:

- Global unicast address: 2001:db8::1/64
- Unique local address: fd00::1/64

Link-local addresses are fixed and not configurable.

Address type

Specify the type of IPv6 address.

Options:

› Unicast

With the Unicast address type, you use the **Address/prefix length** field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64".

› Anycast

With the Anycast address type, you can also use the **Address/prefix length** field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64". Internally, the device handles this address as an anycast address.

› EUI-64

With the address type EUI-64, IPv6 addresses conform to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64". EUI-64 ignores any value set as "interface identifier" in the corresponding IPv6 address and replaces it with an interface identifier as per EUI-64. The prefix length for EUI-64 must be "/64".

› Delegated Auto Configuration

The IPv6 address is formed from the router advertisement prefix received on the selected interface (**Interface name** field) and the host identifier from the field **Address / Prefix length**. The field **Address / Prefix length** can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/64" on the interface to form the address "2001:db8::2/64".

› Delegated DHCPv6

The IPv6 address is formed from the delegated DHCPv6 prefix received on the selected interface (**Interface name** field) and the host identifier from the field **Address / Prefix length**. The field **Address / Prefix length** can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/56" on the interface to form the address "2001:db8::2/64". Similarly, an address can be formed from any subnet of the delegated prefix, e.g "0:0:0:0001::1" and the prefix "2001:db8::/56" go to form the address "2001:db8:0:0001::1/64".

› Stable privacy

Automatically generated IPv6 addresses on the configured interface are formed according to RFC 7217. The generation no longer relies on the unique MAC address of the device or the interface but, for privacy reasons, uses a combination of random values and the received provider prefix. The generated interface identifier remains stable or identical as long as the received prefix is the same. If the prefix changes, the interface identifier and, therefore, the entire IPv6 address of the device also changes.

Network group

Enter a descriptive name for this combination of IPv6 address and prefix. This label of the network group does not have to be unique. Consequently, several different prefixes can belong to a network group.

The network group can be referenced in the IPv6 firewall in the station table under **Firewall/QoS** > **IPv6 rules** > **Station objects** in the field **Network name** if the **Type** there is set to "Named network". The station then consists of all prefixes in this network group.

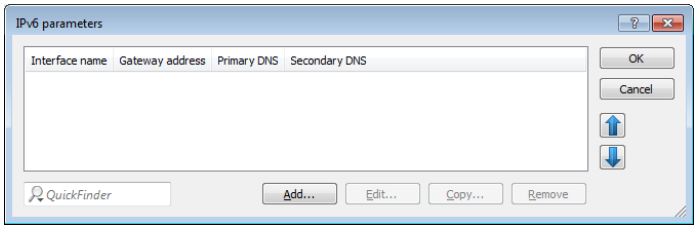
Furthermore, you can reference it in the VPN in the table **VPN** > **General** > **Network rules** > **IPv6 rules** in the field **Local networks**. As a result, all prefixes of the network group end up on the local side of the network relationship.

Comment

Enter a descriptive comment for this entry.

7.2.5 IPv6 parameters

The table **IPv6 parameters** is used to manually configure static parameters for LAN or WAN interfaces, an IPv6 DNS server, or an IPv6 gateway if you choose not to use autoconfiguration or DHCPv6.



Entries in the **IPv6 parameters** table have the following meaning:

Interface name

Give a name to the interface for which the IPv6 parameters are to be configured.

Gateway address

Specify the IPv6 gateway to be used by this interface.

This parameter overrides gateway information that the device may receive via router advertisements, for example.

DNS default

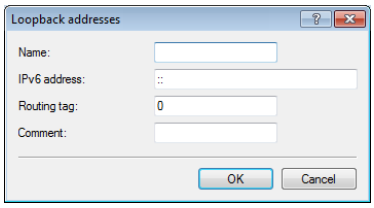
Specify the primary IPv6 DNS server to be used by this interface.

Secondary DNS

Specify the secondary IPv6 DNS server to be used by this interface.

7.2.6 Loopback addresses

IPv6 loopback addresses can be specified in the **Loopback addresses** table. The device sees each of these addresses as its own address, which is also available if a physical interface is disabled, for example.



Entries in the **Loopback addresses** table have the following meaning:

Name

Enter a unique name for this loopback address.

IPv6 address

Enter a valid IPv6 address here.

Routing tag

Here you specify the routing tag of the network that the loopback address belongs to. Only packets with this routing tag will reach this address.

Comment

You have the option to enter a comment here.

7.2.7 Setting up IPv6 Internet access

You can set up access to an IPv6 network if

- You have an IPv6-capable device,
- You use a tunneling technology and
- Your provider supports a native IPv6 network or you have access to a so-called tunnel broker who can mediate your IPv6 packets.

7.2.7.1 IPv6 access using the Setup Wizard in LANconfig

The Setup Wizard assists you with the configuration of IPv6 access with your equipment.

The Wizard presents following options:

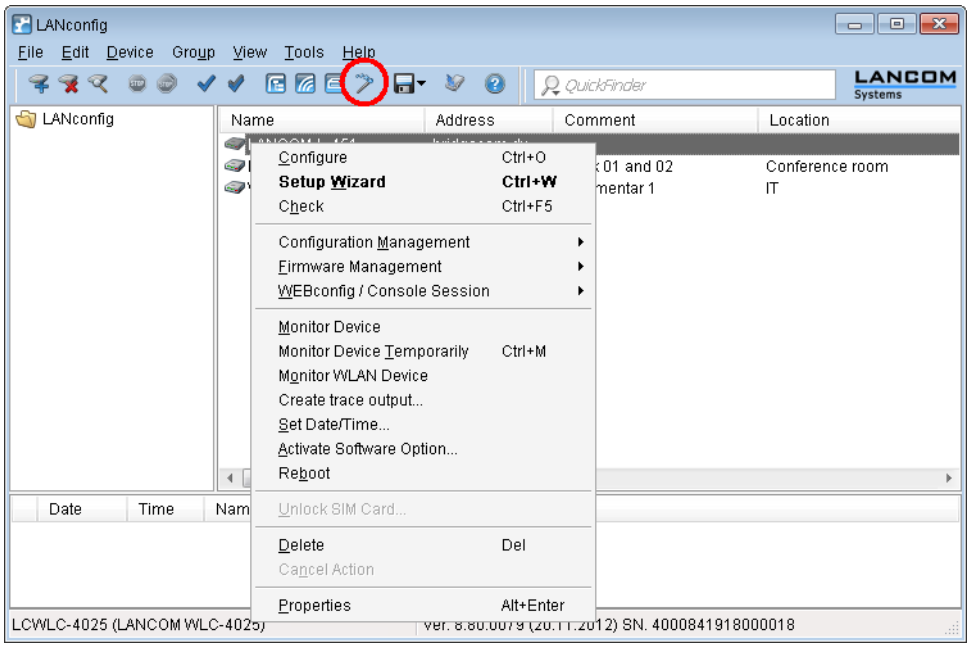
- *Set up IPv6 access for a new, unconfigured device.*
- *Set up IPv6 access on an existing device in addition to the existing IPv4 access.*

Setup Wizard – setting up IPv6 in a new device

If you have connected up a new device but not have yet configured it, you have the option of using a Setup Wizard to set up IPv4 and IPv6 connections.

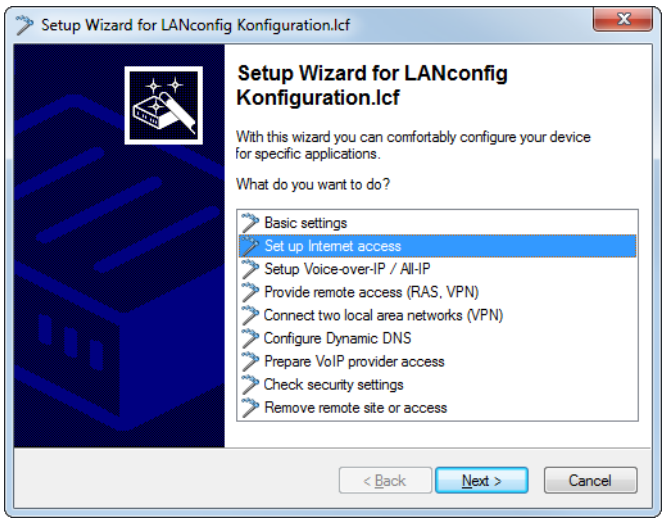
To save your entries and proceed to the next screen, click **Next**.

1. Start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



The options displayed by the wizard depend on the options available with your device and from your Internet provider.

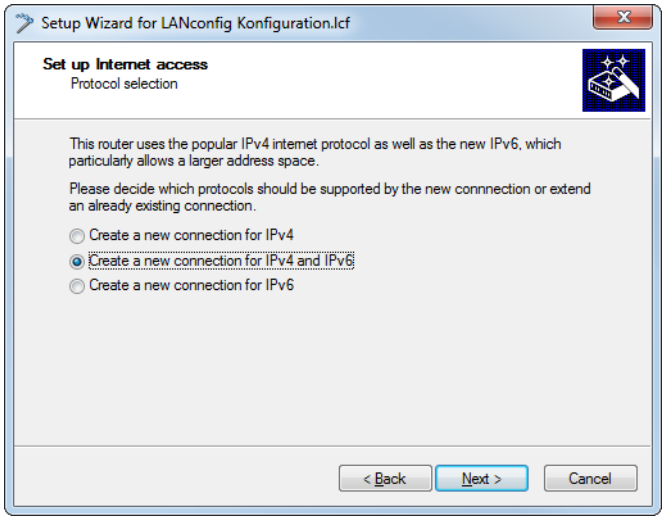
2. In the Setup Wizard, select the option **Set up Internet access**.



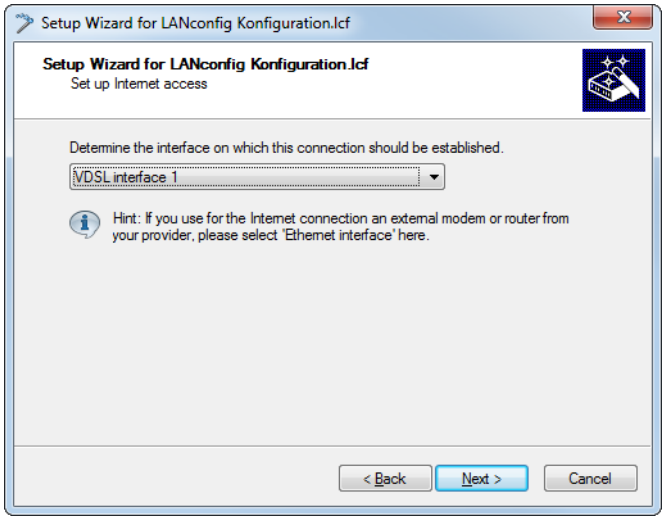
3. You can choose from the following options:

   - Set up a connection for both IPv4 and IPv6. This is the recommended option for a new device.
   - Set up an IPv4-only connection.
   - Set up an IPv6-only connection.
   - Supplementing an existing IPv4 connection with IPv6

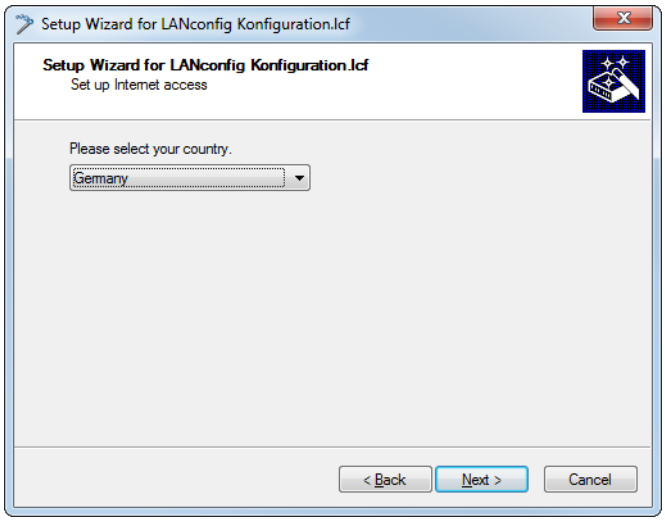
   In the following we take you through the setup of a dual-stack connection. Activate the appropriate selection.



4. Set the interface to be used for the connection.



5. Select your country from the list.

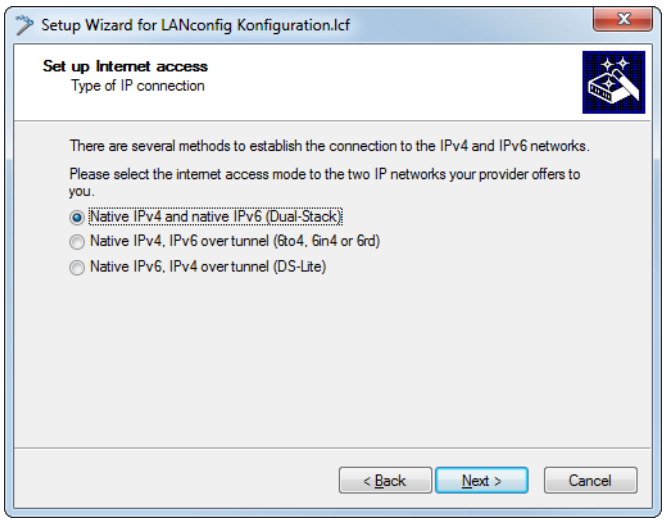


6. Select your Internet provider.

   You can select from the following entries:

   - A selection of relevant Internet providers
   - Internet connection via PPP over ATM
   - Internet connection via PPP over Ethernet
   - Internet access via Plain Ethernet
   - Internet access via PPTP
   - Internet access via DHCP
   - Internet access with static IP

7. The type of IP access depends on your Internet provider.



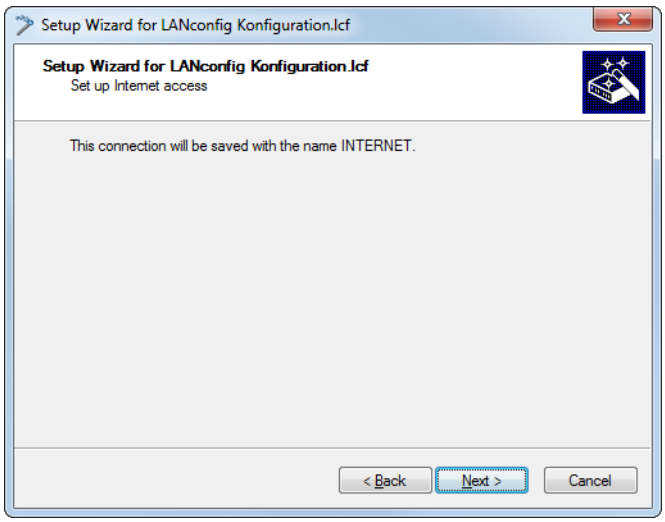
You can select from the following options:

- **Native IPv4 and native IPv6 (dual-stack)**: Configure a direct connection without a tunnel.
- **Native IPv4, IPv6 via tunnel**: Start the wizard to configure a 6to4, 6in4 or 6rd tunnel.
- **Native IPv6, IPv4 via tunnel (DS-Lite)**: Start the wizard to configure a DS-Lite tunnel.

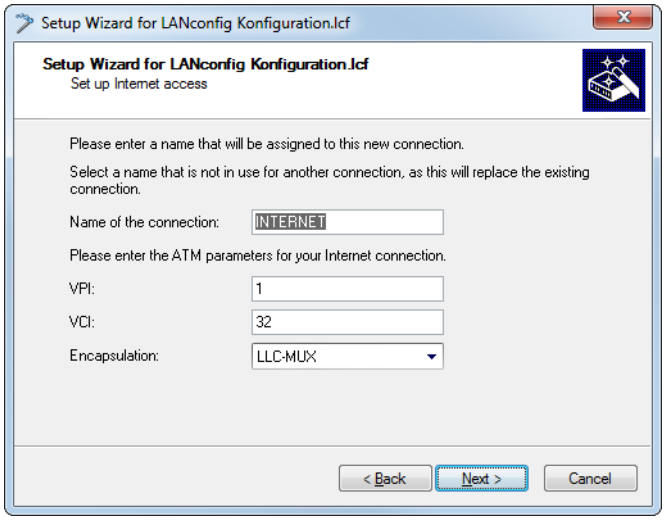
Select the option for setting up a native IPv6 Internet connection.

8. The name for this connection is “INTERNET”.

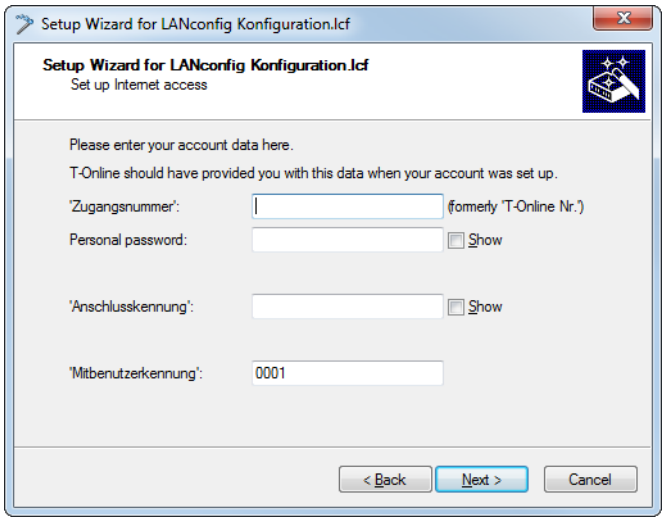
If a connection already exists with this name, you can specify a separate name for this connection.



If you access the Internet with an alternative connection, e.g. over a PPPoE connection, you should additionally enter the appropriate ATM parameters.

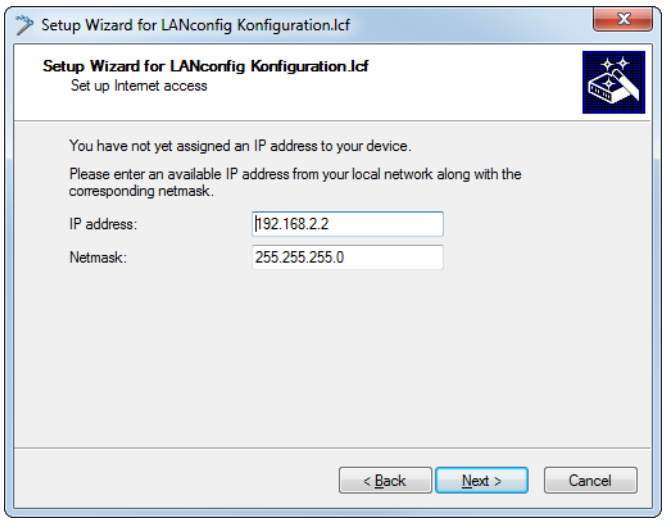


9. Enter the login details given to you by your provider for setting up your Internet access.

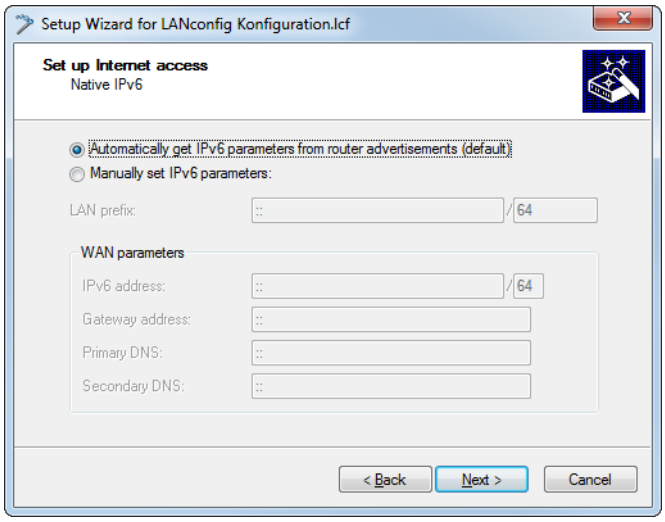


Depending on the provider, the type and number of fields may vary.

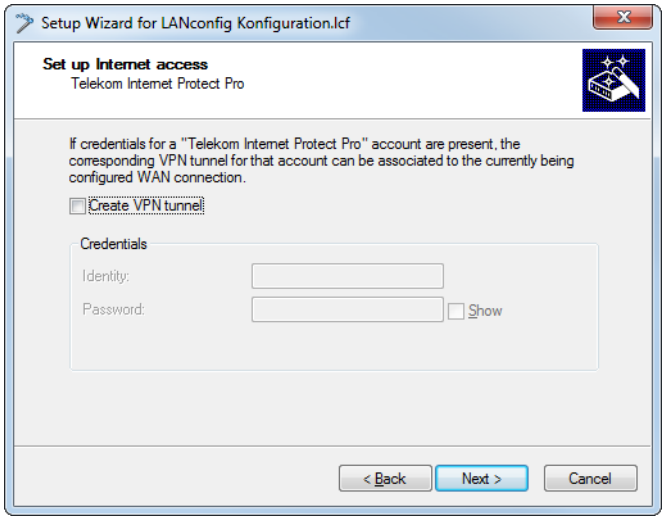
10. If your device does not yet have an IP address, enter a new IP address and corresponding netmask.



11. Accept the default setting of **Automatically take IPv6 parameters from router advertisements.**



12. Further options may be set up, depending on the Internet provider.



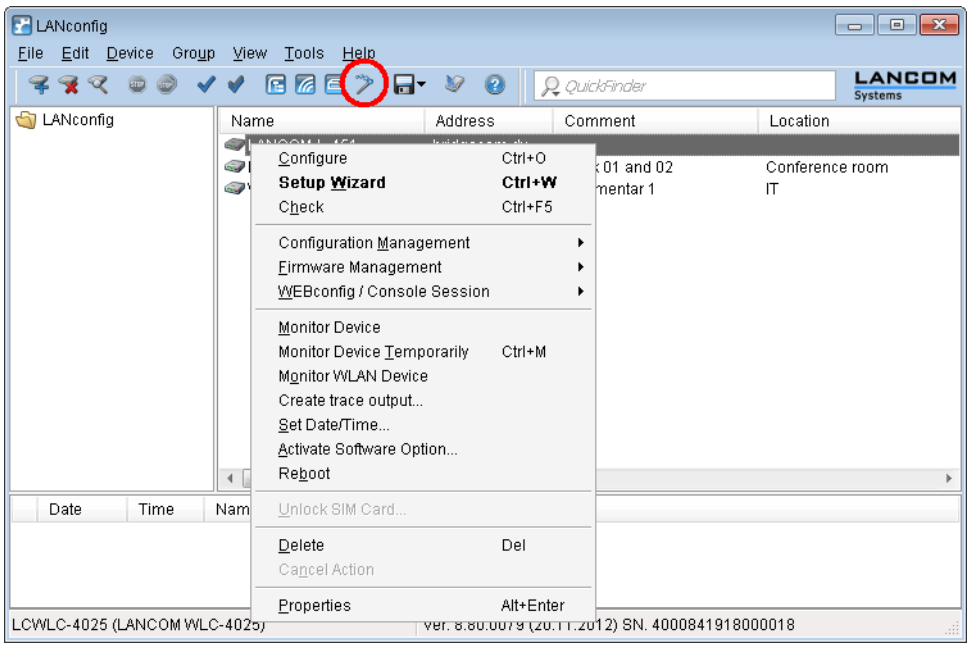
13. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.

Setup Wizard – Setting up IPv6 on an existing device

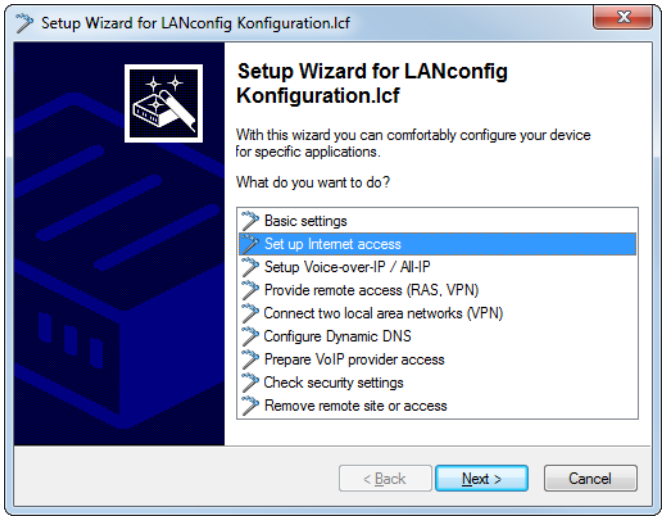
If you have a device configured for IPv4 and you wish to set up an additional IPv6 connection, you have the option of setting up the IPv6 connections with the Setup Wizard.

To save your entries and proceed to the next screen, click **Next**.

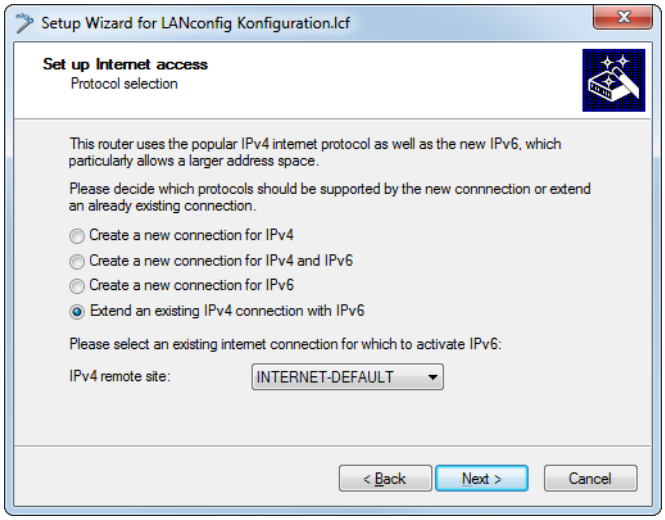
1. Start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



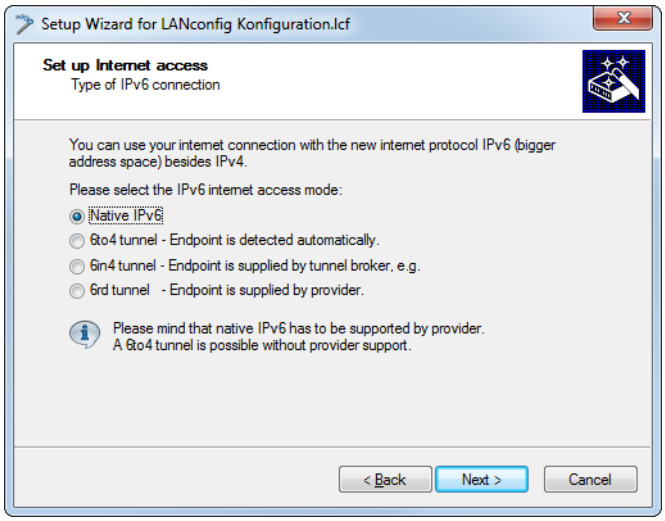
2. In the Setup Wizard, select the option **Set up Internet access**. To continue, click on **Next**.



3. Because your device is already IPv4-capable, the Setup Wizard gives you the opportunity to extend your existing settings with IPv6. Select this option and click on **Next.**



4. Select the type of IPv6 Internet access.

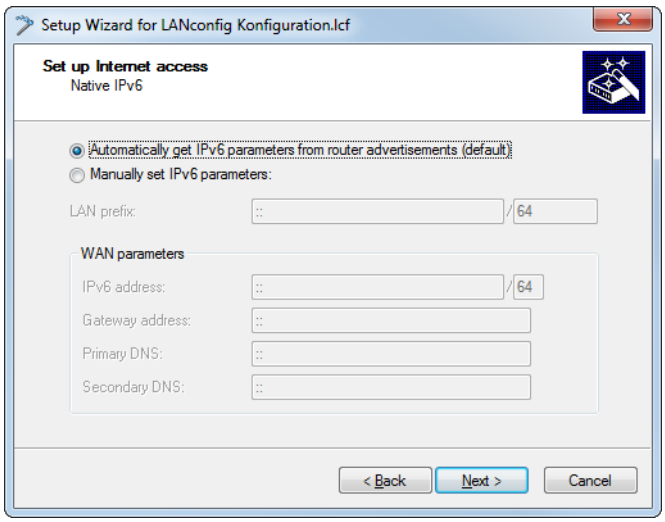


You can select from the following options:

- **Native IPv6**: Configure a direct connection without a tunnel.
- **6to4 tunnel** Start the wizard to configure a 6to4 tunnel.
- **6in4 tunnel**: Use the input mask to set the parameters for the 6in4 tunnel.
- **6rd tunnel**: Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

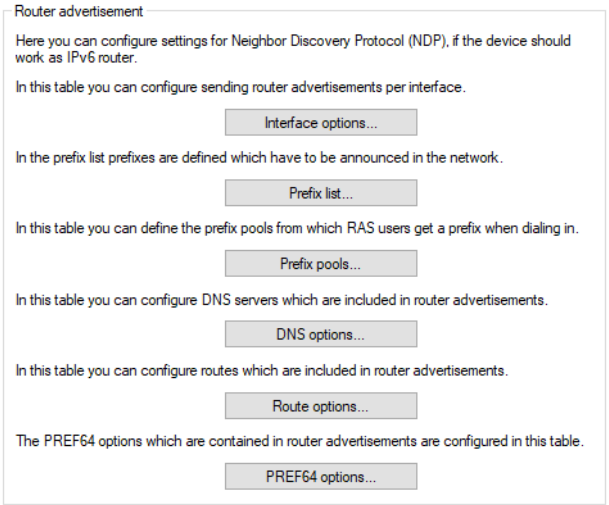
5. Accept the default setting of **Automatically take IPv6 parameters from router advertisements.**



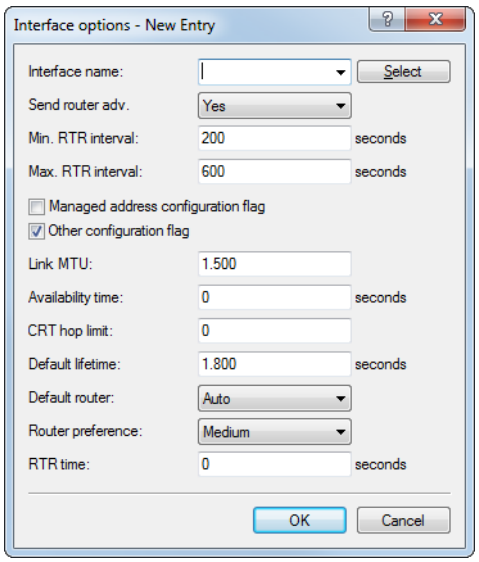
6. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.

7.3 Router-Advertisement

The **Router advertisement** configuration provides you with several buttons for setting up the Neighbor Discovery Protocol (NDP) if the device is to operate as an IPv6 router:



7.3.1 Interface options



Here you can enable or disable the following interface functions:

Interface name

Defines the name of the logical interface to be used for sending router advertisements.

Send router adv.

Regulates the periodic transmission of router advertisements and the response to router solicitations.

Min. RTR interval

Defines in seconds the minimum time allowed between the transmission of unsolicited multicast router advertisements. Min. RTR interval and Max. RTR interval form a time space during which router advertisements are sent at random. Permitted values are between 3 seconds and 0.75 * Max. RTR Interval. Default is 200 seconds.

Max. RTR interval

Maximum value of the RTR interval.

Managed address configuration flag

With this function enabled, clients receiving this router advertisement will configure their addresses with stateful autoconfiguration (DHCPv6). Clients then automatically retrieve other information, e.g. the DNS server.

Other configuration flag

If this function is active, a client will attempt to obtain additional information via DHCPv6, such as DNS server addresses. For each prefix, you can specify whether or not a client should form addresses by auto-configuration: Navigate to the **Prefix list** under **Allow auto-configuration (SLAAC)**.

Link MTU

Specifies the valid MTU for the corresponding link.

Availability time

Specifies the time for which the router is considered to be available. The default 0 means that no availability time is propagated in the router advertisements.

Hop limit

Defines the maximum number of routers to be used to forward an IP data packet. One router corresponds to one "hop". Default is 0, meaning no hop limit is specified.

Default router

Defines how the device advertises itself as the default gateway or router. The parameters have the following functions:

Automatic

As long as a WAN connection exists, the device sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway.

If there is no WAN connection, the router sets the router lifetime to 0. A client then stops using this router as the default gateway.

Always

The router lifetime is always positive—i.e. greater than 0—irrespective of the WAN connection status.

Never

The router lifetime is always 0.

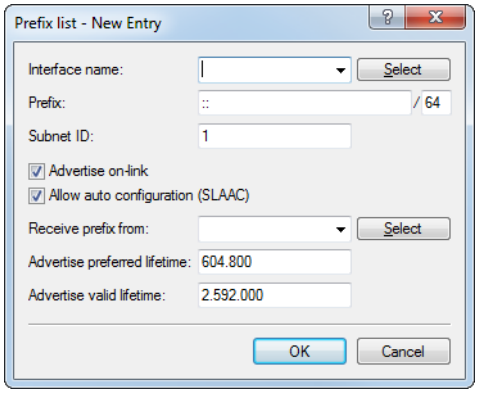
Router priority

Defines the preference of this router. Clients enter this preference into their local routing tables.

RTR time

Specifies the time in seconds between successive transmissions of neighbor-solicitation messages to a neighbor if the address is being resolved or the accessibility is being tested.

7.3.2 Prefix list



Used to set the prefix options for used interfaces. The following settings are possible:

Interface name

Defines the name of the logical interface to be used for sending router advertisements.

Prefix

Enter a prefix that is announced with router advertisements, e.g. "2001:db8::/64". The prefix length must always be exactly "/64", otherwise it will be impossible for clients to generate their addresses by adding their interface identifiers (with a length of 64 bits). If a prefix delegated by the provider is to be propagated automatically, set "::/64" here and enter the name of the corresponding WAN interface as the parameter **Receive prefix from**.

Subnet ID

Here you enter the subnet ID that is to be combined with the prefix delegated by the provider. If the provider assigns the prefix "2001:db8:a::/48", for example, and the subnet ID is "0001" (or "1" for short), then the

router advertisement on this interface is given the prefix “2001:db8:a:0001::/64”. The maximum subnet length with a 48-bit long delegated prefix is 16 bits (i.e. 65,536 subnets), with available subnet IDs ranging from “0000” to “FFFF”. With a delegated prefix of “/56”, the maximum subnet length is 8 bits (i.e. 256 subnets) with subnet IDs ranging from “00” to “FF”. In general, the subnet ID “0” is used when the WAN IPv6 address is formed automatically. This is why subnet IDs for LANs start at “1”. The default setting is “1”.

Advertise on-link

Specifies whether this prefix is linked directly to the interface ('on link').

Allow auto-configuration (SLAAC)

Specifies whether the prefix is to be used for a stateless address autoconfiguration (SLAAC). The default setting is “enabled”.

Receive prefix from

Specifies the name of the interface used to receive a prefix via DHCPv6 prefix delegation or tunnel. This prefix can be used to derive and propagate a subnet for each interface.

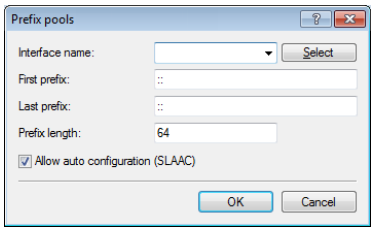
Advertise preferred lifetime

Specifies how long an IPv6 address should be considered as “preferred”. If the preferred lifetime of an address has expired, it is marked as “deprecated” and used only for existing sessions, but not for new ones.

Advertise valid lifetime

Specifies how long an IPv6 address should be considered as “valid”, after which it becomes “invalid” and is discarded.

7.3.3 Prefix pools



This table contains the pools of prefixes which RAS users receive when they connect remotely via IPv6. The following settings are possible:

Interface name

Specifies the name of the RAS interface that is valid for this prefix pool.

First prefix

Specifies the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., “2001:db8::”. Each user is assigned precisely one /64 prefix from the pool.

Last prefix

Specifies the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. “2001:db9:FFFF::”. Each user is assigned precisely one /64 prefix from the pool.

Prefix length

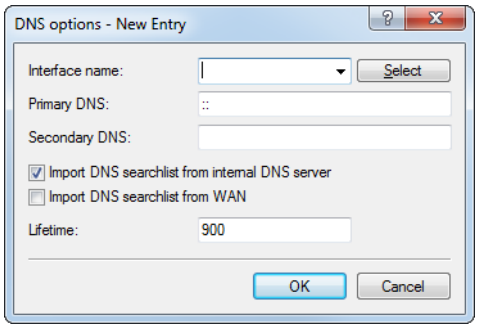
Specifies the length of the prefix that the remote user is assigned by the router advertisement here. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

Allow auto-configuration (SLAAC)

Specifies whether the prefix can be used for a stateless address auto-configuration (SLAAC).

7.3.4 DNS options



Specifies the DNS information in router advertisements according to RFC 6106. The following settings are possible:

Interface name

Name of the interface on which the IPv6 DNS server announces information in router advertisements.

DNS default

IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC 6106) for this interface.

DNS backup

IPv6 address of the secondary IPv6 DNS server for this interface.

Import DNS search list from internal DNS server

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain is configured under **DNS** > **General** > **General settings**. The default setting is **enabled**.

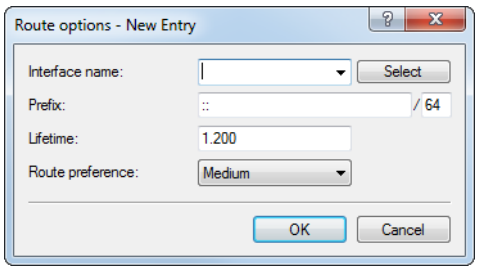
Import DNS search list from WAN

Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under **Receive prefix from**.

Lifetime

Defines the time in seconds for which a client may use this DNS server for name resolution.

7.3.5 Route options



Specifies the route option in router advertisements according to RFC 4191 (Route Information Option). The following settings are possible:

Interface name

Specifies the name of the logical interface to be used for sending router advertisements with this route option.

Prefix

Prefix of the route option, e.g.“2001:db8::/32”.

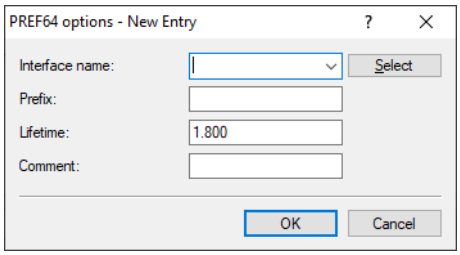
Lifetime

The duration in seconds for the route to remain valid.

Route preference

The preference of the route. Possible values are “high”, “medium” (default) and “low”.

7.3.6 PREF64 options



This table configures the prefix option in router advertisements (PREF64 option as per *RFC 8781*) for NAT64 prefixes, which are announced to clients in the router advertisement. Clients adopt this prefix e.g. for 464XLAT.

Interface name

Specify the name of the interface to be used to advertise the PREF64 option.

Prefix

Defines the NAT64 prefix with prefix length, e.g. 64:ff9b::/96

Lifetime

Validity period of the NAT64 prefix in seconds. Default: 1800 seconds.

Comment

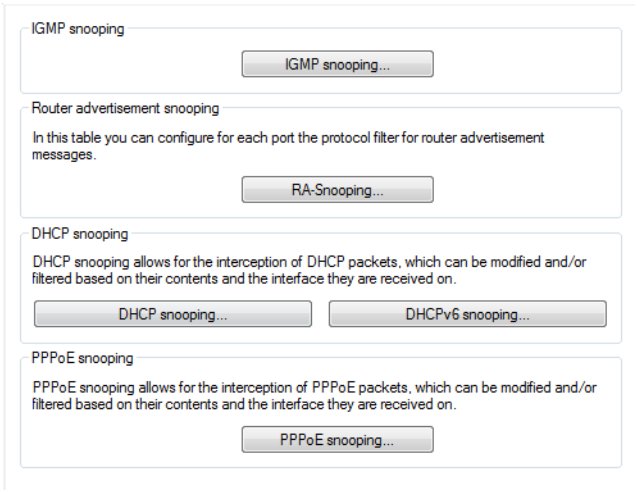
Enter a descriptive comment here.

7.3.7 Router advertisement snooping

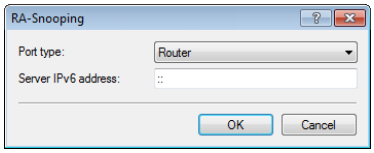
In an IPv6 network, router advertisements are sent by routers, either periodically or upon request, to present themselves as a gateway for networked clients. As with DHCPv4, attackers can use this mechanism to deliver a fake network configuration to the requesting clients.

With RA snooping, the device medaites router advertisements from routers only, and not from clients. By specifying the address of a router, the router advertisements can be restricted to one specific router as the broadcaster.

In LANconfig you can set up RA snooping for each interface under **Interfaces** > **Snooping** and a click on **RA snooping**.



After selecting the appropriate interface, you can set the following:



Port type

Specify the preferred interface type here. The following options are possible:

Router

The device mediates all of the RAs arriving at this interface (default).

Client (activates lock)

The device discards all of the RAs arriving at this interface.

Server IPv6 address

If you have selected the interface type **Router**, enter an optional router address here. If you specify a router address, the device will only mediate RAs from that router.

With the interface type **Client** selected, the device ignores this input field.

7.4 DHCPv6

Compared to IPv4, clients in an IPv6 network do not require automatic address assignment from a DHCP server because they use auto-configuration. However, because certain information such as DNS server addresses are not transmitted during auto-configuration, certain application scenarios can benefit from a DHCP service on the IPv6 network.

DHCPv6 server

The use of a DHCPv6 server is optional for IPv6. In principle, a DHCPv6 server supports two modes:

- **Stateless**: The DHCPv6 server does not distribute addresses but only information, such as DNS server addresses. Using this method, clients generate their own IPv6 addresses by "stateless address auto-configuration (SLAAC)". This method is particularly attractive e.g., for small networks in order to keep administration efforts to a minimum.
- **Stateful**: The DHCPv6 server distributes IPv6 addresses, similar to IPv4. This method is more complicated, since a DHCPv6 server has to assign and manage the addresses.

A DHCPv6 server distributes only the options that are explicitly requested by an IPv6 client, i.e. the server only assigns an address to a client if it explicitly requests one.

Additionally, the DHCPv6 server can pass on prefixes to routers for further distribution. This method is referred to as "prefix delegation". A DHCPv6 client must have explicitly requested this prefix, however.

DHCPv6 client

The auto-configuration available with IPv6 networks makes it very easy and convenient to configure the clients.

However, in order for a client to receive additional information, such as a DNS server address, you must configure the device so that it can activate the DHCPv6 client when necessary.

The settings for the DHCPv6 client ensure that a device receiving certain flags in the router advertisement will start the DHCPv6 client, which can then send requests to the DHCPv6 server:

- **M flag**: If an appropriately configured device receives a router advertisement with the "M flag" set, the DHCPv6 client will request an IPv6 address from the DHCPv6 server along with other information such as DNS server, SIP server and NTP server.
- **O flag**: With an "O flag", the DHCPv6 client requests the DHCPv6 server for information such as a DNS server, SIP server and NTP server only, but not an IPv6 address.

  If the "M flag" is set, the "O flag" does not necessarily have to be set as well.

With IPv6, the default route is distributed via router advertisements and not via DHCPv6.

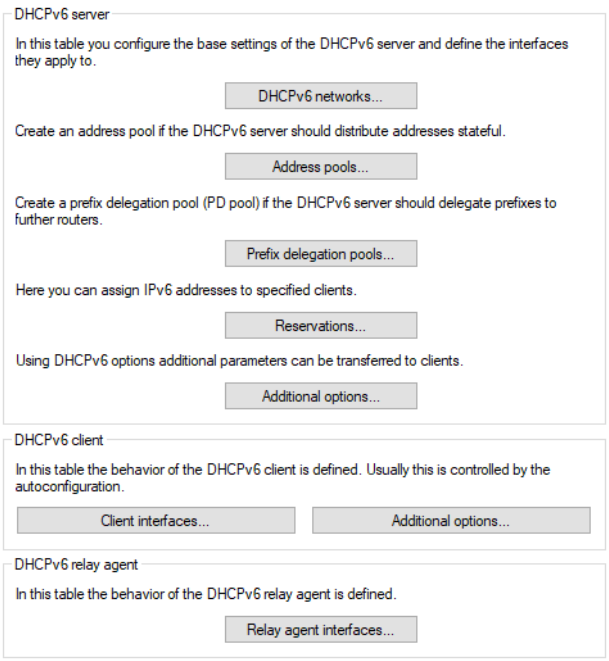
Relay agent

A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks (layer 3).

Lightweight DHCPv6 Relay Agent

A Lightweight DHCPv6 Relay Agent (LDRA) compliant with RFC 6221 enables relay-agent information to be generated and passed between DHCPv6 clients and DHCPv6 servers on layer 2.

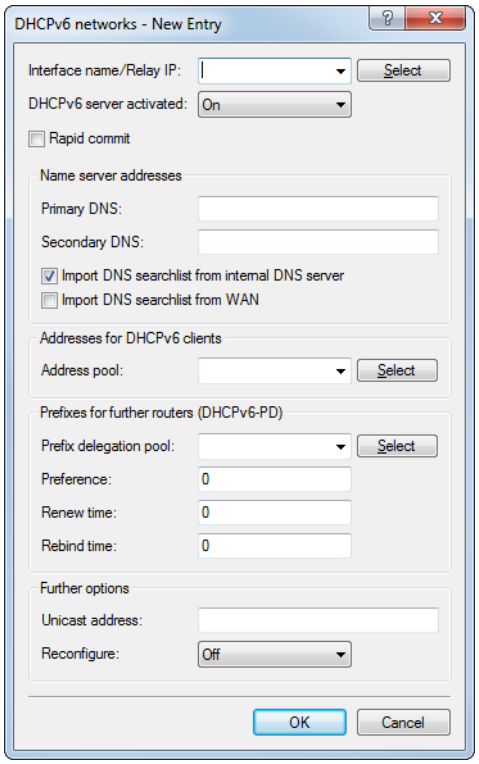
In LANconfig, the settings are located under **IPv6** > **DHCPv6**:



7.4.1 DHCPv6 server

7.4.1.1 DHCPv6 networks

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.



Interface name/Relay IP

Name of the interface on which the DHCPv6 server is working, for example “INTRANET”. Alternatively, you can also enter the IPv6 address of the remote DHCPv6 relay agent.

DHCPv6 server activated

Activates or deactivates the entry.

Rapid commit

With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

The client must explicitly include the rapid commit option in its solicit message.

Primary DNS

IPv6 address of the primary DNS server. The value “::” means that the DHCPv6 server announces its own address as a DNS server to the clients.

Secondary DNS

IPv6 address of the secondary DNS server.

Import DNS search list from internal DNS server

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., “internal”. The own domain is configured under **DNS** > **General** > **General settings**. The default setting is “enabled”.

Import DNS search list from WAN

Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. The default setting is “disabled”.

Address pool

Name of the address pool used for this interface.

If the DHCPv6 server operates *stateful* addresses distribution, you must enter the corresponding addresses into the **Address pools** table.

Prefix delegation pool

Name of prefix pools to be used by the DHCPv6 server.

If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Prefix delegation pools**.

Preference

Where multiple DHCPv6 servers are operated on the network, the preference parameter gives you the control over which server the clients will use. The primary server requires a higher preference value than the backup server.

Renew time

This specifies the time in seconds when the client should contact the server again (using a renew message) to extend the address/prefix received from the server. The parameter is also called T1.

Rebind time

This specifies the time when the client should contact any server (using a rebind message) to extend its delegated address/prefix. The rebind event occurs only if the client receives no answer its renew request. The parameter is also called T2. With the default of 0, this happens automatically.

Unicast address

By default the DHCPv6 server exclusively responds to multicast requests. If the DHCPv6 server should respond to a unicast request, this IPv6 address can be configured here. Generally speaking, multicast is sufficient for communication.

Reconfigure

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

The reconfigure feature allows the DHCPv6 server to require the clients in the network to request a renewal of leases / bindings. If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called *Reconfigure Key*, so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation.

The *Reconfigure Key Authentication Protocol* according to RFC 3315 is supported for *Renew* and *Information-Request*, as well as *Rebind* according to RFC 6644. Reconfiguration is started on the CLI of the device using a "do" command in the status tree:

```
do /Status/IPv6/DHCPv6/Server/Reconfigure
```

The command expects the following parameters:

- `renew`: (optional, default) Asks the client to perform a renewal for his address and/or prefix.
- `rebind`: (optional) Asks the client to perform a rebind for his address and/or prefix.
- `info`: (optional) Asks the client to send an Information-Request, in order to, for example, update its DNS server.
- `-c <Client-ID>`: The reconfigure function applies to the client with the specified client ID.
- `-b <Address/Prefix>`: The reconfigure function applies to the client with the specified address and the specified prefix.
- `-i <Interface/Relay>`: The reconfigure function applies to all clients that are connected to the specified interface or relay.
- `-a`: The reconfigure function applies to all clients.



You can find more about the status of a client regarding the Reconfigure function under **Status** > **IPv6** > **DHCPv6** > **Server** > **Clients**.

In LANconfig the following settings are available for reconfiguration:

Off

Disables the reconfigure function

Reject

Clients that have used the Reconfigure Option in queries are rejected by the server and are not assigned an address, prefix or other options.

Allow

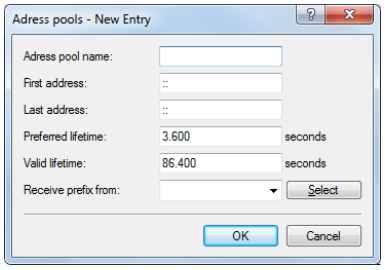
If the client sets the Reconfigure Option in queries, the server negotiates the necessary parameters with the client in order to start a reconfiguration at a later time.

Require

Clients have to set the Reconfigure Option in queries, otherwise the client rejects these clients. This mode is makes sense when you want to ensure that the server only serves clients which support Reconfigure. This ensure that all clients can use Reconfigure to update their addresses, prefixes, or other information at a later point in time.

7.4.1.2 Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:



Address-Pool-Name

Name of the address pool

First address

First address in the pool, e.g. "2001:db8::1"

Last address

Last address in the pool, e.g. "2001:db8::9"

Preferred lifetime:

Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".

Validity period

Here you specify the time in seconds that the client should treat this address as "valid".

If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for **Preferred lifetime** and **Valid lifetime**. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

With this parameter you can assign addresses to the network clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter **First address** to the value "::1" in the **Last address** to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "/56", you must take subnetting for the logical network into account in the address.

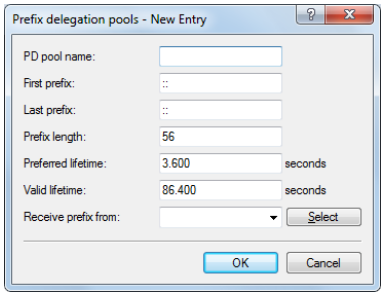
Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- First address: 0:0:0:0001::1
- Last address: 0:0:0:0001::9

You should only use this mechanism if the provider assigns a fixed prefix. Otherwise, it is possible that the provider delegates a new prefix to the router, but the client still has an address from the pool with the old prefix.

7.4.1.3 Prefix delegation pools

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:



PD-Pool-Name

Name of the PD pool

First prefix

First prefix for delegation in the PD pool, e.g. "2001:db8:1100::"

Last prefix

Last prefix for delegation in the PD pool, e.g. "2001:db8:FF00::"

Prefix length

Length of the prefixes in the PD pool, e.g. "56" or "60"

Preferred lifetime:

Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".

Validity period

Here you specify the time in seconds that the client should treat this prefix as "valid".

If you use a prefix from a WAN interface for dynamic address formation, the values **Preferred lifetime** and **Valid lifetime** are unavailable. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

You can use this parameter to assign prefixes from the prefix assigned by the provider to other routers in the network (prefix delegation). Select the desired WAN interface here.

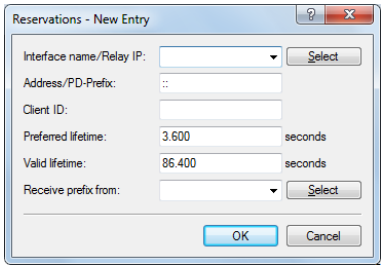
Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- Receive prefix from: INTERNET
- First prefix: 0:0:0:0010::
- Last prefix: 0:0:0:00F0::
- Prefix length 60

In this example, the router uses the provider's dynamically-provided prefix "2001:db8:abcd:aa::/56" to delegate prefixes with the length "/60" from "2001:db8:abcd:aa10::" to "2001:db8:abcd:aaf0::".

7.4.1.4 Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can use this table to make a reservation for each client.



Interface name/Relay IP

Name of the interface on which the DHCPv6 server is working, for example “INTRANET”. Alternatively, you can also enter the IPv6 address of the remote relay agent.

Address/PD prefix

IPv6 address or PD prefix that you want to assign statically.

Identifier type

This type specifies how the **Identifier** is to be interpreted.

Client ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

MAC address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- Specification as a client DUID, e.g. 0003000100a057000001
- Specification as a MAC address, e.g. 00a057000001
- Specification as an interface ID or remote ID, e.g. “INTRANET”

Preferred lifetime:

Here you specify the time in seconds that the client should treat this address as “preferred”. After this time elapses, a client classifies this address as “deprecated”.

Validity period

Here you specify the time in seconds that the client should treat this address as “valid”.

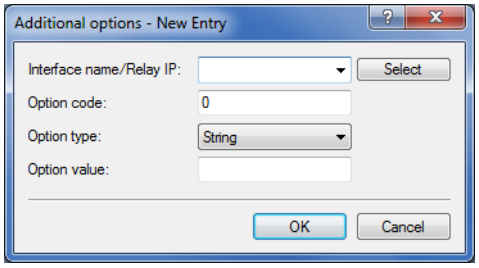
If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for **Preferred lifetime** and **Valid lifetime**. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

7.4.1.5 DHCPv6 options

This feature allows the DHCPv6 server to assign DHCPv6 options to its DHCPv6 clients.



Interface name/Relay IP

Sets the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option

In order for this option to be delivered to clients, the request sent by a client must must also contain the corresponding option code.

Option code

Contains the code of the DHCPv6 option.

Option type

Specifies the type of the DHCPv6 option. You can select from:

String

Accepts the characters as a string.

All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.

Integer types

Accepts whole numbers. These are decimal, octal with a leading 0, and hexadecimal with a leading 0x; capitalization is ignored. The value range for Integer8 is from -128 to 127; for Integer16 from -32768 to 32767; and for Integer32 from -2147483648 to 2147483647. A leading + or - sign is generally allowed.

IPv6 address

Accepts IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses (e.g., "::ffff:1.2.3.4").

Domain list

Accepts all strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain list always ends with the empty label 0.

Hexdump

Expects each block to have hex numbers only, without a leading 0x. Each block is filled with a leading 0 for an even length and ends with the block **bigendian**.

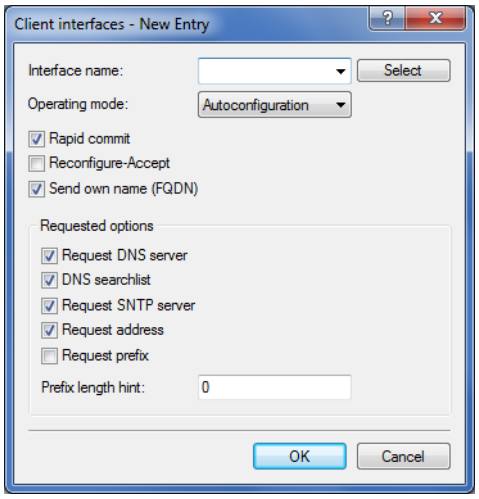
Option value

Contains the contents of the DHCPv6 option, formatted according to the option type.

7.4.2 DHCPv6 client

7.4.2.1 Client interfaces

This table determines the behavior of the DHCPv6 client.



Normally client behavior is controlled by the auto-configuration. Only make entries in this table if you want to use the client in *stand-alone* mode or if there are other specific options that deviate from the default settings.

Interface name

Name of the interface on which the DHCPv6 client is working. These can be LAN interfaces or WAN interfaces (remote sites), e.g. “INTRANET” or “INTERNET”.

Operating mode

Specifies if and how the device enables the client. Possible values are:

Auto configuration

The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.

On

The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements. The device ignores the specifications from router advertisements.

Off

The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

Rapid commit

When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

Reconfigure accept

If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called *Reconfigure Key*, so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation. The client supports the *Reconfigure Key Authentication Protocol* according to RFC 3315 for the options "Renew" and "Information Request", and also "Rebind" as per RFC 6644.

This option is enabled by default for WAN interfaces.

Send own name (FQDN)

The client sends its own host name (Fully Qualified Domain Name). By default, this option is active on LAN interfaces.

Request DNS server

Specifies whether the client queries the DHCPv6 server for DNS servers.

You must enable this option in order for the device to obtain information about a DNS server.

DNS search list

The client queries the DNS search list.

Request SNTP server

Specifies whether the DHCPv6 client requests a list of SNTP servers (Simple Network Time Protocol) from the DHCPv6 server.

For this to work, the periodical synchronization with a time server must be enabled as in *Configuring the time server under LANconfig*.

Request address

Determines whether the client should request the DHCPv6 server for an IPv6 address.

Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i.e. not distributed by SLAAC.

Request prefix

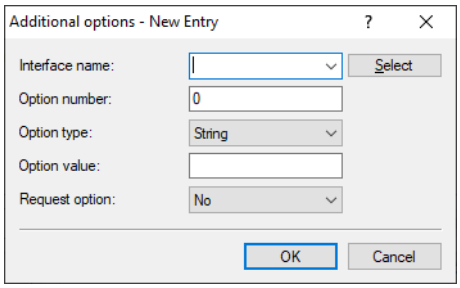
Specifies whether the DHCPv6 client requests a desired prefix length from the DHCPv6 server. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

Prefix length hint

This is a proposal from the client to the server regarding the length of the prefix requested by the server.

7.4.2.2 Further options

Certain options can be configured for the DHCPv6 client, which are then transmitted. This is required if the Internet provider expects certain data in DHCPv6 messages. The options is found in the DHCP Options table under **IPv6** > **DHCPv6** > **DHCPv6-Client** > **Additional options** and can be freely configured.



Interface name

Interface that the DHCPv6 client should use for this option, e.g. WAN remote site or IPv6 LAN network.

Option number

Specifies the assigned IANA number of the DHCPv6 option as defined in the RFC.

Option type

Specifies the type of the DHCPv6 option. Possible values: String, Integer8, Integer16, Integer32, IPv6-Addresses, Domain-List, Hexdump, or Dont-Send

The option type "Dont-Send" means that no option content is sent, only the option number in the option request if no option value is provided in the RFC.

Option value

Specifies the content of the DHCPv6 option

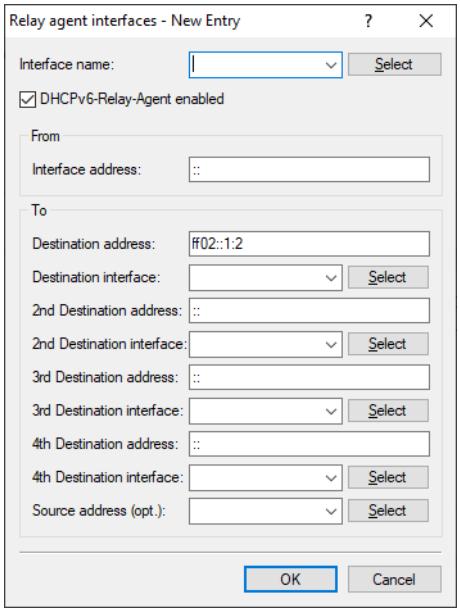
A comma and/or space-separated list can also be specified, except in the case of a string. For integer values the C-codes for numbers apply, i.e. 0x results in a hex value and if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden or configured: Elapsed-Time, Server-DUID, Reconfigure-Accept and Rapid-Commit.

Request option

Specifies whether the DHCPv6 request should request the option number. The behavior is defined via the respective RFC of the DHCPv6 option. Possible values: Yes, No

7.4.3 DHCPv6 Relay Agent

A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks. This table determines the behavior of the DHCPv6 relay agent.



Interface name

The name of the interface on which the relay agent receives requests from DHCPv6 clients, e.g. “INTRANET”.

DHCPv6-Relay-Agent enabled

Enables or disabled the relay agent on your device.

Interface address

The relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.

Destination address

The IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address “ff02::1:2”.

Using the parameters **2nd Destination address** to **4th Destination address** you can define additional server destinations.

If multiple server destinations are configured, the requests are always sent to all configured servers at the same time.

Destination interface

The destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

Using the parameters **2nd Destination interface** to **4th Destination interface** you can define additional server destinations.

If multiple server destinations are configured, the requests are always sent to all configured servers at the same time.

Source address (optional)

Set an optional source address that the relay agent uses for packets directed to the DHCPv6 server.

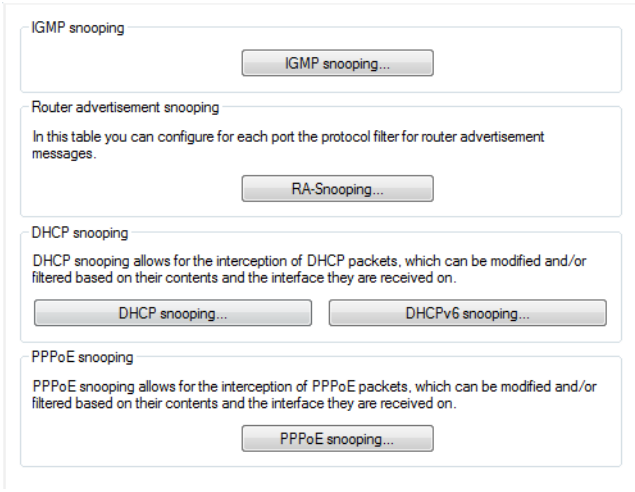
7.4.4 Lightweight DHCPv6 Relay Agent (LDRA)

Unlike a DHCPv6 relay agent, which has the full IPv6 features (such as ICMPv6) and can route data packets on the network (layer 3), a lightweight DHCPv6 relay agent as per RFC 6221 enables only the creation and forwarding of relay-agent information between DHCPv6 clients and DHCPv6 servers (layer 2).

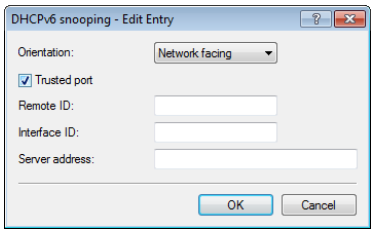
In contrast to DHCPv4 snooping, the LDRA does not simply append the DHCPv6 packets with information about the relay agent: Instead, it packs the message from the client into a separate option, prepends its own relay-agent header and then forwards this DCHPv6 packet with its supplementary information to the DHCPv6 server (relay forward message).

The DHCPv6 server evaluates this data packet and sends a similarly packaged response to the relay agent. This then extracts the message and sends it to the requesting client (relay-reply message).

In LANconfig you can set up DHCPv6 snooping for each interface under **Interfaces** > **Snooping** and a click on **DHCPv6 snooping**.



After selecting the appropriate interface, you can set the following:



Orientation

This is where you enable or disable DHCPv6 snooping. The following options are possible:

- **Network-facing**: The LDRA uses this interface to communicate with a DHCPv6 server.
- **Client-facing**: The LDRA uses this interface to communicate with DHCPv6 clients connected to the network.

The default setting **Network facing** disables the LDRA.

Trusted port

With this option enabled, the LDRA forwards DHCP requests from clients and also DHCP responses from DHCP servers. If this interface is classified as not trusted, the LDRA discards DHCPv6 requests to this interface. Similarly, the LDRA does not forward DHCPv6 responses with the wrong interface ID to the client.

Remote ID

According to RFC 4649, the remote ID uniquely identifies the client making a DHCPv6 request.

Interface ID

The interface ID uniquely identifies the interface used by a client to make a DHCPv6 request.

Server address

You can set the IPv6 address of a DHCPv6 server here.

Leave this field blank if you want to receive responses from all DHCPv6 servers on the network. Otherwise the LDRA reacts only to DHCPv6 responses from the server you have specified. In this case, the LDRA discards responses from other DHCPv6 servers.

You can use the following variables for **Remote ID** and **Interface ID**:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%i`: Inserts the name of the interface where the relay agent received the DHCP request.
- `%n`: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Management** > **General**.

7.5 IPv6 firewall

7.5.1 Feature

While the IPv4 firewall only controls the forwarding of IP data, the IPv6 firewall also regulates the functions of the access lists for all IPv6 server services. Therefore, the IPv6 firewall is similar to a classic firewall design, which separately supports the inbound and outbound communications, as well as forwarding. Since the device configuration specifically controls communication, the device does not require an outbound firewall.

7.5.2 Configuration

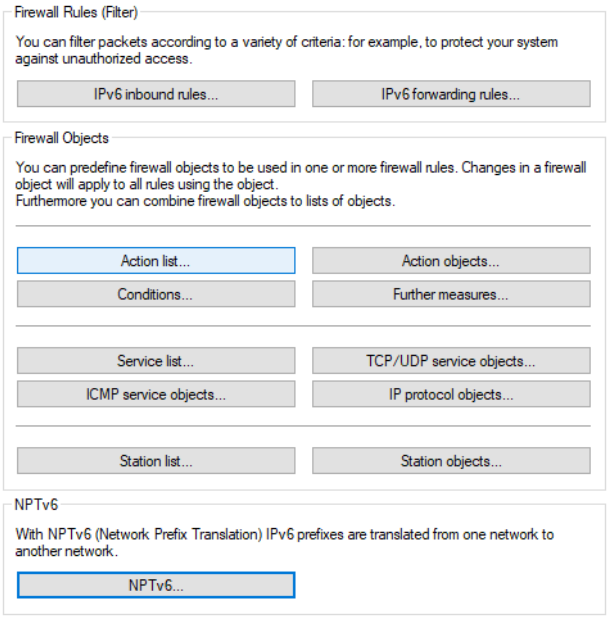
The configuration of the IPv6 firewall is practically the same as the IPv4 firewall; however, it is performed separately.

The inbound and forwarding firewalls each have their own rule tables, which are similar in scope and structure to the IPv4 firewall.

The rules are sorted with decreasing priority, i.e. the rule with the highest priority is at the top of the list. Rules of the same priority are sorted by their precision, analogous to the IPv4 procedure. If a rule requires further actions, these are also performed by firewall in sequence. Otherwise, firewall filtering is terminated after the current rule has been applied.

7.5.2.1 Configuring IPv6 firewall rules

With LANconfig you can set the firewall rules under **Firewall/QoS** > **IPv6 Rules**.



The factory settings provide various objects and lists for the most important applications.



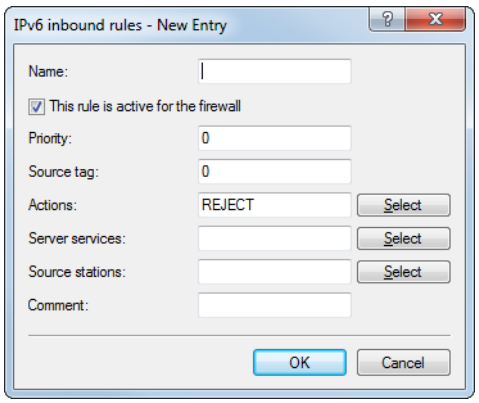
You cannot delete objects or lists if the firewall uses them in a forwarding or inbound rule.

IPv6 inbound rules

Using the **IPv6 inbound rules** you set the rules that the IPv6 firewall should use to handle incoming traffic.

The factory settings provide various rules for the most important applications.

Click on **Add** to create a new rule.



You can set the following properties for the rule:

Name

Specifies the name of the rule.

This rule is active for the firewall

Enables the rule.

Priority

Specifies the priority of the rule: The higher the value, the higher the priority.

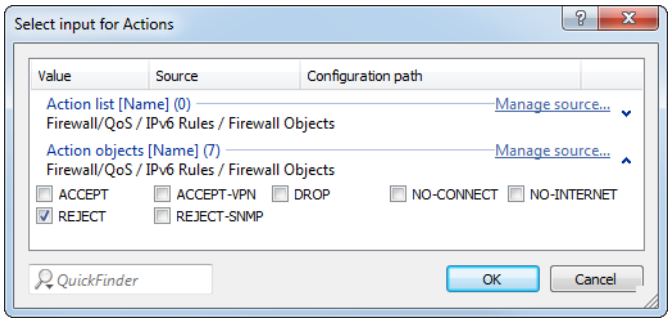
Src-Tag

Enter an interface or routing tag here (tag context) if you want the rule to apply only to packets marked in this way. The default value of 0 means that this rule applies to all packets regardless of the interface or routing tag.

If only packets with the interface or routing tag 0 are to be considered, then 65535 must be specified here.

Actions

Specifies the action that the firewall performs if the rule condition is true. Using **Select** you can choose one action or a list of actions.



If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source.** Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Server services

Determines the services which the firewall applies this rule to. Using **Select** you can choose one service or a list of services.

Source stations

Determines the source stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

Comment

Here you assign a meaningful description for the filter rule.

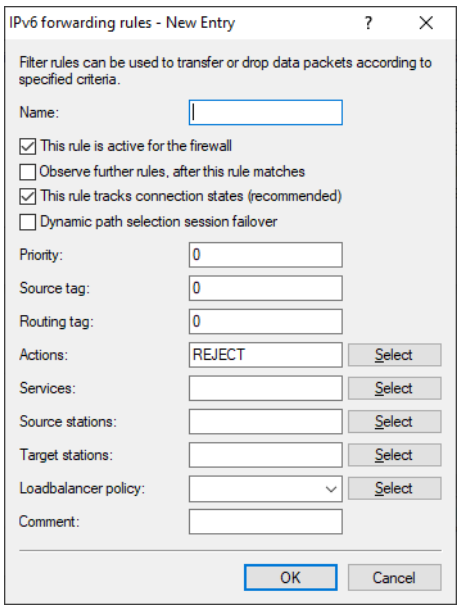
IPv6 forwarding rules

The **IPv6 forwarding rules** button accesses dialog where you set the rules that the IPv6 firewall should use to handle forwarded traffic.

The factory settings provide various rules for the most important applications.

In order to change the order of the rules, highlight the specific rule in the table and move it up or down in the table by clicking on the arrow buttons. The firewall applies the rules one after the other from top to bottom.

Click on **Add** to create a new rule.



You can set the following properties for the rule:

Name

Specifies the name of the rule.

This rule is active for the firewall

Enables the rule.

Observe further rules after this one matches

If you enable this option, the firewall also applies the subsequent rules in the list. This is useful if the firewall should, for example, initially apply a group rule and then apply each rule to the individual objects in the group.

This rule tracks connection states (recommended)

Select this option if the rule should track the TCP connection states.

Dynamic Path Selection Session Failover

Specifies whether the sessions under these rules should be moved to a better line as identified by Dynamic Path Selection. This is only possible for unmasked connections, e.g. VPN connections. See also *Switchover-Profiles* on page 445.

Priority

Specifies the priority of the rule: The higher the value, the higher the priority.

Src-Tag

Enter an interface or routing tag here (tag context) if you want the rule to apply only to packets marked in this way. The default value of 0 means that this rule applies to all packets regardless of the interface or routing tag.

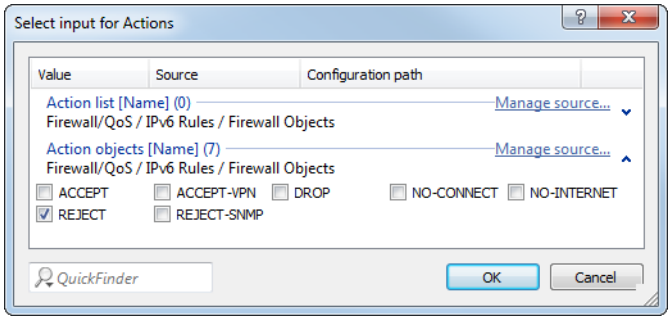
If only packets with the interface or routing tag 0 are to be considered, then 65535 must be specified here.

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

Actions

Specifies the action that the firewall performs if the rule condition is true. Using **Select** you can choose one action or a list of actions.



If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source.** Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Services

Determines the services which the firewall applies this rule to. Using **Select** you can choose one service or a list of services.

Source stations

Determines the source stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

Target stations

Determines the target stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

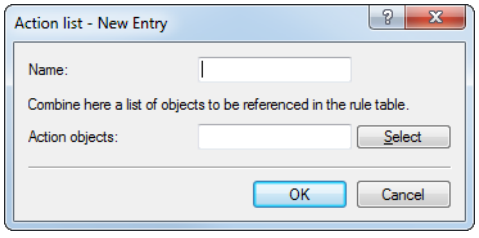
Comment

Here you assign a meaningful description for the filter rule.

Action list

Using the **Action list** button, you can collect actions into groups. The actions available here must first be defined using **Action objects**.

Click on **Add** to create a new rule.



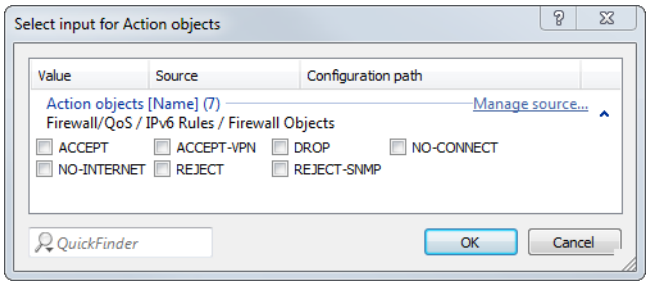
You can set the following properties for a list:

Name

Determines the name of the list.

Action objects

Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

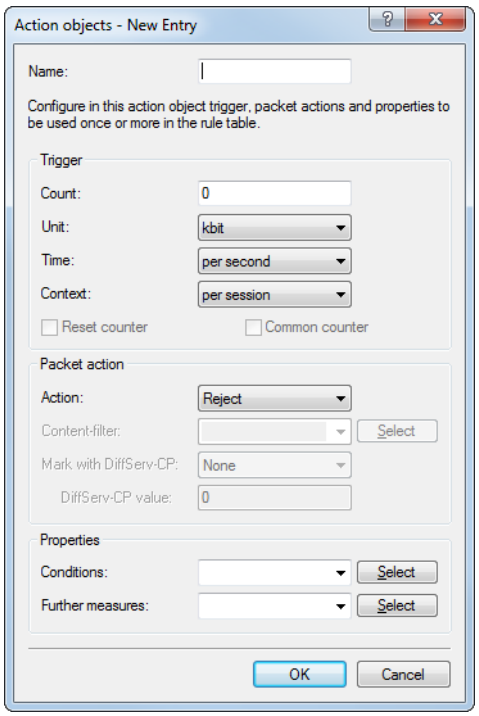


If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source.** Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Action objects

Using the **Action objects** button, you define actions that the IPv6 firewall runs when a filter is true.

Click on **Add** to create a new action.



You can set the following properties for the object:

Name

Specifies the name of the object.

Count

When this limit is exceeded, the firewall performs the action.

Unit

Determines the unit for the limits. Select the corresponding value in the drop-down menu.

Time

Determines the measurement period that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

Context

Determines the context that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

Reset counter

If you enable this option, the firewall resets the counter after running the action.

You can only activate this option if you set the **Time** value to “absolute”.

Common counter

If you enable this option, the firewall adds all action triggers together in one counter.

You can only activate this option if you set the **Context** value to “per station” or “global”.

Action

Determines the action the firewall performs when the limit is reached.

The following options are possible:

Reject

The firewall rejects the data packet and sends an appropriate notification to the sender.

Drop

The firewall discards the data packet without notification.

Transmit

The firewall accepts the data packet.

Check via proxy

The proxy checks the data packet.

Content filter

The content filter profile. See *Firewall settings for the content filter* on page 1667

Mark with DiffServ-CP

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.

You can only activate this option if you set the **Action** value to “Transmit”.

Further information about DiffServ CodePoints is available in the section *Quality of Service* on page 697.

DiffServ-CP value

Determines the value for the Differentiated Services Code Point (DSCP).

You can only activate this option if you set **Mark with DiffServ-CP** to the option “Value”.

Conditions

Determines which conditions must be met in order for the action to be performed. You can specify the conditions under *Conditions* on page 627.

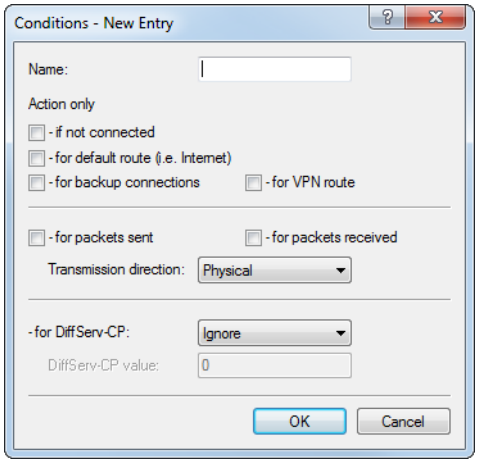
Further measures

Determines which trigger actions the firewall should start in addition to filtering the data packets. You can specify trigger actions under *Further measures* on page 628.

Conditions

Use the **Conditions** button to specify the conditions that have to be met for the forwarding and inbound rules to apply.

Click on **Add** to create a new condition.



You can set the following properties for the condition:

Name

Specifies the name of the object.

Action only – if not connected

Select this option if the firewall should only perform the action if there is no connection.

Action only – for default route (e.g. Internet)

Select this option if the firewall should only perform the action if there is a connection over the default route.

Action only – for backup connections

Select this option if the firewall should only perform the action if the connection is a backup connection.

Action only – for VPN route

Select this option if the firewall should only perform the action if the connection is a VPN connection.

Action only – for packets sent

Select this option if the firewall should only perform the action for packets sent.

Action only – for packets received

Select this option if the firewall should only perform the action for packets received.

Transport direction

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

Action only – for DiffServ-CP

Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

Further information about DiffServ CodePoints is available in the section *Quality of Service* on page 697.

DiffServ-CP value

Determines the value for the Differentiated Services Code Point (DSCP).

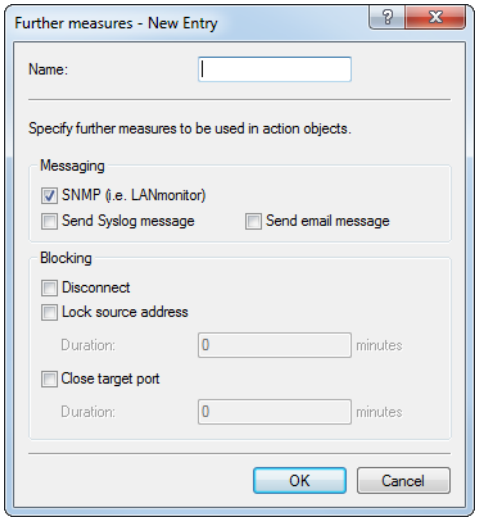
Enter a value here if you set the **for DiffServ-CP** field to the option “Value”.

Further information about DiffServ CodePoints is available in the section *Quality of Service* on page 697.

Further measures

Use the **Further measures** button to define further measures that the firewall performs after you apply the forwarding and inbound rules.

Click on **Add** to create a new measure.



You can set the following properties for the trigger actions:

Name

Specifies the name of the object.

SNMP (e.g. LANmonitor)

Select this option if the firewall should send a notification via SNMP. You can receive this notification, e.g., with LANmonitor.

Send SYSLOG message

Select this option if the firewall should send a SYSLOG notification via SNMP.



Refer to section *The SYSLOG module* on page 324 for further information on SYSLOG.

Send e-mail message

Select this option, if the firewall should send a notification by e-mail.



If you want to receive e-mail notifications, you must enter an e-mail address in **Firewall/QoS** > **General** > **Administrator e-mail**.

Disconnect

Select this option if the firewall should disconnect.

Lock source address

Select this option if the firewall should block the source address. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the **Host-lock-list** under **Status** > **IPv6** > **Firewall**.

Duration

If the firewall should block the sender, you can set the duration of the lock in minutes. The value 0 disables the lock because, in practice, the lockout period expires after 0 minutes.

Close destination port

Select this option, if the firewall should block the target port. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the **Port-block-list** under **Status** > **IPv6** > **Firewall**.

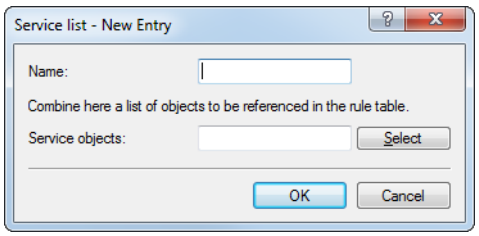
Duration

If the firewall should block the target port, you can set the duration of the lock in minutes. The value 0 disables the lock because, in practice, the lockout period expires after 0 minutes.

Service list

Using the **Service list** button, you can collect services into groups. You first define the services under **TCP/UDP service objects**, **ICMP service objects** and **IP protocol objects**.

Click on **Add...** to specify a new service.



You can set the following properties for a list:

Name

Determines the name of the list.

Service objects

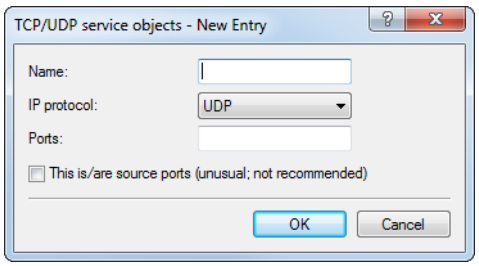
Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source.** Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

TCP/UDP service objects

Using the **TCP/UDP service objects** button, you define TCP/UDP services that the IPv6 firewall can use in filter rules.

Click on **Add** to create a new service.



You can set the following properties for the rule:

Name

Specifies the name of the object.

IP protocol

Specifies the protocol of the service

Ports

Specifies the ports for the service. Separate multiple ports with a comma.

Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

This is/are source ports

Determines whether the specified ports are source ports.

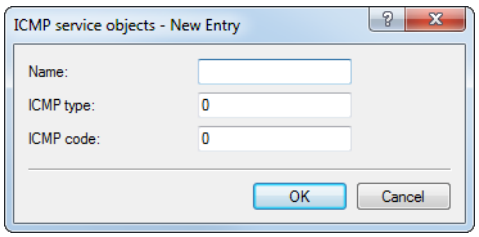
In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

ICMP service objects

Using the **ICMP service objects** button, you define ICMP services that the IPv6 firewall can use in filter rules.

Lists with the official ICMP types and port codes are available in the Internet under *www.iana.org*.

Click on **Add** to create a new service.



You can set the following properties for the rule:

Name

Specifies the name of the object.

ICMP type

Specifies the type of the ICMP service.

ICMP code

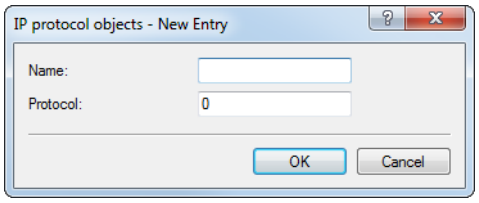
Specifies the code of the ICMP service.

IP protocol objects

Using the **IP protocol objects** button, you define IP protocol objects for the IPv6 firewall to use in filter rules.

Lists with the official protocol and port numbers are available in the Internet at *www.iana.org*.

Click on **Add** to create a new object.



You can set the following properties for the rule:

Name

Specifies the name of the object.

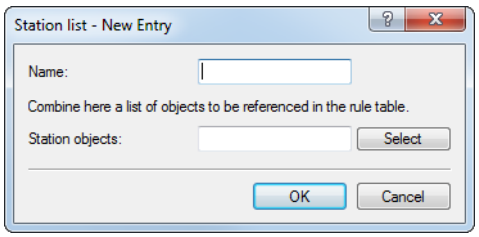
Protocol

Defines the protocol number.

Station list

Using the **Station list** button, you can collect stations into groups. Stations must previously be defined using **Station objects**.

Click on **Add** to create a new list.



You can set the following properties for a list:

Name

Determines the name of the list.

Station objects

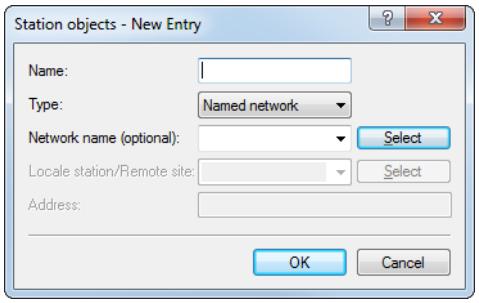
Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source.** Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Station objects

Using the **Station objects** button, you define stations that the IPv6 firewall can use in filter rules.

Click on **Add** to create a new object.



You can set the following properties for the object:

Name

Specifies the name of the object.

Type

Determines the station type. The selection made here determines which of the following table columns (**Network name**, **Local station/Remote site** and **Address/Prefix**) have to be filled out. Possible values:

Named network

Name of a local network, e.g. INTRANET.

- The only column to be filled out is **Network name**.
- If it contains an interface name, then the station consists of all networks on this interface.
- If you specify a network group, then the station consists of all prefixes under *IPv6 addresses* on page 589 with this group.

Peer

Name of a WAN remote site, e.g. INTERNET.

- The only column to be filled out is **Local station/Remote site**.
- It can contain a WAN interface or a RAS template. With a WAN interface it resolves to all prefixes/networks to which a route exists via this WAN interface, and with a RAS template it resolves to all prefixes/networks to which a route exists via a RAS interface from this template.

Network prefix

IPv6 prefix

- The only column to be filled out is **Address/Prefix**.
- It contains an IPv6 prefix, e.g. "2001:db8::/32".

Host identifier or Interface identifier

- The columns **Network name** and **Address/Prefix** both have to be filled out
- **Network name** contains a WAN interface or a RAS template.
- **Address/Prefix** contains an IPv6 identifier. These are the last 64 bits of the IPv6 address of an IPv6 host, e.g. "::2a0:57ff:fe1b:3a6a". The value must contain two leading colons.
- This identifier forms an address when combined with all of the networks of the interface **Network name** or with the networks of the RAS interface from the specified template.
- Furthermore, a link-local address with this identifier is formed for each of these interfaces.

IP address

- The only column to be filled out is **Address/Prefix**.
- It contains an IPv6 address, e.g. "2001:db8::/1".

Local station

Name of a local IPv6 host or local station.

- The **Local station/Remote site** column must be filled out and contains a hostname.
- The **Network name** column is optional and can include a LAN interface.
- The host name is resolved to a host address using the DHCPv6 server or the DNS server in the device.
- If an interface has been specified, the address is only taken if it can be reached via this interface.

MAC address

This allows rules to be created for resources on the internal network that are identified by their MAC address. In dual-stack networks, this helps with the correlation to IPv4 station objects that are also handled by an IPv4 rule based on their MAC address.

- The **Network name** column is optional and can contain the name of a network where the station object is located.
- The column **Address/Prefix** contains the MAC address used to identify the object.



In rules, MAC addresses can be a source but not a target.

Delegated prefix

Especially where the provider prefix is dynamic, this allows a rule to be defined for downstream routers or resources.

- The **Network name** column is optional and can contain the name of a network where the station object is located. This can be used as a restriction on the local network.
- The column **Local station/Remote site** is required and should contain the remote peer from which the delegated prefix is obtained or derived.

- The column **Address/Prefix** contains a prefix or address that is linked (OR operator) with the prefix obtained from the provider. If the object should refer to the entire prefix, you can either configure ::/0 or the entry can be left blank.

  Example: The provider delegates the prefix 2001:db8:1234::/48 to the remote peer INTERNET.

  - To use the subnet abcd, the **Address/Prefix** has to be configured as the value 0:0:0:abcd::/48.
  - If the address to be used is 2001:db8:0:23::dead:beef/128, then the **Address/Prefix** can be configured as 0:0:0:23::dead:beef/128.
  - If the entire prefix is to be used, then the **Address/Prefix** can be configured as ::/0 or the entry can be left blank.

Network name

Here you enter the name of the network if you selected the appropriate option in the **Type** field.

Local station/Remote site

Here you enter the name of the remote site if you selected the appropriate option in the **Type** field.

Address/Prefix

Here you enter the address if you selected the appropriate option in the **Type** field.

NPTv6

NPTv6 (Network Prefix Translation) according to *RFC 6296* allows the translation of one IPv6 prefix to another IPv6 prefix. The translation is 1:1, in that an address from prefix A is mapped to an address from prefix B. Only the prefix part is mapped, the host part is retained. This method thus works “stateless”. NPTv6 cannot be used to mask an entire network behind a single address, as with IPv4.

Application scenarios for NPTv6 are, for example, VPNs or networks with dynamic prefixes that should be reachable whatever the public address. If the provider assigns a dynamic prefix, the prefix usually changes every time a connection is established. This is not desirable if certain resources require fixed IP addresses. With NPTv6, addresses from the (private) ULA range fd00::/8 are then assigned to the clients in the network and an NPTv6 rule maps these addresses to the provider prefix.

Another use case is a load balancer scenario with several Internet providers, with each provider assigning its own prefix. With NPTv6, addresses from the ULA range fd00::/8 are assigned to the clients in the network and a number of NPTv6 rules map these addresses to the provider prefixes.

NPTv6 guarantees checksum neutrality, i.e. the converted IPv6 address is changed so that the checksum in the IPv6 packet does not have to be adjusted. Therefore, an address X is not converted exactly 1:1 to address Y, but 16 bits must be encoded in the address for checksum neutrality during conversion.

The position of the 16 bits depends on the prefixes that are to be converted. For prefixes longer than 48 bits, e.g. /56 or /60, part of the interface identifier is also changed during mapping due to checksum neutrality (16 bits). This affects access from outside to internal stations in the LAN. Only with prefixes that are 48 bits or shorter, e.g. /48 or /40, can the 16 bits be encoded in the prefix.

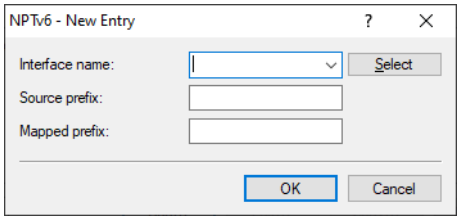
For dynamic prefixes, the 16 bits change with each new prefix assignment. External access to the internal network is therefore only possible with a static provider prefix, since the entire address changes when the 16 bits are changed.

External access to stations in the LAN is therefore only possible without problems with a static /48 provider prefix due to the unchanging IPv6 addresses of the internal station after conversion by the router.

A possible solution for access from the outside with NPTv6 with dynamic prefixes and prefixes longer than /48, is the use of a DynDNS client directly on the station in the LAN, which does not insert its address itself in the update URL, but the provider registers the received IP address.

The IPv6 firewall must be enabled for NPTv6.

The configuration in LANconfig is done under **Firewall/QoS** > **IPv6 Rules** > **NPTv6**.



Interface name

Name of the network or the peer on which NPTv6 is to be performed. If a prefix is to be mapped for a dynamic provider prefix, the name of the Internet connection or peer has to be configured here, e.g. INTERNET.

Source prefix

Source network prefix, e.g. an explicit prefix fd00::/64.

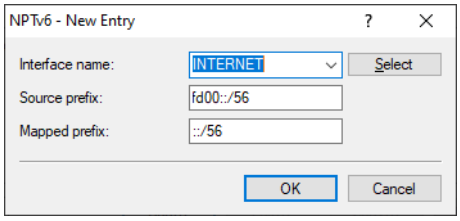
Mapped prefix

Prefix that the source prefix is mapped to. Here you can configure either an explicit prefix such as 2001:db8::/32, or the placeholder :: with the appropriate prefix length in the case that the provider assigns a dynamic prefix.

Examples

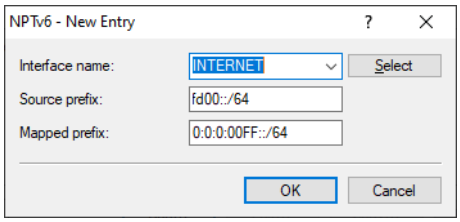
Example 1

The provider (remote site INTERNET) assigns a dynamic prefix of length /56. The intranet is configured with the prefix fd00::/64. The source prefix fd00::/56 should be mapped 1:1 to the entire provider prefix (::/56).



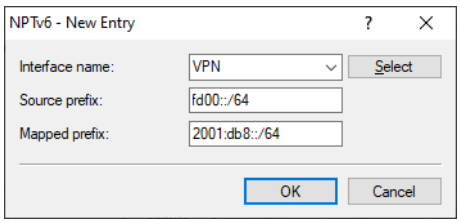
Example 2

The provider (remote site INTERNET) assigns a dynamic prefix of length /56. The intranet is configured with the prefix fd00::/64. The source prefix fd00::/64 should be mapped to the special subnet "FF" from the dynamic provider prefix. For the mapped prefix, the placeholder :: is configured with the subnet ID FF, i.e. 0:0:0:00FF::/64.



Example 3

For a VPN scenario, the internal source prefix fd00::/64 should be mapped to the prefix 2001:db8::/64.



Show commands via CLI

The available show commands are listed in the following:

- **show ipv6-npt**

  Shows the NPTv6 mapping rule.

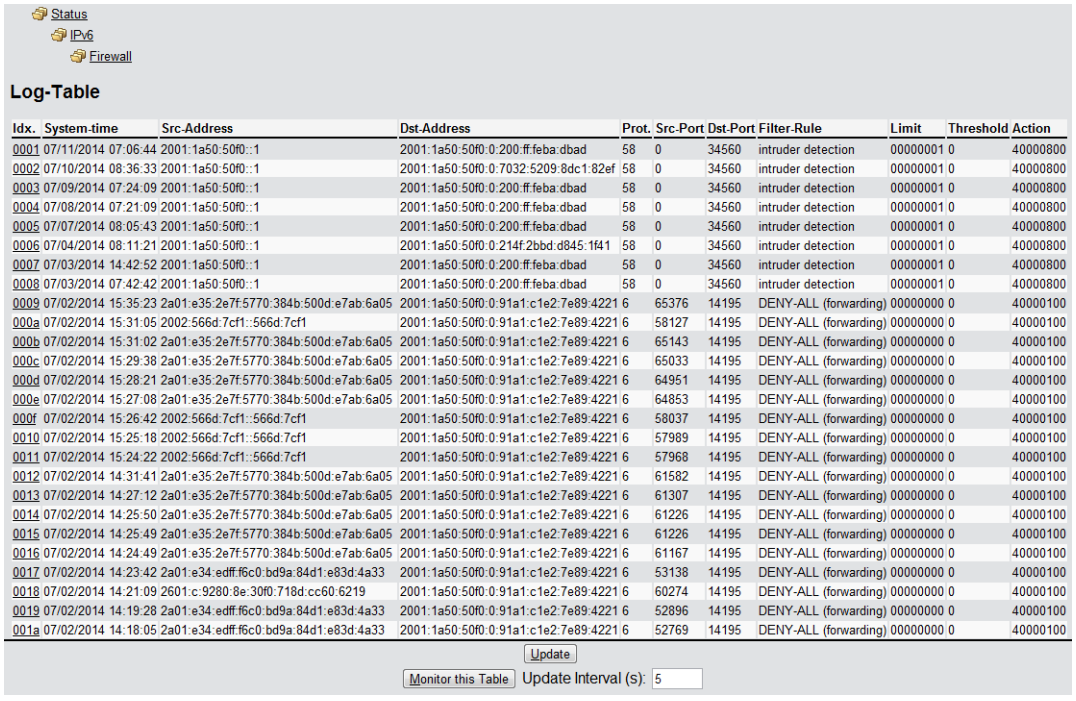
7.5.3 IPv6 firewall log table

Similar to the IPv4 firewall, the IPv6 firewall provides a log table of events in the IPv6 environment.

The syntax of the log table is the same as the IPv4 log table with the exception of the IP address format (IPv6 addresses are in hexadecimal format, IPv4 in decimal format).

7.5.3.1 Analyzing the IPv6 firewall log table with WEBconfig

You can open IPv6 log tables in WEBconfig with **Extras** > **LCOS menu tree** > **Status** > **IPv6** > **Firewall** > **Log-Table**.



The items have the following meanings:

- **Idx.**: Sequential index. Furthermore, the table can also be checked via SNMP.
- **System time**: System time in UTC encoding (converted to cleartext for display).
- **Source address**: Source address of the filtered packet.

- **Destination address**: Destination address of the filtered packet.
- **Prot.**: Protocol (TCP, UDP, etc.) of the filtered packet.
- **Source port**: Source port of the filtered packet (only for port related protocols).
- **Dst port**: Destination port of the filtered packet (only for port related protocols).
- **Filter rule**: Name of the rule that created the entry. If filtering is based on several rules, these rules are listed in the column. If there is too little space, the abbreviation '...' is displayed.
- **Limit**: Bit field that contains the description of the limit that caused the firewall to apply the filter. There following values are currently defined:
  - 0x01: Absolute number
  - 0x02: Number per second
  - 0x04: Number per minute
  - 0x08: Number per hour:
  - 0X10: Global limit
  - 0x20: Byte limit (if not set, it is a packet limit)
  - 0x40: Limit only applies in the inbound direction
  - 0x80: Limit only applies in the outbound direction
- **Threshold**:Threshold limit value of the triggering limit.
- **Action**: Bit field which lists all the actions performed. There following values are currently defined:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Establish filter
  - 0x00000400: Internet (default router) filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Block source address
  - 0x00020000: Lock destination address and port
  - 0x20000000: Send SYSLOG notification
  - 0x40000000: Send SNMP trap
  - 0x80000000: Send e-mail

All firewall actions also appear in the IP router trace .

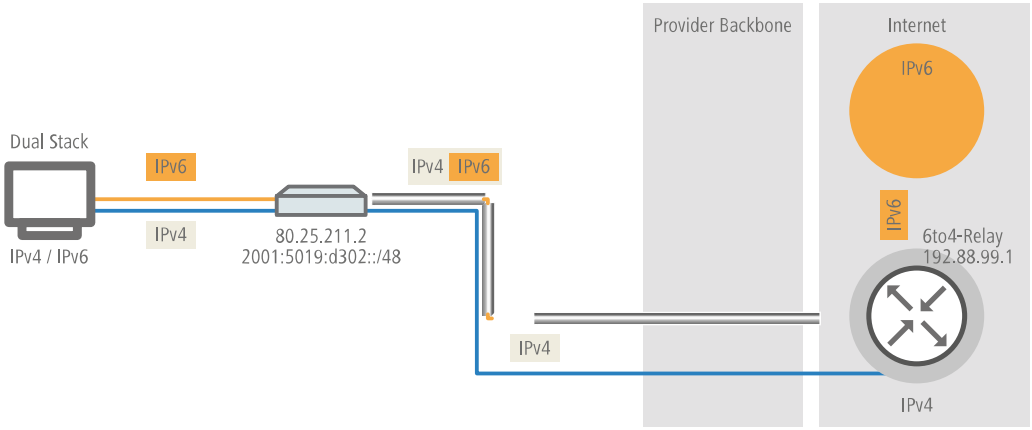
7.6 IPv6 tunnel technologies

7.6.1 6to4 tunnel

The 6to4 tunnel offers you an easy way to set up a connection between two IPv6 networks via an IPv4 network. To this end, what is known as a 6to4 tunnel is set up:

- A router between the local IPv6 networks and an IPv4 network serves to mediate between the networks.
- The router has both a public IPv4 address and an IPv6 address. The IPv6 address consists of an IPv6 prefix and the IPv4 address in hexadecimal notation. If a router such has the IPv4 address 80.25.211.2, this will first be converted into hexadecimal notation: 5019:d302. Supplementing this is an IPv6 prefix (e.g. 2002::/16), so that the IPv6 address for the router appears as follows: 2002:5019:d302::/48.
- If a device in the IPv6 network sends data packets via the router to an IPv6 destination address, then the router first of all encapsulates the IPv6 packets in a packet with an IPv4 header. The router then forwards the encapsulated

packet to a 6to4 relay. The 6to4 relay unpacks the packet and forwards it to the desired destination. The following illustration shows the operating principle of 6to4 tunnels:

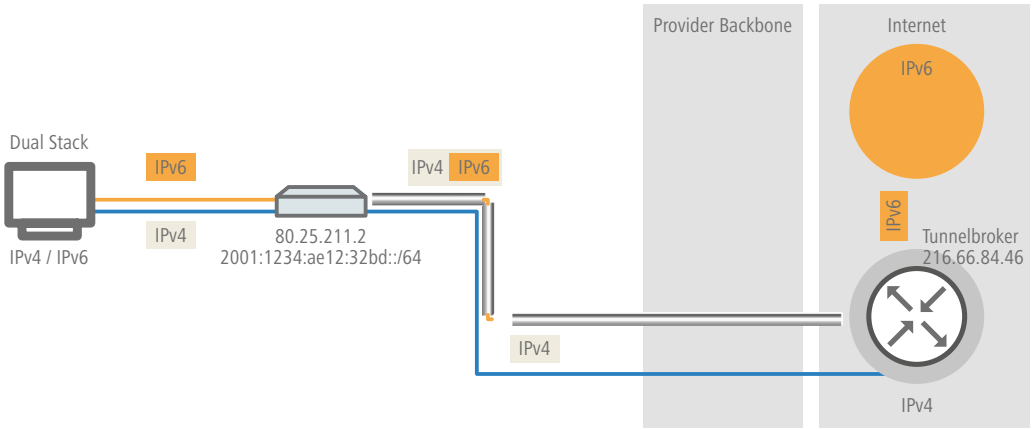


6to4 tunnels establish a dynamic connection between IPv6 and IPv4 networks: the response packets may be routed back via a different 6to4 relay. 6to4 tunnels are not a point-to-point connection. For every new connection, the router always looks for the "nearest" public 6to4 relay. This is done using the anycast address 192.88.99.1. This aspect is an advantage of 6to4 tunnels on the one hand, but it also presents a disadvantage on the other. Public 6to4 relays do not require registration and are freely accessible. What's more, the dynamic connection is easily configured. In this way it is possible for any user to create a 6to4 tunnel over a public relay, quickly and easily.

On the other hand, the dynamic connection means that the user has no influence on the choice of the 6to4 relay. The provider of the relay is able to intercept or manipulate data.

7.6.2 6in4 tunnel

6in4 tunnels are used to connect two hosts, routers, or to interconnect a host and router. This means that 6in4 tunnels can connect two IPv6 networks via an IPv4 network. The diagram shows a static 6in4 tunnel between the local router and a 6in4 gateway belonging to a tunnel broker.



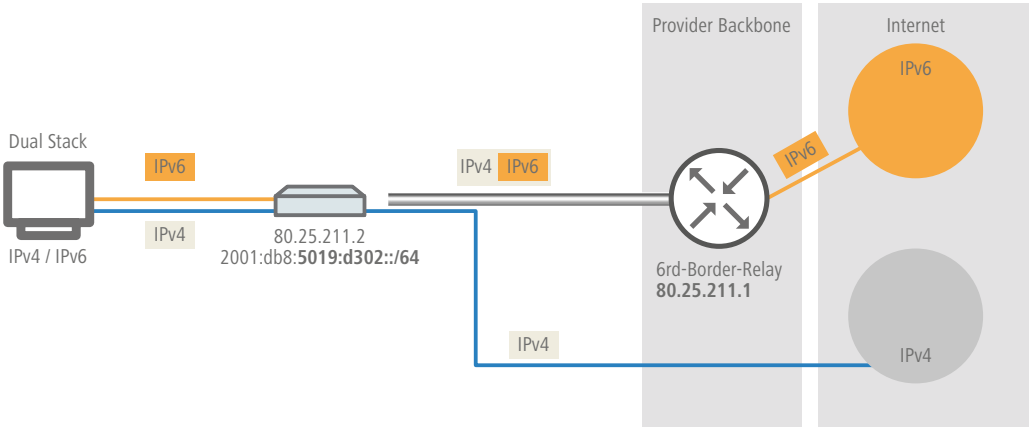
These are dedicated services operated by a known provider. The end-points are fixed and the tunnel broker assigns a static prefix. The advantages of a 6in4 solution are that the gateways are fixed and the operator is known. The fixed prefix from the tunnel broker also determines the number of possible subnets that can be used. A 64-bit prefix (e.g. 2001:db8::/64) allows one subnet to be used. If a 48-bit prefix is used, 16 bits of the 64-bit prefix are available for use. This allows the implementation of up to 65,536 subnets.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router.

6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is suitable for professional use.

7.6.3 6rd tunnel

6rd (rapid deployment) is a development of 6to4. The underlying function is identical. The difference is that just one particular relay is used, as operated by a provider. This solves the two basic problems of the 6to4 technology; the lack of security and stability. The prefix with 6rd is either configured manually or sent via DHCP (IPv4), which further reduces the effort involved with configuration. The diagram is a schematic representation of a 6rd scenario.



The provider assigns the router with a prefix (2001:db8::/32), which the router then supplements with its own IPv4 address. The IPv6 address generated in this way has the form: 2001:db8:5019:d302::/64. This makes 6rd interesting from two perspectives. The provider has a simple way to give its customers access to the IPv6 Internet. In addition, customers benefit from greatly simplified usage. They do not have to accept the security risks of 6to4, nor do they have to handle the complicated configuration of 6in4.

7.6.4 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, abbreviated DS-Lite, is used so that Internet providers can supply their customers with access to IPv4 servers over an IPv6 connection. That is necessary, for example, if an Internet provider is forced to supply its customer with an IPv6 address due to the limited availability of IPv4 addresses. In contrast to the other three IPv6 tunnel methods "6in4", "6rd" and "6to4", DS-Lite is also used to transmit IPv4 packets on an IPv6 connection (IPv4 viaIPv6 tunnel).

For this, the router packages the IPv4 packets in an IPv4-in-IPv6 tunnel and transmits them unmasked to the provider, who then performs a NAT with one of their own remaining IPv4 addresses.

To define a DS-Lite tunnel, all the router needs is the IPv6 address of the tunnel endpoint and the routing tag with which it can reach this address.

By default, the router uses the IPv4 address of the corresponding internal network, e.g., from "INTRANET". If you would like to define a different IP address instead (e.g., 192.0.0.2), it must be entered in the IP parameter list along with the remote site name of the DS-Lite tunnel.

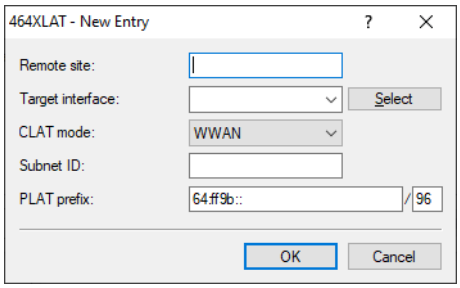
Entering an IPv4 DNS server is not recommended for a DS-Lite tunnel, since its entries would unnecessarily fill the NAT table of the Internet provider.

7.6.5 464XLAT

464XLAT according to *RFC 6877* is a procedure that translates from IPv4 to IPv6 and back to IPv4. The method is often used by mobile network providers to enable IPv4 access in an IPv6-only APN based on NAT64. Two sides are involved in 464XLAT: The client side or client translator (CLAT - customer-side translator) and the provider translator (PLAT - provider-side translator) or NAT64 gateway of the provider. The LCOS supports the CLAT side to enable a network behind a router to access IPv4 networks. In contrast to DS-Lite, which establishes a 4in6 tunnel to the AFTR gateway, 464XLAT

uses a translation of the IPv4 packet to IPv6. On the PLAT side, the packet is translated back into IPv4. The name 464 results from the two-way translation. Generally, the NAT64 prefix 64:ff9b::/96 is used for the translation on the provider side. To use 464XLAT, it is first necessary to configure an IPv6 connection. A 464XLAT peer is then added. The IPv4 default route then points to this peer.

The configuration takes place in LANconfig under **IPv6** > **Tunnel** > **464XLAT**.



Peer

Set a unique name for this peer. Max. 16 characters as capital letters.

Destination interface

Name of the underlying WAN interface or the underlying peer, e.g. INTERNET. Max. 16 characters as capital letters.

CLAT mode

Defines with which method the CLAT prefix should be generated.

DHCPv6-PD

If the Internet provider uses DHCPv6 prefix delegation, e.g. for DSL or cable connections, the CLAT mode DHCPv6-PD must be used. The subnet ID can be used to control which subnet of the delegated prefix should be used for the CLAT prefix. The subnet ID can be configured as 0, 1 or FF, for example.

WWAN (Default)

If the Internet connection is a cellular connection (WWAN), the CLAT mode WWAN must be used. The CLAT prefix is formed from the /64 WAN prefix. The subnet ID must be 0 or empty. NAT must be enabled in the IPv4 routing table for the WAN connection.

Static

If the Internet provider uses a static prefix, the static /64 prefix for the CLAT prefix can be used in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification). This mode can also be used if 464XLAT is to be used on a VPN connection or tunnel interface. In this case, the VPN interface must have a static IPv6 address configured.

Subnet ID

Subnet ID that is combined with the provider's delegated DHCPv6 prefix. The IPv4 source address is embedded in the resulting prefix when the packet is sent over the WAN. In the case of a WWAN connection (/64 prefix), the parameter can be configured either with the value 0 or left empty (default). If the value static is used for CLAT mode, the static /64 prefix can be configured as the CLAT prefix in the Subnet ID field, e.g. 2001:db8:: (without the /64 specification).

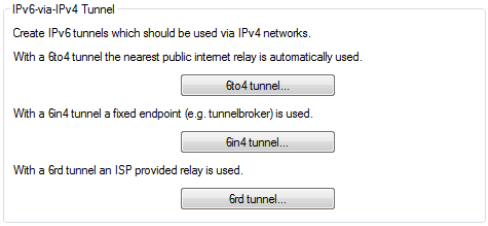
Example for subnet IDs: 0, 1, 12, 1f3b or 2001:db8::

PLAT prefix

IPv6 prefix used on the provider side for translation. If the value is left empty, a DNS prefix discovery according to *RFC 7050* is performed to automatically determine the PLAT prefix. Default: 64:ff9b::/96

7.6.6 Setting up tunnels

The **Tunnel** configuration offers you 3 buttons to create IPv6 tunnels that can be used over IPv4 networks. Use these options to gain access to the IPv6 Internet using an IPv4 connection.



6to4 tunnel

This button opens the 6to4 tunnel settings.

Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

6in4 tunnel

This button opens the 6in4 tunnel settings.

6in4 tunnels require more administrative effort, but they represent a secure and stable technology for IPv6 Internet access. This option is also suitable for professional use.

6rd tunnel

This button opens the 6rd tunnel settings.

6rd tunneling is suitable for end users and for professional applications because configuration is less complex than with 6in4 tunneling and the technology avoids the security risks of 6to4 tunneling.

7.6.6.1 Setting up a 6to4 tunnel

The use of a 6to4 tunnel is feasible when

- Your device is IPv6 capable and you want to access IPv6 services,
- Your provider does not support a native IPv6 network and
- You do not have access to a so-called tunnel broker who can mediate your IPv6 packets.

When using a 6to4 tunnel, the lack of support of IPv6 by the provider means the device does not receive an IPv6 address or an IPv6 prefix.

The device calculates its own unique prefix from "2002::/16" and the hexadecimal representation of its own public IPv4 address from the provider. This application only works if the device has a public IPv4 address. The device does not receive a public IPv4 address, but only an IPv4 address from a private address range, if

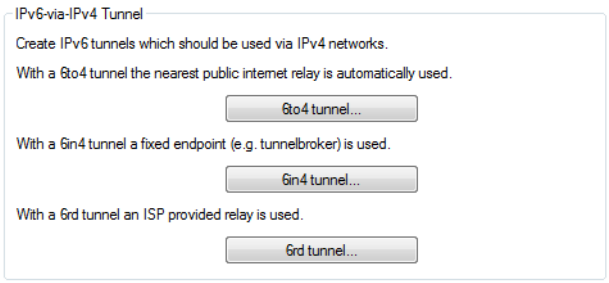
- the device connects to the Internet via cellular network and the provider only provides private IP addresses for this purpose; or
- the device itself does not provide Internet access but is “behind" another router.

Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the relay used can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

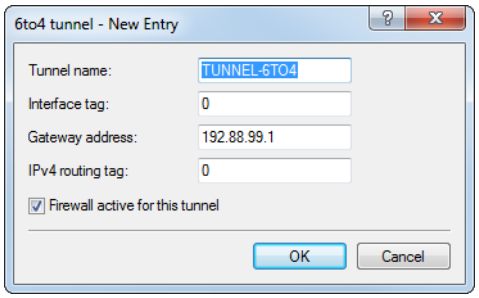
Configuration

To set up a 6to4 tunnel with LANconfig, proceed as follows:

1. Start LANconfig. LANconfig now automatically searches the local network for devices.
2. Select the device on which you want to set up a 6to4 tunnel. Select it with a left-click and start the configuration from the menu bar with **Device** > **Configure**.
3. Navigate to **IPv6** > **Tunnel** and click on **6to4 tunnel**.



4. Click on **Add** to create a new 6to4 tunnel.

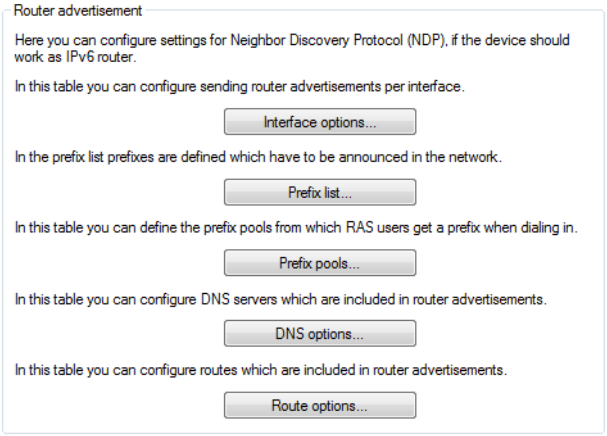


5. Set the name of the 6to4 tunnel.
6. Set the **Interface tag** to a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
7. The **Gateway address** is set by default to the anycast address "192.88.99.1".
8. Here you specify the routing tag that the device uses to determine the route to the associated remote gateway. The **IPv4 routing tag** specifies which tagged IPv4 route is to be used for the data packets to reach their destination address.
9. The default value is this tunnel's firewall.

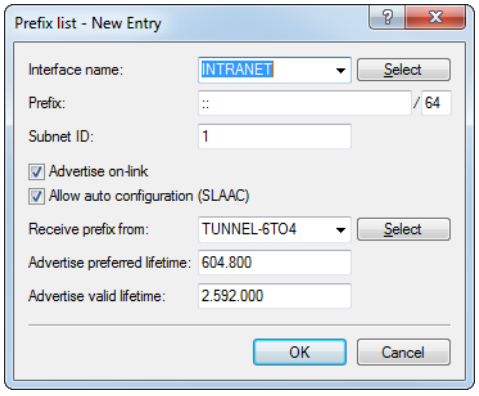
   If you disable the global firewall, you should also disable the firewall for the tunnel.

10. Accept your entries with **OK**.

11. Change to the directory **IPv6** > **Router advertisements**.

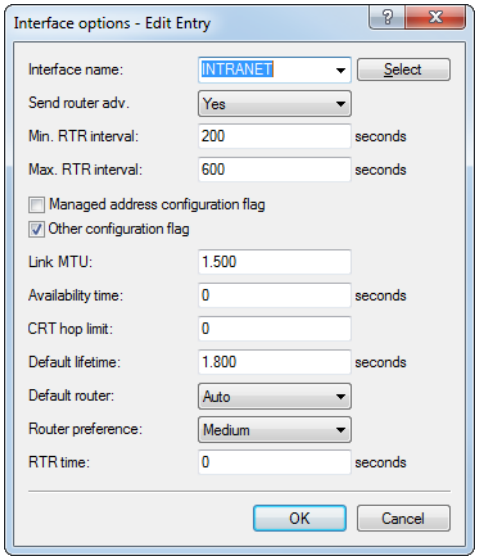


12. Open the **Prefix list** and click on **Add.**



13. Enter a name for the interface that is used by the 6to4 tunnel, e.g. "INTRANET".
14. Set the value for the **Prefix** to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
15. Accept the default value of "1" for the **Subnet ID**.
16. Accept the activated option **Allow auto-configuration (SLAAC)**.
17. In the field **Prefix delegation from**, enter the name of the tunnel that you have defined earlier, e.g. in the example above "TUNNEL-6TO4".
18. Accept your entries with **OK**.
19. In the directory **IPv6** > **Router advertisements**, open the **Interface options**, select the entry INTRANET and click on **Edit**.

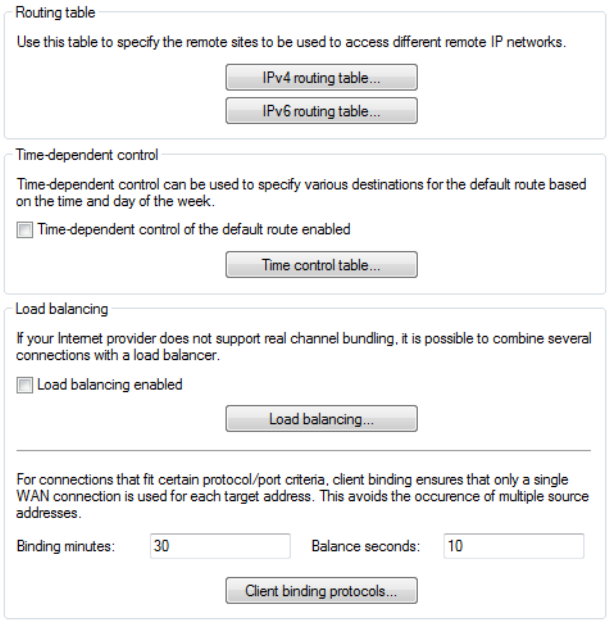
20. In the drop-down menu **Send router advertisements** select the option 'Yes'.



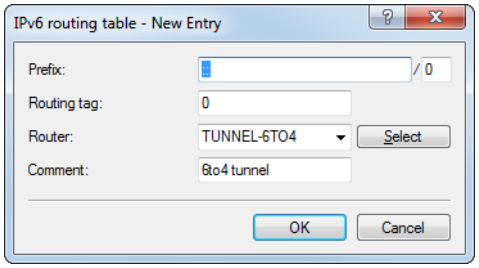
21. Accept all other default values without change.

22. Save your entries with **OK**.

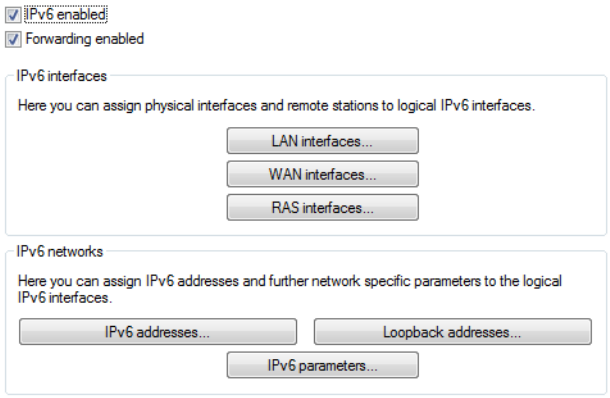
23. Change to the directory **IP router** > **Routing**.



24. Open the **IPv6 routing table** and click on **Add**.



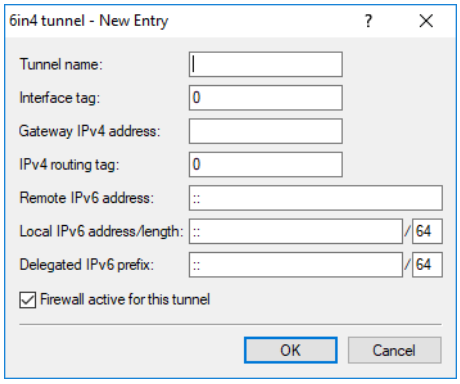
25. Set the **Prefix** to the value "::/0".
26. In the field **Routing tag** accept the default value "0".
27. In the field **Router**, select from the list the name of the tunnel that you defined earlier, e.g. in the example above "TUNNEL-6TO4".
28. Enter a descriptive **comment** for this entry.
29. Save your entries with **OK**.
30. Change to the directory **IPv6** > **General** and enable the IPv6 stack.



7.6.6.2 Configuring a 6in4 tunnel

The button **6in4 tunnel** opens the configuration for a 6in4 tunnel.

Click on **Add** to create a new tunnel.



You can set the following properties for the tunnel:

Tunnel name

Specifies the name of the 6in4 tunnel.

Interface tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received on this network are marked internally with this tag.

The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Gateway IPv4 address

The IPv4 address of the remote 6in4 gateway. The tunnel is only established if the gateway can be reached by ping.

IPv4 routing tag

Enter the routing tag for setting the route to the relevant remote gateway.

Remote IPv6 address

IPv6 address of the remote tunnel endpoint on the intermediate network, for example, 2001:db8::1.

Local IPv6 address / length

Local IPv6 address of the device on the intermediate network, for example 2001:db8::2/64.

Delegated IPv6 prefix

Prefix that is routed from the remote gateway to the local device and that is to be used in LAN, e.g. 2001:db8:1:1::/64 or 2001:db8:1::/48.

Firewall active for this tunnel

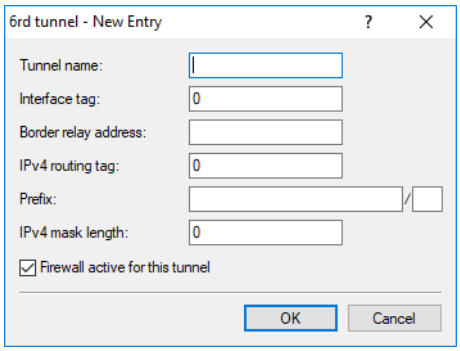
If the global IPv6 firewall is enabled, you can enable or disable the firewall for this tunnel interface here. To enable the IPv6 firewall globally, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

Disabling the global IPv6 firewall means that the firewall is disabled for all interfaces, even if you enable this option.

7.6.6.3 Configuring a 6rd tunnel

The button **6rd tunnel** opens the configuration for a 6rd tunnel.

Click on **Add** to create a new tunnel.



You can set the following properties for the tunnel:

Tunnel name

Specifies the name of the 6rd tunnel.

Interface tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received on this network are marked internally with this tag.

The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

Border relay address

This is the IPv4 address of the 6rd border relay.

If this field is left blank, the data is obtained via DHCPv4.

IPv4 routing tag

Enter the routing tag for setting the route to the relevant remote gateway.

Prefix

The prefix used by the provider for 6rd services, e.g. 2001:db8::/32.

If the 6rd prefix is assigned via DHCPv4 (i.e. the border relay address is empty), this field is ignored or can be left empty.

IPv4 mask length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. For example, if the mask length is 0, then there are no identical bits and the entire IPv4 address is used to generate the delegated 6rd prefix.

The mask length is specified by the provider.

Example: The IPv4 address of the router is 192.168.1.99 (in hexadecimal: c0a8:163). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8:1::/32	0	2001:db8:1:c0a8:163::/64
2001:db8:1:2::/48	16	2001:db8:1:2:163::/64
2001:db8:1:2:3300::/56	24	2001:db8:1:2:3363::/64

Default is 0

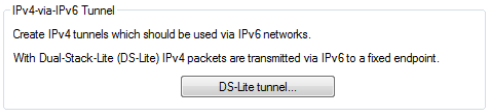
Firewall active for this tunnel

If the global IPv6 firewall is enabled, you can enable or disable the firewall for this tunnel interface here. To enable the IPv6 firewall globally, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS** > **General** .

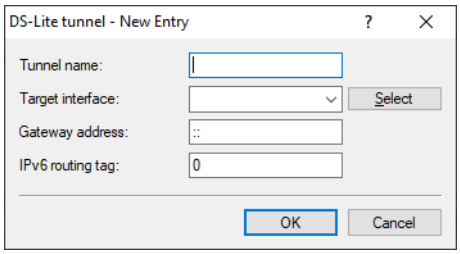
Disabling the global IPv6 firewall means that the firewall is disabled for all interfaces, even if you enable this option.

7.6.6.4 Setting up a Dual-Stack Lite (DS-Lite) tunnel

You set up a DS-Lite tunnel in LANconfig via **IPv6** > **Tunnel** by clicking on **DS-Lite tunnel**.



Then click on the **Add** button and enter the designation of the tunnel, the IPv6 address of the gateway, and the routing tag.



Name of the tunnel

This entry determines the name of the IPv4-over-IPv6 tunnel.

Target interface

Name of the underlying WAN interface or the underlying peer, e.g. INTERNET. Max. 16 characters as capital letters.

Gateway address

This entry defines the address of the DS-Lite gateway, the so-called Address Family Transition Router (AFTR).

The following values are possible:

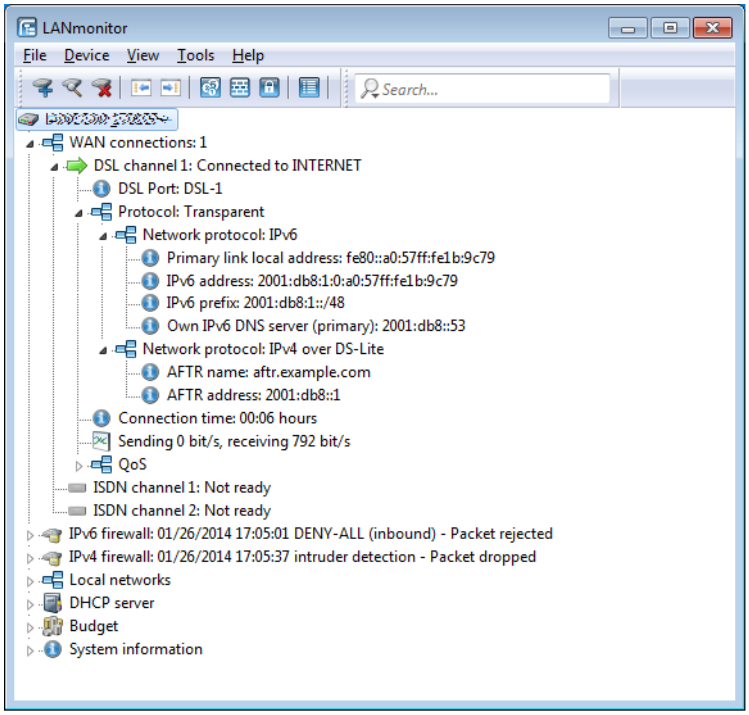
- One IPv6 address, e.g. 2001:db8::1
- An FQDN (Fully Qualified Domain Name) that can be resolved by DNS, e.g., aftr.example.com
- The IPv6 unspecified address "::" determines that the device should retrieve the address of the AFTRs via DHCPv6 (factory setting).
- An empty field behaves the same as the entry "::".

IPv6 routing tag

The routing tag uniquely specifies the route to the DS-Lite gateway.

With DS-Lite, since the NAT is performed by the provider, the function of many applications depends on the settings of the NAT provider (e.g., SIP, IRC or IPSec). PPTP does not work via DS-Lite. If the provider does not operate port forwarding, the IPv4 server services do not function.

The status table and the number of current DS-Lite connections can be shown using LANmonitor:

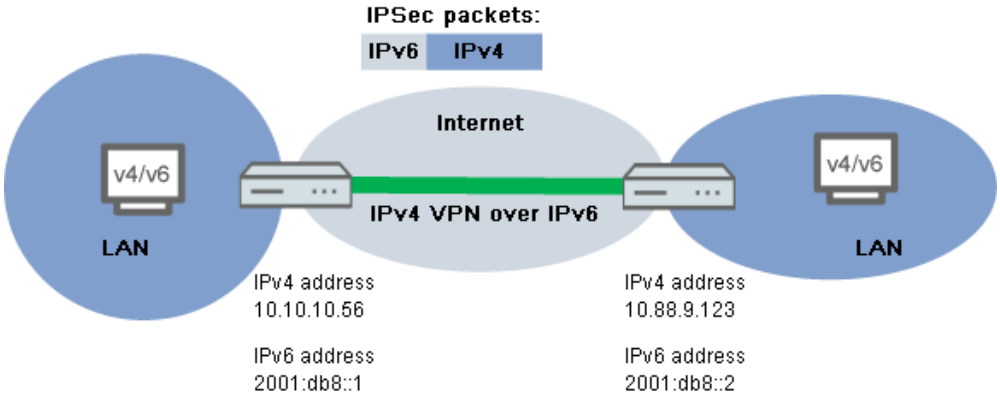


7.6.6.5 IPv4 VPN tunnel over IPv6

If a provider no longer offers public IPv4 addresses, then a VPN tunnel that couples IPv4 networks can also be established over IPv6 WAN addresses.

This requires IPv6 addresses to be configured for the VPN gateway addresses.

In the example shown, two local IPv4 networks are connected via an IPv4 VPN tunnel, which is established over an IPv6 Internet connection. The IPv4 VPN packets are given IPv6 headers and sent to the remote site via the IPv6 Internet connection (either native or via tunnel broker).



Setup Wizard – setting up an IPv4 VPN connection over IPv6

The Setup Wizard option "Connect two local area networks" helps you to set up a VPN connection.

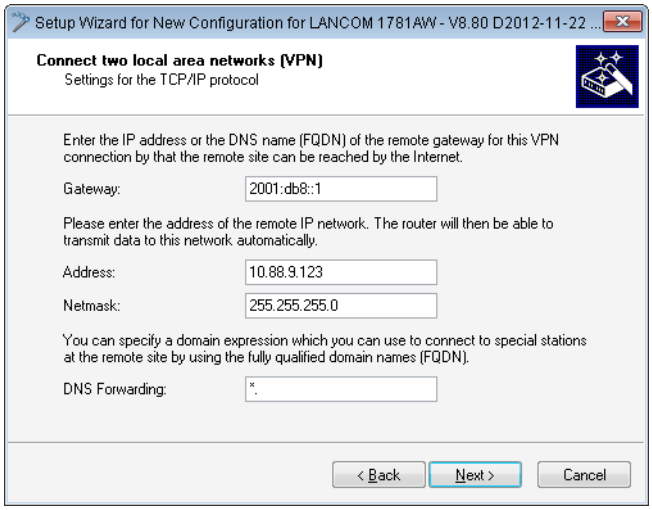
1. Start LANconfig.

   LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.

2. Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools** > **Setup Wizard**.

   LANconfig first reads out the device configuration and displays the selection window with the optional applications.

3. Launch the action **Connect two local area networks**.
4. Follow the Wizard's instructions and enter the necessary data.
5. As the gateway address, enter the IPv6 address of the gateway.



6. You can then close the Wizard with **Finish**.

   The Setup Wizard writes the configuration to the device.

8 Firewall

For most companies and many private users a work without the Internet is no longer conceivable. E-mail and web are indispensable for communication and information search. But each connection of the workstations from the own, local network to the Internet represents however a potential danger: Unauthorized users can try to see your data via this Internet connection, to modify it or to manipulate your PCs.

Therefore this chapter covers an important topic: the firewall as defensive measure against unauthorized access. Besides a brief introduction to the topic of Internet security, we show you which protection a router is able to offer you by right configuration and how to make the needed specific settings.

8.1 Threat analysis

In order to plan and implement appropriate security measures, we first need to be aware of the potential sources of danger:

- Which dangers threaten your LAN or your data?
- Which paths can intruders take to gain access to your network?

Intruding into protected networks is generally referred to as an “attack”, so an intruder is also known as an “attacker”.

8.1.1 The dangers

The dangers on the Internet arise from all sorts of different motives. On the one hand, perpetrators are trying to personally enrich themselves or to specifically harm their victims. The increasingly widespread knowledge of “hacking” means it has become a kind of sport, which often attracts juveniles competing to see who can be the fastest to overcome the hurdles of cybersecurity.

Regardless of the individual motivation, the perpetrators' intentions usually following certain patterns:

- Insight into confidential information such as company secrets, access information, passwords for bank accounts, etc.
- Hijacking computers in the LAN for the purpose of the attackers, e.g. for the distribution of their own content, attacks on further computers, etc.
- Modifying data on the computers in the LAN, for example to create further means of access
- Destruction of data on computers in the LAN
- Disabling computers in the LAN or the Internet connection

We will concentrate on the attacks on local area networks (LAN) or on workstations and servers in these LANs.

8.1.2 The paths of the attackers

In order to achieve their objectives, the attackers first need a way to access your PCs and data. In principle, the following paths are open to them as long as they are not blocked or protected:

- Via the central Internet connection, e.g. via a router
- Via decentralized connections to the Internet, e.g. using modems on individual PCs or mobile phones connected to laptops
- Via wireless networks operating to supplement wired networks

This section concentrates exclusively on the paths through the central Internet connection, the router.

For information on protecting your wireless networks, please refer to the corresponding sections of this Reference Manual or the relevant device documentation.

8.1.3 The methods

Usually, strangers do not have access to your local network or the computers on it. So nobody can access the protected area without the corresponding access credentials or passwords. If these credentials cannot be gained by espionage, the attackers will attempt to reach their objectives in a different way.

One basic approach is to smuggle data into the network using one of the approved routes for data exchange, which then opens up access to the attacker from within. Attachments in e-mails or active content on web pages can be used to install a small program on a computer, which is then caused to crash. The program then uses the crash to create a new administrator on the computer, which can then be remotely used for further actions in the LAN.

If access via e-mail or WWW is not possible, an attacker may also search for a server on the LAN that offers certain services that can be used for their own purposes. The services on these servers are identified through specific ports in the TCP/IP protocol, so the search for open ports is referred to as port scanning. The attacker initiates this with a certain program that requests the desired services either from the Internet in general or from specific networks only. The corresponding response will come from unprotected computers.

A third option is to intercept and eavesdrop on an existing data connection. The attacker observes the victim's Internet connection and analyzes the connections. They then use an active FTP connection to insert their own data packets into the LAN.

One variant of this method is the "man-in-the-middle" attack. The attacker first observes to the communication between two computers and then intervenes.

8.1.4 The victims

The question of the degree of danger of an attack greatly influences the expenditure that one wishes to, or must, make on protection. You as a potential victim can assess whether your network is of particular interest to an attacker by means of the following criteria:

- At particular risk are networks of well-known companies or institutions, where valuable information may be available. This may include the research results that are of interest to industrial espionage, or bank servers that control large sums of money.
- However, the networks of smaller organizations are also at risk as they may be of interest to specific groups. The computers of tax consultants, lawyers or doctors certainly contain information that could be of interest to third parties.
- Last but not least, computers and networks are victims of attacks that offer no apparent benefit to the attackers. In particular "script kiddies", who test their abilities out of youthful ambition, are sometimes just looking for a defenseless victim as practice for tougher tasks.

  Attacking a private person's unprotected computer, which is not really very interesting at all, may serve as a starting point for attacks on the actual targets in the second step. The "uninteresting" computer becomes the starting point of the later attack, and the identity of the attacker is disguised.

All things considered, the statistical probability of an attack on the network of a global player is far greater than for a home-office network. But it is surely only a matter of time until a defenseless workstation on the Internet will, perhaps even accidentally, become the victim of attacks.

8.2 What is a firewall?

There are very different ways to interpret the concept of the "firewall". At this point we would like to explain the meaning of firewall in this manual:

A firewall is a centrally located collection of components for monitoring data exchange between two networks. In most cases, the firewall monitors the data exchange between an internal, local area network (LAN) and an external network such as the Internet.

The firewall can consist of hardware and / or software components:

- In purely hardware systems, the firewall software often runs on a proprietary operating system.
- The firewall software can also run on a normal computer with Linux, Unix or Windows, which is dedicated to this task.
- As a third and common alternative is the firewall software that runs directly within the router connecting the LAN to the Internet.

In the following sections, we will only consider the firewall in a router.

The functions "intrusion detection" and "DoS prevention" are a part a firewall in some applications. These functions are also included in our router, although they are implemented as separate modules alongside the firewall. Refer to sections *Protection against break-in attempts: Intrusion detection* on page 688 and *Protection against Denial-of-Service attacks* on page 689 for further information on this.

8.2.1 The tasks of a firewall

8.2.1.1 Checking data packets

How does the firewall monitor the traffic? In principle, the firewall works like a doorman for data packets: Each packet is inspected to see if it is allowed to pass the door of the network (the firewall) in the desired direction or not. This firewall inspection makes use of various criteria referred to as "rules" or "guidelines". Different types of firewalls are distinguished according to the type of information that is used to create the rules and that is inspected by firewall operations.

Above all, the aspect of central positioning is important: Only when all of the data traffic between the inside and outside passes through the firewall can it reliably fulfill its task. Any alternative path would reduce or even disable the security of the firewall. This central location of the firewall also makes maintenance easier: A firewall as a common transition between two networks is easier to maintain than a "personal firewall" on each computer in the LAN.

In principle, firewalls work at the interface between two or more networks. For the following explanation, we will focus on the transition between a local network at a company and the Internet. However, these explanations do apply analogously to other network constellations, such as for protecting a Human Resources subnet in an organization from the other network users.

8.2.1.2 Logging and alerting

Important functions of a firewall include not only inspecting the data packets and responding appropriately to the results of this check, but also the logging of all actions triggered by the firewall. By evaluating these logs, the admin can draw conclusions about the attacks and further improve the configuration of the firewall.

But sometimes, logging alone can come too late. Often, quick intervention by the admins can prevent further damage. For this reason, firewalls usually have an alert function which reports firewall messages to the administrator, possibly by e-mail.

8.2.2 Different types of firewalls

In recent years, the ways firewalls operate have continued to evolve. "Firewall" as a generic term refers to a whole range of different technologies used to protect the LAN. We introduce the most important types here.

8.2.2.1 Packet filters

A packet-filter based firewall inspects the information in the header of the data packets and uses this information to decide whether the packet should be allowed through or not. The information checked for data packets includes:

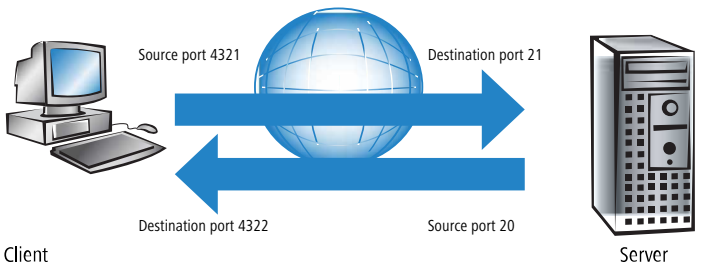
- Source and destination IP addresses
- Transmission protocol (TCP, UDP or ICMP)
- Source and destination port numbers
- MAC address

The rules defined in a packet-filter based firewall can decide, for example, whether packets from a particular IP address range are allowed to be forwarded to the local network, or whether packets for certain services (i.e., specific port numbers) should be filtered. These measures can be used to restrict or prevent communication with certain computers or entire networks, or the use of particular services. Rules can be combined. For example, you may want to allow only computers with specific IP addresses to access the Internet via TCP port 80, while disabling this service for all other computers.

The configuration of packet-filtering firewalls is relatively simple, and the list of allowed or forbidden packets can be quickly extended. Since the resources required for a packet filter to perform well are relatively modest, packet filters are usually implemented directly in routers, which anyway operate as an interface between the networks.

The disadvantage of packet filters is that the list of rules can become difficult to manage over time. Furthermore, some services negotiate the ports for their connections dynamically. For this communication to work, the administrator is forced to leave open any ports that may potentially be required, which of course goes against the principles of most security concepts.

An example of a process that causes difficulties for simple packet filters is establishing an FTP connection from a computer in its own LAN to an FTP server on the Internet. With the widely used active FTP, the client sends a request (from the protected LAN) via a higher numbered port (> 1023) to port 21 of the server. The client informs the server about which port it expects for the connection. The server then establishes a connection from its port 20 to the port requested by the client.



To enable this operation, even though it is impossible to know in advance which ports the client will request for the FTP connection, the administrator of the packet filter is forced to open all ports for inbound connections. An alternative is to use passive FTP. Here, the client itself establishes the connection to the server using a port which it previously communicated to the server. However, this method is not supported by all clients/servers.

Using the comparison of the firewall with a doorman once again, the doorman only checks whether or not he knows the courier at the door with the parcel. If the doorman knows the courier and has previously allowed him to enter the building, the courier may enter unhindered and unchecked and go to the recipient's workstation for all subsequent orders.

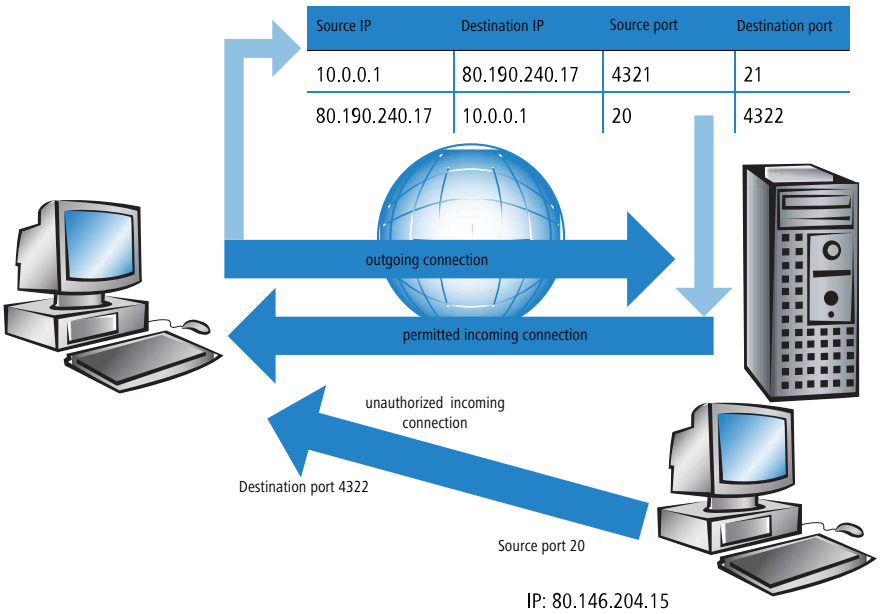
8.2.2.2 Stateful packet inspection

Stateful packet inspection (SPF), or stateful inspection for short, enhances the packet filter approach by checking additional information about the connection state. In addition to the static table with the permitted ports and address ranges, this technology maintains a dynamic table containing information about the status of the individual connections. This dynamic table initially allows all vulnerable ports to be blocked; only when an approved connection (defined by source and destination address) requests it will a port be opened. The act of opening ports is always initiated from the protected network towards the unprotected network, i.e. generally speaking from the LAN to the WAN (Internet). Data packets that are not associated with a valid connection in the state table are automatically dropped.

The rules used by stateful-inspection firewalls—unlike for conventional port-filter firewalls—are direction-dependent: A connection is always established from the source to the destination, unless there is an explicit entry for the return direction. Once a connection is established, the only the data packets that are transmitted are those that belong to this connection—in both directions, of course. This ensures that any unsolicited access attempts that are not from the local network are reliably blocked.

In addition, stateful inspection can see from the connection establishment whether additional channels are being negotiated for the data exchange. Protocols such as FTP (for data transfer), T.120, H.225 and H.245 for Netmeeting or IP telephony), PPTP (for VPN tunnels) or IRC (for chat) establishing a connection from the LAN to the Internet using a particular source port indicate whether they are negotiating additional ports with the remote site. Stateful inspection enters these additional ports into the connection list, of course restricting them to the corresponding source and destination addresses.

Let's take another look at the example of an FTP download. When starting the FTP session, the client establishes a connection from the source port '4321' to the destination port '21' at the server. Provided that the FTP protocol is allowed from local computers to the outside, stateful inspection permits this initial connection to be established. The firewall enters the source and destination addresses along with the corresponding ports into the dynamic table. At the same time, the stateful inspection can inspect the control information sent to port 21 of the server. These control signals show that the client is requesting a connection from the server port 20 to the client port 4322. The firewall enters these values into the dynamic table because the client is requesting the connection into the LAN. The server can then send the data to the client as desired.



Should another computer on the Internet attempt to send data from its port 20 to the protected client via the now open port 4322, the firewall will prevent this because the IP address of the attacker does not match with the one permitted for this connection.

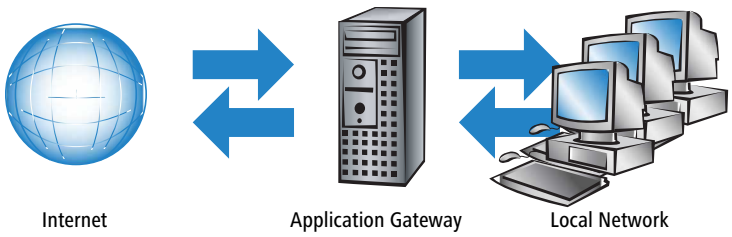
After a successful data transfer, the entries are automatically deleted from the dynamic table and the ports are closed again.

Moreover, a firewall with stateful inspection is usually able to re-assemble the data packets it receives, i.e. to buffer individual fragments and reassemble them into a complete packet. As a result, the firewall inspects not only the individual parts of fragmented packets, but also the complete IP packet itself.

This doorman is dong a much better job. A courier ordered by this company now has to call the doorman, tell them to expect a courier, what time he will be there, and what is written on the parcel delivery note. Only if this information agrees with the doorman's instructions will the courier be allowed through. If the courier brings not just one parcel, but two, then only the one with the correct delivery note will be allowed to pass. Similarly, a second courier demanding to see the employee will be turned away at the door.

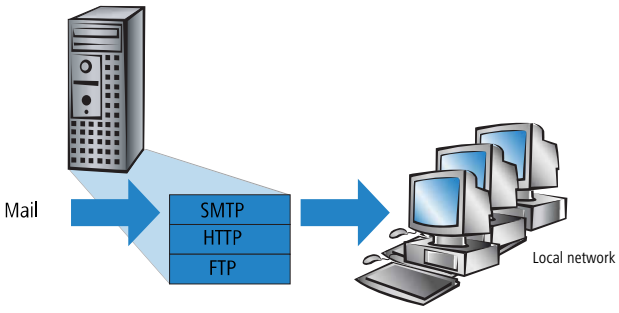
8.2.2.3 Application gateway

By checking content at application level, application gateways are a supplement to the packet-filter address validation and stateful-packet-inspection connection monitoring. As a rule, the high demands on hardware performance require the application gateway to run on a separate computer. This computer is located between the local network and the Internet. Seen from either direction, this computer is the only way to exchange data with the other network. There is no direct connection between the two networks, just to the application gateway.



The application gateway acts as a proxy for each of the two networks. Another name for this is a "dual-homed gateway" as this computer is, so to speak, at home in two networks.

A dedicated service is set up on the gateway for each of the permitted applications, such as SMTP for mail, HTTP for surfing the Internet, or FTP for data download.



This service receives the data received from one side and maps it to the other side. What at first glance looks like a rather superfluous mirroring of data actually represents the basic concept of application gateways: There is never a direct connection between a client on the local network and a server on the Internet. The computers in the LAN can only "see"

the proxy, as can the computers from the Internet. This physical separation of LAN and WAN makes it much harder for an attacker to invade the protected network.

Put in terms of our earlier doorman's example, the parcel in this case is delivered at the gate and the courier may not even enter the company premises. The doorman accepts the parcel, opens it after checking the address and delivery note, and checks the contents. Once the parcel has successfully taken all these hurdles, an in-house messenger will take the parcel directly to the recipient in the company. The messenger thus becomes the representative of the courier on the company premises. Conversely, employees who want to send a parcel must call the doorman, who has the parcel picked up at the workplace and handed over to an appointed courier at the gate.

The function of an application gateway is not supported by the device due to the high demands on the hardware.

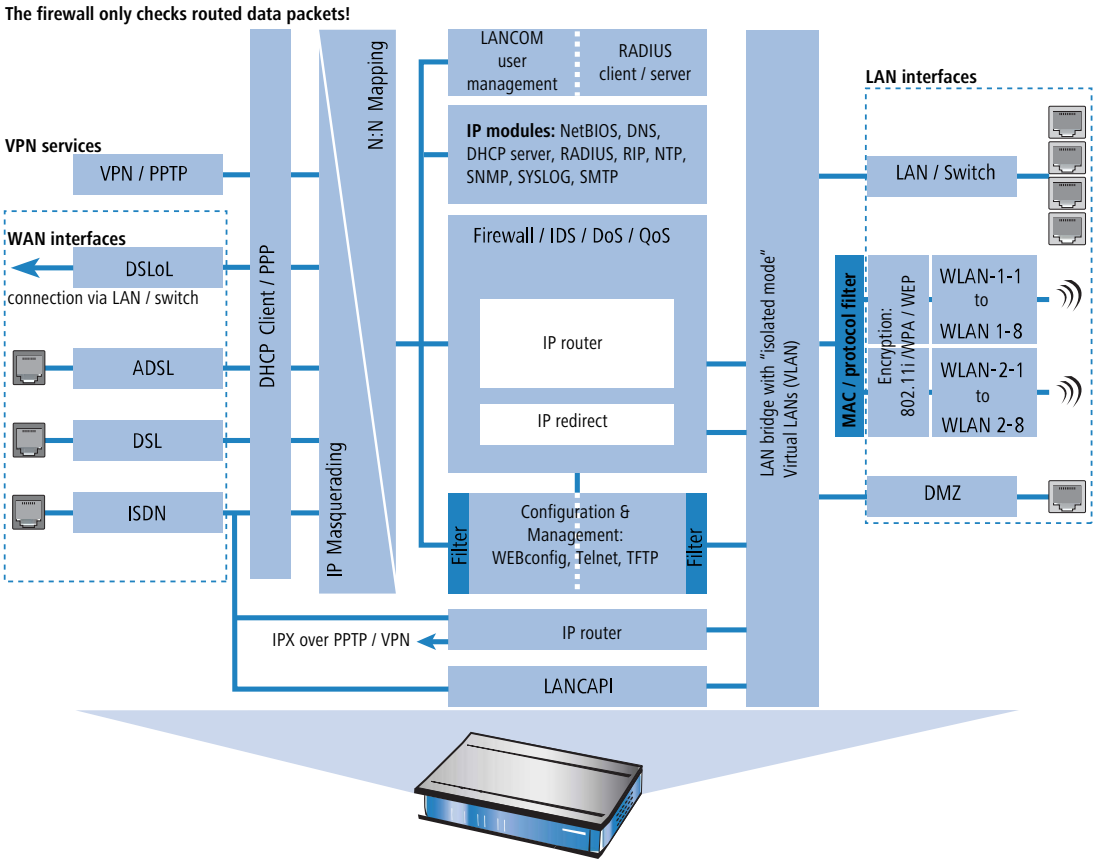
8.3 The firewall in the device

This section presents a general explanation of the dangers from the Internet, the tasks and types of firewalls, descriptions of the special functions of the firewall in the device, and information on its specific configuration.

For devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

8.3.1 How the firewall inspects data packets

From the entire data stream passing through the IP router, the firewall filters out all data packets that have been targeted for special treatment.



The firewall only inspects the data packets that are routed by the IP router in the device. In general, these are data packets being exchanged between the internal networks (LAN, WLAN, DMZ) and the "outside world" via one of the WAN interfaces. Communication between the LAN and WLAN is not usually handled by the router, assuming that the LAN bridge allows a direct exchange. Thus the firewall rules do not apply here. The same applies to the so-called "internal services" such as Telnet, TFTP, SNMP and the web server for configuration via WEBconfig. The data packets for these services do not travel through the router and are therefore not affected by the firewall.



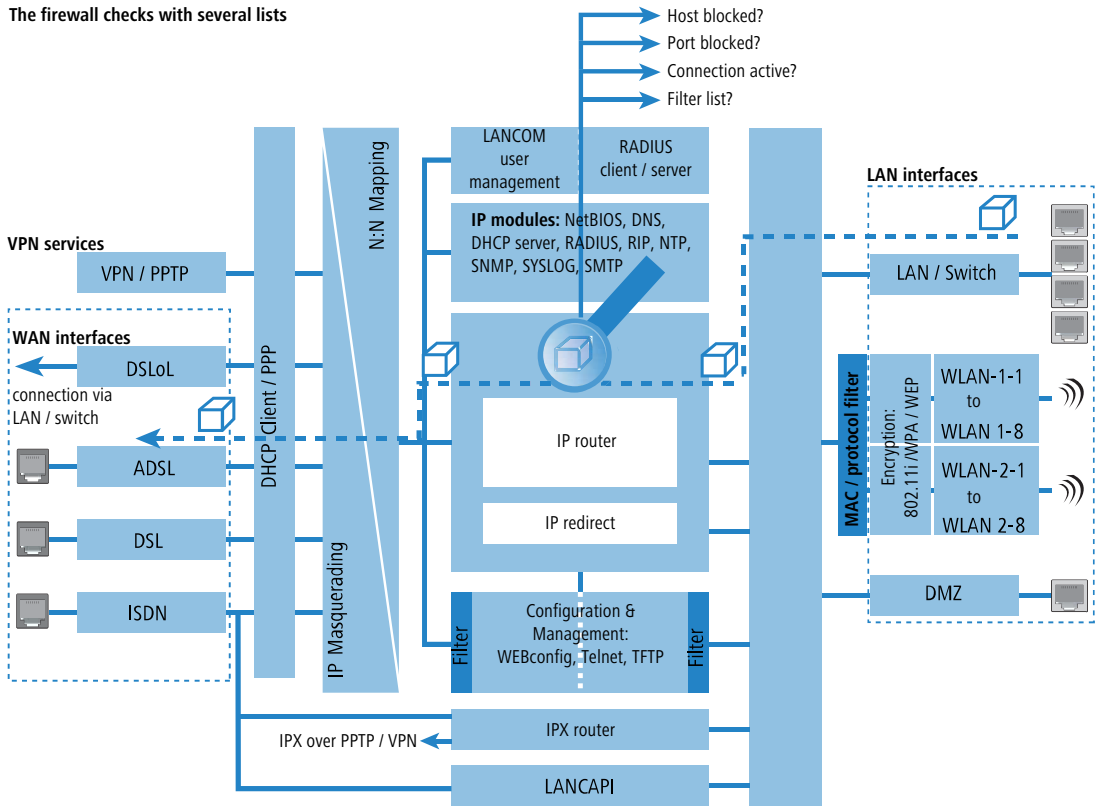
As it is located behind the masquerading module (as seen from the WAN), the firewall works with the "real" internal IP addresses of the LAN stations and not with the external Internet address of the device.

The firewall in the device inspects the data packets using a number of lists, which are generated automatically from the firewall rules, the firewall actions triggered by them, or the active data connections:

- Host blocking list
- Port blocking list
- Connection list
- Filter list

When a data packet is to be routed via the IP router, the firewall uses the lists as follows:

1. The first check is, whether the packet has arrived from a workstation that is in the **host block list**. If the sender is blocked, the packet is dropped.
2. If the sender is not blocked, the **port block list** is checked to see whether the port/protocol combination used on the target computer is closed. In this case these packet is dropped.
3. If the sender and the destination are not blocked in the first two lists, a check is made as to whether this connection is entered in the **connection list**. If an entry exists, then the packet is treated as is noted in the list.
4. If no entry is found for the packet, the **filter list** is scanned for a suitable entry and the action indicated there is performed. If the action indicates that the packet is to be accepted, an entry is made in the connection list and any further actions are noted there.



If there is no explicit firewall rule for a data packet, the packet is accepted (allow all). This ensures backwards compatibility with existing installations. To maximize protection by stateful inspection, please refer to the section *Establishing an explicit deny-all strategy* on page 675.

The four lists obtain their information as follows:

- The host blocking list contains those stations that are blocked for a certain time due to a firewall event. This list is dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.
- The port blocking list contains those protocols and services that are blocked for a certain time due to a firewall event. This list is also dynamic and new entries can be added continuously by corresponding firewall events; entries disappear automatically after the blocking time expires.
- Established connections are entered into the connection list if the checked packet is accepted by the filter list. The connection list records the source and destination, the protocol, and the port that a connection is currently allowed to use. The list also indicates how long the entry remains in the list and which firewall rule generated the entry. This list is highly dynamic and always "on the move".
- The filter list is generated from the rules in the firewall. The filters it contains are static and can only be changed when firewall rules are added, edited or deleted.

All lists used by the firewall to inspect the data packets are therefore ultimately based on the firewall rules (*Parameters of the firewall rules* on page 666).

8.3.2 Special protocols

An important point in connection monitoring is how to handle protocols that dynamically negotiate ports and/or addresses that are used for other communications. Examples of these protocols are FTP or even many UDP-based protocols. These require further connections to be opened in addition to the initial one. (Also see *Different types of firewalls* on page 653).

8.3.2.1 UDP connections

Although UDP is actually a stateless protocol, even UDP-based protocols can be said to be short-term connections, as most of them are request-response protocols: Here, a client sends its request to the server's well-known port (e.g. 53 for DNS), and this sends back its response to the source port selected by the client:

Client port	Connection	Server port
12345	Request	53
	→	
12345	Response	53
	←	

However, for a server to send larger amounts of data, for example using TFTP where it does not need to differentiate between requests and acknowledgments on the well-known port, it first sends the response packet to the source port of the sender. In doing so, it sets an arbitrary free port as its own source port for exchanging data with the client:

Client port	Connection	Server port
12345	Request	69
	→	
12345	Response	54321
	←	
12345	AckData	54321
	→	
12345	Data/Ack	54321
	←	

With data transmission ongoing via the ports 12345 and 54321, the server can accept further requests on its well-known port (69). If the device pursues a "deny-all strategy", the client's first request creates an entry in the connection list that only allows the server's data packets on port 69. The answer from the server would simply be dropped. To prevent this, the entry created in the connection list initially has no value for the connection's destination port, and this is only set when the first response packet arrives. This caters for both possible cases of a UDP connection.

8.3.2.2 TCP connections

TCP connections cannot be tracked simply by inspecting the ports. For some protocols such as FTP or PPTP, checks of the payload are necessary to open all subsequently negotiated connections, so that only those packets that genuinely belong to the connections are accepted. This is a simpler version of how IP masquerading works, but without address and port mapping. It is sufficient to follow the negotiation, open the appropriate ports and link them with the main connection. This means that these ports are also closed when the main connection is closed, and the data traffic on the secondary connections also keeps the main connection open.

8.3.2.3 ICMP connections

For ICMP, we differentiate between two cases: These are the ICMP request/reply connections as used by "ping", and the ICMP error messages that can be received in response to any IP packet.

ICMP request/reply connections can be uniquely assigned to the initiator according to the identifier used, i.e. when an ICMP request is sent, an entry is created in the state database that only allows ICMP replies with the correct identifier to pass. All other ICMP replies are silently dropped.

For ICMP error messages, the IP header and the first 8 bytes of the IP packet (usually UDP or TCP header) are inside the ICMP packet. On receipt of an ICMP error message, this information is used to search for the corresponding entry in the

status database. The packet is forwarded only if a suitable entry exists, otherwise it is silently dropped. Furthermore, potentially dangerous ICMP error messages (redirect route) are filtered out.

8.3.2.4 Connections using other protocols

For all other protocols, no related connections can be tracked, i.e. only one connection between the participating hosts can be stored in the state database. These can only be initiated from one side, unless there is a dedicated entry for the "opposite direction" in the firewall.

8.3.3 General settings of the firewall

In addition to the individual firewall rules that generate the entries in the filter, connection and revocation lists, other settings are for the firewall in general:

- *Firewall / QoS enabled*
- *Administrator e-mail*
- *Fragments*
- *Session recovery*
- *Ping block*
- *Stealth mode*
- *Mask authentication port*
- *Application definitions*
- *Layer-7 application detection*
- *Application-based routing*

8.3.3.1 Firewall / QoS enabled

This option turns the entire firewall on or off, including the Quality of Service features, for IPv4 and/or IPv6.

Please note that the N:N mapping function is only effective when the firewall is activated.

8.3.3.2 Administrator e-mail

One of the actions that the firewall can trigger is to alert the administrator by e-mail. The administrator e-mail is the e-mail address to which the corresponding alerting e-mails are sent.

8.3.3.3 Fragments

Some attacks from the Internet try to outsmart the firewall with fragmented packets (packets split into several small units). One of the key features of stateful inspection is the ability to reassemble fragmented packets and then inspect the entire IP packet.

The desired behavior of the firewall can be set centrally. The following options are available:

- **Filter**: The fragmented packets are immediately dropped by the firewall.
- **Route**: Fragmented packets are passed through by the firewall without further checks, provided that the valid filter settings permit this.
- **Re-assemble**: The fragmented packets are cached and reassembled into a complete IP packet. The reassembled packet is then inspected with the valid filter settings and handled accordingly.

8.3.3.4 Session recovery

The firewall enters all currently permitted connections into the connection list. After a certain time (timeout) the entries automatically disappear from the connection list again, unless data is transmitted over the connection, which resets the timeout.

The general aging settings occasionally cause connections to be terminated before the requested data packets have been received by the remote site. In this case, there may still be an entry for a valid connection in the connection list even though the connection itself no longer exists.

The session-recovery parameter determines the firewall's behavior for packets that point to a former connection:

- **Always denied**: The firewall does not restore the session and drops the packet.
- **Denied for default route**: The firewall only restores the session if the packet was not received via the default route.
- **Denied for WAN**: The firewall only restores the session if the packet was not received over any of the WAN interfaces.
- **Always allowed**: The firewall always restores the connection if the packet belongs to a "former" connection from the connection list.

Because the function of the virtual router is based on checks of the interface tags, additional routes must be included as “default routes” in addition to the untagged default routes:

- When a packet is received at a **WAN interface**, the firewall considers the WAN interface to be a default route if either a tagged or an untagged default route refers to this WAN interface.
- If a packet is received at a **LAN interface** and is to be routed to a WAN interface, then this WAN interface is considered to be a default route if either the untagged default route or a default route tagged with the interface tag refers to this WAN interface.

Similarly, the default-router filters take effect even if the default route is in the LAN. Here it applies that the filter takes effect when

- A packet was received over a tagged LAN interface and is to be sent over a default route tagged with the interface, or
- A packet from another router was received at a tagged LAN interface and there is a default route with the interface tag to the packet's source address, or
- A packet was received from the WAN and is to be sent to the LAN via a default route with any tag

8.3.3.5 Ping blocking

One—not uncontroversial—way to increase security is to hide the router according to the motto: “If you can’t see me, you won’t attack me ..”. Many attacks start by looking for computers and/or open ports with the help of harmless requests, e.g. with the ping command or a port scan. Any response to these requests, including the “I am not here” response, informs the attacker about a potential target. Because if you answer, you're there. To prevent this, the device can suppress the responses to these requests.

It does this by simply not responding to ICMP echo requests. At the same time, the TTL-exceeded messages used with a traceroute are suppressed, so that the device cannot be found by a ping or a traceroute.

The available settings are:

- **Off**: ICMP responses are not blocked
- **Always**: ICMP responses are always blocked
- **WAN only**: ICMP responses are blocked on all WAN connections
- **Default route only**: ICMP responses are blocked on the default route (usually Internet)

For the choice of “default routes”, the same tips apply as for *Session recovery* on page 660.

8.3.3.6 TCP stealth mode

Along with ICMP messages, the behavior of TCP and UDP connections also provides information on the existence or non-existence of the addressed computer. Depending on the network environment, it may be useful to simply drop TCP and UDP packets instead of responding with a TCP reset or an ICMP message (port unreachable) if there is no listener for that particular port. The desired behavior can be set in the device.

By hiding ports without listeners, masked connections have the problem that the "authenticate" and "ident" service no longer works (or is no longer denied correctly). The corresponding port can therefore be treated separately (*Mask authentication port* on page 662).

The available settings are:

- **off**: All ports are closed and TCP packets are answered with a TCP reset
- **Always**: All ports are hidden and TCP packets are dropped silently.
- **WAN only**: All ports are hidden on the WAN side and closed on the LAN side
- **Default route only**: The ports are hidden on the default route (usually Internet) and closed on all other routes

For the choice of “default routes”, the same tips apply as for *Session recovery* on page 660.

8.3.3.7 Mask authentication port

Concealing TCP or UDP ports can mean that requests from servers (e.g. mail servers) to authenticate users are no longer answered correctly. Requests from the server run into a timeout, and the delivery of the mails is delayed considerably.

Even with TCP stealth mode enabled, the firewall detects a station's intention to connect to a mail server. The port required for the authentication request is then opened briefly (for 20 seconds).

This behavior of the firewall in TCP stealth mode can be suppressed specifically with the parameter “Always mask authentication port too”.

Activating the option “Always mask authentication port too” can lead to considerable delays in sending and receiving e-mails or news.

A mail or news server that requests any additional information from the user first runs into a disturbing timeout before it starts to deliver the mails. This service thus needs its own switch to hide it while remaining compliant.

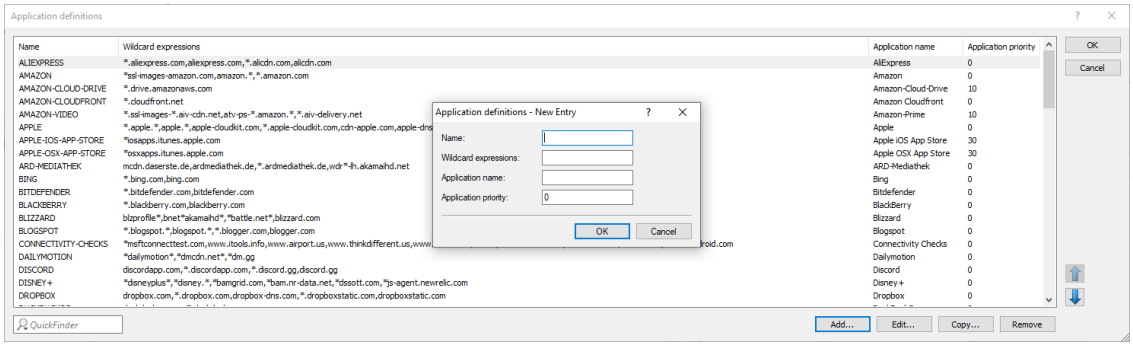
The problem is that a setting that hides all of the ports but issues rejects from the ident port is nonsensical, simply because these rejects (i.e. destination unreachable) reveal the presence of the device.

In order to solve this problem, the device has the option of rejecting ident requests from mail and news servers only. Requests from all other computers are simply dropped. To this end, requests sent to a mail (SMTP, POP3, IMAP2) or news server (NNTP) cause ident requests from the respective servers to be rejected for a brief period (20 seconds).

When the time has expired, the port is hidden again.

8.3.3.8 Application definitions for layer-7 detection and layer-7 application control

The application definitions for layer-7 detection and layer-7 application control are located in a central table for DNS-based applications (layer-7 app) in LANconfig under **Configuration** > **Firewall/QoS** > **General** > **Application definitions** (CLI: **Setup** > **App-Definitions**).



Name

The name for the destination. The name is used to reference this object.

There can be multiple entries for a name by appending the name of the destination with the # character and adding a number with up to three digits (e.g. “LANCOM”, “LANCOM#1”, “LANCOM#2” etc.).

To use this entry in the firewall, it has to be referenced under **Configuration** > **Firewall/QoS** > **General** > **DNS destination lists**.

Wildcard expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. “*.lancom.*”. The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- UTF-8: Here, one to four bytes must be entered individually as '\x' followed by two hexadecimal digits.
- UTF-16: Here, one or two double bytes must be entered as '\u' followed by four hexadecimal digits.
- UTF-32: Here, the value must be entered as '\U' followed by eight hexadecimal digits.

For the layer-7 application detection, use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

Application name

Name for the tracking of HTTP/HTTPS connections for layer-7 application detection (e.g. youtube). Specifying this name activates the layer-7 application detection.

Application priority

By specifying the priority you set the order in which services are evaluated if certain host-name parts appear in multiple entries (e.g. *google).

8.3.3.9 SD-WAN application routing / Layer-7 application control

You can benefit from significant performance gains by operating modern business applications in the cloud (e.g. Microsoft Office 365, AWS, etc). Application routing uses rules to direct trusted applications from the branch office directly to the Internet. This relieves the load on the VPN connection to the main office and also on the Internet connection at the main office.

Microsoft explicitly recommends this mode for Office 365. Because these web-based services often have no fixed IP address, they can only be recognized by DNS names. For this purpose, the corresponding DNS targets can be created in the firewall with an appropriate wildcard expression. These packets are marked with a different routing tag so that the router directs them straight to the Internet. As an alternative, layer-7 application control can be implemented in the firewall. This gives you full control over how applications operate on your network. By defining rules for DNS-based applications, you decide which Internet applications are allowed, blocked, limited or prioritized.

If a user now invokes one of these DNS targets in his or her browser, the computer sends a DNS request for this domain. The DNS forwarder in the LANCOM router then forwards this request to the Internet Service Provider. When the response arrives the router stores the returned IP address, and from that moment on this resolution is available in the firewall. The response then continues on to the computer that made the original request. This allows the browser to open the connection to the returned IP address. The firewall recognizes the previously learned IP address and can assign a routing tag correspondingly. Other defined firewall actions can also be applied to this destination, such as allow, block, limit, or prioritize.

Because the firewall remembers the exact DNS address that the user uses for the domain, this mechanism will also work if the domain name resolves to many different IP addresses or to IP addresses that change over time.

Recommendations

The LANCOM router must operate as a DNS server or DNS forwarder on the network, i.e. clients on the local network must use the router as the DNS server. In addition, clients need to be prevented from using DNS-over-TLS and DNS-over-HTTPS (also in the browser) directly with external DNS servers.

This can be done as follows:

- The DHCP server has to communicate the IP address of the router as a DNS server (set by default by the Internet wizard)
- Firewall rules have to be set up that prevent the direct use of external DNS servers, e.g. by blocking the outgoing port 53 (UDP) for clients on the source network
- Firewall rules have to be set up that prevent the direct use of external DNS servers that support DNS-over-TLS, e.g. by blocking the outgoing port 853 (TCP) for clients on the source network
- Disable DNS-over-HTTPS (DoH) in the browser

Notes on how to synchronize the firewall's DNS database:

Since the firewall learns its information from the DNS requests of the clients, in certain situations the DNS database will be incomplete. This can happen in the following situations:

- A new firewall rule is added, but the client still has a cached DNS entry
- The router was recently restarted, and the client still has a cached DNS entry

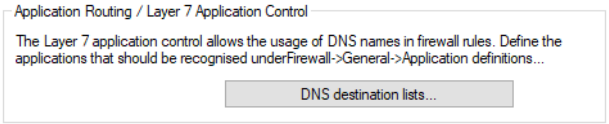
Helpful in these cases are emptying the DNS cache on the client, rebooting the client, or a time-out of the DNS record on the client.

The router's own services, such as ping, are not handled by the firewall rules. By sending a ping to a full DNS name (without wildcard expressions), the generation of rule resolutions (DNS to IP addresses) can be performed on-demand either from the CLI (once) or by a cron job.

Different DNS names that resolve to the same IP address cannot be distinguished. In this case, the first rule that references one of these DNS names will apply. That should not be a problem for large service providers. However, it could occur with small websites hosted by the same vendor.

Configuration

The settings for application-based routing and layer-7 application control are located under **Firewall/QoS** > **General** > **Application routing / Layer-7 application control**.

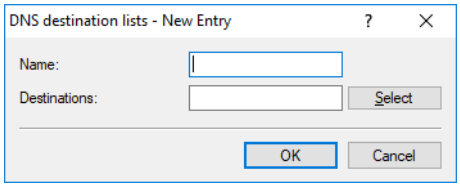


DNS destinations

In LANconfig, you specify the names and wildcard expressions for the DNS destinations that you want to treat separately in the firewall under **Configuration** > **Firewall/QoS** > **General** > **Application definitions** (also see *Application definitions for layer-7 detection and layer-7 application control* on page 662).

DNS destination list

In LANconfig, specify the DNS destinations that you want to reference as a single object in the firewall under **Firewall/QoS** > **General** > **Application-based routing** > **DNS destinations lists**.



Name

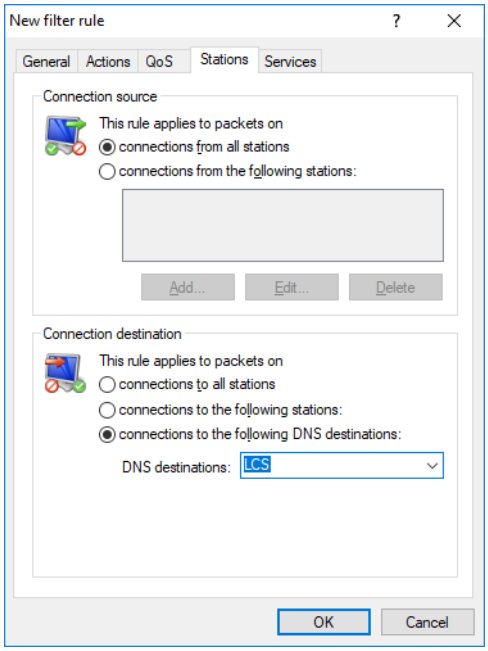
Name of the list of DNS destinations

Targets

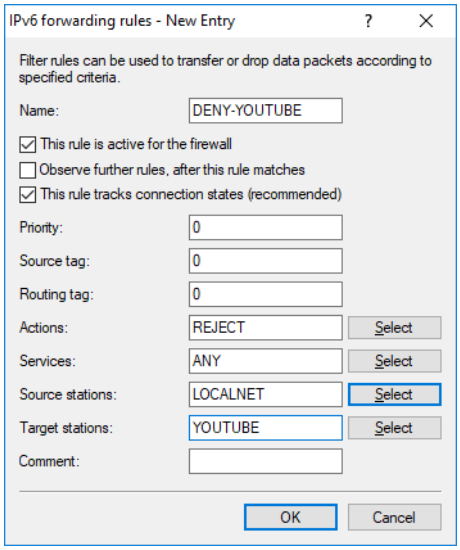
Contains a comma-separated or space-separated list of names of the DNS destinations.

Referencing in firewall rules

In **Firewall / Qos** > **IPv4-Rules** > **Rules** you can create a new filter rule and, then, go to the **Stations** tab and select from the configured DNS destinations under **connections to the following DNS destinations**.



You create a new rule under **Firewall/QoS** > **IPv6 rules** > **IPv6 forwarding rules**. **Target stations** can be selected from entries in the tables **DNS destinations** or **DNS destination lists**.



8.3.4 Parameters of the firewall rules

In this section, we describe the components of a firewall rule and the options available for setting the various parameters.

8.3.4.1 Components of a firewall rule

A firewall rule is first determined by its name and a few other options:

- **On/off switch**: Is the rule enabled?
- Observe further rules: Should further firewall rules be observed if this rule applies to a data packet? *Observe further rules* on page 667
- **Priority**: Which priority does the rule have? *Priority* on page 666
- **Source tag**: Using a source tag you add the source network where the device applies the firewall rule to the routing tag. Enter the source tag in order to uniquely specify the relationship between the source and destination hosts in ARF contexts: The device only forwards data packets to an ARF network when they originate from hosts in an ARF network with the specified source tag.
- **Routing tag**: By using the routing tag, additional information obtained via the destination IP addresses, such as the service or protocol used, can be used to select the destination route. The policy-based routing implemented in this way is used to achieve a significantly finer-grained routing behavior.

  The routing tag 0 means 'do not mark'. If the device is to route data packets to a network tagged with 0, please enter 65535 here.

8.3.4.2 Priority

When the device uses the firewall rules to generate the filter list, the entries are sorted automatically. The "degree of detail" is considered here: The first rules to be processed are those that have been specified, followed by the general ones (e.g. deny-all).

If the automatic sorting does not produce the desired behavior from the firewall, the priority can be modified manually. The higher the priority of the firewall rule, the higher the corresponding filter is placed in the filter list.

For complex rule sets, check the filter list as described in the section *Firewall diagnosis* on page 682.

8.3.4.3 Observe further rules

Some requirements of the firewall cannot be achieved by a single rule alone. If the firewall is used to limit the Internet traffic of different departments (each in their own IP subnet), no individual rule is able to simultaneously reproduce the common upper limit. For example, if each of the three departments has a maximum bandwidth of 512 kbps, but the total data rate of the three departments together cannot exceed a limit of 1024 kbps, then a multi-level check of the data packets must be established:

- The first stage checks that the current data rate of each individual department does not exceed the limit of 512 kbps.
- The second stage checks that the data rate of all the departments together does not exceed the limit of 1024 kbps.

Normally the list of firewall rules is applied sequentially to a received data packet. If one of the rules applies, the corresponding action is executed. This completes the firewall check; no further rules are applied to the packet.

To achieve two-stage or multi-level checks on data packets, the "Observe further rules" option is activated for the rules. If a firewall rule with the "Observer further rules" option enabled applies to a data packet, the corresponding action is executed first and then the firewall inspection is continued. If one of the other rules also applies to this packet, the action that corresponds to this rule is also executed. If the "Observer further rules" option is also enabled for this subsequent rule, the inspection continues until

- either a rule with the "Observer further rules" option not enabled applies to the packet
- or the list of firewall rules is processed completely and no further rules apply to the packet.

To implement the aforementioned scenario, a firewall rule is set up for each subnet to drop additional packets of the FTP and HTTP protocols from a data rate of 512 kbps and upwards. For these rules, the "Observer further rules" option is enabled. An additional rule is set up for all stations in the LAN to drop all packets exceeding 1024 kbps.

8.3.4.4 Application of the firewall rules

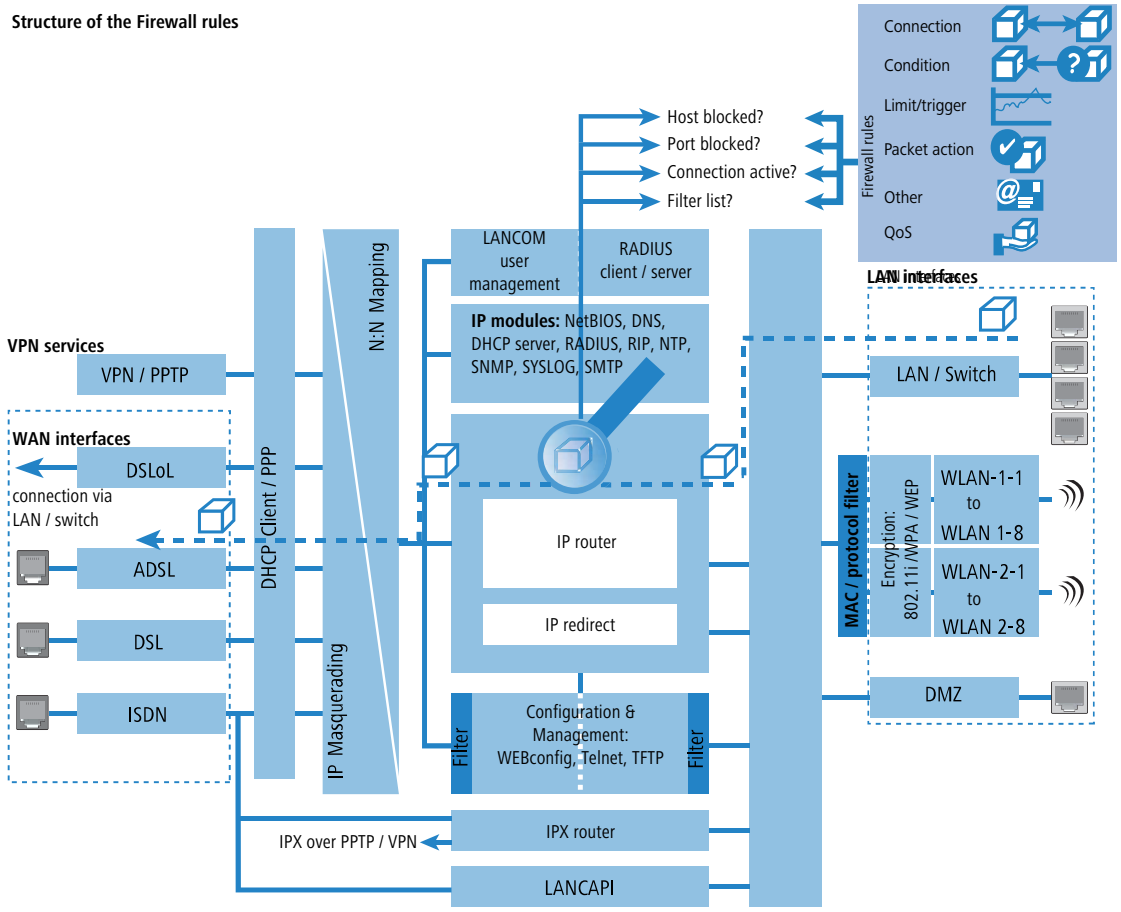
In addition to this basic information, a firewall rule answers questions such as when and to what it is to be applied, and what actions should be executed, if any:

- Connection: Which stations/networks and services/protocols does the rule refer to? *Connection* on page 668
- Conditions: Is the effectiveness of the rule restricted by other conditions? *Condition* on page 669
- Trigger: When reaching which thresholds should the rule trigger? *Limit (trigger)* on page 669
- Packet action: What should happen to the data packets when the condition is met and the threshold is reached? *Packet action* on page 669
- Further measures: Should other measures be initiated in addition to the packet action? *Further measures* on page 669
- Quality of Service (QoS): Are data packets for particular applications or with the corresponding markings given preferential treatment by Quality of Service? *Quality of Service (QoS)* on page 670



Condition, trigger, packet action, and further measures are collectively known as the "action set". Each firewall rule can contain several action sets. If the same trigger is used for several action sets, the order of the action sets can be adjusted.

In the section *How the firewall inspects data packets* on page 656 we have already shown that the lists for checking the data packets are ultimately formed from the firewall rules. The block diagram in further detail appears as follows:



8.3.4.5 Connection

The connection in the firewall rule specifies which data packets the rule refers to. A connection is defined by the source, the destination and the service used. The following details are used to specify the source or destination:

- All stations
- The entire local area network (LAN)
- Certain remote sites (designated by the name in the list of remote sites)
- Certain stations in the LAN (designated by the host name)
- Certain MAC address

> MAC stands for Media Access Control and is the linchpin for communications on a LAN. Every network adapter has its own MAC address. MAC addresses are unique and distinctive worldwide, similar to device serial numbers. Using the MAC addresses, the PCs in the LAN can be specifically granted or denied rights at the IP packet level. Network devices are often labeled with their MAC addresses in hexadecimal notation (for example, 00:A0:57:01:02:03).

- Ranges of IP addresses
- Complete IP networks
- DNS destinations for application-based routing

Host names can only be used if the device can resolve the names into IP addresses. To this end, the device must have learned the names via DHCP, or the assignment must be entered statically in the DNS or IP routing table. An entry in the IP routing table can therefore assign a host name to a whole network.

If the source or the destination for a firewall rule has not been specified, the rule applies in general to data packets “from all stations” or “to all stations”.

The service is determined by combining an IP protocol with the corresponding source and/or destination ports. For frequently used services (WWW, e-mail, etc.), the necessary combinations are predefined in the device, and others can be created as required.

8.3.4.6 Condition

Additional conditions can be used to restrict the effectiveness of a firewall rule. The following conditions are available:

- Only for packets with certain ToS and/or DiffServ markings
- Only if not connected
- Only for the default route (Internet)
- Only for VPN routes

8.3.4.7 Limit (trigger)

The limit (or trigger) denotes a quantified threshold that must be exceeded on the defined connection before the filter action is executed for a data packet. A limit is made up of the following parameters:

- Unit (kbit, kbyte or packets)
- Amount, i.e. data rate or number
- Reference value (per second, per minute, per hour or absolute)

Additionally, you can determine whether the limit relates to a logical connection or to all of the various connections existing between the specified destination and source stations and using the corresponding services. This controls whether the filter applies when the sum of all user HTTP connections in the LAN exceed the limit, for example, or whether it is sufficient for just one of the parallel established HTTP connections to exceed the threshold value.

For absolute values, you can also define whether the relevant counter should be reset to zero when the limit has been reached.

Data is always transferred until the limit is reached. With a trigger value of “0” a rule is activated immediately when data packets arrive for transmission over the specified connection.

8.3.4.8 Packet action

The firewall has three ways to handle a filtered packet:

- **Transmit**: The packet is transmitted normally.
- **Drop**: The packet is dropped silently.
- **Reject**: The packet is rejected and the recipient is sent a corresponding message via ICMP.

8.3.4.9 Further measures

The firewall is not only used to drop or accept filtered data packets. It can also take further measures once a data packet has been inspected by the filter. The measures are divided into two functions: “Logging/Notification” and “Prevention of further attacks”:

- Send SYSLOG message: Sends a message via the SYSLOG module to a SYSLOG client specified in the “Log & Trace” configuration section.
- Send e-mail message: Sends an e-mail message to the administrator specified in the “Log & Trace” configuration section.
- Send SNMP: Sends an SNMP trap for processing by LANmonitor, for example.

  Each of these three messaging actions automatically results in an entry in the firewall event log.

- Disconnect: Cuts the connection from which the filtered packet was received.

This cuts the physical connection, i.e. the Internet connection, and not just the logical connection between the two computers!

- Lock source address: Blocks the IP address where the filtered packet was received from, for an adjustable time.
- Lock target port: Blocks the destination port to which the filtered packet was sent, for an adjustable time.

8.3.4.10 Quality of Service (QoS)

In addition to restricting the transmission of data packets, the firewall can also grant "special treatment" for certain applications. The QoS settings use the firewall to assign data packets to specific connections or services.

8.3.5 Alert functions of the firewall

This section contains detailed descriptions of the messages sent by the firewall during security-related events. The following message types are available:

- E-mail notification
- SYSLOG report
- SNMP trap

Alerts are triggered either by the intrusion detection system, the denial of service protection, or by freely adjustable actions in the firewall. You can specify the specific parameters for the different types of notification (e.g. the e-mail account to be used) in the following places:

LANconfig: **Log & Trace** > **SMTP account** and **Log & Trace** > **System events**

Command line: **Setup** > **Mail** and **Setup** > **SYSLOG**

An example:

Let us assume a filter named 'BLOCKHTTP' is defined to block access to an HTTP server (192.168.200.10). In the event that someone attempts to access this server anyway, all traffic to and from that computer is blocked and the administrator is alerted via SYSLOG.

8.3.5.1 SYSLOG notifications

When the port filter firewall drops a packet, SYSLOG displays a message, such as:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
```

The ports are output for ported protocols only. Furthermore, computer names are output when they can be directly resolved by the device (i.e. without a DNS request).

If the SYSLOG flag is set for a filter entry (`%s` action), this notification becomes more detailed. In this case the name of the filter, the exceeded limit, and the executed filter actions are also output. For the example above, the notification might look like this:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port filter
PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

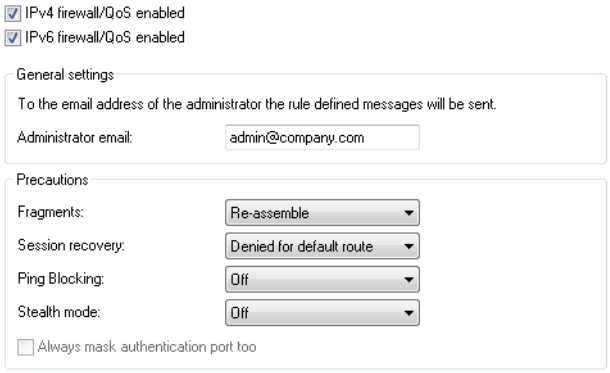
8.3.5.2 Notification by e-mail

If the e-mail system on the device is enabled, you can use the convenient e-mail notification. As soon as the firewall action is performed, the device sends an e-mail to the administrator in the following form:

```
FROM: device@company.com
TO: admin@company.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46
The packet below
Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)
45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....
```

```
matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a connection
because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

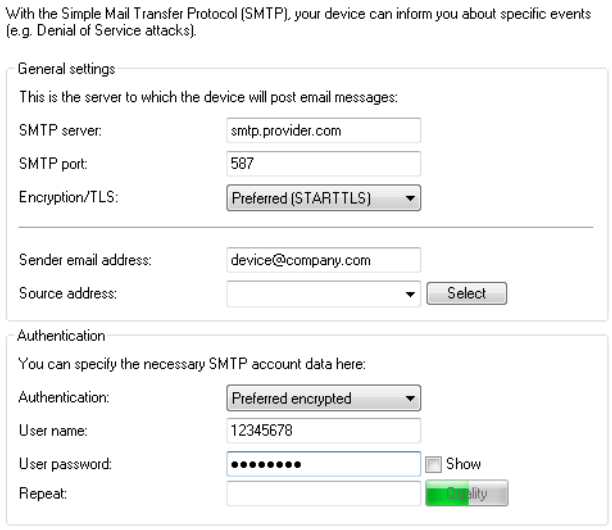
Sending e-mail from the device to the administrator only works if the correct e-mail address is entered.



LANconfig: **Firewall/QoS** > **General**

Command line: **Setup** > **IP-Router** > **Firewall**

In addition, a mailbox must be set up in order to send e-mail.



LANconfig: **Log & Trace** > **SMTP account**

Command line: **Setup** > **SMTP** > **Firewall**

8.3.5.3 Notification by SNMP trap

If sending SNMP traps is the selected notification method, then the first line of the logging table is sent as enterprise-specific trap 26. This trap additionally contains the system descriptor and the system name from the MIB-2.

For the example, an SNMP trap is generated with the following information:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
```

```
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

› System descriptor:

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.
SNMP: String Value = LANCOM Business 6021 2.80.0001 / 23.09.2002 8699.000.036
```

› Device string:

```
SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name
SNMP: String Value = LANCOM Business 6021
```

› Time stamp:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
```

› Source address:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
```

› Destination address

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
```

› Protocol (6 = TCP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

› Source port

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.
SNMP: Integer Value = 4353 (0x1101)
```

› Destination port (80 = HTTP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.
SNMP: Integer Value = 80 (0x50)
```

› Name of the filter rule:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.
SNMP: String Value = BLOCKHTTP
```



This trap and all other traps generated in the device are sent to all manually configured trap receivers and to any authenticated LANmonitor, which can evaluate this and possibly all other traps.

8.3.6 Strategies for configuring the firewall

Firewalls form the interfaces between networks and, to a greater or lesser extent, they restrict the unhindered exchange of data. The purpose of a firewall is thus diametrically opposed to that of the network to which it belongs: Networks are supposed to connect computers, firewalls aim to prevent connections.

This contradiction indicates the dilemma of the responsible administrators who, as a result, have developed various strategies as a solution.

8.3.6.1 Allow all

The allow-all strategy prioritizes the unobstructed communication between network users over security. It basically allows any communication, and the LAN is open to attackers. The LAN only becomes more secure when the administrator successively configures new rules that restrict or prevent elements of the communication.

8.3.6.2 Deny all

The deny-all strategy starts with a "block everything" approach with the firewall blocking all communication between the network and the rest of the world. As a second step the administrator then opens up address ranges or ports that are required for day-to-day communication with the Internet, etc.

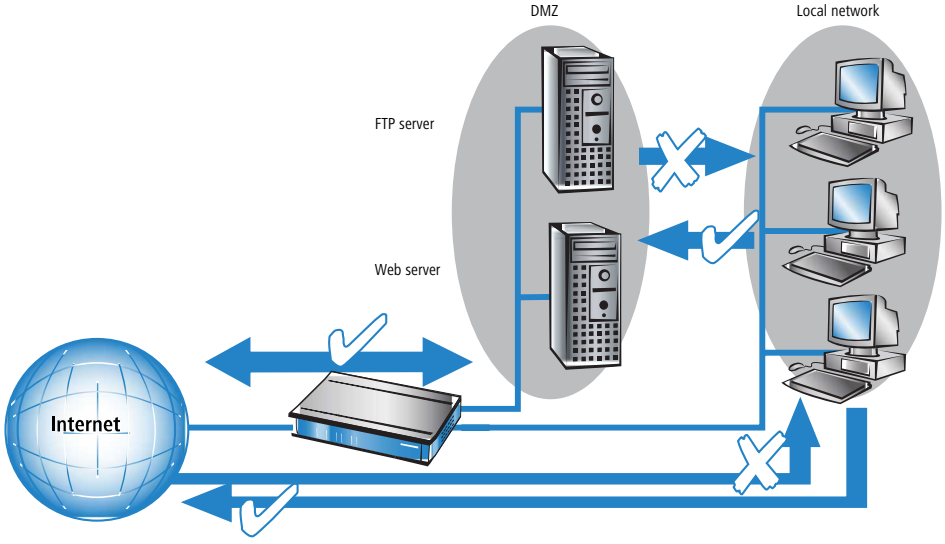
This approach is better for the security of the LAN than the allow-all strategy but often leads to difficulties for users in the initial phase. Some things may simply not work in the same way after the deny-all firewall is activated and some computers may not be reachable, etc.

8.3.6.3 Firewall with DMZ

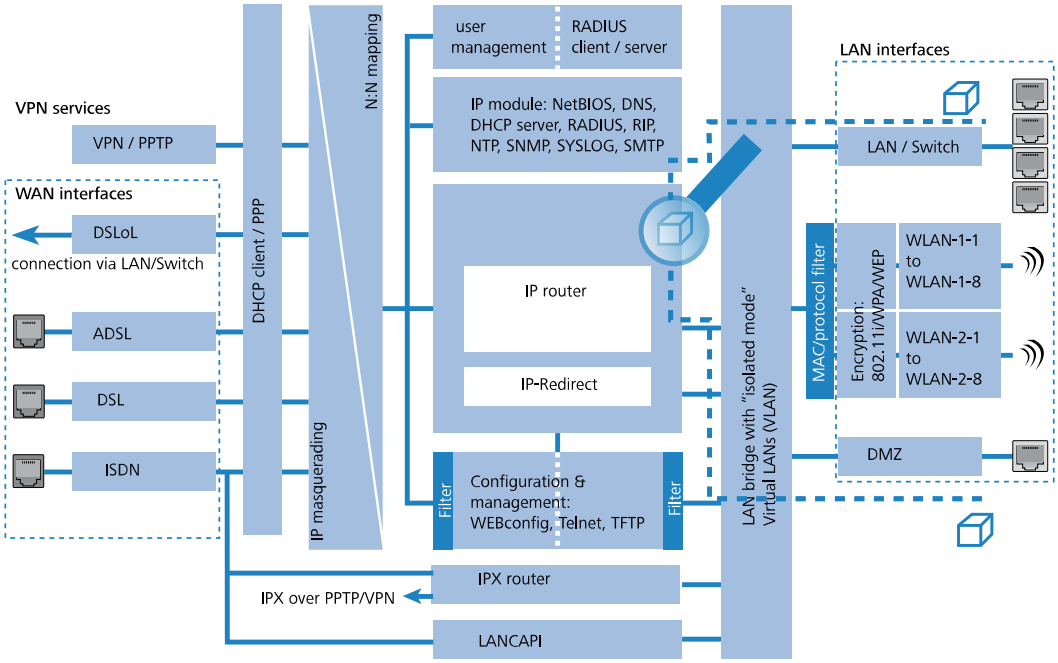
The demilitarized zone (DMZ) represents a special area of the local area network, which is shielded by a firewall both from the Internet and from the LAN itself. Computers or servers that should be accessible from the unsecured network (Internet) should be placed into this network. These include, for example, your own FTP and Web servers.

First and foremost, the firewall protects the DMZ against attacks from the Internet. Additionally, the firewall also protects the LAN against the DMZ. The firewall is configured so that only the following accesses are possible:

- Stations from the Internet can access the servers in the DMZ, but access to the LAN from the Internet is not possible.
- The stations on the LAN can access the Internet and the servers in the DMZ.
- The servers in the DMZ cannot access the stations in the LAN. This ensures that even a “cracked” server in the DMZ does not pose a security risk for the LAN.



Some router models support this setup by means of a separate LAN interface used only for the DMZ. Looking at the data path through the device, the function of the firewall for shielding the LAN from the DMZ becomes clear.



The direct data exchange between LAN and DMZ is not possible via the LAN bridge if a dedicated DMZ port is used. The path from the LAN to the DMZ and vice versa is therefore only through the router, and thus through the firewall. This in turn shields the LAN against requests from the DMZ as well as against the Internet.

For many network structures, shielding the DMZ against the Internet on the one hand and the LAN on the other requires the use of two separate firewalls. When using a device with a DMZ port, only one device is needed for this configuration, which has the advantage of a much simplified configuration.

8.3.7 Tips for setting the firewall

The firewall in the device is an extremely versatile and powerful tool. To help you to create custom firewall rules, here are some tips for finding the best settings for your specific application.

For devices with VoIP functions that were already integrated or added in with a software option, the ports required for voice connections are activated automatically.

8.3.7.1 Default firewall settings

Ex-factory there is just one entry in the firewall rule table, the "WINS rule". This rule prevents unwanted connections over the default route (usually to the Internet) by means of the NetBIOS protocol. Windows networks send requests to the network at regular intervals to find out if the known stations are still available. In combination with time-based billing of a network connection, this results in unwanted connection being setup.

8.3.7.2 Security through NAT and stateful inspection

If no other firewall rule is entered, the local network is protected by the interaction of network address translation and stateful inspection: Only connections from the local network generate an entry in the NAT table, whereupon the device opens a communication port. Communication over this port is monitored by stateful inspection: Only packets belonging to this connection may be communicated over this port. Attempts to access the local network from outside are met with an implicit deny-all strategy.

If you operate a server on your LAN that is made accessible from the Internet by means of entries in the service table, then stations from the Internet can establish connections to this server from the outside. In this case, inverse masquerading takes precedence over the firewall unless an explicit deny-all rule has been set up.

Transferring firewall rules with scripts

Firewall rules can be easily and conveniently transferred via scripts across device and software versions. Explicit example scripts can be found in the LANCOM Knowledge Base.

8.3.7.3 Establishing an explicit “deny-all” strategy

In order to achieve the maximum degree of security and control over data traffic, we recommend that you initially block all data transfers through the firewall. Subsequently, only those functions and communication paths that are really required are selectively activated. This provides protection for example from so-called 'Trojan horses' or e-mail viruses that actively establish an outgoing connection via certain ports.

The “deny-all” rule is by far the most important rule for the protection of your LAN. With this rule the firewall acts in accordance with the following principle: “Anything not explicitly allowed is forbidden.” This is the only strategy with which the administrator can be really sure that no possibility of access has been overseen—only those points of access that have been explicitly allowed are available.

We recommend that you set the deny-all rule before attaching the LAN to the Internet via a device. You can then use the logging table (that can be launched from LANmonitor) to easily see which connections have been blocked by the firewall. Using this information you can then successively add “allow-rules” to the firewall.

Some typical applications are shown below.

The filters described here are easily set up with the Firewall Wizard. If necessary, they can be further refined with LANconfig, for example.

› Sample configuration “Basic Internet”

Rule name	Source	Destination	Action	Service (target port)
ALLOW_HTTP	Local network	All stations	Transmit	HTTP, HTTPS
ALLOW_FTP	Local network	All stations	Transmit	FTP
ALLOW_EMAIL	Local network	All stations	Transmit	MAIL, NEWS
ALLOW_DNS_FORWARDING	Local network	Router IP address (option: Local network)	Transmit	DNS
DENY_ALL	All stations	All stations	Reject	ANY

› If you want to allow VPN dial-in to a device as a VPN gateway, you need a firewall rule that allows incoming communication from the client to the local network:

Rule name	Source	Destination	Action	Service
ALLOW_VPN_DIAL_IN	Remote site name	Local network	Transmit	ANY

› In the situation where a VPN is not terminated by the device itself (e.g. VPN client in the local network, or the device is a firewall in front of an additional VPN gateway), then you also need to allow IPSec and/or PPTP (for the 'IPSec over PPTP' used by the LANCOM VPN client):

Rule name	Source	Destination	Action	Service (target port)
ALLOW_VPN	VPN client	VPN server	Transmit	IPSEC, PPTP

› For connectivity between networks, you also have to allow communications between the participating networks:

Rule name	Source	Destination	Action	Service
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	Transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	Transmit	ANY

› If you operate your own web server, you selectively allow access to the server:

Rule name	Source	Destination	Action	Service (target port)
ALLOW_WEBSERVER	ANY	Web server	Transmit	HTTP, HTTPS

› For diagnostic purposes, it is recommended that you enable the ICMP protocol (e.g. for the ping command):

Rule name	Source	Destination	Action	Service
ALLOW_PING	Local network	All stations	Transmit	ICMP

These rules can now be refined as required, for example by specifying minimum and maximum bandwidths for server access, or by the granular restriction to certain services, stations or remote sites.

When the filter list is set up, the device automatically sorts the firewall rules. The rules are sorted according to their level of detail. The first rules to be processed are the specific ones followed by the general ones (e.g. deny-all). For complex rule sets, check the filter list as described in the following section.

8.4 Configuring the firewall with LANconfig

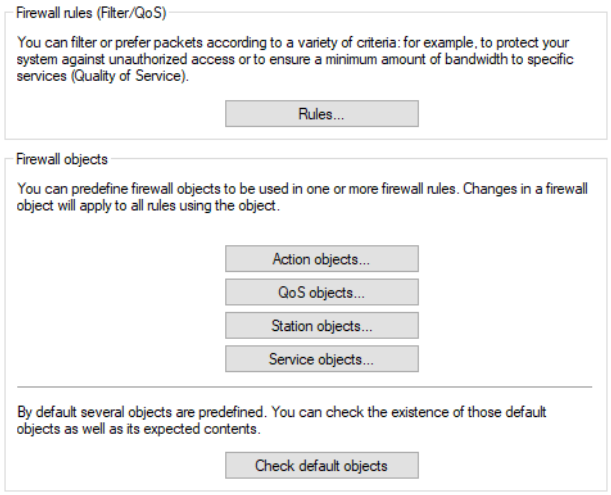
The corresponding configurations are located under **Firewall/QoS** > **IPv4 rules** and **Firewall/QoS** > **IPv6 rules** respectively.

8.4.1 Definition of firewall objects

When configuring the firewall with LANconfig, various objects can be defined that are used in the firewall rules. This means that frequently used definitions (such as a particular action) do not need to be re-entered for every rule. Instead they can be stored once at a central location.

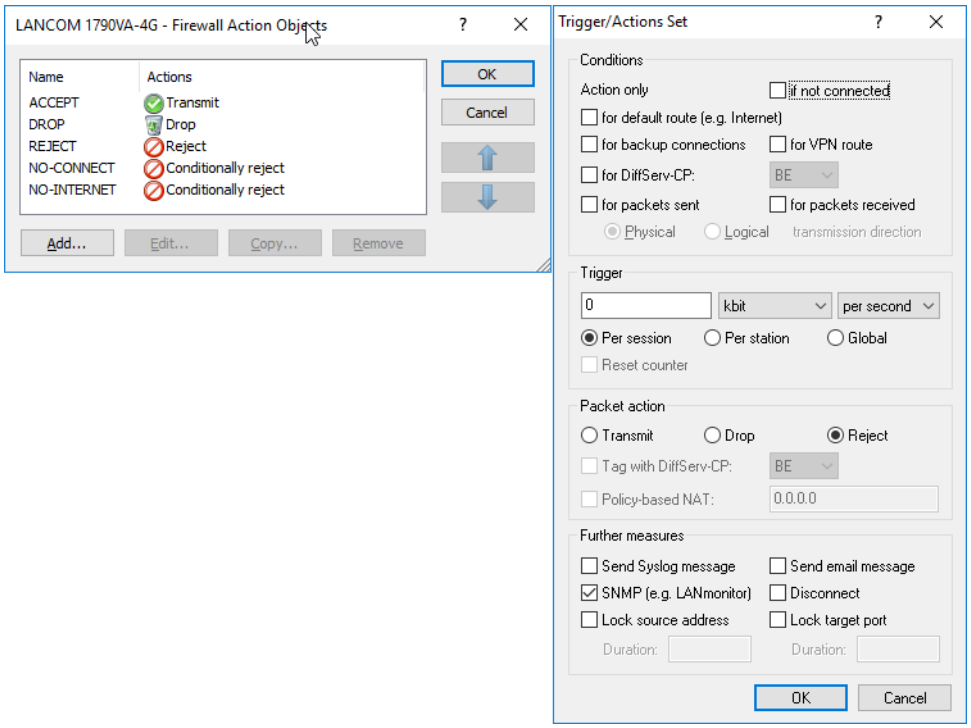
Please note that a change to firewall objects affects all of the firewall rules that use this object. For this reason, all firewall rules that also use these objects are displayed when you make changes to firewall objects.

Existing firewalls (in the % notation) are not automatically converted to the object-oriented form when the configuration is opened in LANconfig. The LANCOM Knowledge Base contains the pre-defined firewall settings used by the new objects.



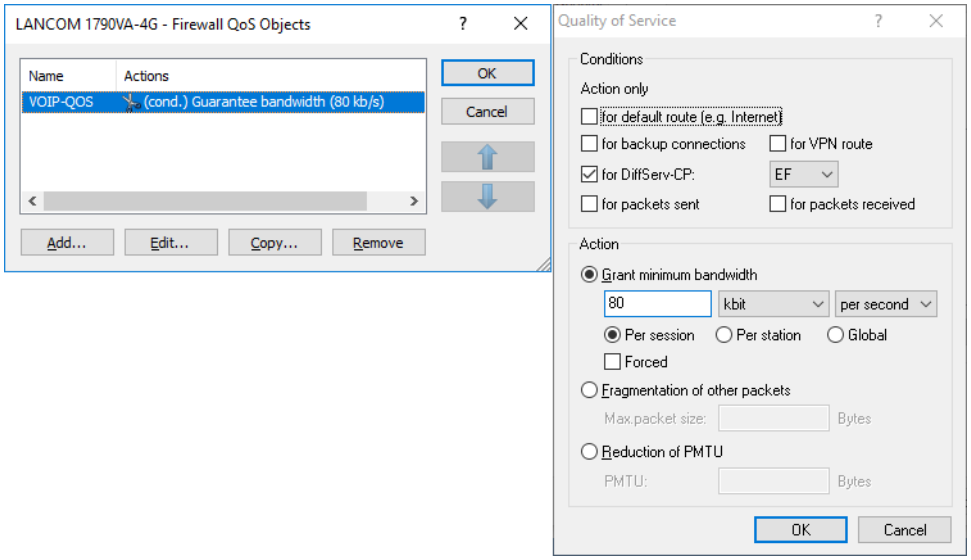
8.4.1.1 Action objects

Here you specify here the firewall action, which is comprised of condition, limit, packet action and other measures to be used by the firewall rules.



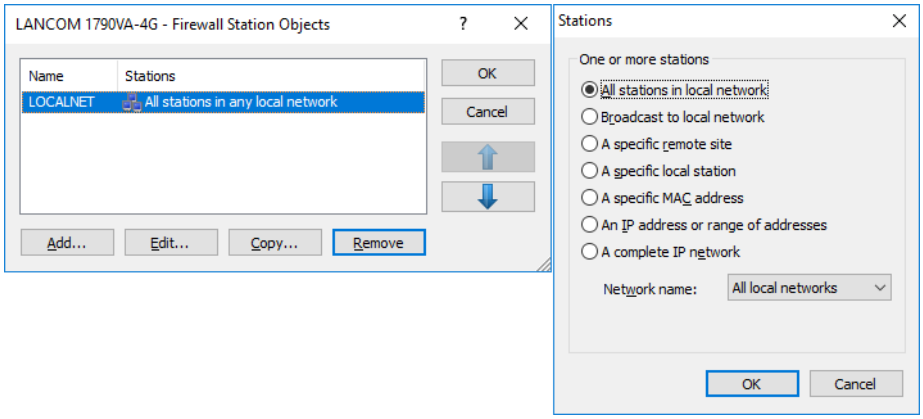
8.4.1.2 QoS objects

Here you set the minimum bandwidths that the firewall rules allocate to data packets.



8.4.1.3 Station objects

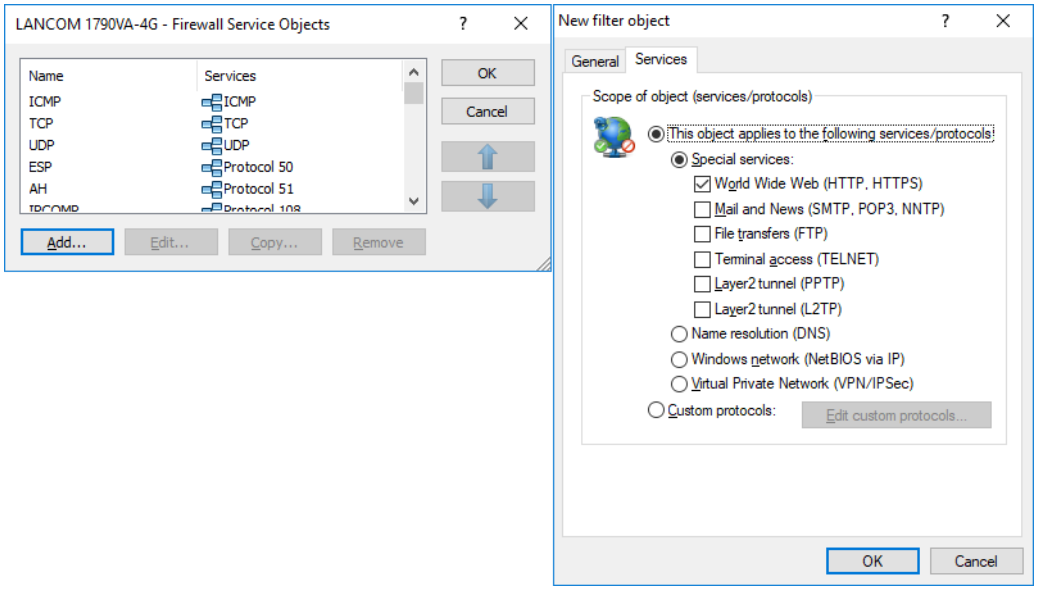
This is where the stations are defined that the firewall rules are to use as packet sender or addressee. The station objects are not restricted to any particular source or destination, but can be used as required by the firewall rules. In conjunction with ARF, for example, it is possible to define a specific IP network as a station object.



MAC addresses are not supported as destinations in a firewall rule.

8.4.1.4 Service objects

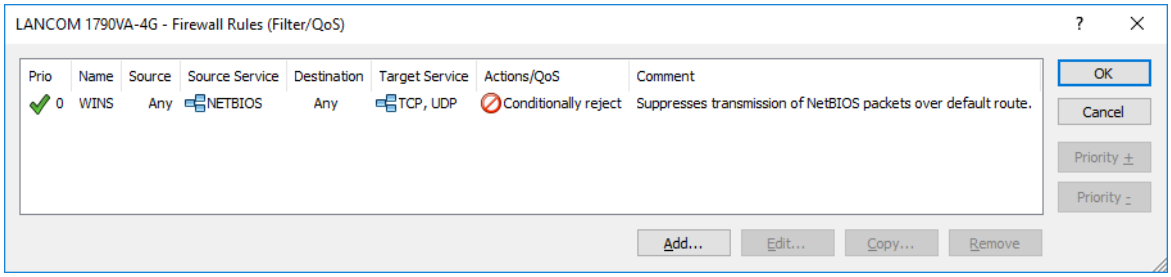
The IP protocols and the source/destination ports to be used by the firewall rules are defined here.



8.4.2 Defining firewall rules

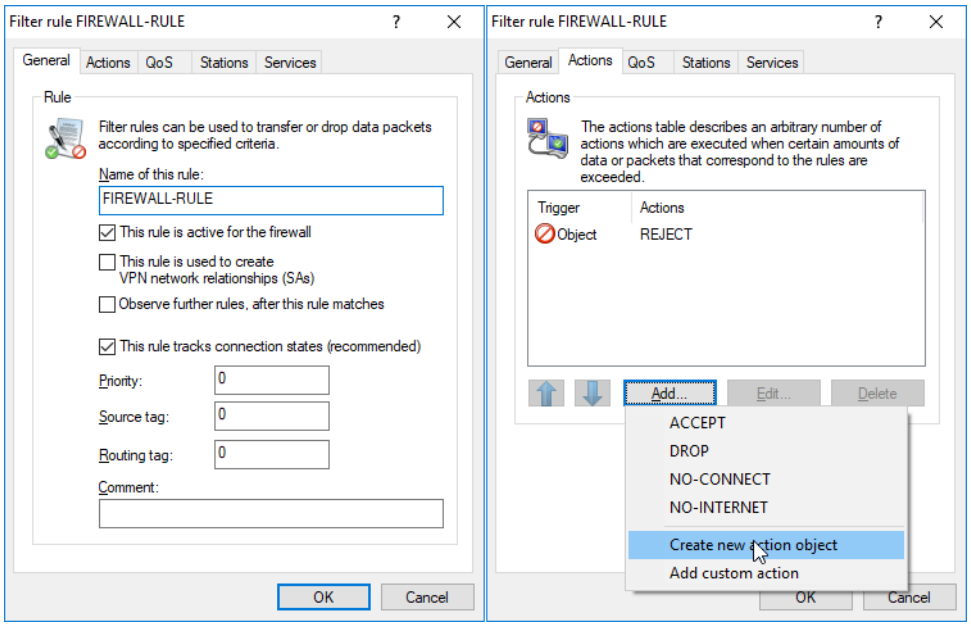
The firewall rules are shown in a clearly laid-out table containing the following information:

- In the left-most column, icons indicate the status of the firewall rule:
  - Green check-mark: Firewall rule is enabled.
  - Red cross: Firewall rule is disabled.
  - Lock: Firewall rule is used to create VPN rules manually.
  - Two interlinked arrows: If this firewall rule applies, consider other rules.
- Name of firewall rule
- Source
- Destination
- Source and destination service
- Action/QoS
- Comment



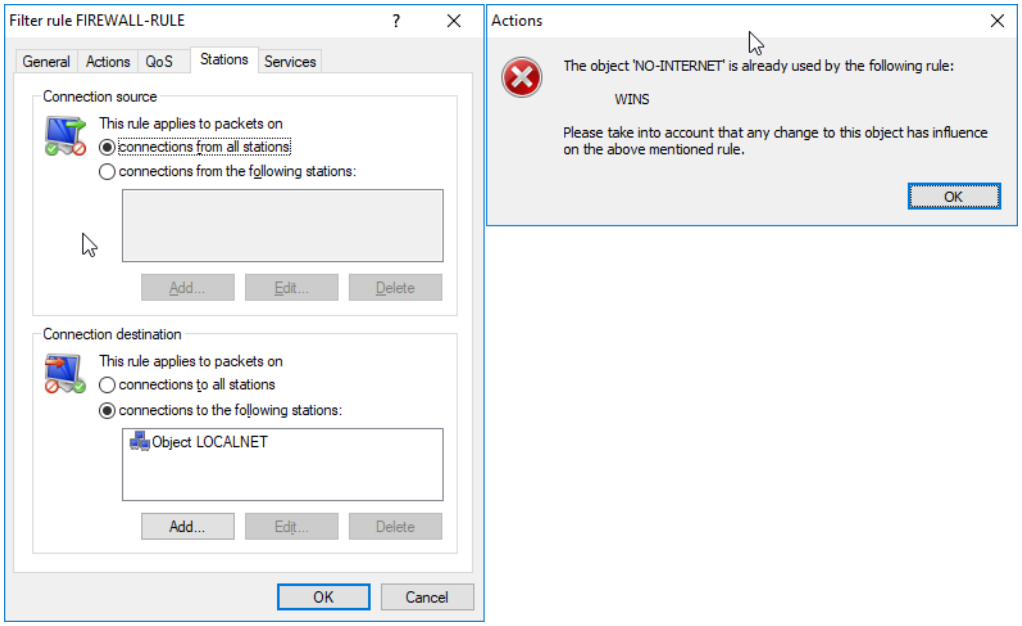
8.4.2.1 Adding a new firewall rule

When creating a new firewall rule, the general data is entered first. Objects already defined can be selected directly from the tabs for Actions, QoS, Stations and Services. New objects that can also be used in other rules can be created here, as can user-defined entries that are only to be used in the active firewall rule.



8.4.2.2 Editing firewall rules

When editing an existing firewall rule, the user is shown whether actions, QoS, stations or services have been added as pre-defined objects. A message is displayed if you try to edit a referenced object that is already used by another firewall.



8.5 Configuring firewall rules from the command line

8.5.1 Rules

Command line: **Setup** > **IP-Router** > **Firewall** > **Rules**

The rules table links various pieces of information on a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules, and activation of the rule for VPN connections.

The routing tag 0 means 'do not mark'. If the device is to route data packets to a network tagged with 0, please enter 65535 here.

The firewall is configured using objects. The % notation described as follows is only necessary for defining objects or actions.

Existing firewalls in the % notation are not automatically converted to the object-oriented form. However, the LANCOM Knowledge Base contains the pre-defined firewall settings used by the new objects.

Devices with firmware version 7.6 or later are automatically pre-defined with the main firewall objects. When processing older configurations with LANconfig, the firewall's standard objects are added automatically.

The firmware uses a special syntax to define firewall rules. This syntax enables the representation of complex interrelationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the firmware syntax every time:

- The firewall actions are stored in the action table
- The object table holds the stations and services

The objects from these tables can be used for rule definition, although this is not compulsory. They merely simplify the use of frequently used objects.

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate firmware syntax (e.g. %P6 for TCP).

For direct input of level parameters in the firmware syntax, the same rules apply as specified for protocols, source/destination and firewall actions.

8.5.2 Object table

Command line: **Setup** > **IP-Router** > **Firewall** > **Objects**

Elements/objects that are to be used in the firewall rules table are defined in the objects table. Objects can be:

- Individual computers (MAC or IP address, host name)
- Complete networks
- Protocols
- Services (ports or port areas, e.g. HTTP, Mail&News, FTP,…)

These elements can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for FTP (= TCP + ports 20 and 21), HTTP (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains all the definitions of the individual objects.

8.5.3 Action table

Command line: **Setup** > **IP-Router** > **Firewall** > **Actions**

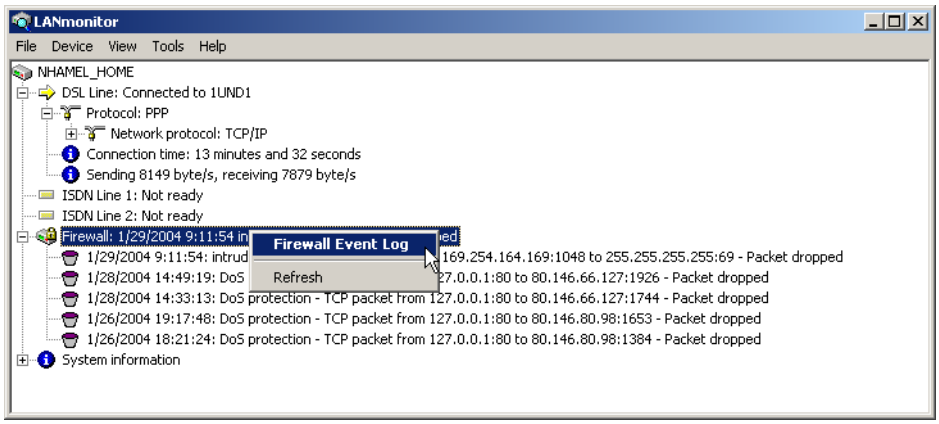
A firewall action comprises of a condition, a limit, a packet action and other measures.

As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

8.6 Firewall diagnosis

All events, states and connections of the firewall can be logged and monitored in detail.

The easiest way to inspect the log is to display the log table in LANmonitor (see below). In LANmonitor, the Firewall section displays the last five events triggered by a firewall rule, the DoS, or the IDS system with the SNMP option enabled.



With a right-click on this section, the context menu allows the log to be displayed in full by clicking on Firewall Event Log *The firewall table* on page 682.

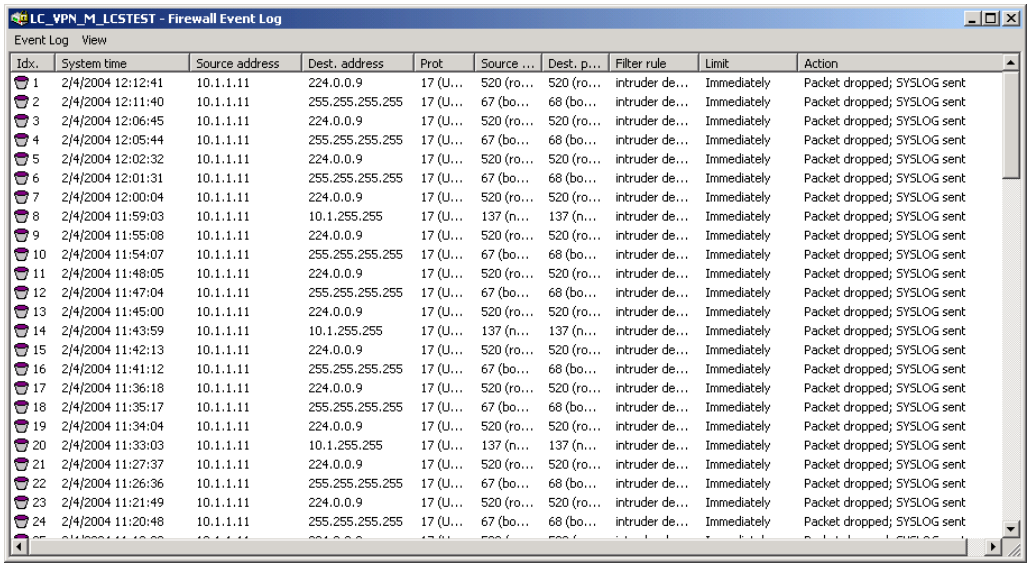
All of the lists and tables described in this section are to be found under the following menu items:

WEBconfig: **Extras** > **LCOS menu tree** > **Status** > **IP-Router-Statistics**

8.6.1 The firewall table

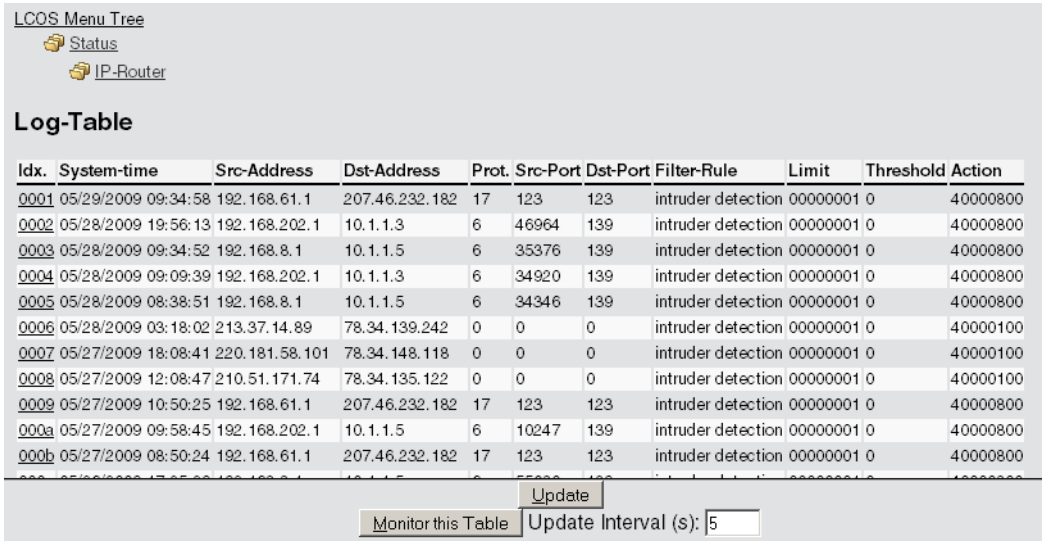
When a loggable event occurs, i.e. an action is taken when a packet is received, or a message is sent by e-mail, syslog or SNMP, this event is recorded in the log table.

Viewing the log table in LANmonitor appears as follows:



Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Action
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
3	2/4/2004 12:06:45	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
4	2/4/2004 12:05:44	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
5	2/4/2004 12:02:32	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
6	2/4/2004 12:01:31	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
7	2/4/2004 12:00:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
8	2/4/2004 11:59:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
9	2/4/2004 11:55:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
10	2/4/2004 11:54:07	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
11	2/4/2004 11:48:05	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
12	2/4/2004 11:47:04	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
13	2/4/2004 11:45:00	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
14	2/4/2004 11:43:59	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
15	2/4/2004 11:42:13	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
16	2/4/2004 11:41:12	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
17	2/4/2004 11:36:18	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
18	2/4/2004 11:35:17	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
19	2/4/2004 11:34:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
20	2/4/2004 11:33:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
21	2/4/2004 11:27:37	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
22	2/4/2004 11:26:36	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
23	2/4/2004 11:21:49	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
24	2/4/2004 11:20:48	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent

Viewing the log table in WEBconfig appears as follows:



Idx.	System-time	Src-Address	Dst-Address	Prot.	Src-Port	Dst-Port	Filter-Rule	Limit	Threshold	Action
0001	05/29/2009 09:34:58	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800
0002	05/28/2009 19:56:13	192.168.202.1	10.1.1.3	6	46964	139	intruder detection	00000001	0	40000800
0003	05/28/2009 09:34:52	192.168.8.1	10.1.1.5	6	35376	139	intruder detection	00000001	0	40000800
0004	05/28/2009 09:09:39	192.168.202.1	10.1.1.3	6	34920	139	intruder detection	00000001	0	40000800
0005	05/28/2009 08:38:51	192.168.8.1	10.1.1.5	6	34346	139	intruder detection	00000001	0	40000800
0006	05/28/2009 03:18:02	213.37.14.89	78.34.139.242	0	0	0	intruder detection	00000001	0	40000100
0007	05/27/2009 18:08:41	220.181.58.101	78.34.148.118	0	0	0	intruder detection	00000001	0	40000100
0008	05/27/2009 12:08:47	210.51.171.74	78.34.135.122	0	0	0	intruder detection	00000001	0	40000100
0009	05/27/2009 10:50:25	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800
000a	05/27/2009 09:58:45	192.168.202.1	10.1.1.5	6	10247	139	intruder detection	00000001	0	40000800
000b	05/27/2009 08:50:24	192.168.61.1	207.46.232.182	17	123	123	intruder detection	00000001	0	40000800

The table contains the following values:

Element	Meaning
Idx.	Sequential index (so that the table can also be polled via SNMP)
System time	System time in UTC encoding (converted to cleartext for display)
Source address	Source address of the filtered packet
Destination address	Destination address of the filtered packet
Prot.	Protocol (TCP, UDP, etc.) of the filtered packet
Source port	Source port of the filtered packet (only for port related protocols).
Destination port	Destination port of the filtered packet (only for port related protocols)
Filter rule	Name of the rule that created the entry.

Element	Meaning
Limit	Bit field describing the exceeded limit by which the packet was filtered. The following values are currently defined: › 0x01 Absolute number › 0x02 Number per second › 0x04 Number per minute › 0x08 Number per hour › 0X10 Global limit › 0x20 Byte limit (if not set, it is a packet limit) › 0x40 Limit only applies in the inbound direction › 0x80 Limit only applies in the outbound direction
Threshold	Threshold limit value of the triggering limit
Action	Bit field which lists all the actions performed. The following values are currently defined: › 0x00000001 Accept › 0x00000100 Reject › 0x00000200 Connect filter › 0x00000400 Internet (default router) filter › 0x00000800 Drop › 0x00001000 Disconnect › 0x00004000 Block source address › 0x00020000 Block destination address and port › 0x20000000 Send SYSLOG notification › 0x40000000 Send SNMP trap › 0x80000000 Send e-mail

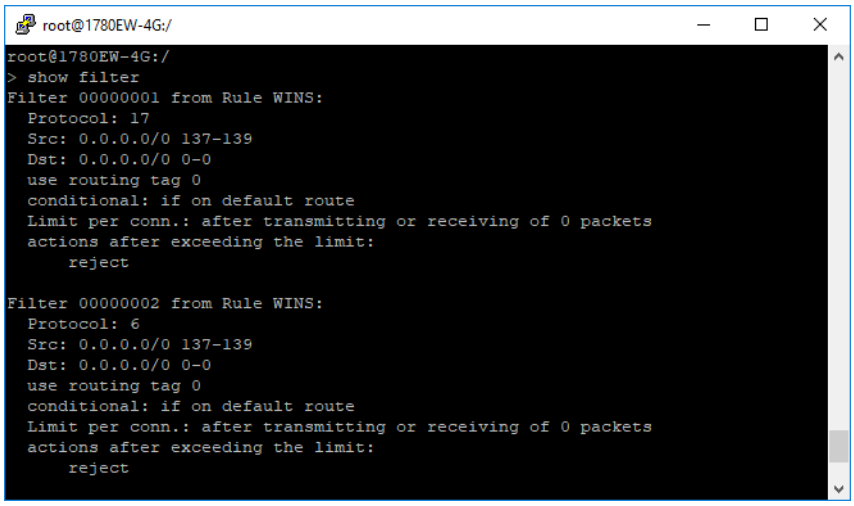
All firewall actions are also displayed in the IP router trace. Some models also have a firewall LED, which indicates each packet filtered.

8.6.1.1 Filter list

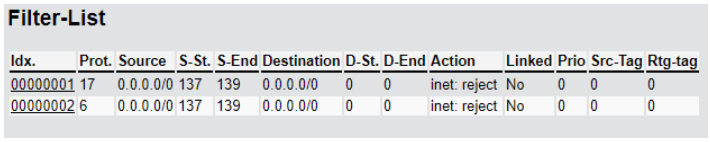
The filter list allows you to examine the filters that are generated from the rules specified in the action, object and rule tables.

If a filter is defined manually from the command line or in WEBconfig and there are errors in the syntax, no entry will be created in the filter list. In this case, no error message will be output. If you configure the filters manually, you should always use the filter list to check whether the desired filters have actually been created.

On the command line, the filters that have been configured are listed by using the command `show filter`:



Under WEBconfig, you invoke the filter list under **Extras** > **LCOS menu tree** > **Status** > **IP-Router** > **Filter-List**. It is structured as follows:



Filter-List

Idx.	Prot.	Source	S-St.	S-End	Destination	D-St.	D-End	Action	Linked	Prio	Src-Tag	Rtg-tag
00000001	17	0.0.0.0/0	137	139	0.0.0.0/0	0	0	inet: reject	No	0	0	0
00000002	6	0.0.0.0/0	137	139	0.0.0.0/0	0	0	inet: reject	No	0	0	0

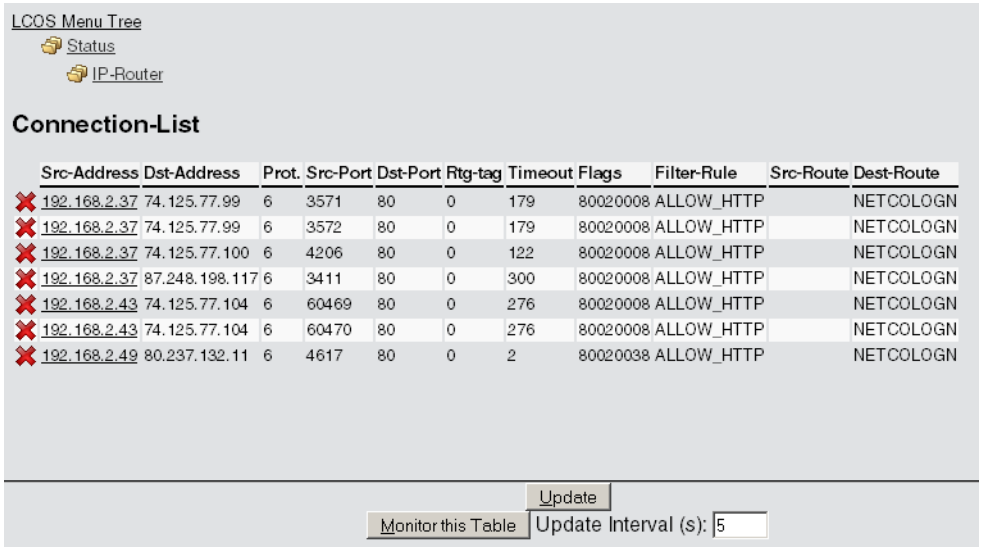
The individual fields in the filter list have the following meaning:

Entry	Description
Idx.	Sequential index
Prot.	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP
Source	This column displays either the MAC address or the network as an address with the prefix length.
Q start	Start source port of the packets to be filtered.
Q end	End source port of the packets to be filtered. Together with the start source port, this defines a port range in which the filter takes effect. If start and end port are 0, the filter applies to all source ports.
Destination	This column displays either the MAC address, the network as an address with the prefix length, or the DNS destination.
Z start	Start destination port of the packets to be filtered.
Z end	End destination port of the packets to be filtered. Together with the start destination port, this defines a port range in which the filter takes effect. If start and end port are 0, the filter applies to all destination ports.
Action	This column displays the “main action” as text, i.e. the action that is executed when the first limit is exceeded. The first limit can also be an implicit limit. For example, when throughput is limited by a single value only, an implicit limit is added that is linked with an “accept” action. The main action in this case is “accept”. Actions can be viewed in full with the command `show filter`.
Linked	Indicates whether this rule is a first match rule (linked = no). Only in the case of linked rules will further rules be evaluated if this rule applies.
Prio	Priority of the rule that created the entry.
Src-Tag	Original routing tag
Rtg-Tag	Assigned routing tag after the filter was applied.

8.6.1.2 Connection list

The connection list monitors the source address, destination address, protocol, source port, destination port, etc. of a connection, along with any actions that may be executed. This list is sorted by the source address, destination address, protocol, source port and destination port of the packet that caused the entry in the list.

Under WEBconfig the filter list is structured as follows:



The list contains the following elements:

Element	Meaning
Src address	Source address of the connection
Dst address	Destination address of the connection
Prot.	Protocol used (TCP/UDP, etc.), shown as a decimal
Src port	Source port of the connection. The port is only shown for port-related protocols (TCP/UDP) or protocols that have a comparable field (ICMP/GRE)
Dst port	Destination port of the connection (in the case of UDP connections, this contains the first answer only)
Timeout	Each entry ages out of this list over time, which prevents the list from overflowing with “dead” connections.
Flags	The flags are used to store information on the connection state and other (internal) information to a bit field. The states can have the following values: New, establish, open, closing, closed, rejected (corresponding to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST) UDP connections know the states, open and closing (the latter only if the UDP connection is linked by a stateful control channel.
Src route	Name of the remote site from which the first packet was received.
Dst route	Name of the remote site to which the first packet is sent.
Filter rule	Name of the rule that created the entry. It also determines the actions to take when a matching packet is received.

Meaning of the flags in the connection list

Flag	Meaning
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received

Flag	Meaning
00000004	TCP: Waiting for ACK from server
00000008	All: Connection open
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received
00000080	TCP: Session being restored
00000100	FTP: Passive FTP connection being established
00000400	H.323: Related T.120 connection
00000800	Connection via loopback interface
00001000	Checking linked rules
00002000	Rule is linked
00010000	Destination is on "local route"
00020000	Destination is on default route
00040000	Destination is on VPN route
00080000	No physical connection established
00100000	Source is on default route
00200000	Source is on VPN route
00800000	No route to destination
01000000	Contains global action with condition

8.6.1.3 Port block list

If the blocking of the destination port on the destination computer has been selected as the action, the address, protocol and port of the destination computer are stored in the port block list. This list is also a sorted semi-dynamic list. The list is sorted by address, protocol and port. The list contains the following elements:

Element	Meaning
Address	Address of the computer to be blocked.
Protocol	Protocol used (TCP/UDP, etc.), shown as a decimal.
Port	The port to be blocked on the computer. If the protocol is not port-related, then the entire protocol is blocked for this computer.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule that created the entry. It also determines the actions to take when a matching packet is received.

8.6.1.4 Host block list

If the action selected for a filter is to block the sender, then the address of the computer is stored in the host block list. This list is a semi-dynamic list sorted by sender address. It contains the following elements:

Element	Meaning
Address	Address of the blocked computer
Timeout	Duration of the blocking in minutes
Filter rule	Name of the rule that created the entry. It also determines the actions to take when a matching packet is received.

8.7 Firewall limitations

Apart from understanding how firewalls function, it is also very important to recognize their limitations and to supplement them if necessary. For example, the firewall provides no protection against malicious content entering the local network on the permitted routes. Although it is true to say that the effects of some viruses and worms are reduced because they cannot communicate via the required ports, the firewall by itself does not provide real protection against viruses.

Similarly, the interception to confidential data on the Internet cannot be prevented by the firewall. Data that has passed the firewall and reached the insecure network is exposed to the known dangers there. Even when using a firewall, confidential information such as contracts, passwords, development information, etc., should therefore only be transferred with suitable protection, such as by using suitable encryption methods or via VPN connections.

8.8 Protection against break-in attempts: Intrusion detection

The task of the firewall is to check the traffic crossing the boundaries between networks and to reject or drop packets that have no permission for transmission. Along with direct attacks on computers in protected networks, attacks can also be directed to the firewall itself, or attempts can be made to outwit the firewall with fake data packets.

These attempts are detected, repelled and logged by an intrusion detection system (IDS). There is a choice of alerts including in-device logging, e-mail messaging, SNMP traps or SYSLOG alarms. The IDS checks the traffic for certain properties and can detect new attacks from conspicuous patterns.

8.8.1 Examples of attempted break-ins

Typical break-in attempts include fake source addresses (IP spoofing) and port scans, as well as the misuse of special protocols such as FTP to open a port on the attacked computer and bypass the firewall in front of it.

8.8.1.1 IP spoofing

In IP spoofing, the sender of a packet pretends to be another computer. This is done either to outsmart firewalls that trust packets from their own network more than packets from untrusted networks, or to disguise the originator of an attack.

The device firewall protects against spoofing by route examination, i.e. whether a packet is allowed to be received at the interface where it arrived.

8.8.1.2 Port scan detection

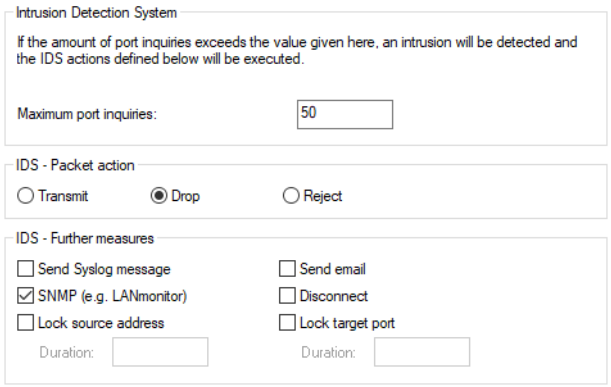
The intrusion detection system tries to detect port scans, to report them, and to react to the attack. This is similar to detecting a SYN flood attack (see *SYN flooding* on page 690): A count is kept of the number of "half-open" connections, whereby a TCP reset sent by the scanned computer leaves a "half-open" connection open again.

Once a certain number of half-open connections exists between the scanned and the scanned computer, this is reported as a port scan.

Similarly, the reception of empty UDP packets is interpreted as an attempted port scan.

8.8.2 Configuring the IDS

The settings for the IDS are located here.



LANconfig: **Firewall/QoS** > **IDS**

Command line: **Setup** > **IP-Router** > **Firewall**

Along with the maximum number of port requests, the packet action and the available reporting mechanisms, there are further reaction options:

- Disconnection
- The source address is blocked for an adjustable time
- The target port of the scan is blocked for an adjustable time

8.9 Protection against "Denial-of-Service" attacks

In addition to conventional break-ins, attacks from the Internet may aim to block the availability of individual services. These attacks are also called "Denial of Service" (DoS). The routers are equipped with appropriate security mechanisms to recognize popular hacker attacks and keep the router functioning.

Distributed Denial of Service (DDoS) is a special case of DoS in which the attacks are launched from a large number of computers. originates. This special case is also covered by this protection mechanism.

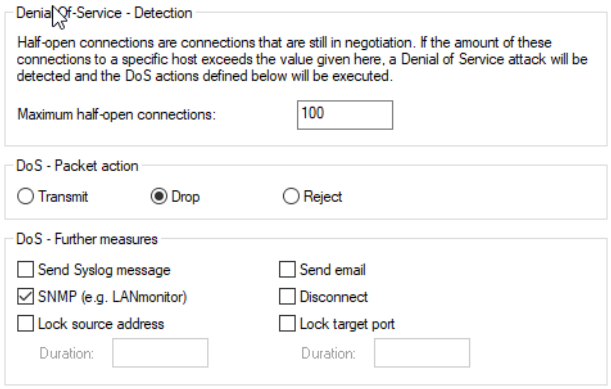
8.9.1 Increased DoS threshold value for central devices

Denial-of-Service attacks take advantage of inherent weaknesses in the TCP/IP protocol in combination with poor implementations.

- Attacks which target these inherent weaknesses include SYN Flood and Smurf.
- Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land).

Your device detects most of these attacks and reacts with appropriate countermeasures. Detecting these attacks relies on counting the number of connections which are concurrently under negotiation (half-open connections). If the number of half-open connections exceeds a certain threshold value, then the device assumes that a DoS attack is underway. The actions and measures which are taken in this case can be defined, similar to firewall rules.

Central devices are connected to a large number of users, so it is possible for a large number of half-open connections to exist without being caused by a DoS attack. For this reason, a higher default threshold value is required for the accurate detection of DoS attacks.



LANconfig: **Firewall/QoS** > **DoS**

Command line: **Setup** > **IP-Router** > **Firewall**

› **Maximum half-open connections**

Specifies the number of half-open connections which triggers DoS-attack countermeasures.

Possible values:

› 0 to 9999

Default:

› 100
› 1000 for central devices

8.9.2 Examples of Denial-of-Service attacks

Denial-of-Service attacks exploit the inherent weaknesses in the TCP/IP protocol and poor implementations of the TCP/IP protocol stack. Attacks which target these inherent weaknesses include SYN Flood and Smurf. Attacks which target erroneous implementations include those operating with erroneously fragmented packets (e.g. Teardrop) or with fake sender addresses (e.g. Land). A number of these attacks, their effects and possible countermeasures are described in the following.

8.9.2.1 SYN flooding

With SYN flooding, an attacker sends a rapid and continuous succession of TCP packets set with a SYN flag from constantly changing source ports to open ports of the victim. The computer under attack then sets up a TCP connection, returns a packet with set SYN and ACK flags to the attacker, and waits in vain for confirmation of the connection establishment. This results in hundreds of "half-open" TCP connections that consume resources (e.g. memory) on the computer under attack. This can result in the victim no longer being able to accept any further TCP connections, or it may even crash the machine due to a lack of memory.

As a countermeasure, the firewall monitors and limits the number of half-open TCP connections between two computers. Any further TCP connections being established between these computers are blocked by the firewall.

8.9.2.2 Smurf

The Smurf attack works in two stages and paralyzes two networks at once. In the first step a ping (ICMP echo request) packet with a fake sender address is sent to the broadcast address of the first network. Now all workstations in this network respond with an ICMP echo reply to the fake sender address, which is located in the second network. If the rate

of the incoming echo requests and the number of responding computers is high enough, the entire incoming traffic of the second network is blocked for the duration of the attack and, furthermore, the owner of the fake address is unable to accept normal data for this time. If the fake sender address is also the broadcast address of the second network, then all of the computers in this network are blocked as well.

In this case, DoS detection in the device blocks packets that are directed to the local broadcast address.

8.9.2.3 LAND

The LAND attack is a TCP packet that is sent to the target computer with a SYN flag set and a fake sender address. The tricky thing here is that the fake sender address is the same as the victim's address. If TCP has been implemented poorly, the victim interprets its own SYN-ACK response as a SYN request and sends yet another SYN-ACK. This leads to an infinite loop that causes the computer to freeze.

In a newer variant, the sender address of the packet is not the address of the attacked computer, but the loopback address 127.0.0.1. The purpose of this trick is to outsmart personal firewalls that respond to the classic variant (sender address = destination address), but which let the new form through unhindered. This form is also recognized and blocked by the device.

8.9.2.4 Ping of Death

The Ping of Death is an attack that exploits errors in the re-assembly of fragmented packets. This works as follows:

The IP header contains the fragment-offset field, which identifies where the received fragment is inserted into the assembled IP packet. This field is 13 bits long and specifies the point of insertion in 8-byte increments. The point of insertion can thus take on a value between 0 and 65528 bytes. With an MTU on the Ethernet of 1500 bytes, an IP packet can be generated with a potential size of up to 65528 + 1500 - 20 = 67008 bytes. This, however, would provoke internal counter overflows or even buffer overflows, which can give attackers a potential way to execute their own code on the victim computer.

The firewall provides two options here: Either the firewall re-assembles the entire incoming packet and checks its integrity, or else the fragment that exceeds the maximum packet size is discarded. In the first case, the firewall itself can become a victim of a faulty implementation. In the second case, the victim keeps collecting partially re-assembled packets and, since these are only discarded after a certain time, this could result in a new Denial-of-Service attack if the victim runs out of memory.

8.9.2.5 Teardrop

The teardrop attack works with overlapping fragments. In this case, an initial fragment is followed by a further fragment that apparently belongs entirely inside the first packet, i.e. the end of the second fragment is before the end of the first. Now, if the programmer of the IP stack took the easy option of calculating the number of bytes for re-assembly simply by using “new end” - “old end”, the result is either a negative value or a very large positive value. This causes parts of the victim machine's memory to be overwritten during copy operations, which leads to the computer crashing.

Here, too, the firewall has two options: Either it performs re-assembly itself and, if necessary, drops the entire packet, or it keeps track of the minimum offset and maximum end of the packet, and discards any fragments with an offset or end that falls within that range. The first case requires the correct implementation in the firewall so that it does not itself become a victim; in the second case, partially re-assembled packets are again collected by the victim.

8.9.2.6 Bonk / Fragrouter

Bonk is a variant of the Teardrop attack. However, it does not aim to crash the attacked computer, but instead it outsmarts simple port-filter firewalls, which also accept fragmented packets, and penetrates the network that requires protection. This attack uses carefully chosen fragment offsets to overwrite the UDP or TCP header of the first fragment. As a result, simple port-filter firewalls accept the first packet and the associated fragments. By overwriting the header in the second fragment, an apparently legitimate packet suddenly becomes a packet that should actually be blocked in the firewall.

Again, the firewall can either perform re-assembly itself, or it can filter out the erroneous fragment (and all subsequent ones) with the consequences outlined for the other solutions described above.

Ex-factory, all settings are configured to “secure”, i.e. a maximum of 100 half-open connections are allowed from different computers (see SYN flooding), a maximum of 50 half-open connections are allowed from a single computer (see Port scan), and fragmented packets are re-assembled.

8.9.3 Configuring DoS blocking

LANconfig: **Firewall/QoS** > **DoS**

Command line: **Setup** > **IP-Router** > **Firewall**

In order to drastically reduce the vulnerability of the network to DoS attacks, packets from remote networks should only be accepted if either a connection from the internal network was initiated or if the incoming packets are allowed through by an explicit filter entry (source: remote network, destination: local network). This measure already blocks a large number of attacks.

For all permitted accesses, the device explicitly checks the connection state, the source addresses, and the correctness of the fragments. This is performed both for incoming and outgoing packets, since an attack can also be launched from within the local network.

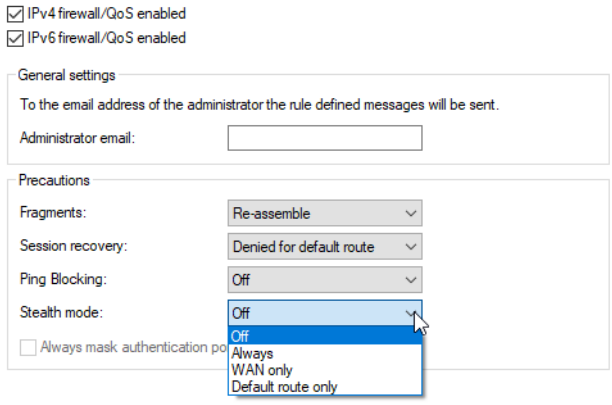
In order to avoid opening a path for DoS attacks due to the incorrect configuration of the firewall, this aspect is configured centrally. Along with the maximum number of half-open connections, the packet action and the available reporting mechanisms, there are further reaction options:

- Disconnection
- The source address is blocked for an adjustable time
- The target port of the scan is blocked for an adjustable time

The following protection mechanisms are always active:

- Address inspection (against IP spoofing)
- Blocking broadcasts into local network (against Smurf, etc.)

8.9.4 Configuring ping blocking and stealth mode



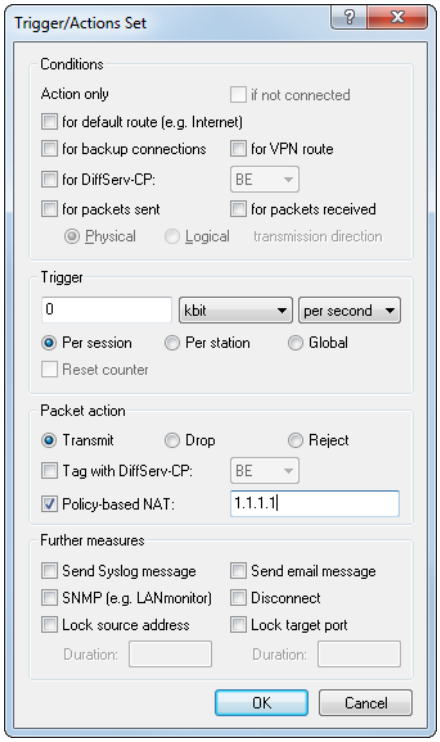
LANconfig: **Firewall/QoS** > **General**

Command line: **Setup** > **IP-Router** > **Firewall**

8.10 WAN policy-based NAT

WAN policy-based NAT allows address translation (masking) of connections based on firewall rules. You can now configure which of the WAN-IPv4 addresses assigned by the provider is to be used to mask internal addresses. This is ideal for scenarios where a provider assigns multiple static IPv4 addresses, e.g. for operating mail servers and web servers with different WAN addresses.

For this purpose, the firewall features the new packet option **Policy-based NAT** under **Firewall/QoS** > **IPv4 Rules** > **Action objects**. This action can be used together with the option **Transmit** and allows masking or NAT behind a specified IPv4 address.



The parameter must be entered as a fixed IP address. Dynamic IP addresses are not supported.

NAT is only possible if a WAN interface is involved. NAT between two LAN interfaces is not supported.

The CLI under (`/Setup/IP-Router/Firewall/Action-Table`) provides the variable `%Y` as an action.

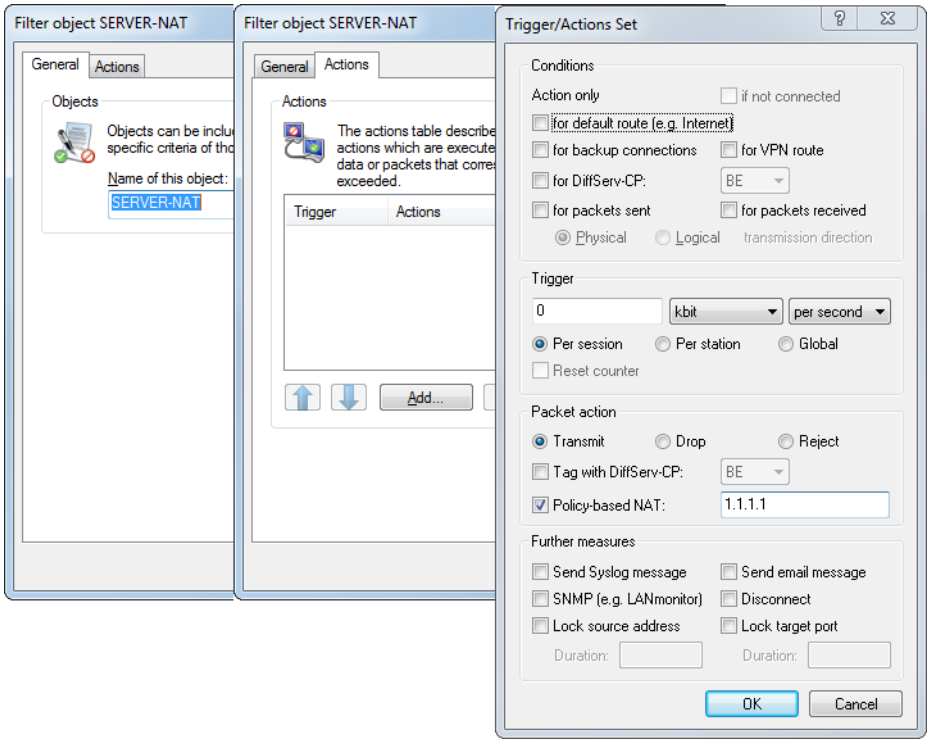
8.10.1 Configuring policy-based NAT with firewall rules

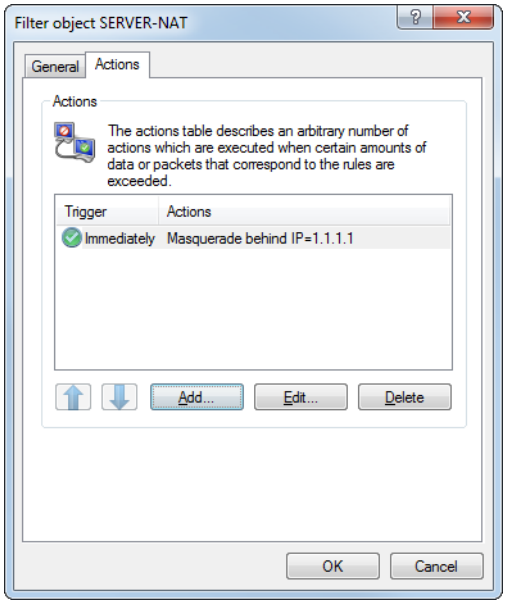
The following example configures an IPv4 network (intranet) with the subnet 192.168.80.0/24. The Internet provider has assigned a number of public IP addresses. Internet access has been set up using the Setup Wizard. Clients on the intranet are automatically masked behind the public IP address that was created with the Wizard.

Now we want to mask a server with the internal IP address 192.168.80.21 behind the public IP address 1.1.1.1.

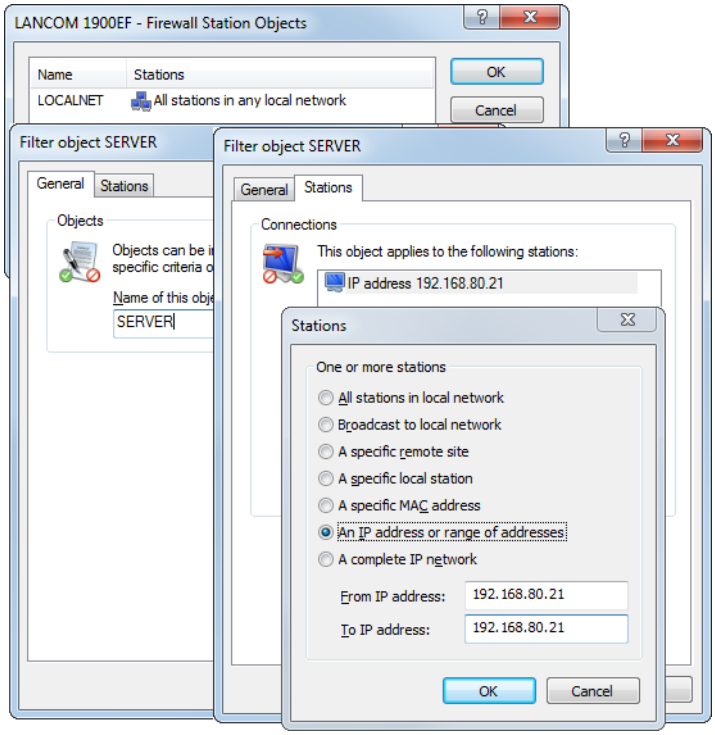
The "return direction" of the masking, i.e. the server's accessibility from the outside, is realized by a port-forwarding entry, which is not part of this example.

1. Create a new action object in the firewall under **Firewall/QoS** > **IPv4 rules** > **Action objects**. Under Action, set the packet action to **Transmit** and the **Policy-based NAT** to 1.1.1.1.

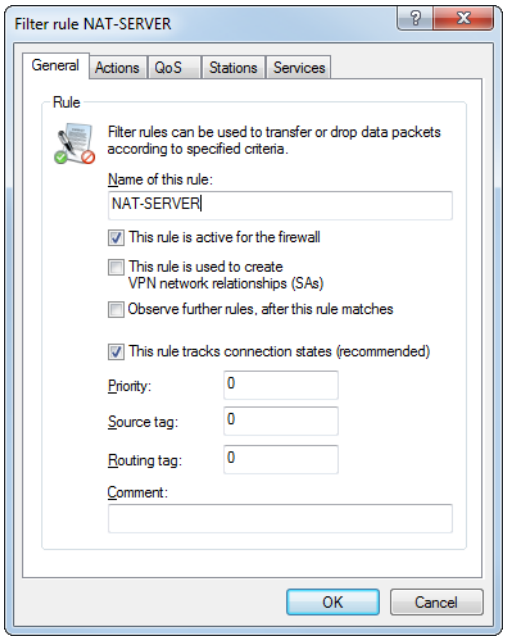




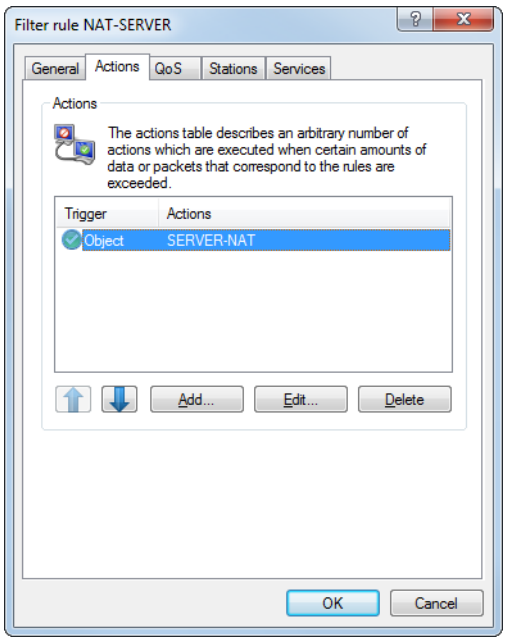
2. Under **Firewall/QoS** > **IPv4 rules** > **Station objects** create a new station object defined for the IP address 192.168.80.21.



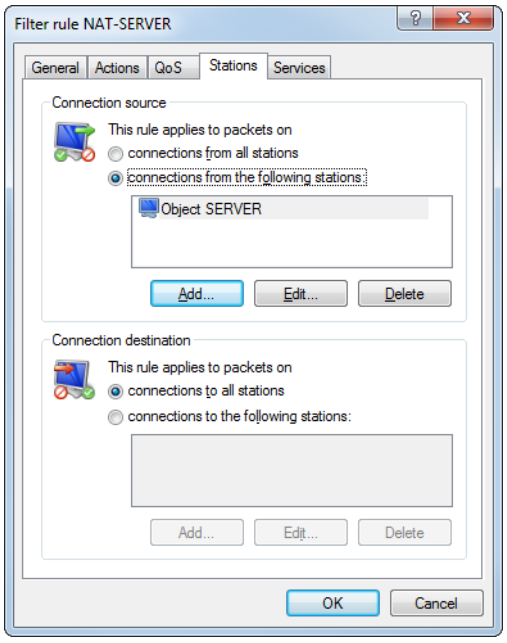
3. Next, go to **Firewall/QoS** > **IPv4 rules** > **Firewall rules** and create a filter rule.

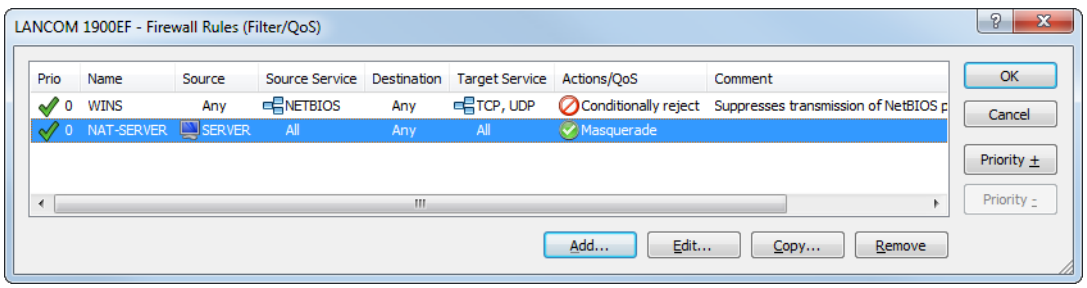


4. In this filter rule, go to **Actions** and select the new action “SERVER-NAT” that was defined above.



5. Then go to **Stations** and use the newly created station object. If necessary. you can also specify the Internet line under **Connection destination**.





9 Quality of Service

This chapter is devoted to the topic of Quality-of-Service (abbreviation: QoS). This term embraces a range of functions in your LCOS that assure a certain quality of service.

9.1 What is QoS used for?

In general, the aim of the Quality of Service is to ensure that particular data packets are transmitted either with high certainty or as quickly as possible.

- When transmitting data, it may well happen that data packets do not arrive at the recipient. However, some applications strongly depend on all of the sent data packets actually arriving. For example, an e-mail that is divided into numerous small data packets can only be reassembled at the receiver when all of its parts have arrived. The occasional packet arriving with a slight time delay is uncritical. These applications usually rely on the connection-oriented Transmission Control Protocol (TCP). This protocol ensures that the data is transported over the network correctly and in the right sequence. It reduces the transmission rate by itself if the confirmations of the sent data packets take longer to arrive, and automatically repeats transmission in the event of packet loss.
- For other applications, such as Internet telephony (Voice over IP, VoIP), it is vital that the data packets arrive at the recipient with a minimum of delay. The occasional data packet getting lost on the way is not so important here. The subscriber at the other end of the line can still understand the caller even if small parts of the speech get lost. This application therefore places priority on data packets being transmitted as quickly as possible. These applications frequently rely on the connectionless User Datagram Protocol (UDP). The administration overhead for this protocol is very small. However, there is no guarantee that the data packets are delivered in the correct order; they are simply sent off. There is no acknowledgment of receipt, so lost packets are not re-sent.

9.2 Which data packets to prefer?

The need for the QoS concept arises from the fact that the available bandwidth is not always sufficient to transmit all of the pending data packets reliably and on time. Load peaks can quickly occur when running FTP downloads, exchanging e-mails and using IP telephones over the data line all at the same time. In order to meet the needs for data transmission even in these situations, certain data packets need to be treated preferentially. This of course requires the device to recognize which data packets should be preferred.

There are two ways to signal the need for preferential treatment of data packets in the device:

- The application, such as the software of an IP phone, can mark the data packets accordingly. This mark, or “tag”, is inserted into the header of the IP packets. The two types of tagging “ToS” and “DiffServ” can, in simplified terms, take on the following states:
  - ToS “Low Delay“
  - ToS “High Reliability“
  - DiffServ “Expedited Forwarding“
  - DiffServ “Assured Forwarding“



In the case of a VPN route, the IP header bits of the ToS or DiffServ field are also copied to the enclosing IP header of the IPSec VPN packet. This allows QoS to be used on VPN routes over the Internet as long as the provider supports preferential treatment of the corresponding packets in the WAN.

- If the application itself is unable to tag the data packets appropriately, the device can handle this. This makes use of the functions available in the firewall, which classify the data packets by subnets or services (applications). These functions allow, for example, the data packets of an FTP connection or those of a specific company department (i.e. in a separate subnet) to be treated differently.

  The following two options are available for the treatment of data packets that are classified by the firewall:

  - Guaranteed minimum bandwidth
  - Limited maximum bandwidth

9.2.1 What is DiffServ?

DiffServ stands for "Differentiated Services" and is a model that signals the priority of the data packets. DiffServ is based on the Type of Service (ToS) field and uses the same byte in the IP header.

ToS uses the first three bits to denote the precedence of 0 to 7, and four more bits (the ToS bits) to optimize the data flow (including "low delay" and "high reliability"). This model is rather inflexible and has been little used in the past.

The DiffServ model uses the first 6 bits to distinguish different classes. This allows up to 64 differentiated services code points (DSCPs), which allow a finer prioritization of the data flow:

- To ensure backwards compatibility with the ToS implementation, the "Class Selectors" (CS0 to CS7) are used to map the former precedence levels. The level CS0 is also called "Best effort" (BE) and represents the normal transmission of data packets without special treatment.
- The "Assured Forwarding" (AF) classes are used for the certain transmission of data packets. The first digit of the AF class stands for the priority of the transmission (1 to 4), the second digit for "Drop Probability" (1 to 3). Packets marked with AFxx are "assured" of being transmitted and are not dropped.

With the class "Expedited Forwarding" marks those packets that are to be transmitted before all other packets (preferred).

Codepoint	DSCP bits	Dec.	Codepoint	DSCP bits	Dec.	Codepoint	DSCP bits	Dec.
CS0 (BE)	000000	0	AF11	001010	10	AF33	011110	30
CS1	001000	8	AF12	001100	12	AF41	100010	34
CS2	010000	16	AF13	001110	14	AF42	100100	36
CS3	011000	24	AF21	010010	18	AF43	100110	38
CS4	100000	32	AF22	010100	20	EF	101110	46
CS5	101000	40	AF23	010110	22			
CS6	110000	48	AF31	011010	26			
CS7	111000	56	AF32	011100	28			

9.2.2 Guaranteed minimum bandwidth

This gives priority to important applicationssuch as Voice-over-IP (VoIP) PBX systems or specific user groups.

For devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are set automatically.

9.2.2.1 Fully dynamic bandwidth management when sending

Bandwidth in the send direction is managed dynamically. This means that a guaranteed minimum bandwidth is only made available for as long as a data transfer is actually in progress.

An example:

VoIP data being transmitted by a VoIP gateway should always have a guaranteed bandwidth of 256 kbps. A single VoIP connection requires 32 kbps.

As long as nobody is on the phone, all the bandwidth is available to other services. With each new VoIP connection established, the other applications have 32 kbps less, until 8 VoIP connections are active. As soon as a VoIP connection is terminated, the corresponding bandwidth is available again to all other applications.

For this mechanism to operate correctly, the sum of the configured minimum bandwidths must not exceed the effective transmission bandwidth available.

9.2.2.2 Dynamic bandwidth management also for reception

For bandwidth control during reception, packets can be buffered and acknowledged only later. A result of this is that TCP/IP connections automatically regulate themselves to a lower bandwidth.

Each WAN interface is assigned a maximum receive bandwidth. Any QoS rule that guarantees a minimum receive bandwidth on a particular interface will reduce the bandwidth accordingly.

- If the QoS rule is connection-based, immediately after the connection is terminated the reserved bandwidth is released and the maximum available bandwidth on the WAN interface increases accordingly.
- If the QoS rule is defined globally, the reserved bandwidth is released again only after the last connection has been terminated.

9.2.3 Limited maximum bandwidths

This allows you to limit the overall or connection-related maximum bandwidth used for server access.

An example:

You operate a web server and a local network at a shared Internet connection.

To prevent your productive network (LAN) from being overloaded by large numbers of Internet accesses to your web server, you can limit server access to half of the available bandwidth. You can also ensure that users have simultaneous and equal access to your server services by setting a maximum bandwidth per connection to the server.

9.2.3.1 Combination possible

Minimum and maximum bandwidths can be used together in combination. This allows you to distribute the available bandwidth to meet your needs, e.g. by favoring certain user groups or applications.

9.3 The queue concept

9.3.1 Queues in the send direction

The quality of service requirements are implemented in LCOS by using multiple queues for data packets. On the sending side, the queues described in *Quality-of-Service (QoS) with 8 queues* on page 713 are used.

9.3.2 Queues in the receiving direction

Along with the transmission rate in the transmitting direction, the same consideration also applies to the receiving direction. In this case, the device's WAN interface receives significantly less data from the DSL modem than the Ethernet interface can theoretically handle. All data packets received on the WAN interface are transferred to the LAN with equal priority.

In order to be able to prioritize incoming data, an artificial “brake” needs to be applied to the received data. As with the transmitting direction, the transmission rate of the interface in the receive direction is adapted to match the speed of the provider, e.g. a downstream rate of 16 Mbps. Again, as with the upstream rate, the gross data rate may also be entered, if known.

Reducing the reception bandwidth now makes it possible to handle the received data packets in a suitable manner. The preferred data packets are passed directly to the LAN up to the guaranteed minimum bandwidth, the remaining data packets run into congestion. This congestion usually leads to the acknowledgment of the packets being delayed. On a TCP connection, the sending server will respond to these delays, decreasing its transmit frequency and adapting to the available bandwidth.

The following queues are used when receiving data:

- Deferred acknowledge queue

  Each WAN interface additionally has a QoS receive queue, which receives the packets to be slowed down. The storage period of each individual packet depends on the length of the packet and the currently permitted reception bandwidth. Packets that are granted a minimum receive bandwidth by a QoS rule are allowed to pass without delay, as long as the minimum bandwidth is not exceeded.

- Standard reception queue

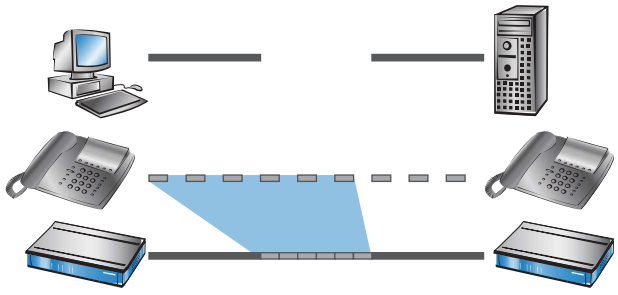
  All received packets not given priority treatment by a QoS rule end up in this queue. Packets in this queue are forwarded or acknowledged directly, without consideration of maximum bandwidths.

9.4 Reducing the packet length

The preferred handling of data packets from an important application can be jeopardized by extremely long data packets from other applications. This may be the case, for example, when IP telephony and FTP data transfer are simultaneously active on the WAN connection.

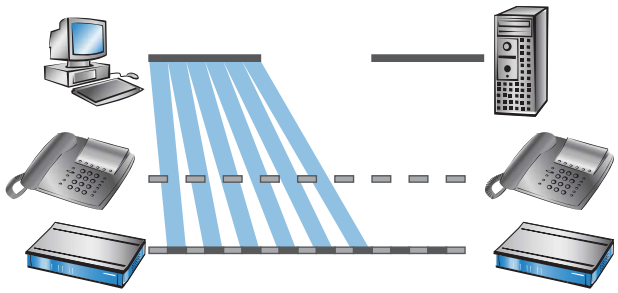


FTP transfer uses quite large data packets of 1500 bytes, while the Voice-over-IP connection packets are of 24 bytes net and are sent in relatively frequent intervals. If FTP packets are present in the send queue of the device at the moment when a VoIP packet is to be transmitted, the VoIP packet cannot be sent until the line is free again. Depending on the connection's transmission rate, this can lead to a noticeable delay in voice transmission.



This disruptive behavior can be offset if data packets not belonging to the preferred QoS connection do not exceed a certain length. For example, the FTP connection only sends packets small enough to ensure that the time-critical VoIP

connection can deliver packets at the necessary frequency and without delay. For TCP-secured FTP transfers, delays are not critical.



There are two different ways to influence the length of a packet:

- The device can inform the users of the data connection that they should only send data packets up to a certain length. This is done by forcing a suitable PMTU (Path Maximum Transmission Unit) at the sending end in a process referred to as "PMTU reduction".

  PMTU reduction can be operated in both the transmit and receive directions. For the transmit direction, the senders in their own LAN are set to a smaller packet size by PMTU reduction; for the receive direction, the senders in the WAN, e.g. Web or FTP servers on the Internet, are also instructed to deliver a smaller packet size.

  If the data connection is already established when the VoIP connection starts, the senders very quickly regulate the packet length down to the permissible value. When a data connection is established with a VoIP connection already in place, the maximum permissible packet length is negotiated directly during the connection handshake.

  The reduced packet length on the data connection is still used even after the VoIP connection is terminated and until the sender re-checks the PMTU value.

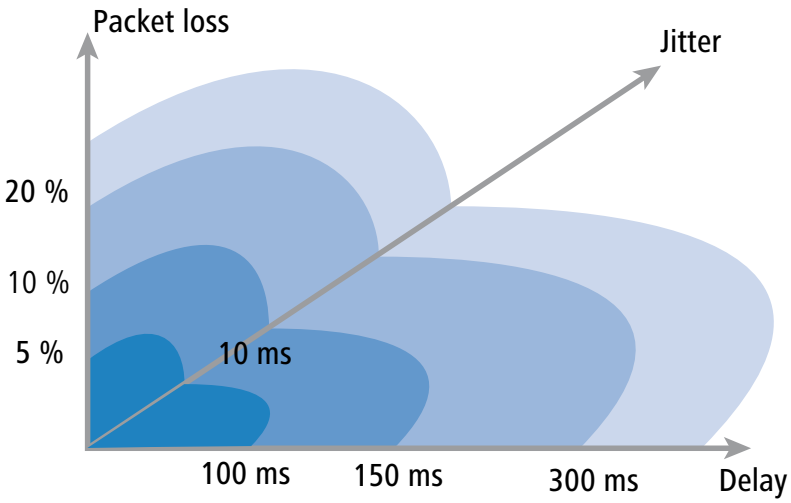
- The device itself is able to split packets due for transmission but which are above an adjustable maximum size (e.g. 256 bytes) into smaller units. This method referred to as "fragmentation" is not supported by all servers on the Internet, because processing fragmented packets is considered a security risk, so it is often turned off. This may cause disruptions when downloading data or when transferring websites, for example.

  This method is therefore recommended only for connections that do not involve unknown Internet servers, such as for the direct connection of branches to a central office over a VPN connection that does not simultaneously run Internet traffic.

9.5 QoS parameters for Voice-over-IP applications

An important task when configuring VoIP systems is to ensure sufficient voice quality. Two factors significantly affect the voice quality of a VoIP connection: The voice delay on its way from the sender to the receiver, and the loss or late arrival of data packets on their way to the receiver. The International Telecommunication Union (ITU) has extensively tested what people perceive to be sufficient voice quality, and has published the result in the ITU G.114 recommendation.

For devices with VoIP functions that were already integrated or added in with a software option, the QoS settings for SIP calls are set automatically.



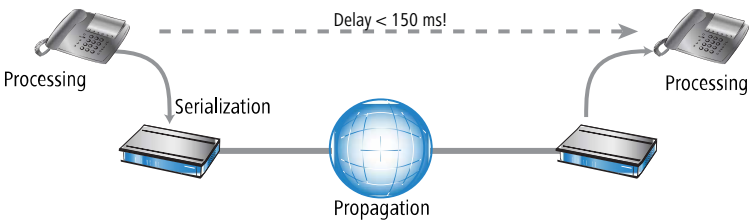
The quality of a telephone connection is perceived as normal with a delay of no more than 100 ms and a packet loss of less than 5%, and still as good quality with no more than a 150 ms delay and less than 10% packet loss. Ultimately, some listeners still find the quality to be acceptable with up to 300 ms at 20%, although this is the limit before the connection becomes no longer useful for voice transmission.

Along with the average delay time, the fluctuation in this delay can also be perceived by the human ear. Variations in the runtime of the speech information from the sender to the receiver (jitter) are tolerable at up to 10 ms, but more is perceived as irritating.

A VoIP connection should be configured to remain within these marginal values: Packet loss up to 10%, delay up to 150 ms, jitter up to 10 ms.

- Jitter can be offset by using a buffer at the receiver. This jitter buffer caches a quantity of packets and passes them to the receiver at regular intervals. This buffering compensates for the fluctuations in the transmission time between the individual packets.
- The delay is influenced by several components:
  - The fixed portion of the delay consists of the processing (packet assembly, encoding and compression at the sender and the receiver), serialization (the time for transferring the packet from the application to the interface), and propagation (the time for transmission over the WAN link).
  - The variable component is determined by the jitter or the jitter-buffer setting.

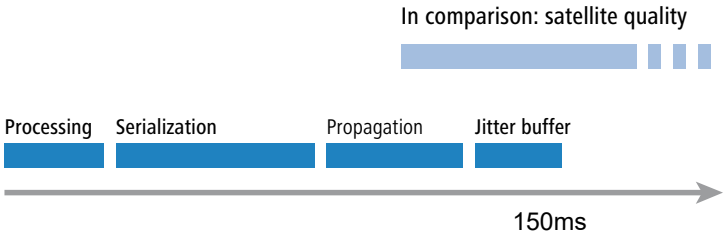
  These two components together make up the delay, which ideally should not be more than 150 ms.



- Along with the general network losses, packet loss is ultimately significantly affected by the jitter buffer. If packets arriving have a greater delay than the jitter buffer can counterbalance, the packets are dropped and packet loss

increases. The larger the jitter buffer, the smaller the loss. Conversely, the jitter buffer also increases the overall delay. The jitter buffer should thus be set small enough for the quality to still be considered sufficient.

Going into detail, the delay is determined in particular by the codec used, the resulting packet size, and the available bandwidth:



- The time of processing is determined by the codec used. With a sampling time of 20 ms, a new packet is generated every 20 ms precisely. The times for compression, etc. are usually negligible.
- The time to transfer packets to the interface is defined by the quotient of packet size and available bandwidth:

	Packet size in bytes						
	1	64	128	256	512	1024	1500
56 kbps	0.14	9	18	36	73	146	215
64 kbps	0.13	8	16	32	64	128	187
128 kbps	0.06	4	8	16	32	64	93
256 kbps	0.03	2	4	8	16	32	47
512 kbps	0.016	1	2	4	8	16	23
768 kbps	0.010	0.6	1.3	2.6	5	11	16
1536 kbps	0.005	0.3	0.6	1.3	3	5	8

- A 512-byte packet on an FTP connection over a 128-kbps upstream link occupies the line for at least 32 ms.

Apart from that, the packets on a VoIP connection often consist of much more than just the payload itself. In additional to the payload, there are also IP headers and, if applicable, IPSec headers. The payload results from the product of payload data rate and the codec sampling interval. In addition, all codecs require 40 bytes for IP, RTP and UDP headers and at least 20 bytes for the IPSec header (although the RTP and IPSec headers can be larger, depending on the configuration).

Without IPSec	Payload	IP payload	Ethernet / PPPoE	ATM net Bps	ATM gross Bps
Code	20 ms	20 ms	20 ms	20 ms	20 ms
G711-64	160	200	222	96000.0	106000.0
G722-64	160	200	222	96000.0	106000.0
G726-40	100	140	162	76800.0	84800.0
G726-32	80	120	142	76800.0	84800.0
G726-24	60	100	122	57600.0	63600.0
G726-16	40	80	102	57600.0	63600.0
G729-8	20	60	82	57600.0	63600.0

Without IPSec	Payload	IP payload	Ethernet / PPPoE	ATM net Bps	ATM gross Bps
Code	30 ms	30 ms	30 ms	30 ms	30 ms
G711-64	240	280	302	89600.0	98933.3

Without IPSec	Payload	IP payload	Ethernet / PPPoE	ATM net Bps	ATM gross Bps
G722-64	240	280	302	89600.0	98933.3
G726-40	150	190	212	64000.0	70666.7
G726-32	120	160	182	64000.0	70666.7
G726-24	90	130	152	51200.0	56533.3
G726-16	60	100	122	38400.0	42400.0
G729-8	30	70	92	38400.0	42400.0
G723-6,3	24	64	86	38400.0	42400.0

With IPSec	Payload	IP payload	IPSec payload	Ethernet / PPPoE	ATM net Bps	ATM gross Bps
Code	20 ms	20 ms	20 ms	20 ms	20 ms	20 ms
G711-64	160	200	260	282	134400.0	148400.0
G722-64	160	200	260	282	134400.0	148400.0
G726-40	100	140	200	222	96000.0	106000.0
G726-32	80	120	180	202	96000.0	106000.0
G726-24	60	100	160	182	96000.0	106000.0
G726-16	40	80	140	162	76800.0	84800.0
G729-8	20	60	120	142	76800.0	84800.0

With IPSec	Payload	IP payload	IPSec payload	Ethernet / PPPoE	ATM net Bps	ATM gross Bps
Code	30 ms	30 ms	30 ms	30 ms	30 ms	30 ms
G711-64	240	280	340	362	102400.0	113066.7
G722-64	240	280	340	362	102400.0	113066.7
G726-40	150	190	250	272	89600.0	98933.3
G726-32	120	160	220	242	76800.0	84800.0
G726-24	90	130	190	212	64000.0	70666.7
G726-16	60	100	160	182	64000.0	70666.7
G729-8	30	70	130	152	51200.0	56533.3
G723-6,3	24	64	124	146	51200.0	56533.3

- IP payload: Voice payload + 40 byte header (12 byte RTP; 8 byte UDP; 20 byte IP header)
- IPSec payload: IP packet + padding + 2 byte (padding length & next header) = multiple of the IPSec initialization vector

The values in the table apply to the use of AES. For other encryption methods, the resulting packet size may vary slightly.

For further information on bandwidth requirements for Voice over IP with IPSec is available in the LANCOM techpaper Performance Analysis of Routers.

- The time for transmission over the Internet depends on the distance (about 1 ms per 200 km) and the other routers en route (about 1 ms per hop). This time is approximately half the average time of a series of pings to the remote site.

- Many IP telephones allow the jitter buffer to be set directly, i.e. as a fixed number of packets for caching. The phones then load up to 50% of the set number of packets, and then start the playback. The jitter buffer thus corresponds to half the set number of packets multiplied by the sampling time of the codec.
- Conclusion: The total delay in the following example results from the bandwidth, a ping time of 100 ms to the remote station, and a jitter buffer of 4 packets for the two codecs:

Codec	Processing	Serialization	Propagation	Jitter buffer	Total
G.723.1	30 ms + 7.5 ms look ahead	32 ms	50 ms	60 ms	179.5 ms
G.711	20 ms	32 ms	50 ms	40 ms	142 ms

- The packet transmission time to the interface (serialization) is based on a PMTU of 512 bytes for a 128 kbit connection. For slower interfaces or other codecs, you may need to set other jitter buffers and / or PMTU values.

Please note that the bandwidths are required in the sending and receiving direction, as well as just for one single connection.

These explanations relate to very low bandwidth Internet connections. Where higher bandwidths are available, reducing the size of the PMTU has a barely perceptible influence on performance.

9.6 QoS in send or receive direction

When using QoS to regulate data transfer, you can decide whether the corresponding rule applies to the send or receive direction. Of course, whether a particular data transmission is being sent or received is a question of perspective. There are two variants:

- The direction corresponds to the logical connection establishment
- The direction corresponds to the physical data transmission over the respective interface

The differences are made clear when we consider an FTP transfer. A client on the LAN is connected to the Internet via a device.

- In an active FTP session, the client uses the PORT command to inform the server on which port it expects to receive the DATA connection. The server then establishes the connection to the client and sends the data in the same direction. In this case the logical connection and the actual data stream are sent from the server over the interface to the client, so the device considers both to be the receive direction.
- The situation is different with a passive FTP session. Here, the client establishes the connection to the server. Consequently the logical connection is from the client towards the server, but the data transmission over the physical interface is in the reverse direction, from the server to the client.

By default, a device evaluates the send or receive direction based on the logical connection establishment. In some applications this way of seeing things is not so obvious, and an alternative is to switch to considering the physical data stream.

The distinction between the send and receive directions only applies for the setup of maximum bandwidths. For guaranteed minimum bandwidths, fragmentation and PMTU reduction, the direction is always taken to be the physical data transfer over the respective interface.

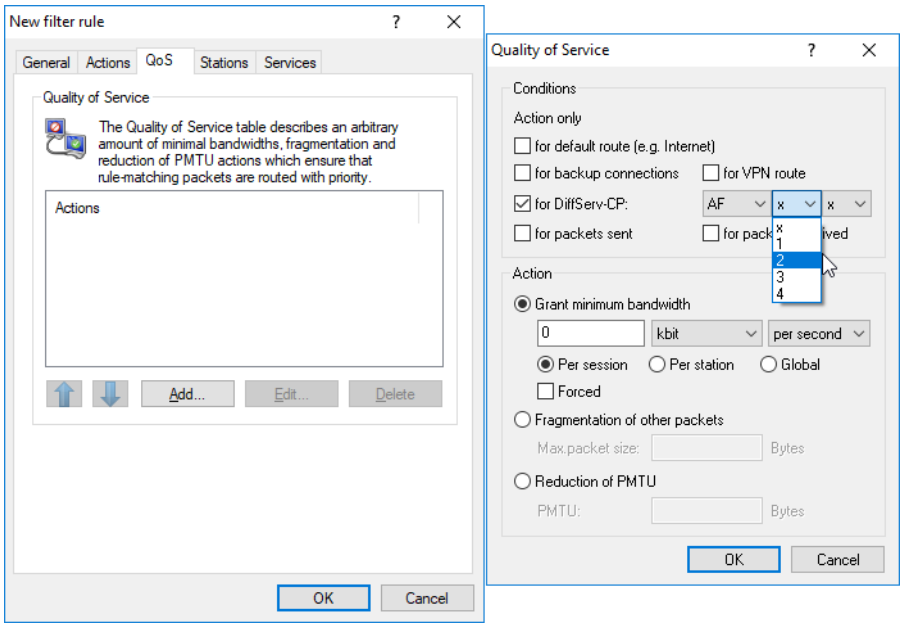
9.7 QoS configuration

9.7.1 Evaluate DiffServ Field in the Firewall

9.7.1.1 DiffServ in firewall rules

The code points from the DiffServ field can be evaluated by firewall rules for further control over QoS parameters such as minimum bandwidth or PMTU reduction.

In LANconfig, the parameters for evaluating the DiffServ fields are set when the QoS rule is defined:



Depending on the selected DSCP type (BE, CS, AF, EF), additional drop-down lists enable you to set the applicable values. Alternatively, the DSCP decimal value can be entered directly. A table listing the valid values can be found under *What is DiffServ?* on page 698.

When configuring from the command line, these parameters are entered here: **Setup** > **IP-Router** > **Firewall** > **Rule-List**

The rule in the firewall is extended by the condition "@d" and the DSCP (Differentiated Services Code Point). The code point can be specified either by its name (CS0 - CS7, AF11 to AF 43, EF or BE) or its decimal or hexadecimal representation. For example, “Expedited Forwarding” can be specified as “@dEF”, “@d46” or “@d0x2e”. Collective names (CSx or AFxx) are also possible.

Examples:

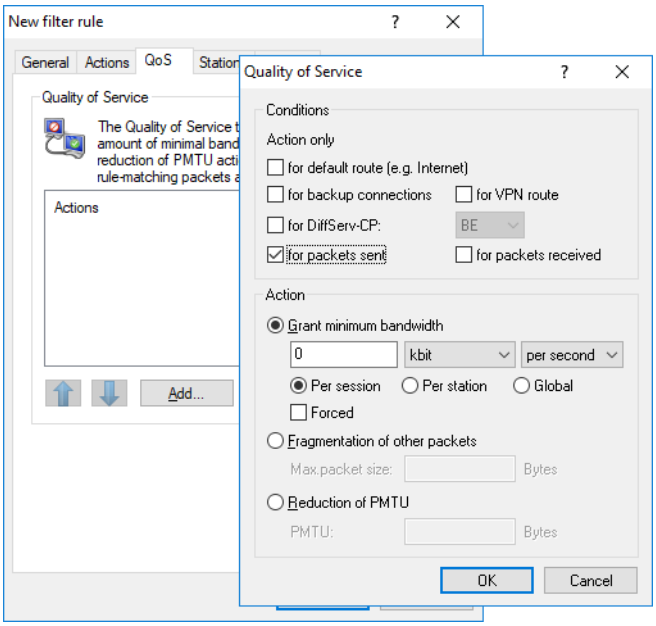
- **%Lcds0 @dAFxx %A**: Accept (secure transmission) with DiffServ “AF”, limit ““0”
- **%Qcds32 @dEF**: Minimum bandwidth for DiffServ EF of 32 kbps
- **%Fprw256 @dEF**: PMTU reduction on reception for DiffServ EF to 256 bytes

The examples listed here reserve a required bandwidth for Voice-over-IP phone calls. The first element “%Lcds0 @dAFxx %A” accepts packets marked with DSCP “AFxx” that are used for signaling calls. Voice data marked with EF is transmitted prioritized by the entry “%Qcds32@dEF” with a guaranteed bandwidth of 32 kbps. In parallel, “%Fprw256 @dEF” sets the PMTU to 256 bytes in order to guarantee the necessary bandwidth in the receive direction.

9.7.2 Defining minimum and maximum bandwidths

A minimum bandwidth for a specific application is defined in LANconfig by means of a firewall rule according to the following conditions:

- The rule does not need an action, because QoS rules always implicitly assume “transfer” to be the action.
- The guaranteed bandwidth is set on the tab **QoS**.



- The option **Action only for default route** restricts the rule to packets that are sent or received over the default route.
  - The option **Action only for VPN routes** restricts the rule to packets sent or received over a VPN tunnel.
  - The option **Forced** defines a static reservation of bandwidth. Bandwidth reserved in this way cannot be used for any other connections, even while the preferred connection is inactive.
  - The option **Per connection** or **Globally** specifies whether the minimum bandwidth set here applies to every single connection that complies with this rule (per connection), or if it is the upper limit for the sum of all connections together (globally).
- The tabs **Stations** and **Services** are used, as with the other firewall rules, to decide which stations in the LAN/WAN and which protocols this rule applies to.

When configuring from the command line, the minimum and maximum bandwidths in a new firewall rule are entered here: **Setup** > **IP-Router** > **Firewall** > **Rule-List**

A required minimum bandwidth is initiated in the rules by the identifier ““%Q”. The implicit assumption here is that the rule involves an “Accept” action, so the packets will thus be transmitted.

For a maximum bandwidth, a simple limit rule is defined that uses a “Drop” action to discard all packets that go beyond the set bandwidth.

Examples:

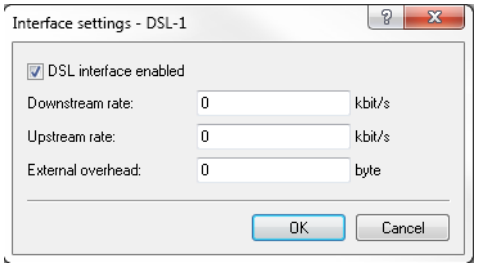
- **%Qcds32**: Minimum bandwidth of 32 kbps for each connection
- **%Lgds256 %d**: Maximum bandwidth of 256 kbps for all connections (globally)

9.7.3 Setting transmission rates for interfaces

Restrictions on the data transmission rate for Ethernet, DSL and DSLoL interfaces are set in LANconfig by navigating to **Interfaces** > **WAN** and clicking the button **Interface settings**:

The values for the upstream rate and the downstream rate are specified in kbps, and the values for the external overhead are set in bytes per packet.

Ethernet, DSL and DSLoL interfaces



- A DSL interface can be completely switched off in this dialog.
- The upstream and downstream rates specified here are the gross data rates, which are usually slightly higher than the net data rates as specified by providers as the guaranteed data rate (also see *The queue concept* on page 699).
- The "external overhead" allows for the extra information that is appended to the packets during data transmission. For applications with relatively small data packets (e.g. Voice over IP), this extra overhead can have noticeable effects. Examples of external overhead:

Transmission	External overhead	Comment
T-DSL	36 bytes	Additional header, losses due to underused ATM cells
PPTP	24 bytes	Additional header, losses due to underused ATM cells
IPoA (LLC)	22 bytes	Additional header, losses due to underused ATM cells
IPoA (VC-MUX)	18 bytes	Additional header, losses due to underused ATM cells
Cable modem	0	Direct transmission of Ethernet packets

From the CLI, you can enter the limits on the data transmission rates for the Ethernet, DSL and DSLoL interfaces at the following location: **Setup** > **Interfaces** > **DSL-Interfaces**

VDSL and ADSL interfaces

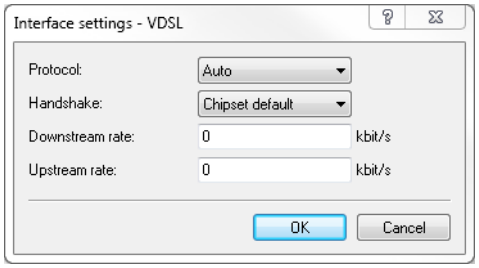
In order for Quality of Service to function properly, you need to know the actual bandwidth of the WAN connection. Sometimes, the bandwidth negotiated by the DSL modem may not agree with the actual data transfer rate. In this case, it is necessary to manually correct the speed of DSL connection to the actual value.

This only applies to devices with an integrated ADSL / VDSL modem.

Example:

The bandwidth negotiated during the DSL synchronization is 100 Mbps. In fact, the actual available bandwidth is a transmission speed of just 50 Mbps.

Settings for devices with an integrated VDSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode.

VDSL2 (G.993.2)

Operating mode VDSL2 for transmission rates of up to 100 Mbps upstream and downstream.

ADSL

Operating mode ADSL with up to 8 Mbps downstream and 0.6 Mbps upstream.

ADSL2+ (G.992.5)

Operating mode ADSL2+ with up to 24 Mbps downstream and 1 Mbps upstream.

ADSL2 (G.992.3)

Operating mode ADSL2 with up to 12 Mbps downstream and 1.2 Mbps upstream.

ADSL1 (G.992.1/G.DMT)

Operating mode ADSL (G.DMT) with up to 8 Mbps downstream and 1 Mbps upstream.

ADSL2+ (Annex J)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.5 Mbps upstream.

ADSL2 (Annex J)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.5 Mbps upstream.

No

The interface is not active.

Handshake

Select from the following handshake methods for this interface:

Chipset-default

The handshake is carried out according to the default for the chipset in the device.

V43 if needed

The V43 carrier set is used for the handshake if required.

V43 enabled

The carrier set V43 is enabled for the handshake.

V43 disabled

The carrier set V43 is disabled for the handshake.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

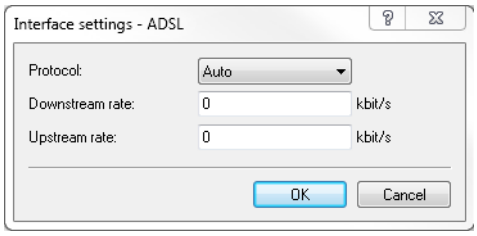
If the default value is 0, the value used is negotiated automatically.

Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is 0, the value used is negotiated automatically.

Settings for devices with an integrated ADSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode.

ADSL1 (autom. Annex A/B)

Operating mode ADSL over POTS/ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (autom. Annex A/B)

Operating mode ADSL2 over POTS/ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (autom. Annex A/B)

Operating mode ADSL2+ over POTS/ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

Auto-POTS (autom. Annex A/I/L/M)

Operating mode ADSL over POTS for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex A)

Operating mode ADSL over POTS for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex A)

Operating mode ADSL2 over POTS with up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (Annex A)

Operating mode ADSL2+ over POTS with up to 24 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex I)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.2 Mbps upstream.

ADSL2+ (Annex I)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.2 Mbps upstream.

ADSL2 (Annex L)

Operating mode RE-ADSL2 with up to 6 Mbps downstream and 1.2 Mbps upstream.

ADSL2 (Annex M)

Operating mode ADSL2 with up to 24 Mbps downstream and 3.5 Mbps upstream.

ADSL2+ (Annex M)

Operating mode ADSL2+ with up to 24 Mbps downstream and 3.7 Mbps upstream.

Auto-ISDN (autom. Annex B/J)

Operating mode ADSL over ISDN for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 3.5 Mbps upstream.

ADSL2+ (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 3.5 Mbps upstream.

No

The interface is not active.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is 0, the value used is negotiated automatically.

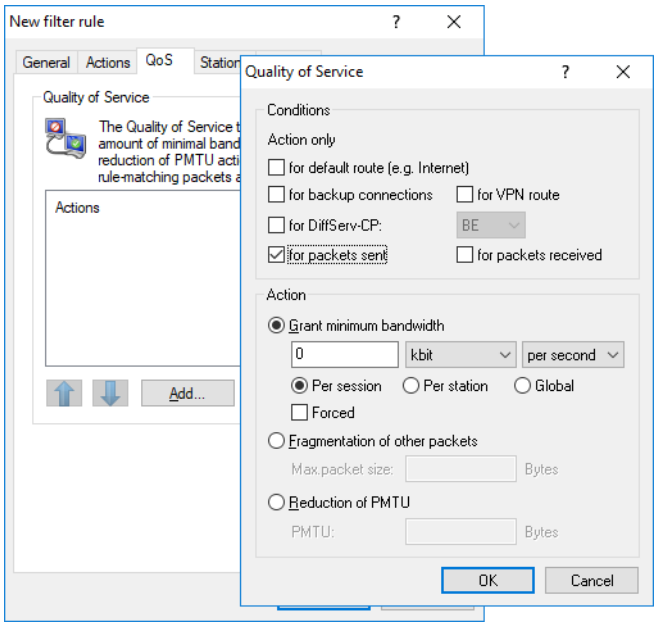
Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is 0, the value used is negotiated automatically.

9.7.4 Sending and receiving direction

The sense of the direction of data transmission is set in LANconfig when defining the QoS rule:



When configuring a new rule in the firewall from the command line, the sense of the direction of data transmission is set using the parameter "R" for receive, "T" for transmit and "W" for reference to the WAN interface in the following location: **Setup** > **IP-Router** > **Firewall** > **Rule-List**

The following rule in the firewall restricts the data transmission with respect to the physical WAN interface to 16 Kbps in the send direction:

- %Lcdstw16%d

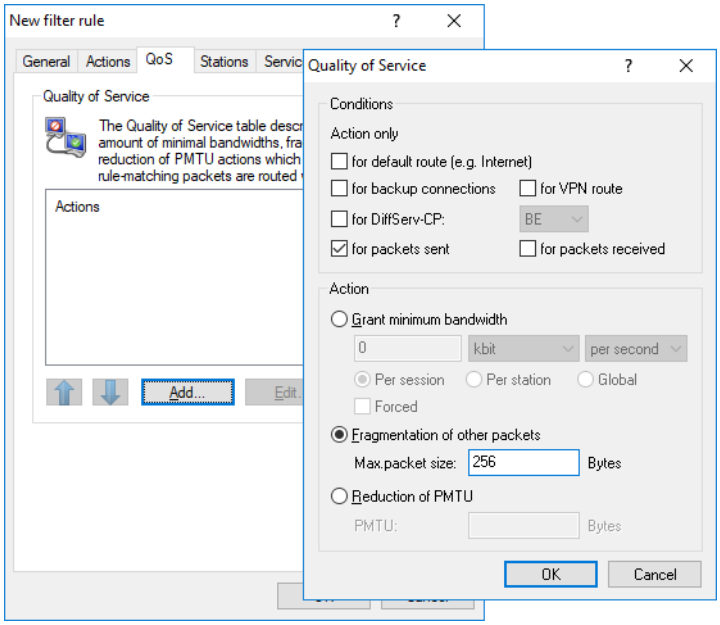
9.7.5 Reducing the packet length

The length reduction of the data packets is defined with a firewall rule, which observes the following conditions:

- The reduction affects to **all** packets that are sent to the interface and **do not** match the rule.
- Reduction applies globally to all packets on the interface; there is no exception of certain protocols.

For devices with VoIP functions that were already integrated or added in with a software option, fragmentation and PMTU reduction can be set separately for SIP calls.

The reduction in the length of data packets is set in LANconfig when defining the QoS rule:



When configuring a new rule in the firewall from the command line, the reduction is set in the following location whereby parameter "P" is for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and "F" for the fragment size: **Setup** > **IP-Router** > **Firewall** > **Rule-List**

PMTU reduction and fragmentation are always related to the physical connection. Specification of the parameter "W" for the WAN transmission direction is therefore not required here and is ignored, if available.

The following example shows a setting for Voice-over-IP telephony:

Policy	Source	Destination	Action	Protocol
VOIP	IP addresses of the IP phones in the LAN, all ports	IP addresses of the IP phones in the LAN, all ports	%Qcds32 %Fpt256	UDP

This rule sets the minimum send and receive bandwidth to 32 kbps while enforcing the reduction of the PMTU of sent packets to 256 bytes. For the TCP connections, the maximum segment size of the local workstation is set to 216, so that the server sends packets of a maximum of 256 bytes in size (PMTU reduction in the transmit direction).

9.8 Quality-of-Service (QoS) with 8 queues

In the following explains the concept of how Quality of Service functions with eight queues. Routers should fundamentally be able to prioritize packets according to the DSCP value in the IP header. A total of eight **queues** are available for this purpose, which are strictly prioritized. This means that packets are sent starting with the **queue** with the highest priority and working through to the **queue** with the lowest priority. A packet is assigned to a **queue** based either on the DSCP value in the IP header or by a firewall rule. Of the eight available **queues** two are reserved, one for the **Urgent-Queue** (highest priority, for internal services such as VCM and protocol packets) and the other for the **Best-Effort-Queue** (lowest priority, for all non-priority packets). The remaining six **queues** are freely available to the user. The priority levels of the individual **queues** are set by placing them in a **Queue-List** in descending order of priority. The internal **Urgent-Queue** and **Best-Effort-Queue** are inserted at the front and end of this **Queue-List**. The completed **queue list** must then be assigned to a physical **WAN interface**. Following this, any packets sent to this **WAN interface** are prioritized according to the configuration of the **queues**.

For QoS to work, the bandwidths or rates of an interface must be known in order for QoS to correctly distribute the load, e.g. in the case where bandwidths are allocated as a percentage. The bandwidths are usually taken from the upstream and downstream data rates from the internal DSL modems or from the bandwidth transmitted in the PPP by the provider.

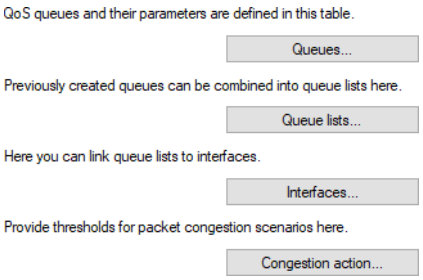
For WAN connections via external modems or pure Ethernet connections, the actual bandwidths for the corresponding interfaces must be specified in the table **Interfaces** > **WAN** > **Interface settings** under **Downstream rate** and **Upstream rate**.

Please note that certain internal packets are automatically sorted by LCOS into the Urgent Queue. These include

- All packets assigned a specific minimum bandwidth via a firewall rule, as long as the limit is not exceeded
- Voice packets from the VCM or SIP ALG
- Important protocol packets (IKE, BGP, line polling)

Additionally, forwarded TCP SYN and ACK packets are prioritized and also sorted into the Urgent Queue. This behavior can be configured under **IP Router** > **General** > **Routing options** > **Pass on TCP SYN and ACK packets preferentially**.

These **queues** are configured in LANconfig under **Firewall/QoS** > **QoS**.

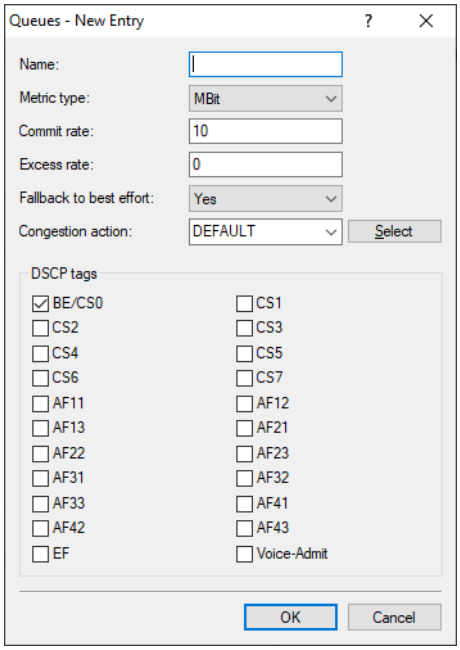


9.8.1 Queues

This table is used to configure **queue templates**. This does not mean that every entry in this table creates a queue. A **queue** is only created when it is used in a **Queue-List** and assigned to a **WAN interface**. This means a template created here can be the basis for any number of **queues** or none at all.

Example: If an entry named “Test” is created and this entry is then divided into two **Queue-List** objects, each of which is assigned to a different **WAN interface**, then the result will be two **queues** with name “Test”, which are completely independent of one another.

The configuration of the queues and their parameters in LANconfig is done under **Firewall/QoS** > **QoS** > **Queues**.



Name

This is where the name of the **queue template** is entered. Other tables reference the template by using this name. The name must be unique within the table.

Metric type

Here the metric of the columns **Commit rate** and **Excess rate** is set.

Commit rate

Here you enter how much bandwidth is available to this **Queue**. The value is also commonly referred to as CIR (Committed Information Rate). The unit of the input is specified in the column **Metric Type**. The following value ranges apply:

- *Percent:* 1 < x < 100
- *Kbit:* 1 < x < 4294967295
- *Mbit:* 1 < x < 4294967295

Excess rate

Here you enter the bandwidth the **Queue** can use in addition to its **Commit-Rate**. The value is also commonly referred to as EIR (Excess Information Rate). To prevent higher-priority **queues** from taking the **commit rate** of lower-priority **queues**, the following concept was used:

The QoS operates in time slots, during which each **queue** can use its **commit rate**. At the end of the time slot, the unused **Commit-Rate** from all **queues** is carried over into the next time slot and used as a pool for the **Excess-Rate**. This pool then limits the bandwidth that can be used with the **Excess-Rate**. This fulfills two important aspects: Firstly, the **Excess-Rate** of a queue is not subtracted from another queue's current **Commit-Rate**, but from the unused rate of the previous time slot. Second, the pool for the **Excess-Rate** is reset at the beginning of each time slot and is not added up, which means the unused **Commit-Rate** of a time slot can only be used in the following time slot. This prevents an accumulation, which could cause **queues** with a configured excess rate to starve the lower-priority queues.

Example: Two **queues** are configured, concatenated into a **Queue-List**, and assigned to a **WAN interface**. **Queue A** has a **commit rate** of 10 Mbps and an **excess rate** of 4 Mbps. **Queue B** has a **commit rate** of 5 Mbps and an **excess rate** of 0. If now in time slot 1 **Queue A** uses 9 Mbps and **Queue B** uses 4 Mbps, then

2 Mbps are unused rate and added to the pool of the **excess rate** for time slot 2. In this time slot, **Queue A** can then use its 10 Mbps **commit rate** and an additional 2 Mbps from the pool as part of its **excess rate**. Important is that only as much **Excess-Rate** can be used as the pool provides.

The unit of the input is specified in the column **Metric Type**. The following value ranges apply:

- *Percent:* 0 < x < 100
- *Kbit:* 0 < x < 4294967295
- *Mbit:* 0 < x < 4294967295

Fallback to best effort

This control determines what happens to packets that cannot be sent as part of the commit rate or excess rate. If **Yes** the packets are sent via the best-effort queue, otherwise they are discarded.

Congestion action

An object from the *Congestion Action* on page 717 table is referenced here, which determines when packets are discarded because the send queues are filling up.

DSCP tags

The DSCP tags (Differentiated Services Code Point) to be assigned to this queue are entered here. Multiple values can be passed.

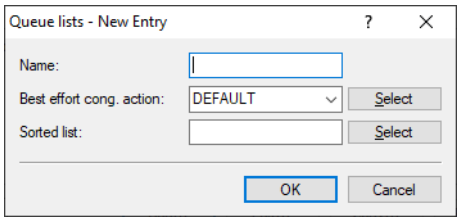
9.8.2 Queue lists

The configured **queue templates** are concatenated into a **queue list** here. This is done by a comma-separated list, with the order specifying the priority from high to low.

It is when creating a **queue list**, make sure that the **commit rates** of the **queues** do not overbook the bandwidth of the **WAN interface**. Otherwise, the low priority **queues** may be starved.

It is also important to ensure that **DSCP tags** are not assigned multiple times. If this happens, the nature of the implementation means that the tag is assigned to the lowest-priority **queue**.

Previously created queues can be found in LANconfig under **Firewall/QoS** > **QoS** > **Queue lists**.



Name

This name is used to reference the **Queue-List** from other tables. It must be unique within the table.

Best effort cong. action

This references a **Congestion action** in the Congestion action table to assign a **Congestion action** to the **Best-Effort-Queue**. By default, the DEFAULT entry is used.

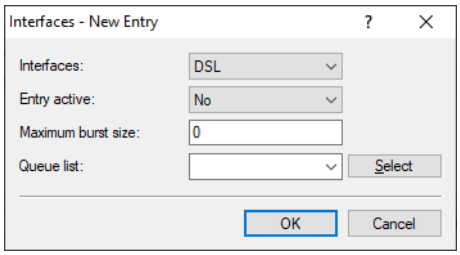
Sorted list

A comma-separated list of **queue templates** is entered here, with their priorities ranging from high to low. Up to six of your own custom **queue templates** be concatenated here, since two places are reserved for the internal **Urgent-Queue** and **Best-Effort-Queue**.

Example of a list: Gold, silver, bronze. The priority of the queues starts with gold, then silver and bronze.

9.8.3 Interfaces

In LANconfig under **Firewall/QoS** > **QoS** > **Interfaces** you link queue lists to interfaces.



Interfaces

The name of the physical **WAN interface** is entered here. The input is limited to an input set of the **WAN interfaces available on the device**.

Entry active

The configured QoS on the **WAN interface** is switched on and off here.

Maximum burst size

The Maximum Burst Size (MBS) regulates the number of bytes that can be sent within a short period (burst). This parameter ensures that massively or continuously oversubscribed traffic does not completely exhaust the available buffer resources, e.g., on upstream provider routers. The default value of 0 means that the operating system manages the parameter internally. Typically, the internal value corresponds to the MTU of the WAN connection in use. The value should be set according to the provider's specifications for the subscribed connection.

Queue list

References an entry from the queue-list table.

9.8.4 Congestion Action

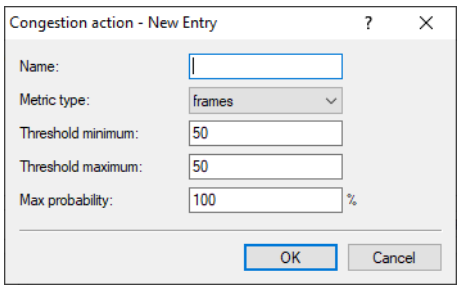
The Congestion action determines how a backed-up send queue is handled. Since this queue cannot grow indefinitely, packets must be discarded at some point. Two mechanisms are available here: Designated as **Taildrop**, **Random Early Detection (RED)**, or **Random Early Discard**. With taildrop, a limit is set beyond which all further incoming packets are discarded. In RED, two limits are determined. As of the first one, packets are discarded with a probability P. P increases the closer you get to the second limit. If the second limit is exceeded, all incoming packets are discarded, like taildrop.

The **Conjestion action** table is defined in such a way that **RED** and **Taildrop** can be configured passively. A **taildrop** can be recognized by the fact that the **threshold minimum** is equal to the **threshold maximum**. **Max-Probability** with a **Taildrop** has no purpose, but should be entered as 100 to specify that everything above the limit will be discarded.

You only specify the **Metric-Type** and **Limit-Minimum**, the other values are set so that a **Taildrop** is configured.

For a **RED**, the **Limit-Minimum** is not equal to **Limit-Maximum**. Starting from the **Limit-Minimum**, the probability of a packet being discarded is P = 0, with P linearly approaching **Max-Probability** the closer you get to the **Threshold-Max**.

In LANconfig, the limits for Congestion incidents are set under **Firewall/QoS** > **QoS** > **Congestion action**.



Name

The name of the **Congestion-Action** entered here is used to reference the entry from other tables. The name must be unique within this table.

Metric type

This specifies which metric is used by the values in columns **Commit-Rate** and **Excess-Rate**.

Threshold minimum

Specifies the lower threshold for the **Congestion action**.

Threshold maximum

Specifies the upper threshold for the **Congestion action**. From here on, all packets are discarded.

Max. probability

Specifies the maximum drop probability for a configured **RED**. Is ignored if there is a **Taildrop** and should be set to 100 there.

9.8.5 Example 1: Configuring a QoS concept with four classes

In the following example, a customer needs a router that uses a QoS concept with four QoS classes on the connection. The classes are defined as VoIP, Gold, Silver and Best Effort.

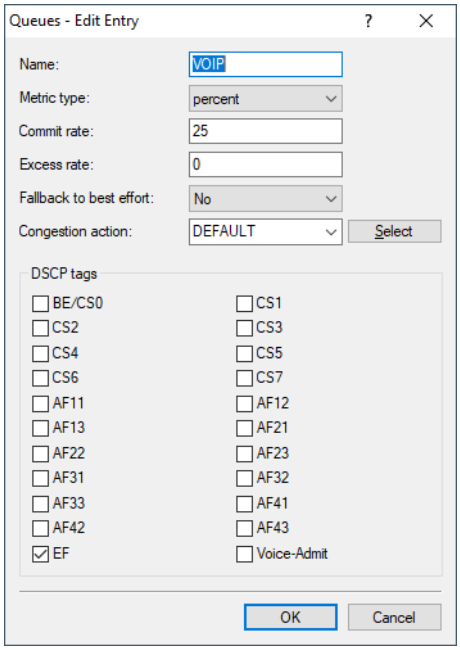
Each service class is allocated 25% of the bandwidth. The customer tags their packets using DSCP so that the packets can be assigned to the correct queue in the router.

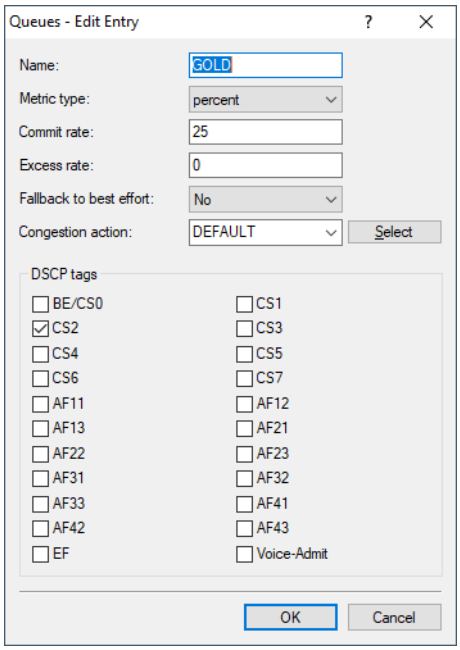
If more data is transmitted in the defined service class than there is bandwidth available, this data is discarded. A reversion to the Best Effort service class is not permitted. The definition is as follows:

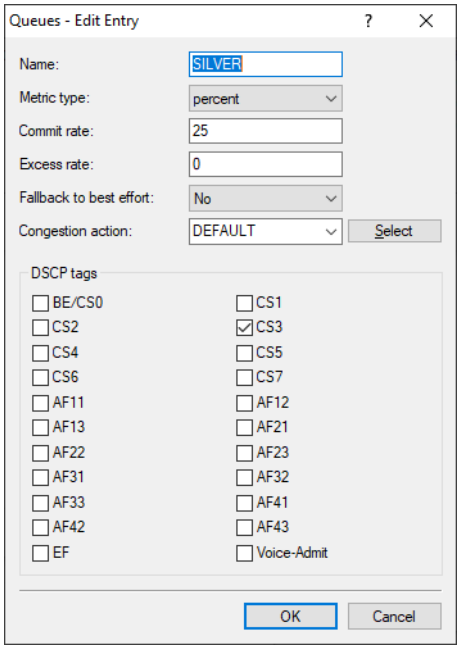
Class	DSCP
VOIP	EF
Gold	CS3
Silver	CS2
Best effort	0

1. Start LANconfig and open the configuration dialog for the device.
2. Go to the dialog **Firewall/QoS** > **QoS** > **Queues**.

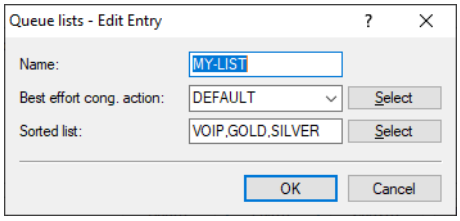
3. Create the three templates for the service classes VOIP, GOLD and SILVER. The Best Effort class does not need to be configured manually as it is present by default.



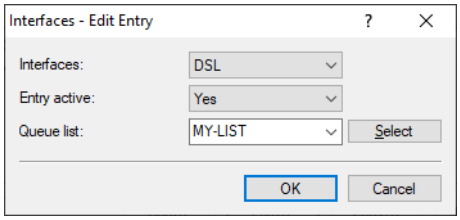




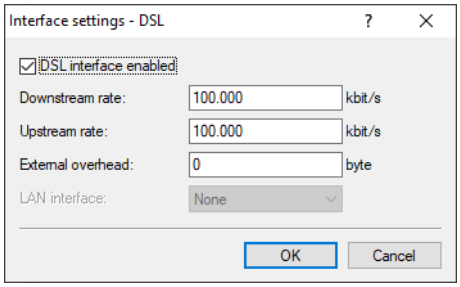
4. Switch to the dialog **Firewall/QoS** > **QoS** > **Queue lists**.
5. Create a list that specifies a strict order for the classes you create. The first class in the list has the highest priority.



6. Finally, the configured list must be assigned to a WAN interface. In this example we take DSL. Switch to the dialog **Firewall/QoS** > **QoS** > **Interfaces**.



7. (Optional): Depending on the WAN interface used, the available data rate in the case of an Ethernet connection must still be configured. This is not necessary if an internal xDSL modem is used. In this case, the synchronized DSL data rate is used. Switch to the dialog **Interfaces** > **WAN** > **Interface settings**.



The packet statistics and the distribution into the queues can be viewed on the CLI under `/status/WAN/QoS/Statistics` can be retrieved (abbreviated version here):

```
root@:/
> ls /status/WAN/QoS/Statistics

Interface  Priority    Queue-Name            Pre-Classified       DSCP-Classified       Total-Classified
=======================-------------------------------------------------------------------------------------
DSL-1      0           #urgent               0                     0                     0

DSL-1      1           VOIP                  0                     0                     0

DSL-1      2           GOLD                  0                     0                     0

DSL-1      3           SILVER                0                     0                     0

DSL-1      4           #best-effort          0                     0                     0
```

9.8.6 Example 2: Configuring a QoS concept on the VDSL connection with two QoS classes

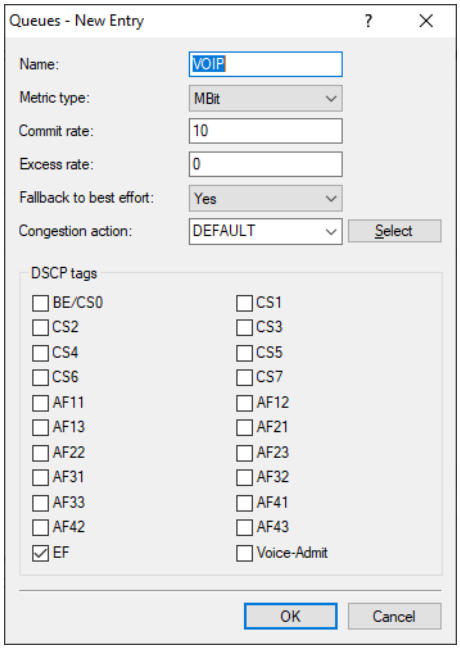
In the following example, a customer needs a router that uses a QoS concept with two QoS classes on the VDSL connection. The classes are defined as VoIP and Best Effort. The device used is a router with an internal xDSL modem.

The VoIP service class is assigned an absolute bandwidth of 10 Mbps. The customer tags their packets using DSCP so that the packets can be assigned to the correct queue in the router.

If more data is transmitted in the defined service class than there is bandwidth available, this data is assigned to the Best Effort class. The definition is as follows:

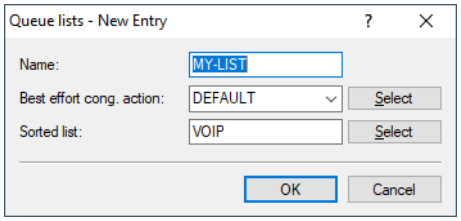
Class	DSCP
VOIP	EF

1. Start LANconfig and open the configuration dialog for the device.
2. Go to the dialog **Firewall/QoS** > **QoS** > **Queues**.
3. Create the template for the VOIP service class. The Best Effort class does not need to be configured manually as it is present by default.

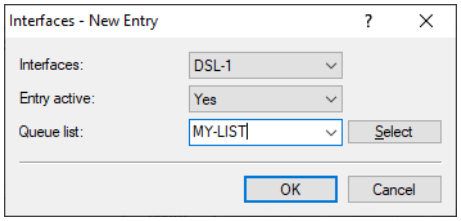


4. Switch to the dialog **Firewall/QoS** > **QoS** > **Queue lists**.

5. Create a list that specifies a strict order for the classes you create. The first class in the list has the highest priority.



6. Finally, the configured list must be assigned to a WAN interface. In this example we use DSL-1. Switch to the dialog **Firewall/QoS** > **QoS** > **Interfaces**.



The packet statistics and the distribution into the queues can be viewed on the CLI under `/status/WAN/QoS/Statistics` can be retrieved (abbreviated version here):

```
root@:/
> ls /status/WAN/QoS/Statistics

Interface  Priority    Queue-Name            Pre-Classified       DSCP-Classified       Total-Classified
=========================================================================================================
DSL-1      0           #urgent               0                     0                     0

DSL-1      1           VOIP                  0                     0                     0

DSL-1      2           #best-effort          0                     0                     0
```

9.8.7 Queue usage in the firewall

The firewall uses rules to assign packets to the queues configured in the QoS. This assignment is independent of the DSCP value in the IP header. The assignment is handled by actions that are assigned to a rule. If a rule matches an action and a session is opened in the firewall, the system checks whether the target or source interface of the session has been assigned to a queue and notes the assignment in the action. When data is flowing during the session and the action is executed, the respective packet is tagged with the assignment, is ignored by the DSCP classifier, and is counted as "Pre-Classified" in the QoS statistics for the respective queue.

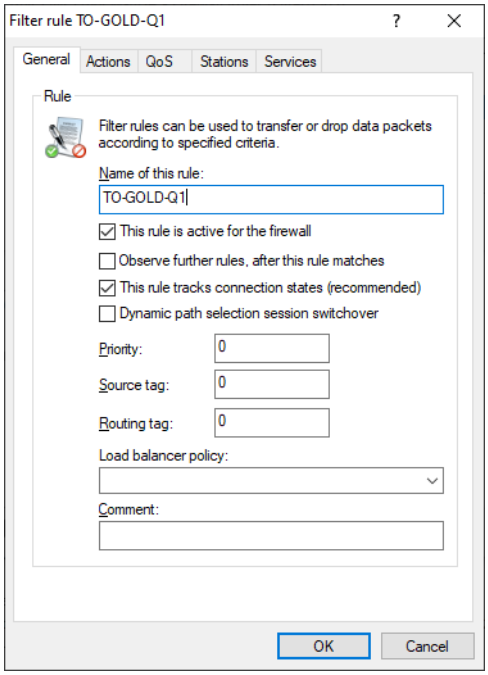
The queue assignment refers to queues that have been assigned to physical interfaces, but is inherited by interfaces stacked above them. For example, if the target interface of a session is a VPN interface, the queue assignment is passed on to the physical interface (WAN) and applied there.

Since the IPv4 and IPv6 firewalls differ in their configuration, they are listed separately below.

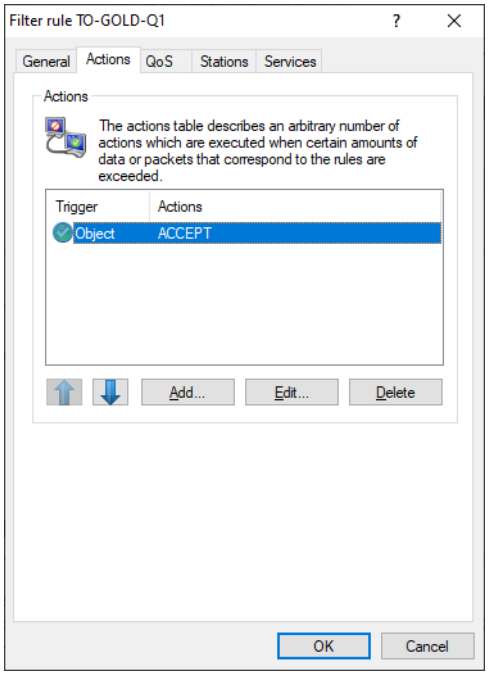
9.8.7.1 IPv4 firewall

Below is an example of the procedure for a queue assignment:

1. A queue assignment is implemented by a firewall rule, which is added under **Firewall/QoS** > **IPv4 Rules** > **Firewall rules (Filter/QoS)** > **Rules**. First, give a name to the rule on the **General** tab.

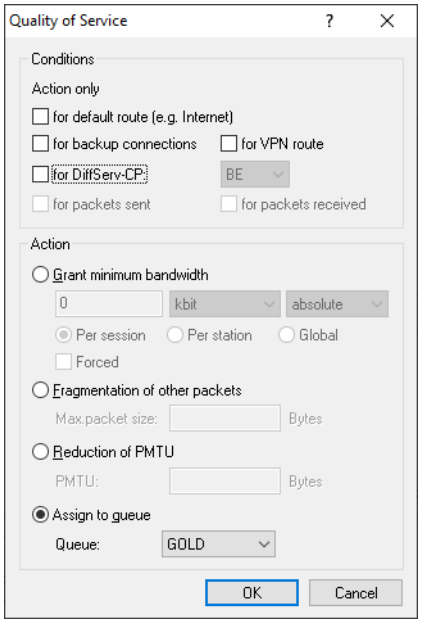


2. On the **Actions** tab you then add an "ACCEPT" action and remove the default "REJECT" action.

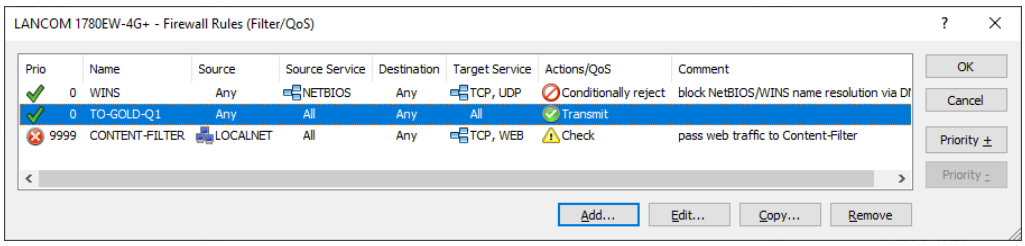


3. Next, add a new QoS object on the tab **QoS**. On the tab **General** give it a name and then assign it to the desired queue on the tab **QoS**.

The action can be restricted with conditions, for example if the assignment should only apply in a certain direction or only for a certain DSCP value.



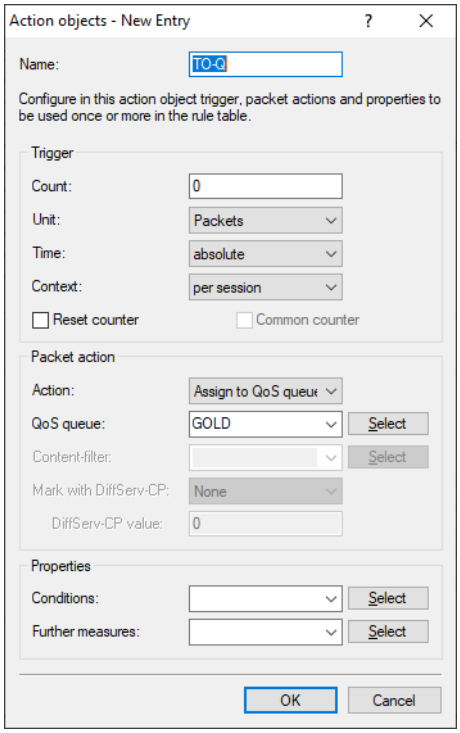
4. The result is a rule that assigns the desired packets to a queue – in this example "GOLD".



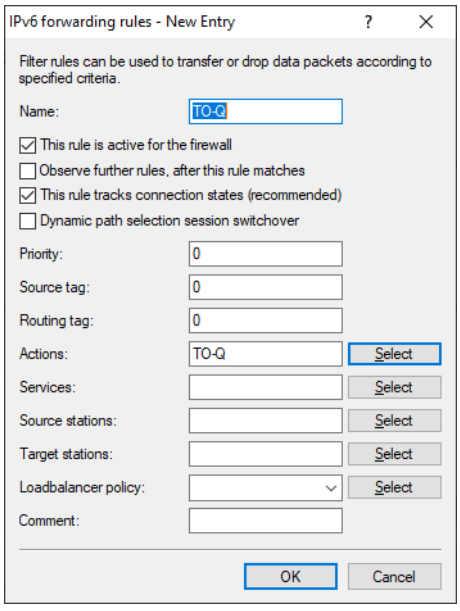
9.8.7.2 IPv6 firewall

Below is an example of the procedure for a queue assignment:

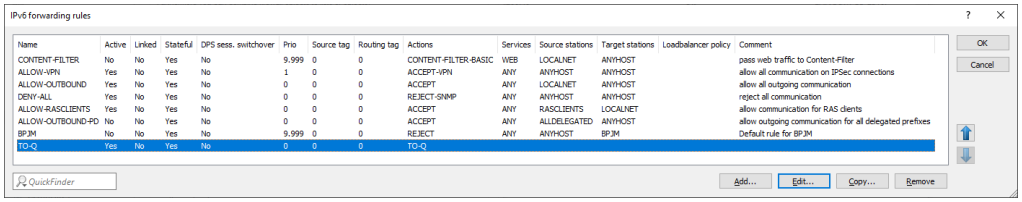
1. A queue is assigned via an action object assigned in an IPv6 forwarding rule. First, create an action object that assigns the desired queue. Do this under **Firewall/QoS** > **IPv6 Rules** > **Firewall Objects** > **Action objects**.



2. Under **Firewall/QoS** > **IPv6 Rules** > **IPv6 forwarding rules** you then create a new rule that uses this action object.



3. The result is a rule that assigns the desired packets to a queue – in this example "GOLD".



9.9 QoS for WLANs according to IEEE 802.11e (WMM/WME)

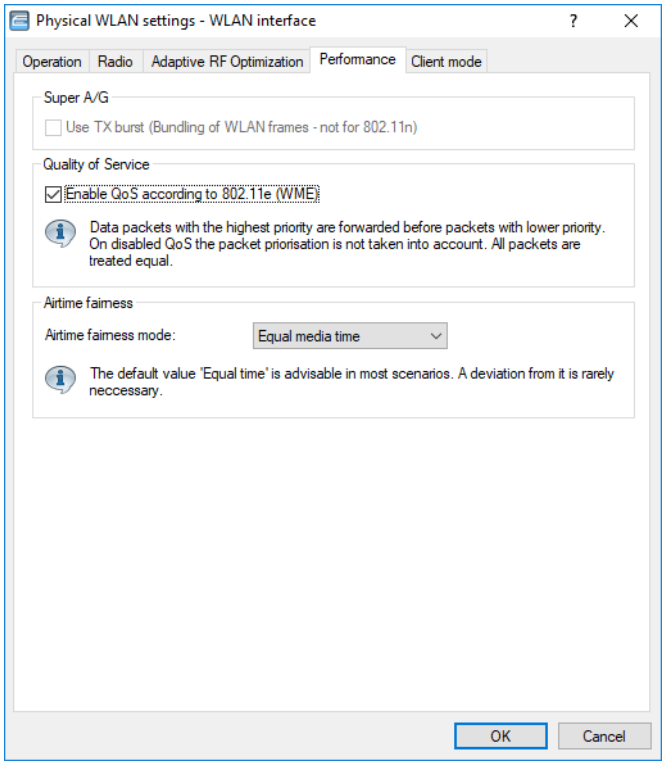
With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN).

The Wi-Fi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (Wi-Fi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization.

The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Priorities can only be set if the WLAN client and the access point both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

An access point can activate 802.11e for each of its physical WLAN networks separately.



LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Performance**

Command line: **Setup** > **Interfaces** > **WLAN** > **Performance**

10 Multicast routing

In data communication, there are four basic categories of communication relationship: Unicast, broadcast, multicast and anycast. Unicast means 1:1 communication, i.e. one sender communicates with one receiver. With a broadcast, one sender sends data to all connected devices (1:n relationship, or "one to all"). This communication method is inefficient for certain services such as IPTV, since all clients would receive the data, including clients who don't want it. This is why there is another method, multicast, for establishing sender / receiver relationships. Multicast is an efficient communication method for a sender to transmit data only to those devices that are interested in it (1:m relationship, or "one to many"). Receivers therefore have to announce their interest in receiving this data. With the communications relationship Anycast, a sender sends the data to any one receiver in a group. This chapter deals with multicast.

With multicast, there are two basic roles: Sender and receiver. A receiver is, for example, an IPTV receiver or a mobile device/PC. A sender is understood to mean the multicast source, e.g. an IPTV sender. If a client wishes to receive multicast data, e.g. an IPTV channel, it signals its interest by sending an IGMP (Internet Group Management Protocol) membership report or, with IPv6, an MLD (Multicast Listener Discovery) membership report. A multicast router will automatically generate a multicast routing entry for this group. In this instance data flow is "reversed", i.e. from the source to the receiver. If the client is no longer interested in the multicast data, it sends a membership report to leave the group.

The IP address range for multicast is defined from 224.0.0.0 to 239.255.255.255 for IPv4, and for IPv6 with the prefix FF00::/8. The multicast address range is divided into different blocks, e.g. link local, source specific multicast (232.0.0.0 to 232.255.255.255) or organization-local scope (239.0.0.0 to 239.255.255.255).

Furthermore, there are two categories of multicast: Any Source Multicast (ASM) and Source Specific Multicast (SSM). For Any Source Multicast, represented as (*,G), the receiver only specifies the multicast group G and accepts it from any source *. Any Source Multicast is the older of the two methods. Source Specific Multicast is the modern variant where a receiver requests one or more sources S as well as the desired group. However, SSM requires IGMPv3 or MLDv2. If possible, SSM should be operated with IGMPv3 as this scales better. As a rule, IPTV architectures are based on SSM.

Multicast routes are not managed in the normal (unicast) routing table, but in a separate multicast routing table. Routing entries there are not usually configured statically, but are generated dynamically by multicast routing protocols such as PIM (Protocol Independent Multicast) or by a proxy, e.g. an IGMP proxy. Multicast basically requires a functional unicast routing table, as the reverse path forward check (RPF check) checks to see whether there is a route to the multicast source. As a rule, a multicast routing protocol such as PIM is always used with a unicast routing protocol, such as OSPF.

There are three approaches to a multicast routing scenario:

1. For a simple multicast routing scenario: Use of the IGMP/MLD proxy.
2. For a complex multicast routing scenario: PIM SSM.
3. Static group entries should only be configured if clients do not support IGMP/MLD.

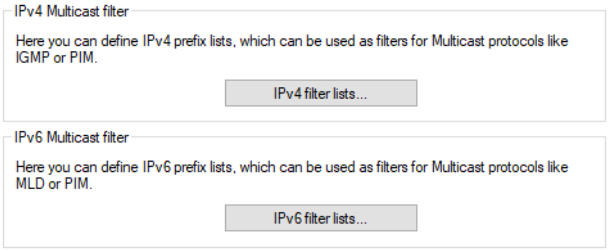
PIM Sparse Mode can also be used instead of PIM SSM, although both the role of the rendezvous point and that of the first-hop router must be performed by a third-party manufacturer directly in front of the multicast source.

10.1 General multicast show commands

- show IPv4-mfib / show IPv4-mfib (an alias is ipv4-mroute / ipv6-mroute): Displays the contents of the Multicast Forwarding Information Base/Routing Table.
- show iPv4-tib / show iPv6-tib: Displays the contents of the Tree Information Base. Contains information about the multicast group status and additional information from PIM.
- show igmp-groups: Displays information about multicast groups that the router itself has joined.

10.2 General settings

To configure the general Multicast settings, open LANconfig and go to **Multicast** > **General**.

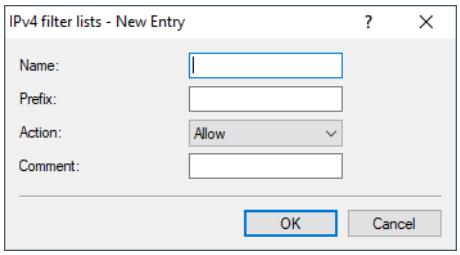


10.2.1 IPv4 filter lists

In LANconfig you configure the IPv4 filter lists for Muilticast under **Muilticast** > **General** > **IPv4 Multicast filter** using **IPv4 filter lists**.

This table can be used to specify lists of desired or unwanted IPv4 multicast addresses and prefixes. Different individual filter rules can be combined into a rules list by using the same name. A rules list can be used to prohibit or allow certain prefixes.

The names of the filter lists can be referenced in various places and managed globally using this table.



Name

Give this entry a name. A list is defined by several entries with the same name.

Prefix

Enter here the IPv4 address followed by the prefix length of the network (CIDR notation). This specifies how many most-significant bits (MSB) of the IP address are necessary for a match.

Action

Specify whether the prefixes in this filter entry should be allowed or denied.

Comment

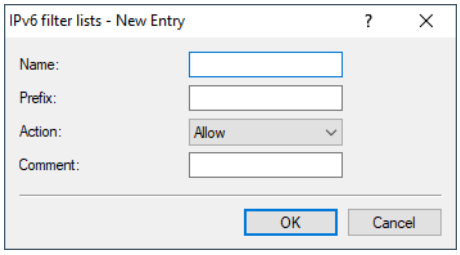
Comment on this entry.

10.2.2 IPv6 filter lists

In LANconfig you configure the IPv4 filter lists for Muilticast under **Multicast** > **General** > **IPv6 Multicast filter** using **IPv6 filter lists**.

This table can be used to specify lists of desired or unwanted IPv6 multicast addresses and prefixes. Different individual filter rules can be combined into a rules list by using the same name. A rules list can be used to prohibit or allow certain prefixes.

The names of the filter lists can be referenced in various places and managed globally using this table.



Name

Give this entry a name. A list is defined by several entries with the same name.

Prefix

Enter the IPv6 multicast address and prefix here.

Action

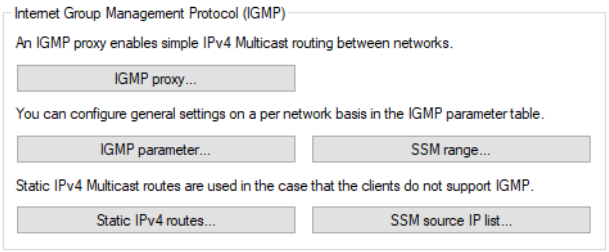
Specify whether the prefixes in this filter entry should be allowed or denied.

Comment

Comment on this entry.

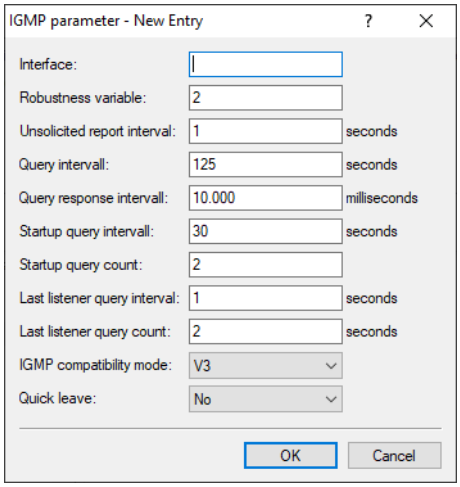
10.3 IGMP (Internet Group Management Protocol)

IGMP is configured with LANconfig under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)**.



10.3.1 IGMP parameters

In LANconfig you configure the general IGMP parameters under **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** via **IGMP parameter**.



Interface

Name of the interface that the IGMP configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv4 networks, e.g. INTRANET or IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. "VPN*".

Robustness variable

Number of IGMP message repeats. (1-10; Default: 2)

Unsolicited report interval

Specifies the time between repetitions of a host's initial report of membership in a group. (1-25 seconds; Default: 2)

Query interval

Interval between IGMP general queries. (2-99999 seconds; Default: 125)

Query response interval

Maximum response time. The maximum response time is inserted into periodic general queries. The value for the query response interval must be less than the value for query interval. (1-999999 milliseconds; Default: 10000)

Startup query interval

The interval between IGMP general queries sent after the querier starts up. (1-99998 seconds; Default: 30)

Startup query count

Number of IGMP general queries sent on startup, separated by the startup query interval. (1-10; Default: 2)

Last listener query interval

Specifies the value of the Maximum Response Time in Multicast Address-Specific Queries that are sent in response to Done messages. The parameter also specifies the time between multicast address-specific queries. (1-25 seconds; Default: 2)

Last listener query count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source. (1-10; Default: 2)

IGMP compatibility mode

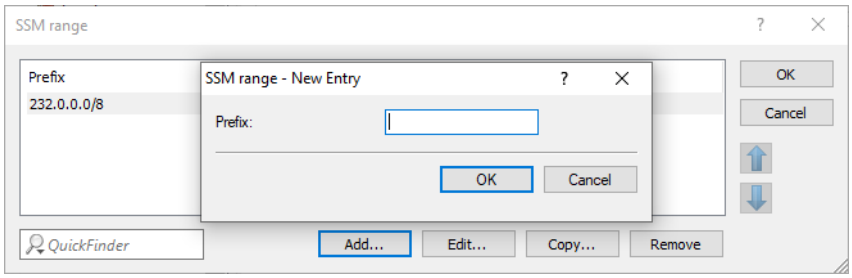
IGMP version used by the device when operating as a multicast router. Possible values: Off, V1, V2, V3. (default: V3)

Quick leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms. Possible values: Yes, No (default: No)

10.3.2 SSM range

In LANconfig you configure the SSM range under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **SSM range**.



Prefix

Specifies the IP address range in prefix notation used for SSM.

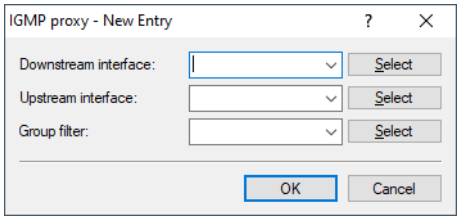
10.3.3 IGMP proxy

An IGMP proxy is typically used for Internet connections with multicast IPTV. Clients or IPTV set top boxes (STBs) on the local network send IGMP messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or IGMP proxy receives the IGMP messages and forwards them to the provider network and filters the groups, if required. The IGMP proxy works for the local network with its clients.

An IGMP proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the IGMP proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. IGMP proxies can be “cascaded” by connecting multiple routers in series.

The IGMP proxy doesn't support BiDirectional Multicast. Therefore the interfaces must not be entered crosswise in the IGMP proxy.

In LANconfig you configure the IGMP proxy under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **IGMP proxy**.



Downstream interface

Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Possible values are IPv4 networks, e.g. INTRANET, IPv4 (WAN) remotes. Also allowed are wildcard entries with * for RAS interfaces, e.g. "VPN*".

For provider-based IPTV scenarios, the local network, e.g. INTRANET, must be configured here.

Upstream interface

Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

For provider-based IPTV scenarios, the WAN remote site, e.g. INTERNET, must be configured here.

Group filter

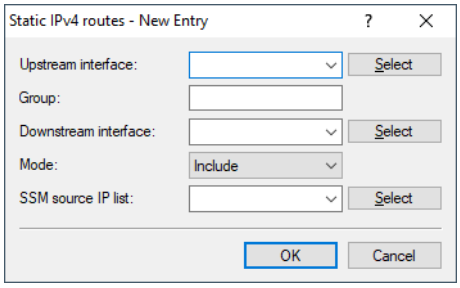
Name of the group filter that is to apply to this proxy. References the table IPv4 filter lists under **Multicast** > **General**. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

10.3.4 Static IPv4 multicast routing

Static multicast routing can be used where multicast clients do not support IGMP and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates IGMP joins and group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

In LANconfig you configure the static IPv4 multicast routes under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **Static IPv4 routes**.



Upstream interface

Interface name where the multicast packets reach the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. 239.0.0.1.

Downstream interface

Interface name where the multicast packets exit the router. Possible values are IPv4 networks, e.g. INTRANET and IPv4 (WAN) remotes.

Mode

If SSM is to be operated: This controls the way in which an IGMP membership report requests the source addresses of multicast sources. Possible values:

Include

An IGMP membership report is sent with the record type "Change to Include Mode". The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting "Include" and the SSM source IP list with an entry "ANY" will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An IGMP membership report is sent with the record type "Change to Exclude Mode". If the source list contains the entry "ANY" or "0.0.0.0", i.e. all sources are allowed, then an IGMP membership report will be sent with a join group for "any sources". If the list contains an entry other than 0.0.0.0, an IGMP membership report "block sources" is sent with the corresponding IP address.

If you want to use an SSM group with any source address, you have to link the mode "Exclude" and SSM source IP list "ANY".

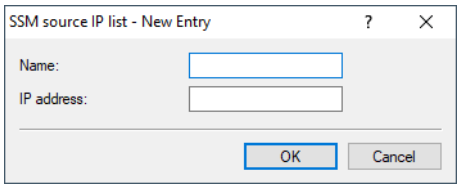
SSM source IP list

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list "ANY" can be used with the entry "0.0.0.0".

10.3.5 SSM source IP list

This table can be used to specify lists of desired or unwanted (unicast) source IP addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

In LANconfig you configure SSM source IP list under **Multicast** > **IGMP / MLD** > **Internet Group Management Protocol (IGMP)** via **SSM source IP list**.



Name

Enter a name for the entry. A list is defined by several entries with the same name.

IP address

Unicast source IPv4 address. Multicast addresses are not a valid entry at this point, since the source IP addresses of a multicast entry (S, G) are defined here.

10.3.6 Tutorial: Setting up an IGMP proxy

The following tutorial describes the steps required to set up an IGMP proxy for multicast routing.

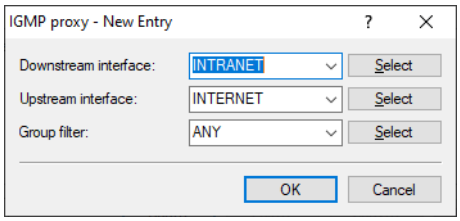
In this example, multicast clients are located in the network "INTRANET" and the multicast sources are reached via the WAN remote site "INTERNET". The IGMP proxy forwards IGMP messages from INTRANET to the INTERNET on behalf of the clients. It is also possible to filter certain multicast groups.

1. Create a new table entry under **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **IGMP proxy**:

   › **Downstream interface**: Interface name used by IGMP clients to join groups and receive IGMP messages from the proxy. Enter the name of the client network, e.g., "INTRANET".

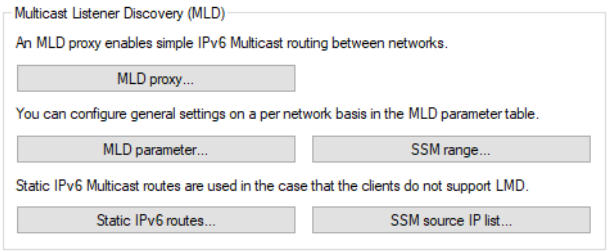
- **Upstream interface**: Interface name used by the IGMP proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Configure the name of the remote site for the Internet connection here, e.g. "INTERNET".
- **Group filter**: Name of the group filter that is to apply to this proxy. References the table **IPv4 filter lists** under **Multicast** > **General**. The group filter can be used to restrict the multicast groups available to clients. Select "ANY" to allow all multicast groups.

Further settings, for example in the firewall, are no longer necessary as of LCOS 10.40.



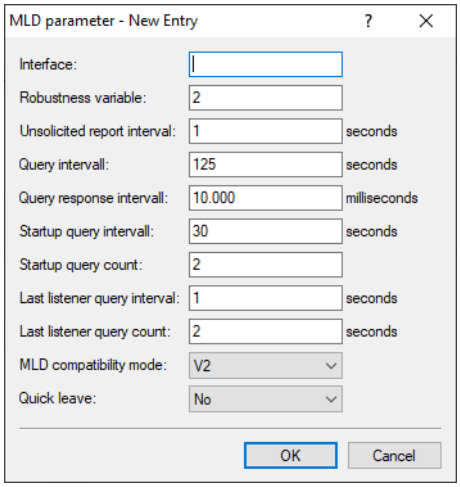
10.4 MLD (Multicast Listener Discovery)

MLD is configured with LANconfig under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)**.



10.4.1 MLD parameters

In LANconfig, you configure the general MLD parameters under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **MLD parameter**.



Interface

Name of the interface that the MLD configuration applies to. The entry named DEFAULT applies to all interfaces without a specific entry. If there is no DEFAULT entry, the internal default values for a DEFAULT entry still apply. Possible values are DEFAULT, IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or IPv6 RAS templates.

Robustness variable

Number of MLD message repeats. (1-10; Default: 2)

Unsolicited report interval

Specifies the time between repetitions of a host's initial report of membership in a group. (1-25 seconds; Default: 2)

Query interval

Interval between MLD general queries. (2-99999 seconds; Default: 125)

Query response interval

The maximum response time is inserted into periodic MLD general queries. The value for the query response interval must be less than the value for query interval. (1-999999 milliseconds; Default: 10000)

Startup query interval

The interval between MLD general queries sent after the querier starts up. (1-99998 seconds; Default: 30)

Startup query count

Number of MLD general messages on startup, separated by the startup query interval. (1-10; Default: 2)

Last listener query interval

Specifies the value of the Maximum Response Code (with IPv6) Multicast Address-Specific Queries that are sent to Done messages. The parameter also specifies the time between multicast address-specific queries. (1-25 seconds; Default: 2)

Last listener query count

Number of multicast address-specific queries sent before the router assumes that there are no more local listeners. It also specifies the number of multicast address-specific queries sent before the router assumes there are no more listeners of a particular source. (1-10; Default: 2)

MLD compatibility mode

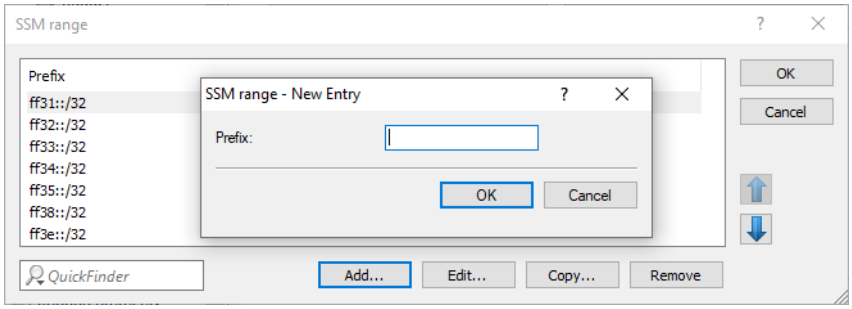
MLD version used by the device when operating as a multicast router. Possible values: Off, V1, V2 (default: V2)

Quick leave

Enables receivers to leave multicast groups quickly. This should only be used if there is only one receiver per group on the interface. Internally, the Last Listener Query Count parameter is set to 1 and the Last Listener Query Interval is set to 20 ms. Possible values: Yes, No (default: No)

10.4.2 SSM range

In LANconfig, you configure the SSM range under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **SSM range**.



Prefix

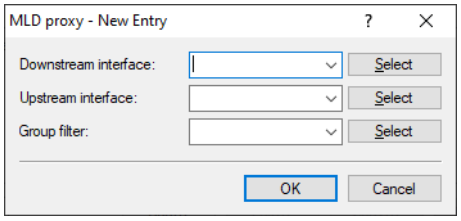
Specifies the IP address range in prefix notation used for SSM.

10.4.3 MLD proxy

An MLD proxy is typically used for multicast IPTV on IPv6 Internet connections. Clients or IPTV set top boxes (STBs) on the local network send MLD messages to receive a specific TV channel. To this end, they join certain multicast groups and later leave them again. The router and/or MLD proxy receives the MLD messages and forwards them to the provider network and filters the groups, if required. The MLD proxy works for the local network with its clients.

An MLD proxy can also be used in simple multicast routing scenarios, for example via VPN, without having to use PIM. The configuration of the MLD proxy creates a static (tree) structure without alternative paths, redundancy or loop prevention. MLD proxies can be "cascaded" by connecting multiple routers in series.

In LANconfig, you configure the MLD proxy under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **MLD proxy**.



Downstream interface

Interface name used by MLD clients to join groups and receive MLD messages from the proxy. Possible values are IPv6 networks, e.g. INTRANET, IPv6 (WAN) remotes or RAS templates.

For provider-based IPTV scenarios, the local network, e.g. INTRANET, must be configured here.

Upstream interface

Interface name used by the MLD proxy to send messages on behalf of clients. The source of the multicast messages must be reached via this interface. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

For provider-based IPTV scenarios, the WAN remote site, e.g. INTERNET, must be configured here.

Group filter

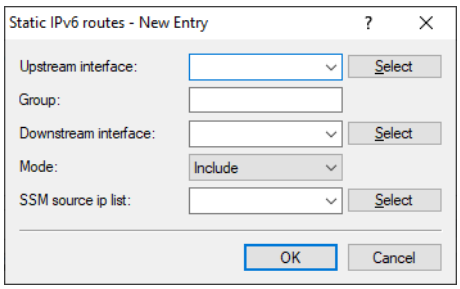
Name of the group filter that is to apply to this proxy. References the table IPv6 filter lists under **Multicast** > **General**. By default, the filter entry is blank or points to the filter list "ANY", which allows all multicast groups. The group filter can be used to restrict the multicast groups available for clients.

10.4.4 Static IPv6 multicast routing

Static multicast routing can be used where multicast clients do not support MLD and in scenarios where multicast traffic has to keep flowing even if the clients do not request to join the corresponding group. When the entry is created, the router creates MLD group reports on the upstream interface.

Please note that static multicast routing can cause high traffic and load because the multicast data is forwarded at all times.

In LANconfig you configure the static IPv6 multicast routes under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **Static IPv6 routes**.



Upstream interface

Interface name where the multicast packets reach the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Group

The static forwarding of multicast data is to be configured for this multicast group, e.g. "ff09::1".

Downstream interface

Interface name where the multicast packets exit the router. Possible values are IPv6 networks, e.g. INTRANET and IPv6 (WAN) remotes.

Mode

If SSM is to be operated: This controls the way in which an MLD membership report requests the source addresses of multicast sources. Possible values:

Include

An MLD membership report is sent with the record type "Change to Include Mode". The entries from the SSM source IP list are sent as the desired source addresses. A combination of the setting "Include" and the SSM source IP list with an entry "ANY" will not produce meaningful results and is not accepted internally as a configuration. Otherwise all source IP addresses would be rejected.

Exclude

An MLD membership report is sent with the record type "Change to Exclude Mode". If the source list contains the entry "ANY" or "::", i.e. all sources are allowed, then an MLD membership report will be sent with a join group for "any sources". If the list contains an entry other than "::", an MLD membership report "block sources" is sent with the corresponding IP address.

If you want to use an SSM group with any source address, you have to link the mode “Exclude” and SSM source IP list “ANY”.

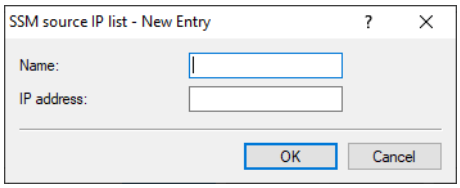
SSM source IP list

If SSM is to be operated, a list of desired sources can be specified here in addition to the multicast group. If all sources are to be allowed, the predefined list “ANY” can be used with the entry “::”.

10.4.5 SSM source IP list

This table can be used to specify lists of desired or unwanted (unicast) source IPv6 addresses. These can be referenced in various places and managed globally using this table. A list is defined by several entries with the same name.

In LANconfig you configure SSM source IP list under **Multicast** > **IGMP / MLD** > **Multicast Listener Discovery (MLD)** via **SSM source IP list**.



Name

Enter a name for the entry. A list is defined by several entries with the same name.

IP address

Unicast source IPv6 address. Multicast addresses are not a valid entry at this point, since the source IPv6 addresses of a multicast entry (S, G) are defined here.

10.5 PIM (Protocol Independent Multicast)

PIM (*RFC 7761*) enables the dynamic routing of multicast packets. Here, PIM uses routing information supplied by the unicast routing protocol operated in the router, although it does this independently of the routing protocols (e.g. RIP, OSPF or BGP).

For a PIM scenario based exclusively on LANCOM routers, only the PIM SSM (Source Specific Multicast) mode is fully supported. Operating the PIM Sparse Mode requires routers or components from third-party manufacturers. The advantage of PIM SSM is that its simpler architecture scales much better, making it ideally suited for modern multicast applications such as IPTV. PIM SSM requires IGMPv3 or MLDv2 (for IPv6) on the client side and does not need an additional rendezvous point (RP), since clients directly request not only the multicast source (S) but the desired multicast group (G) as well.

Basically, PIM SSM distinguishes between two router roles: First-hop router and last-hop router. A first-hop router is directly connected to multicast IGMP or MLD clients/receivers. A last-hop router is connected directly to the multicast source. There are also other routers located between the other two router roles. PIM must always be activated on all interfaces required to perform multicast routing. IGMP or MLD must be activated on client interfaces.

The following PIM functions are supported by the LCOS:

- PIM Sparse Mode (ASM) with external RP from a third-party manufacturer
- Static configuration of the RP in PIM Sparse Mode
- PIM SSM in the roles of last-hop router and first-hop router
- Supports IPv4 and IPv6 PIM

- SSM mapping, where PIM SSM joins are generated from IGMPv2 or MLD messages
- PIM native over IPSec VPN without GRE tunnel

The following PIM functions are not supported:

- The rendezvous point (RP) role
- Role as first-hop router for PIM Sparse, creating an automatic Register Unicast Tunnel to register a multicast source with the RP
- Dense mode, Bi-Dir mode
- Dynamic RP configuration, e.g. via Bootstrap Router (BSR) function

PIM show commands

The following show commands are available for PIM:

- PIM IPv4-Groups: Shows information about joined IPv4 multicast groups
- PIM IPv6-Groups: Shows information about joined IPv6 multicast groups
- PIM IPv4-Hello: Shows extended information about PIM neighbors and the PIM Hello-State on IPv4 interfaces
- PIM IPv6-Hello: Shows extended information about PIM neighbors and the PIM Hello-State on IPv6 interfaces
- PIM IPv4-Neighbors: Shows a short overview of PIM neighbors on IPv4 interfaces. Optionally, you can use the parameter `[-s] [--skip-own-info]` to omit the output of your own interface.
- PIM IPv6-Neighbors: Shows a short overview of PIM neighbors on IPv6 interfaces. Optionally, you can use the parameter `[-s] [--skip-own-info]` to omit the output of your own interface.

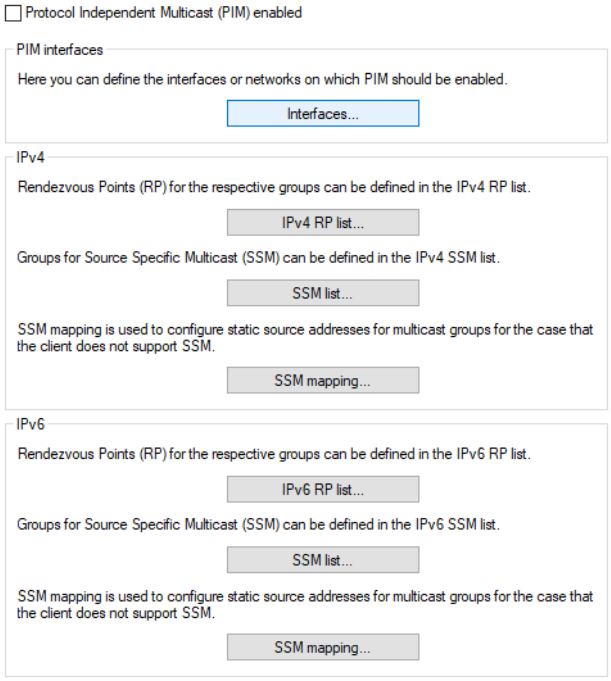
Example of the necessary configuration steps

The following configuration steps are necessary for a simple scenario with PIM SSM:

1. Activate PIM globally
2. An entry is required in the PIM interface table for every interface involved in multicast routing, including client interfaces and the source interface. You can use the default values.
3. To enable SSM, an entry must be made in the IPv4 or IPv6 SSM table. You can use the default values.

Configuration

In order to configure PIM with LANconfig, navigate to the **Multicast** > **PIM** menu.

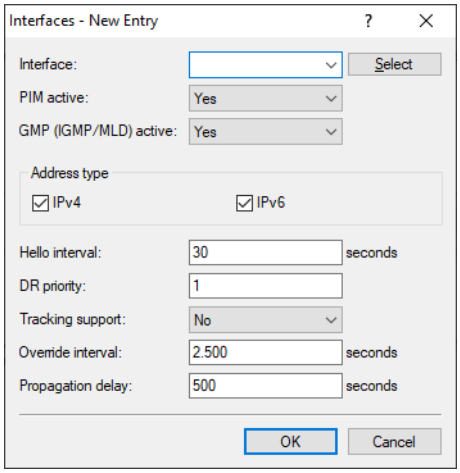


Protocol Independent Multicast (PIM) enabled

Enables or disables PIM on the device.

10.5.1 Interfaces

In LANconfig you configure the interfaces under **Multicast** > **PIM** > **PIM interfaces** using **Interfaces**. This table specifies the interfaces and logical networks where PIM is to be enabled. It also specifies the interfaces where clients can join multicast groups by means of IGMP or MLD. An entry is required in the PIM interface table for every interface involved in multicast routing, including client interfaces and the source interface.



Interface

Name of the logical interface on which PIM or a GMP (group management protocol such as IGMP or MLD) is to be activated. Possible values are IPv4 networks, e.g. INTRANET, WAN remote sites, wildcard entries with * for IPv4 RAS interfaces, for example "VPN*". Other possible values are IPv6 interfaces and IPv6 RAS templates.

PIM active

Enables PIM as well as sending and receiving PIM messages on this logical interface. If this interface is only used by IGMP/MLD clients or multicast recipients, sending and receiving PIM messages can be explicitly disabled. In this case, only GMP (IGMP/MLD) has to be activated.

GMP (IGMP/MLD) active

Enables the IGMP or MLD router role on this logical interface. In this case, IGMP or MLD joins from clients are accepted. GMP can be disabled on interfaces where the network contains no clients but only PIM neighbor routers. IGMP/MLD joins will not be accepted in this case.

Address type

Here you specify the address family for which PIM or GMP should be enabled on this interface. If necessary, you can also activate both types of address at the same time. Possible values: IPv4, IPv6

Hello interval

Sets the time in seconds between the repetition of regular PIM Hello messages. The hold time is automatically 3.5 times the PIM Hello interval and cannot be configured separately.

Possible values: 0-255 seconds, default: 30. The value 0 disables the sending of Hello messages.

DR priority

Specifies the priority as designated router (DR) in the DR election process in PIM. A higher value means a higher priority in the DR election. If several routers have the same (highest) priority, the router with the highest numeric IP address will be the DR.

Possible values: 0 bis 2^{32}, default: 1.

Tracking support

Affects the "T bit" setting in the LAN Prune Delay option in outgoing Hello messages.

Possible values: Yes, No, default: No.

Override interval

Affects the setting of the override interval field in the LAN Prune Delay option in outgoing Hello messages. Specifies the maximum delay for transmitting Override Join messages for multicast networks that have Join-Suppression enabled.

Possible values: 0 bis 2^{32}, default: 0.

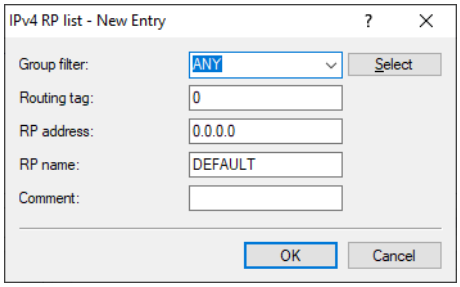
Propagation delay

Configures the setting of the Propagation Delay field in Hello messages sent for the LAN Prune Delay option. Specifies the delay for implementing a PIM prune message on the upstream routing device on a multicast network for which join suppression has been enabled.

Possible values: 250-2000 milliseconds, default: 500.

10.5.2 IPv4 RP list

In LANconfig you configure the IPv4 RP list under **Multicast** > **PIM** > **IPv4** using **IPv4 RP list**. In this table, the IPv4 rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.



Group filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

The routing tag used to reach this rendezvous point.

RP address

IPv4 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

RP name

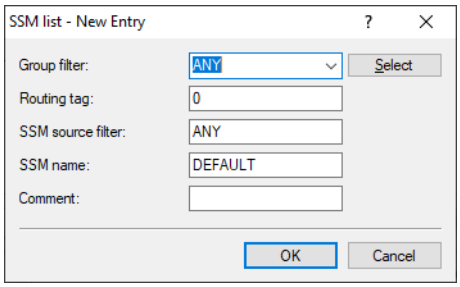
Name of the rendezvous point.

Comment

Optionally enter a meaningful comment as a description.

10.5.3 IPv4 SSM list

In LANconfig you configure the IPv4 SSM list under **Multicast** > **PIM** > **IPv4** using **SSM list**. This table configures the parameters for PIM SSM (Source Specific Multicast) mode.



Group filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **SSM source IP list**.

SSM name

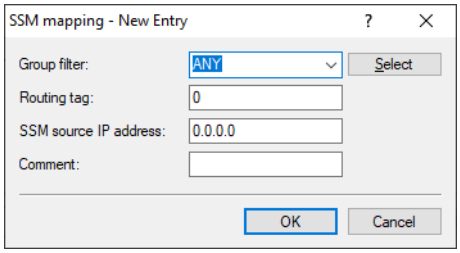
Name of this SSM configuration.

Comment

Optionally enter a meaningful comment as a description.

10.5.4 IPv4 SSM mapping

In LANconfig you configure the IPv4 SSM mapping under **Multicast** > **PIM** > **IPv4** using **SSM mapping**. In this table, IPv4 multicast source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses (S) in received IGMP messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.



Group filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the table **Multicast** > **General** > **IPv4 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source IP address

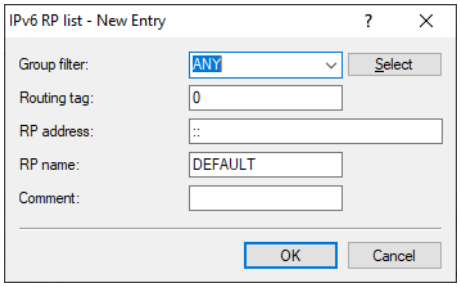
Specifies a source IPv4 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Comment

Optionally enter a meaningful comment as a description.

10.5.5 IPv6 RP list

In LANconfig you configure the IPv6 RP list under **Multicast** > **PIM** > **IPv6** using **IPv6 RP list**. In this table, the rendezvous points (RPs) and their associated multicast groups are configured for PIM sparse mode.



Group filter

Specifies the multicast groups for which the rendezvous points should be responsible. Addresses that match the group filter are managed by this rendezvous point. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

The routing tag used to reach this rendezvous point.

RP address

IPv6 address of the external rendezvous point. The device itself does not support the role of a rendezvous point.

RP name

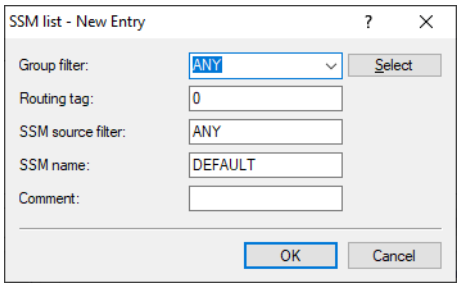
Name of the rendezvous point.

Comment

Optionally enter a meaningful comment as a description.

10.5.6 IPv6 SSM list

In LANconfig you configure the IPv6 SSM list under **Multicast** > **PIM** > **IPv6** using **SSM list**. This table configures the parameters for PIM IPv6 SSM (Source Specific Multicast) mode.



Group filter

Specifies the multicast groups to which this SSM configuration applies. Addresses that match the group filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source filter

Specifies the SSM source filter for this table entry. Multicast source addresses that match the SSM source filter will be applied to this SSM configuration. References a filter list from the table **Multicast** > **IGMP/MLD** > **Internet Group Management Protocol (IGMP)** > **SSM source IP list**.

SSM name

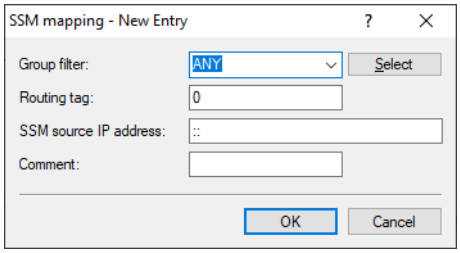
Name of this SSM configuration.

Comment

Optionally enter a meaningful comment as a description.

10.5.7 IPv6 SSM mapping

In LANconfig you configure the IPv6 SSM mapping under **Multicast** > **PIM** > **IPv6** using **SSM mapping**. In this table, IPv6 source addresses (S) can be configured to be automatically inserted into PIM join messages if there are no source addresses in received MLD messages. As a result, the router automatically supplements (*,G) entries to be (S,G) entries.



Group filter

SSM mapping is performed for the multicast groups (G) specified here. References a filter list from the table **Multicast** > **General** > **IPv6 filter lists**.

Routing tag

Routing tag to which this configuration applies.

SSM source IP address

Specifies a source IPv6 address (S) that is automatically inserted into the (*,G) entries of PIM join messages to produce (S,G) entries.

Comment

Optionally enter a meaningful comment as a description.

10.6 Further Multicast Protocols

10.6.1 Bonjour proxy

Apple Bonjour allows devices to discover and operate certain approved services automatically and without prior configuration. This procedure is also known as "Zero Configuration Networking" (ZeroConf).

The most popular services include, among others:

- Printer services (with or without Apple Airprint support)
- File services (folder or file shares)
- Apple Airplay

› iTunes

10.6.1.1 Bonjour basics

Bonjour exchanges information by means of individual multicast DNS packets (mDNS) according to *RFC 6762* and DNS-based service discovery (DNS-SD) according to *RFC 6763*. The clients exchange Bonjour information via the multicast address `224.0.0.251` (IPv4) or `ff02::fb` (IPv6) on port 5353. Bonjour packets are not routed (multicast packet, TTL = 1), which limits their use to the current local area network.

Please note that the Bonjour proxy only serves to aid the discovery of Bonjour services. The actual routing between the communicating parties requires a separate configuration or restriction by means of, for example, routing or firewall entries.

It is often impractical to provide all services on a single network. This is why larger networks are often divided into several subnets. However, Bonjour is unable to operate in this situation.

Example application with two networks

At a school, students use a dedicated IP network to access the WLAN. In parallel to this, the local printer is made available on a second internal IP network. In principal, the appropriate routing and restrictions would make it possible for students to use their smartphones to access the local internal printer. However, because mDNS is only defined as link-local, Bonjour is unable to help students to discover the printer with their smartphones. The LANCOM Bonjour proxy mediates between two networks, which enables students to discover printers in other networks.

Basically, there are two ways of realizing such a scenario:

Multicast routing

A router forwards the search queries and service advertisements between the two networks.

This option causes unnecessary traffic, which makes it rather inefficient.

Caching of services

The router stores discovered mDNS service advertisements in its local cache. A router that receives an mDNS query then responds on behalf of the original service. Before processing the advertisement and before transmitting anything from the cache, the router checks its policies to see whether the service is approved or blocked. The policies are used to control which services are approved for discovery and between which networks.

Please note that reading out the mDNS cache content with the SNMP protocol is not supported.

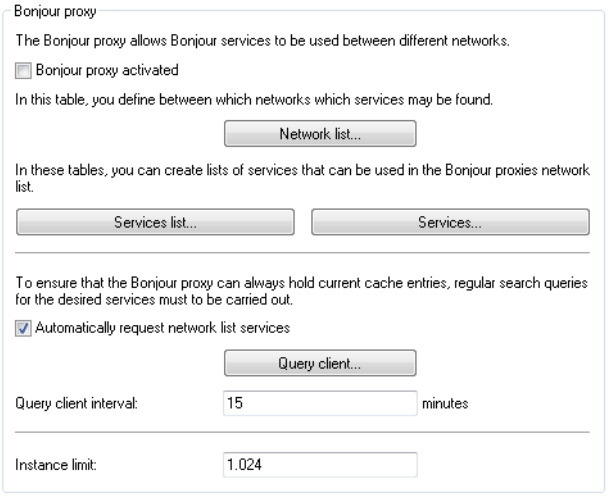
The Bonjour proxy supports an mDNS query client, which at set time intervals queries an interface about the services of interest. This query keeps the cache entries for approved services up to date. In order for the cache to be up-to-date at all times, it is useful to enable automatic searches for services that are permanently available (e.g. print services).

If no automatic queries about frequently used services are configured, the Bonjour proxy may be unable to respond to the corresponding queries even though the services are approved.

Bonjour proxies only operate on logical LAN / WLAN interfaces or on logical networks with an IP address. WAN interfaces / remote sites or tunnels (except for WLC L3 tunnels) and VLANs without address binding are not supported.

10.6.1.2 Configuration with LANconfig

The Bonjour proxy is configured with LANconfig under **Multicast** > **Bonjour**.



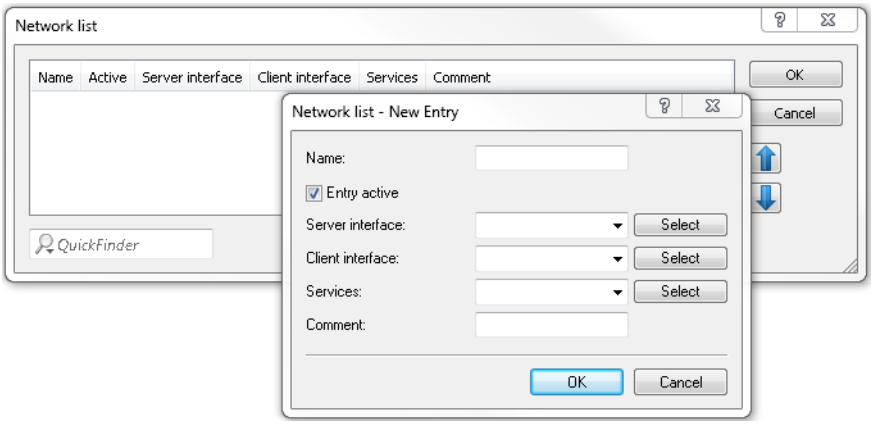
The following settings are available:

Bonjour proxy activated

Use this checkbox to enable or disable the Bonjour proxy.

Network list

Use this table to specify the networks between which Bonjour services may be discovered. To function properly, the networks or interfaces need to be configured with an IPv4 or IPv6 address. This table offers you the following options:



Name

Specify a unique name for this table entry.

Entry active

Enable or disable this table entry.

Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

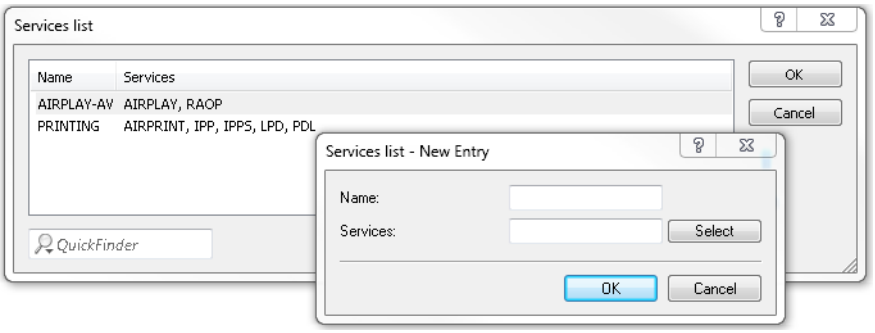
Comment

Enter a comment about this table entry.

Services list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

The following settings are available:



Name

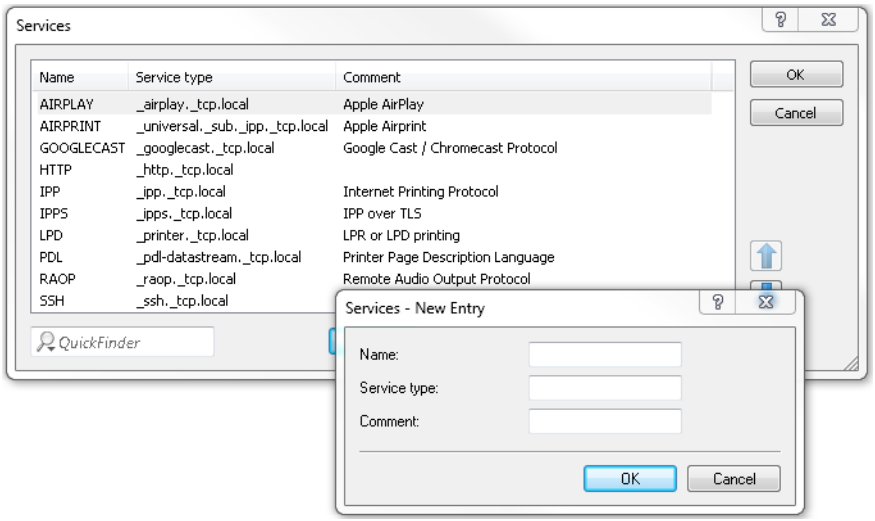
Specify a unique name for this table entry.

Services

Enter a comma-separated list of services that are to be available for use in the **Services** table.

Services

This table is used to specify the Bonjour service types that can be used in the services list. Additional settings are available as follows:



Name

Specify a unique name for this table entry.

Service type

Specify the Bonjour service type as a DNS SRV record, e.g. with `_http._tcp.local`.

Comment

Enter a comment about this table entry.

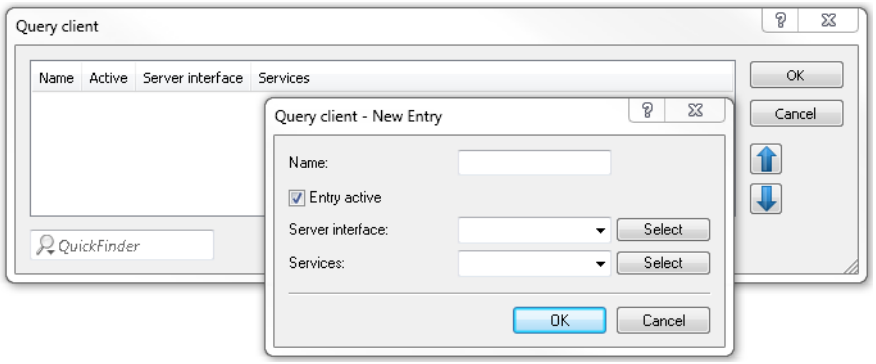
Automatically request network list services

With this item enabled, the device sends regular queries about which services (as specified in the network list) are available from the corresponding server interface. This option is enabled by default. This setting is also recommended.

If this setting is disabled, you need to manually enter the services to be queried into the **Query client** table.

Query client

To keep the Bonjour proxy services cache up-to-date all times, you need to configure regular queries about the desired services. The query client regularly contacts the configured service types for information about their availability.



Name

Specify a unique name for the corresponding entry.

Entry active

Activates or deactivates this table entry.

Server interface

Set an IPv4 network name or an IPv6 interface name that is to offer the Bonjour services (e.g. print services) and which will regularly be used by the router to make the queries.

Services

This references an entry in the list of services. These services are regularly queried by the router at the server interface. This entry may not be empty.

Query client interval

Set the interval in minutes in which the query client updates the Bonjour services configured in the **Query client** table. 15 minutes are defined by default.

Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

11 Virtual Private Networks – VPN

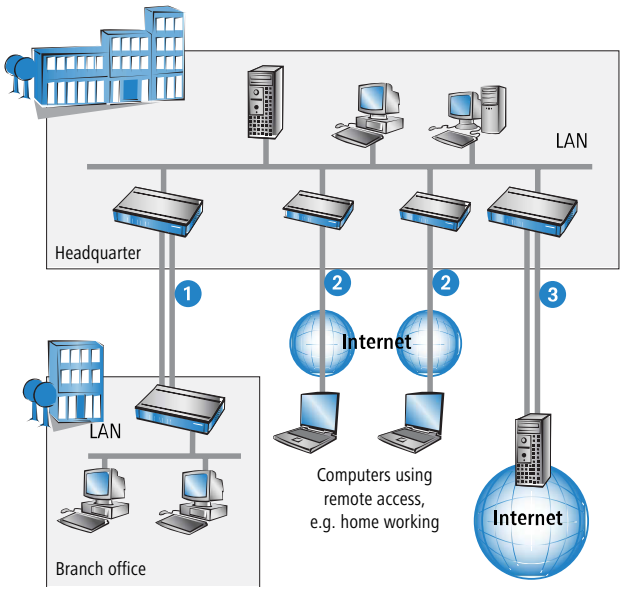
11.1 What does VPN offer?

A VPN (Virtual Private Network) can be used to set up cost-effective, public IP networks, for example via the Internet.

While this may sound unspectacular at first, in practice it has profound effects. To illustrate this, let's first look at a typical corporate network without VPN technology. In the second step, we will see how this network can be optimized by the deployment of VPN.

11.1.1 Conventional network infrastructure

First, let's have a look at a typical network structure that can be found in this form or similar forms in many companies:



The corporate network is based on the internal network (LAN) in the headquarters. This LAN is connected to the outside world in three ways:

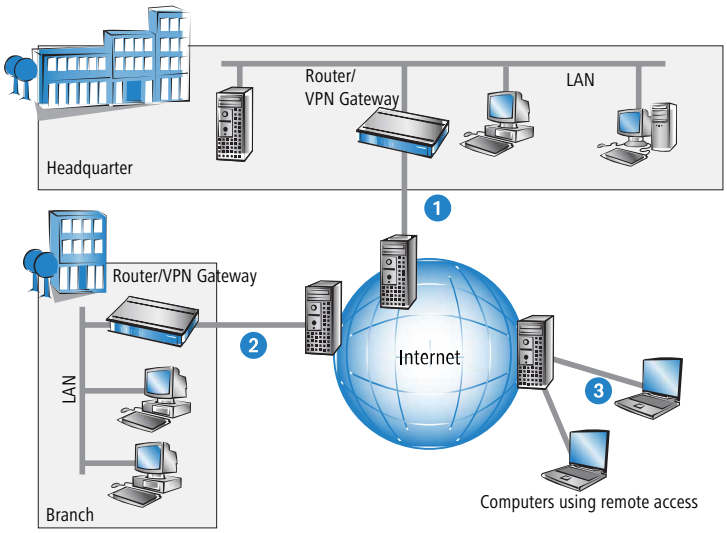
1. A subsidiary is connected to the LAN, typically using a leased line.
2. Computers dial into the central network via the Internet (Remote Access Service – RAS).
3. The central LAN has a connection to the Internet so that its users can access the Web, and send and receive e-mail.

All connections to the outside world are based on dedicated lines, i.e. switched or leased lines. Dedicated lines are very reliable and secure. On the other hand, they involve high costs. In general, the costs for dedicated lines are dependent on the distance. Especially in the case of long-distance connections, keeping an eye out of cost-effective alternatives can be worthwhile.

The appropriate hardware must be available in the headquarters for every type of required connection. In addition to the original investment costs, ongoing costs are also incurred for the administration and maintenance of this equipment.

11.1.2 Networking via the Internet

The following structure results when using the Internet instead of direct connections:



All participants have fixed or dial-up connections to the Internet. Expensive dedicated lines are no longer needed.

1. All that is required is the Internet connection of the LAN in the headquarters. Special switching devices or routers for dedicated lines to individual participants are superfluous.
2. The subsidiary also has its own connection to the Internet.
3. The RAS PCs connect to the headquarters LAN via the Internet.

The Internet is available virtually everywhere and typically has low access costs. Significant savings can thus be achieved in relation to switched or dedicated connections, especially over long distances.

The physical connection no longer exists directly between two participants; instead, the participants rely on their connection to the Internet. The access technology used is not relevant in this case: ideal is the use of broadband technologies such as DSL (Digital Subscriber Line) in combination with flatrate contracts.

The technologies of the individual participants do not have to be compatible to one another, as would be the case for conventional direct connections. A single Internet access can be used to establish multiple simultaneous logical connections to a variety of remote sites.

The resulting savings and high flexibility makes the Internet (or any other IP network) an outstanding backbone for a corporate network.

Two technical properties of the IP standard speak against using the Internet as a part of a corporate network, however:

- The necessity of public IP addresses for all participants
- The lack of data security of unprotected data transfers

11.1.3 Private IP addresses on the Internet?

The IP standard defines two types of IP addresses: Public and private. A public IP address is valid worldwide, while a private IP address only applies within a closed LAN.

Public IP addresses must be unique on a worldwide basis. Private IP addresses can occur any number of times worldwide; they must only be unique within their own closed network.

Normally, PCs in a LAN only have private IP addresses, while the router to the Internet also has a public address. All PCs behind this router have access to the Internet via its public IP address (IP masquerading). In such a case, only the router

itself is responsive via the Internet. PCs behind the router are not responsive to the Internet without intervention by the router.

11.1.3.1 Routing at the IP level with VPN

IP connections must be established between routers with public IP addresses in order to link networks via the Internet. These routers provide the connections between multiple subnetworks. When a computer sends a packet to a private IP address in a remote network segment, the local router forwards the packet to the router of the remote network segment via the Internet.

The "encapsulation" of data packets with private IP addresses inside packets with public IP addresses is handled by the VPN gateway. Without VPN, computers without public IP addresses would not be able to communicate with one another via the Internet.

11.1.4 Secure communications via the Internet?

The idea of using the Internet for corporate communications has been met with skepticism. The reason for this is that the Internet lies beyond a company's field of influence. Unlike dedicated connections, data on the Internet travels through the network structures of third parties that are frequently unknown to the company.

In addition, the Internet is based on a simple form of data transfer using unencrypted data packets. Third parties can monitor and perhaps even manipulate the contents of these packets. Anyone can access the Internet. As a result, third parties may gain unauthorized access to the transferred data.

11.1.4.1 VPN – Security through encryption

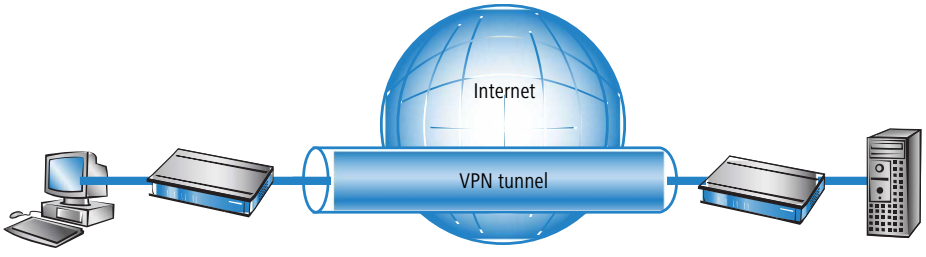
VPN was developed as a solution to this security problem. If necessary, it can encrypt the complete data communications between two participants. The packets are then unreadable for third parties.

The latest and most secure encryption technologies can be used for VPN. A very high level of security can thus be reached. VPN-protected data traffic via the Internet offers a degree of security that at least corresponds to that of dedicated lines.

Codes usually referred to as "keys" are agreed upon between the participants and used for data encryption. Only the participants in the VPN know these keys. Without a valid key, it is not possible to decrypt the data. They thus remain "private", inaccessible to unauthorized parties.

11.1.4.2 Send your data through the tunnel – for security's sake

This also explains the nature of a virtual private network: A fixed, physical connection between the devices of the type required for a direct connection does not exist at any time. Rather, the data flows via suitable routes through the Internet. With the proper technology, third parties can monitor and even record data traffic. As the packets are encrypted by VPN, the actual content of the packets is inaccessible. Experts compare this state to a tunnel: it's open at either end, but perfectly shielded in between. Secure connections within public IP networks are thus also referred to as "tunnels".

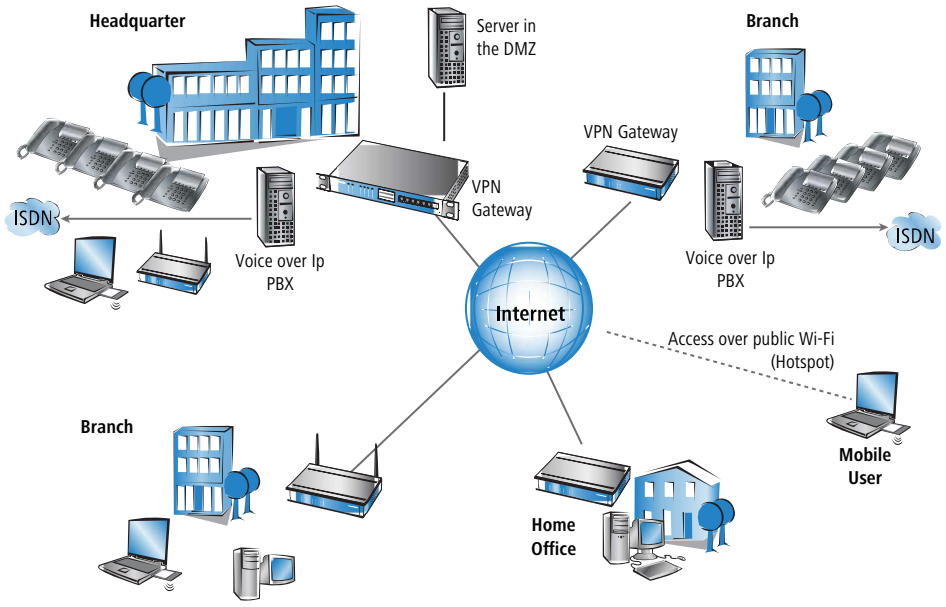


The goal of modern network structures has thus been achieved: secure connections via the largest and most low-cost public IP network, the Internet.

11.2 The VPN module at a glance

11.2.1 VPN example application

VPN connections are used in many different fields of application. In most cases, a variety of communications technologies is used for transferring both data and audio, and VPN unites these systems into an integrated network. The following example illustrates a typical application that is often used in practice.



The principal components and features of these applications:

- The connectivity of networks, for example between headquarters and a branch office
- Connecting external locations without fixed IP addresses via VPN router
- Connecting home offices without fixed IPs
- Connection to Voice-over-IP PBX systems
- Connecting mobile users, for example when using public WLAN access

11.2.2 Functions of the VPN module

This section lists all of the functions and properties of the LCOS VPN module. Experts of the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the VPN, this information is non-essential.

- VPN tunnel via leased lines, switched connections and IP networks
- VPN in accordance with IPSec standard
- IPSec in tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, hash length 128 bits
  - HMAC-SHA-1-96, hash length 160 bits
  - HMAC-SHA-1-256, hash length 256 bits
  - HMAC-SHA-1-384, hash length 384 bits
  - HMAC-SHA-1-512, hash length 512 bits

- Key management as per ISAKMP (IKEv1, IKEv2)
- Symmetrical encryption methods
  - AES, key lengths of 128, 192 and 256 bits
  - Triple-DES (3DES), key length 168 bit
- IKEv1 main and aggressive mode
- IKEv1 / IKEv2 config mode
- IKEv1 with pre-shared keys and IKEv2
- IKEv1 and IKEv2 with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with the following DH groups:
  - DH-1 (768-bit modulus)
  - DH-2 (1024-bit modulus)
  - DH-5 (1536-bit modulus)
  - DH-14 (2048-bit modulus)
  - DH-15 (3072-bit modulus)
  - DH-16 (4096-bit modulus)
  - DH-19 (256-bit random ECP group)
  - DH-20 (384-bit random ECP group)
  - DH-21 (521-bit random ECP group)
  - DH-28 (brainpoolP256r1)
  - DH-29 (brainpoolP384r1)
  - DH-30 (brainpoolP512r1)

11.3 VPN connections in detail

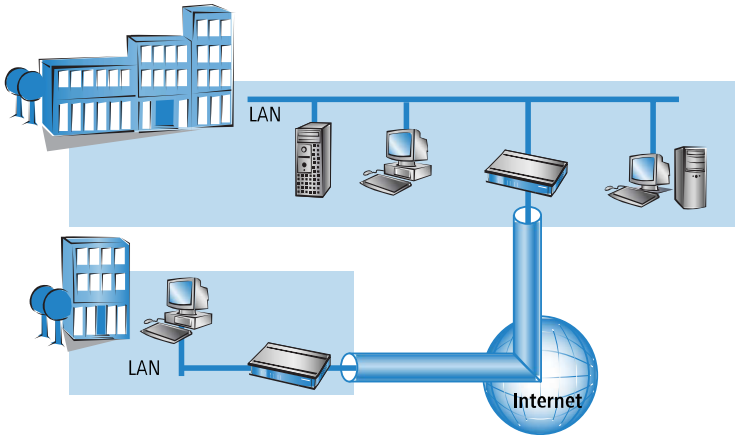
Two types of VPN connections are available:

- VPN connections linking two local networks. This type of connection is also known as a “LAN-LAN link”.
- The connection of an individual computer with a network, generally via a dial-in connection (Remote Access Service – RAS).

11.3.1 LAN-LAN links

The connectivity of two remote networks is known as a “LAN-LAN connectivity”. With such a connection, the devices in one LAN can access those of the remote LAN (assuming they have the necessary access rights).

In practice, LAN-LAN links are frequently used between company headquarters and subsidiaries, or for connections to partner companies.



A VPN-enabled router (VPN gateway) is located at either end of the tunnel. The configuration of both VPN gateways must be matched to one another.

The connections are transparent for the remaining devices in the local networks, i.e., they appear to have a direct connection. Only the two gateways must be configured for the VPN connection.

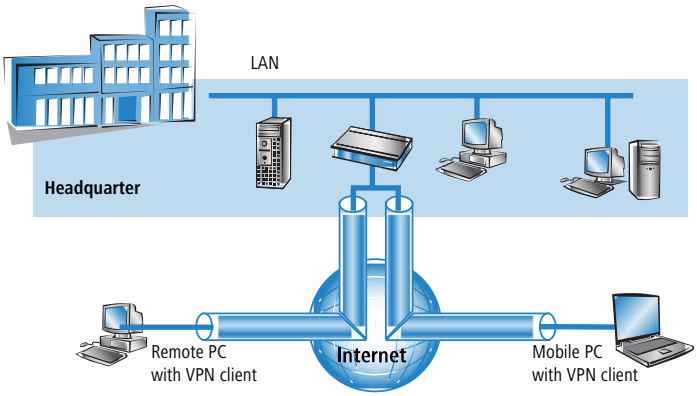
11.3.1.1 Internet access in parallel

The Internet access for VPN can be used simultaneously for other Internet applications, such as web-browsing or e-mail. For security reasons, the parallel Internet access may be unwanted in some cases. For instance, if a branch office should be enforced to access the Internet only via a central firewall. For such applications the parallel Internet access can be disabled as well.

11.3.2 Dial-in connections (Remote Access Service)

Individual remote computers (hosts) can access the resources of the LAN via dial-up connections. Practical examples of this are employees working from home or field staff that dial into the company network.

If the dial-up connection of an individual computer to a LAN is to be realized via VPN, that computer first connects to the Internet. A special VPN client software then sets up a tunnel to the VPN gateway of the LAN using this Internet connection.



The VPN gateway of the LAN must support the establishment of VPN tunnels with the VPN client software of the remote PC.

11.4 What is LANCOM Dynamic VPN?

LANCOM Dynamic VPN is a technology which permits VPN tunnels to be connected even to remote sites that do not have a static IP address, but a dynamic one instead.

Who needs LANCOM Dynamic VPN and how does it work? We will answer this question in two steps: First, a look at the basics of IP addressing will show the problem of dynamic IP addresses. The second step shows the solution thereof with LANCOM Dynamic VPN.

11.4.1 A look at IP addressing

Every participant on the Internet needs an IP address. Participants even need a special kind of IP address - a public one. The administration of public IP addresses is handled from central locations in the Internet. Each public IP address may only occur once on the entire Internet.

Local IP-based networks do not use public, but private IP addresses. For this reason, a number of address ranges within the entire IP address range have been reserved for private IP addresses.

A computer connected to both a local network and directly to the Internet therefore has two IP addresses: a public one for communication with the rest of the Internet and a private one by which the computer can be reached within the local network.

11.4.1.1 Static and dynamic IP addresses

Public IP addresses must be applied for and managed, which involves costs. There is also only a limited number of public IP addresses. For this reason, not every Internet user has his or her own fixed (static) IP address.

The alternative to static IP addresses are the so-called dynamic IP addresses. A dynamic IP address is assigned to an Internet user by the Internet Service Provider (ISP) upon dialing-in, and remains valid for the duration of the connection. The ISP takes an unused address selected at random from their pool of IP addresses. This IP address is only temporarily assigned to the user for the duration of a given connection. When the connection is ended, the IP address is once again free and the ISP can assign it to another user.



Many flatrate connections, too, are realized with via dynamic IP addresses. Every 24 hours or so, the connection is forcibly interrupted. The new connection is generally assigned with a new and different IP address.

11.4.1.2 Advantages and disadvantages of dynamic IP addresses

This process has a very important advantage for ISPs: they only need relatively small pools of IP addresses. Dynamic IP addresses are also favorable for users: it's not necessary for them to apply for static IP addresses in advance - they can connect to the Internet immediately. It's also not necessary for them to manage IP addresses. This saves trouble and costs. The other side of the coin: A user without a static IP address cannot be addressed directly from the Internet.

This is a major problem when setting up VPNs. If, for example, Computer A would like to communicate with Computer B using a VPN tunnel on the Internet, Computer A needs the remote computer's IP address. If B only has a dynamic address, A cannot know that address and therefore cannot contact B.

The LANCOM Dynamic VPN offers the answer here.

11.4.2 This is how LANCOM Dynamic VPN works

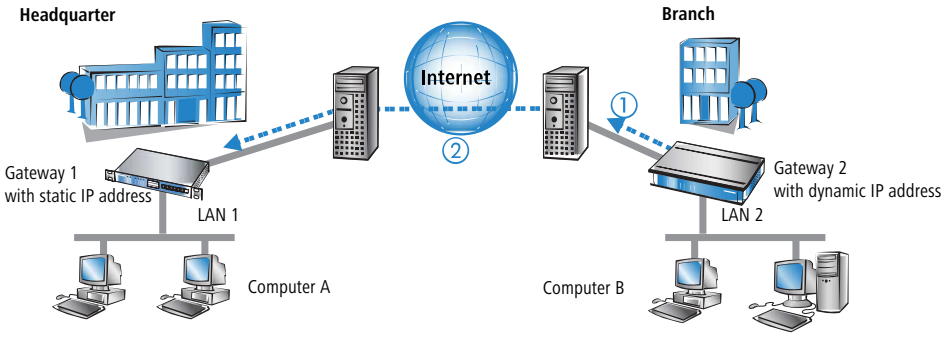
Let us illustrate how LANCOM Dynamic VPN works using the following example (designations refer to the IP address type of the two VPN gateways):

- Dynamic – static

11.4.2.1 Dynamic – static

If a user on computer B in LAN 2 wishes to connect to computer A in LAN 1, then gateway 2 receives a request and tries to establish a VPN tunnel to gateway 1. Gateway 1 has a static IP address and can be directly contacted over the Internet.

A problem arises in that the IP address from gateway 2 is assigned dynamically, and gateway 2 must communicate its current IP address to gateway 1 when attempting to connect. In this case, LANCOM Dynamic VPN takes care of transmitting the IP address during connection establishment.



1. Gateway 2 connects to the Internet and is assigned a dynamic IP address.
2. Gateway 2 contacts Gateway 1 via its known public IP address. LANCOM Dynamic VPN enables the identification and transmission of the actual IP address of Gateway 2. Gateway 1 then initiates the VPN tunnel.

The main advantage here: Rather than the "Aggressive Mode" that is normally used when connecting VPN clients to the headquarters, the far more secure "Main Mode" can be applied instead. Main Mode exchanges significantly more unencrypted messages during the IKE handshake than the Aggressive Mode.

The dynamic end communicates its IP address encrypted via the Internet protocol ICMP (or alternatively via UDP).

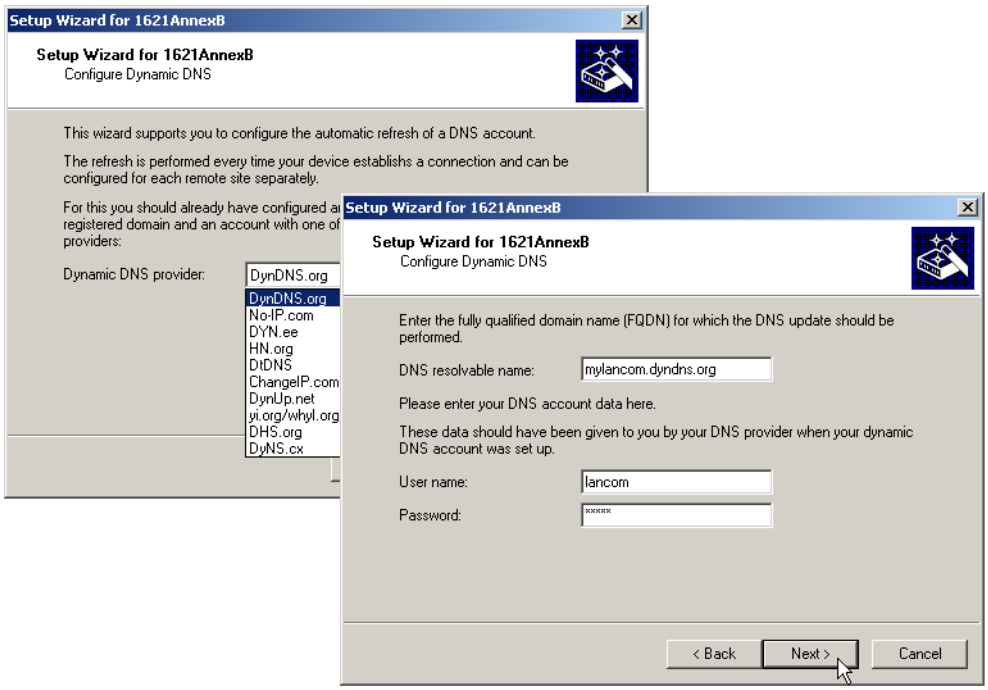
11.4.2.2 Dynamic IP addresses and DynDNS

It is also possible to establish a connection between two stations using dynamic IP addresses by using so-called dynamic DNS services (DynDNS). The address of the tunnel end-point is not defined as an IP number (which is, of course, dynamic and subject to frequent change) but as a static name instead (e.g. MyDevice@DynDNS.org).

Two things are needed for translating a name to its current IP address: A dynamic DNS server and a dynamic DNS client:

› The first, available from numerous providers in the Internet, is a server that is in communication with Internet DNS servers.

- The dynamic DNS client is integrated in the device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP address for the DNS name translation. This can be set up very conveniently with a Wizard under LANconfig:



11.5 Configuring VPN connections

Three questions are answered in the configuration of VPN connections:

- Between which VPN gateways (remote sites) is the connection established?
- What security parameters are used to secure the VPN tunnel between the two gateways?
- Which networks or computers can intercommunicate via these tunnels?

This section introduces the basic considerations for configuring VPN connections. Considered first of all is the simple connection of two local networks. Special cases such as dialing in to LANs with individual computers (RAS) or the connection of structured networks will be covered subsequently.

11.5.1 VPN tunnel: Connections between VPN gateways

Virtual Private Networks (VPNs) are used to interconnect local networks over the Internet. This involves the routing of the private LAN IP addresses via an Internet connection between two gateways with public IP addresses.

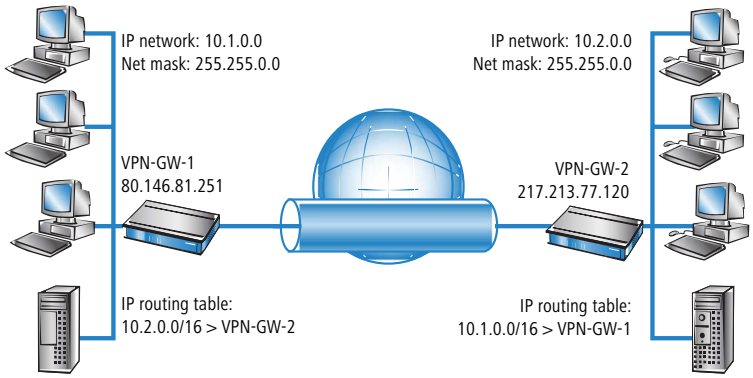
For the secure routing of private IP addresses over the Internet, a VPN connection, also known as a VPN tunnel, is established between the two LANs.

The VPN tunnel has two important tasks:

- To shield the transported data from unauthorized access
- To route private IP addresses via an Internet connection that can normally only be used to route public IP addresses.

The VPN connection between the two gateways is defined by the following parameters:

- The end-points of the tunnel, the VPN gateways, each of which are accessible via public IP addresses (static or dynamic)
- The IP connection between the two gateways
- The private IP address range that are to be routed between the VPN gateways
- Setting relevant to security, such as passwords, IPSec keys etc. to shield the VPN tunnel

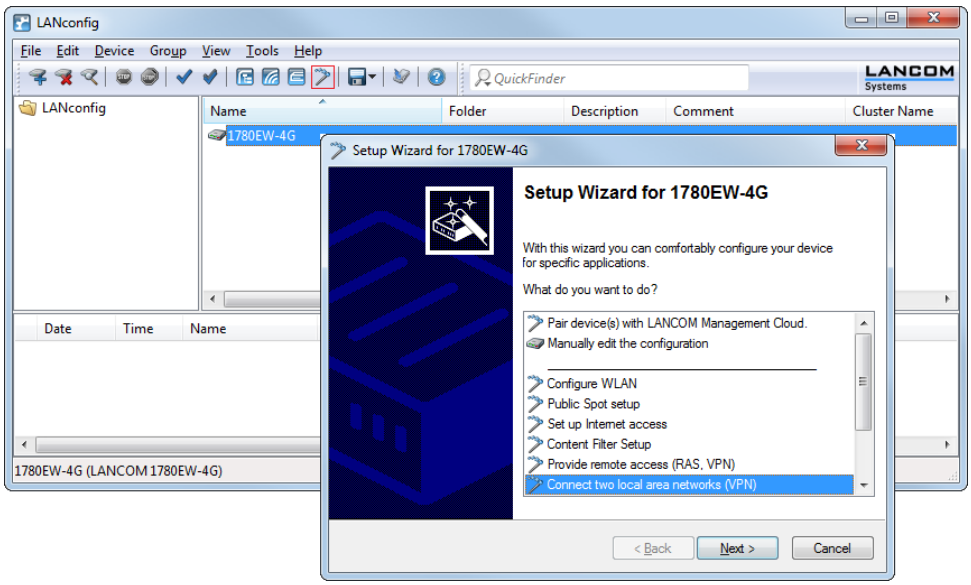


This information is contained in the so-called VPN rules.

11.5.2 Set up VPN connections with the Setup Wizard

If possible, make use of the Setup Wizard within LANconfig to set up VPN connections between local networks. The Wizard guides you through the configuration and makes all the necessary settings for you. Carry out the configuration on both routers, one after the other.

1. Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools** > **Setup Wizard**.



2. Follow the Wizard's instructions and enter the necessary data. The Wizard will inform you when the required information is complete. You can then close the Wizard with **Finish**.
3. Once you have completed the set-up of both routers, you can start testing the network connection. Try to communicate with a computer in the remote LAN (e.g. with `ping`). The device should automatically connect to the remote site and make contact to the requested computer.

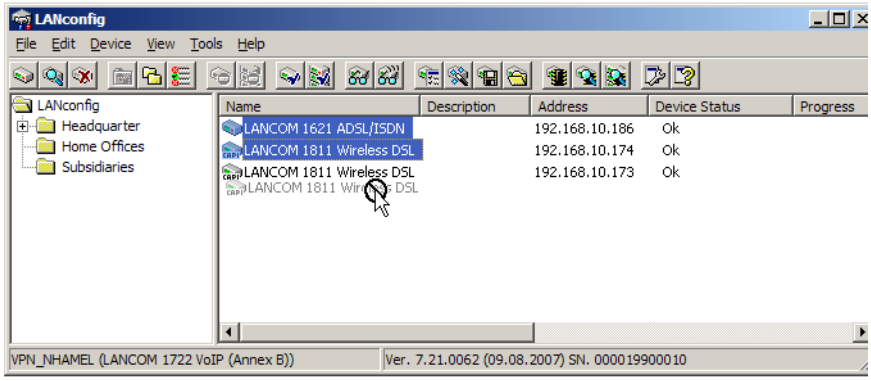
This Wizard automatically sets up the VPN connections essential for typical LAN-LAN connectivity. In the following situations, the VPN connections will have to be configured manually:

- Where no Windows computer with LANconfig is available. In this case, the necessary parameters are set with WEBconfig or via the CLI terminal.
- Where only selected portions of the LAN (intranet) are to communicate with other computers via the VPN connection. This is the case where, for example, the intranet is connected to further subnets with routers, or when only selected portions of the intranet should have access to the VPN connection. In such cases, additional parameters are defined supplementary to those entered in the Setup Wizard.
- Configuring VPN connections to third-party devices.

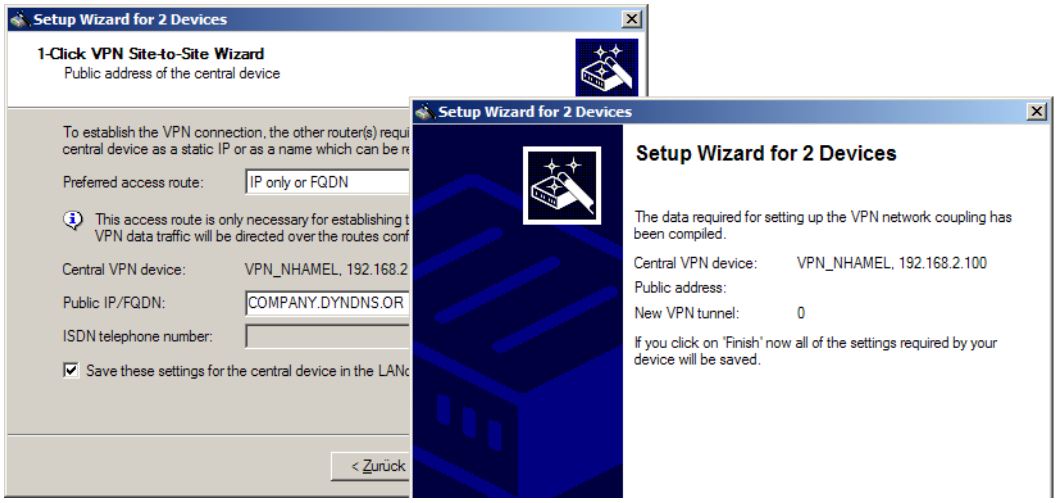
11.5.3 1-Click-VPN for networks (site-to-site)

The site-to-site-to-site connectivity of networks is now very simple with the help of the 1-Click-VPN wizard. It is even possible to simultaneously couple multiple routers to a central network.

1. In LANconfig, mark the routers at branch offices which are to be coupled to a central router via VPN.
2. Use drag&drop by mouse to place the devices onto the entry for the central router.



3. The 1-Click VPN Site-to-Site Wizard opens. Enter a name for this access and select the address under which the router is accessible from the Internet.



4. Select whether connection establishment is to take place via the name or IP address of the central router. Enter the address or name of the central router.
5. The final step is to define how the networks are to intercommunicate:
   - The INTRANET at headquarters only is to be provided to the branch offices.
   - All private networks at the branch offices can also be connected to one another via headquarters.

All entries for the central device are made just once and are then stored to the device properties.

11.5.4 1-Click-VPN for the LANCOM Advanced VPN Client

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the VPN router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

1. Use LANconfig to start the **Set up a RAS Account** wizard and select the **VPN connection**.
2. Activate the options **LANCOM Advanced VPN Client** and **Speed up configuration with 1-Click-VPN**.
3. Enter a name for this access and select the address under which the router is accessible from the Internet.
4. In the final step you can select how the access data is to be entered:
   - Save profile as an import file for the LANCOM Advanced VPN Client
   - Send profile via e-mail
   - Print out profile

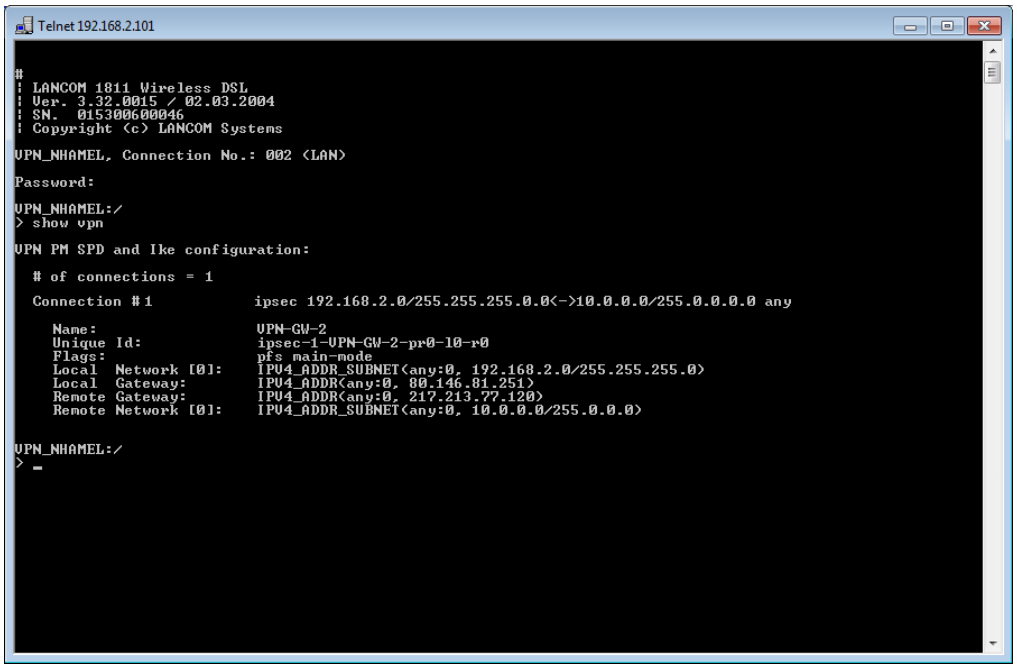
Sending a profile via e-mail could be a security risk should the e-mail be intercepted en route! To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

- Gateway: If defined in the VPN router, a DynDNS name is used here, or alternatively the IP address.
- FQUN: Combination of the name of the connection, a sequential number and the internal domain in the VPN router.
- Domain: If defined in the VPN router, the internal domain is used here, or alternatively a DynDNS name or IP address.
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Pre-shared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated by default.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the VPN router.

11.5.5 Inspecting VPN rules

Information about the current VPN rules in the device can be retrieved with the Telnet terminal. Start a Telnet connection to the VPN gateway and enter the command `show vpn` in the terminal:



The output informs you of the network relationships that are relevant to VPN connections to other networks.

In this example, the local network at a branch office (network `192.168.2.0`, netmask `255.255.255.0`) is connected to the network at the headquarters (network `10.0.0.0`, netmask `255.255.255.0`). The public IP address of the local gateway is `80.146.81.251`, and that of the remote VPN gateway is `217.213.77.120`.

Entering `any:0` displays the protocols and ports that can be used over the connection.

Further output is displayed by the command `show vpn long`. The information displayed here covers network relationships and also the parameters that are relevant to security, such as IKE and IPSec proposals.

11.5.6 Manually setting up VPN connections

Manually setting up VPN connections involves the tasks described previously:

- Definition of the tunnel endpoints
- Definition of the security-related parameters (IKE and IPSec)
- Definition of the VPN network relationships, i.e. the IP address ranges to be connected. Should the IP ranges overlap at both ends of the connection, please refer to the section.
- When using LANCOM Dynamic VPN: Entry for the corresponding remote site in the PPP list with a suitable password for the Dynamic VPN handshake. The username entered here must correspond with the name entered in the remote device that describes the VPN connection to this local device. Activate “IP routing”.

The tunnel endpoints, i.e. the local VPN gateway and each of the VPN remote sites, are entered into the VPN connection list.

Manually configuring the VPN connection involves the following steps:

1. Create an entry for the remote VPN gateway in the connection list and enter its public IP address.

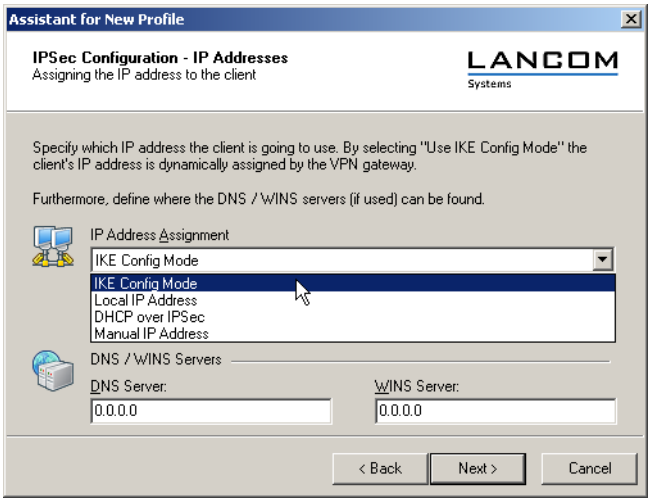
2. The security parameters for the VPN connection are normally taken from the prepared list, and all that is required here is to define an IKE key.
3. For a Dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as the remote site, with the name of the local VPN gateway as the User Name, and set a suitable password. Be sure to activate the IP routing for this PPP connection. The remaining PPP parameters, such as the procedure for checking the remote site, can be defined in the same way as for other PPP connections.
4. The main task in setting up VPN connections is in defining the network relationships. Which IP address ranges at each end of the VPN tunnel should be included in the secured connection?

11.5.7 IKE config mode

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the "IKE-CFG" mode is additionally added to the entries in the connection list. This can assume the following values:

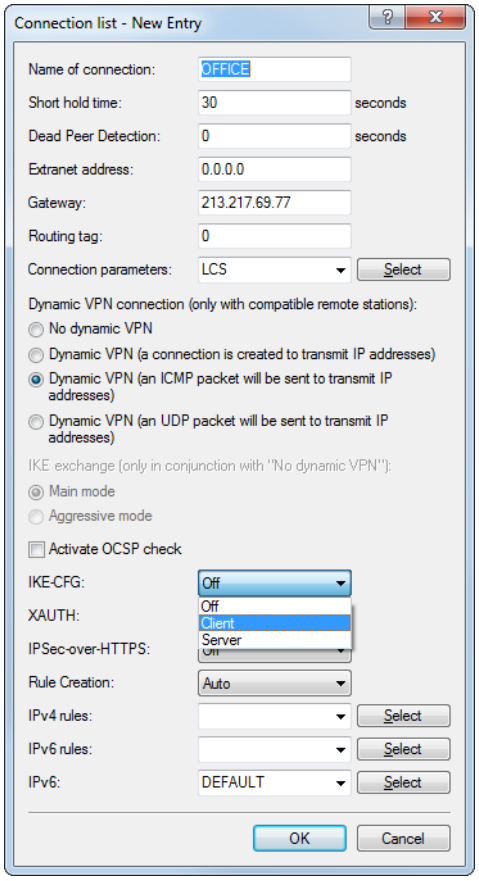
- **Server**: With this setting, the device functions as the server for this VPN connection. The assignment of an IP address to the client can take place in two ways:
  - If the remote site is entered in the routing table, the IP address defined here will be assigned to the client.
  - If the remote site is not entered in the routing table, an IP address which is available from the IP pool will be taken for the dial-in connections.

  The remote site must be configured as IKE-CFG client in this case, and thus has to request an IP address from the server. To dial in with a LANCOM Advanced VPN Client, the option **Use IKE Config Mode** has to be activated in the connection profile.



- **Client**: With this setting, the device functions as the client for this VPN connection and requests an IP address from the remote site (server). The device acts in a similar manner to a VPN client.

- **Off**: If the IKE-CFG mode is switched off, no IP addresses will be assigned for the connection. Fixed IP addresses must be defined for both ends of the connection.



LANconfig: **VPN** > **IKE/IPSec** > **Connection list**

Command line: **Setup** > **VPN** > **VPN-Peers**

11.5.8 Diagnosis of VPN connections

If the VPN connections fail to work after the configuration of the parameters, the following diagnostic methods can be applied:

- The command `show vpn spd` on the CLI calls the "Security Policy Definitions".
- Use the command `show vpn sadb` to access information about the negotiated "Security Associations" (SAs).
- The command `trace + vpn` [status, packet] calls up the status and error messages for the current VPN negotiations.
  - The error message "No proposal chosen" indicates a fault in the configuration at the remote site.
  - The error message "No rule matched", on the other hand, indicates a fault in the configuration of the local gateway.

By default, the device retains the VPN error messages in the status table. Depending on the installation LANmonitor may display a large number of open error messages, which clutters the display. For this reason the command-line setting under **Setup** > **Config** > **Error-Aging-Minutes** enables you to define a period of time in minutes after which the device automatically deletes these error messages from the status table.

To document sporadic errors, disable this option with the entry `0`.

11.6 Working with digital certificates

The security of communications via VPN fulfills three core requirements:

- Confidentiality: Encryption ensures that no unauthorized users can read the transmitted data.
- Integrity: The data cannot be changed during transmission (via authentication).
- Authenticity: The receiver can be certain that received data has genuinely been sent by the supposed sender (via authentication).

A number of encryption and authentication methods exist which provide satisfactory solutions for the first two aspects, confidentiality and integrity. The use of digital certificates aims to provide assurance about the authenticity of the communications partner.

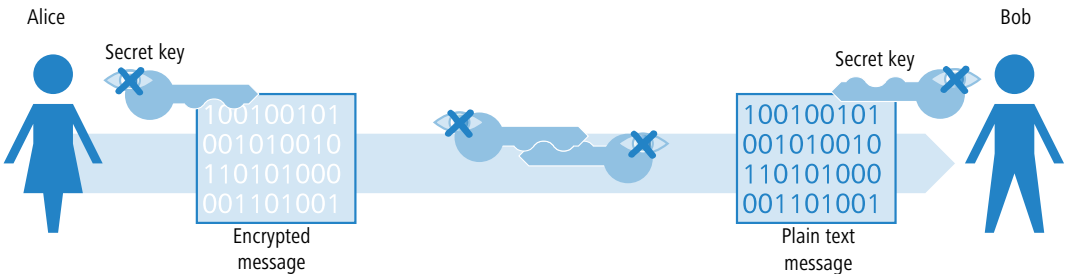
11.6.1 Basics

Encryption methods can be divided into two categories: Symmetrical and the asymmetrical encryption.

11.6.1.1 Symmetrical encryption

This is a method known for thousands of years and is based on the fact that the sender and the recipient both have access to a message by knowing a secret shared key. This key can take on a wide variety of forms: The Romans used a stick of a certain diameter for encryption and decryption.

Today's digital communications rely in the main upon a password as the key. Using this password and an encryption algorithm, the data from the sender are changed. The recipient uses the same key and the fitting encryption algorithm so that the data are legible again. Other persons who do not know the key cannot read the data. A common symmetrical method of encryption is 3DES, for example.



Example:

1. Alice wishes to send a confidential message to Bob. To this end, she encrypts the message with a secret key and a suitable method, e.g. 3DES. She sends the encrypted message to Bob informing him of the encryption method she used.
2. Bob has the same key as Alice. Since he knows the encryption method that was used, he can decrypt the message and transform it back into cleartext.

Symmetrical encryption is simple and efficient but has two serious disadvantages:

- A different key is required for every secret communications relationship. If Alice and Bob are joined by Carol, three keys are necessary for secure data communications between all parties; with four participants, the number of keys required is six; with 12 participants, 66 keys are required and with 1000 participants, almost 500,000 keys are necessary! In a worldwide network with ever increasing demand for secure communications and higher numbers of participants, the nature of this serious problem is obvious.
- While this first disadvantage could be solved with technology, the second problem that is the core problem for symmetrical encryption: The secret key must be known at both ends of the communication and must not fall into the hands of unauthorized persons. Thus it is not possible for Alice simply to send the key to Bob per e-mail before the data connection has been secured sufficiently—which is the whole point of the encryption. She has to give the key

to Bob in person, or at least make use of a communications method which is secure from eavesdroppers. This is a task which is almost impossible to handle in these times of worldwide dynamic communications.

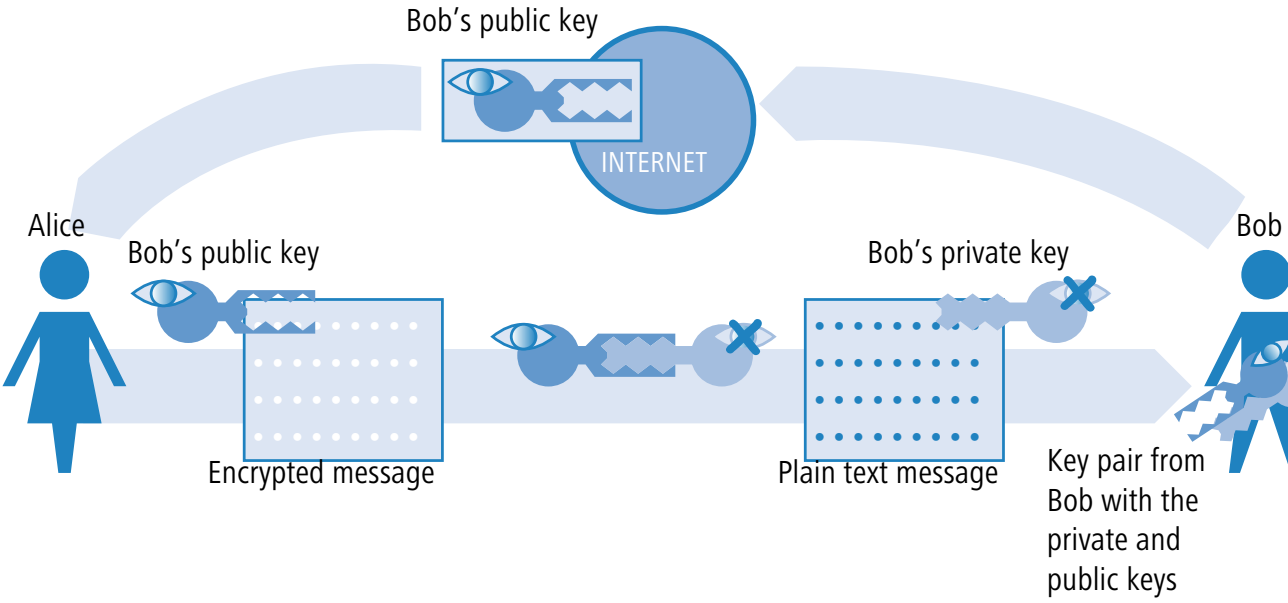
11.6.1.2 Asymmetric encryption

A totally new approach was developed in the 1970s; that of asymmetric encryption. This method no longer relies on a secret key that is known at both ends, but on a pair of keys instead:

- The first part of the key pair is used to encrypt the data that are to be sent to the key owner. This key, subsequently called the public key, can be made publicly available to anybody interested in communication.
- The second part of the key pair is the private key that is only used to decrypt the received message. This key is secret and may not fall into the hands of unauthorized persons.

The main difference to symmetrical methods: A publicly available key is used in this so-called “public key method”. An example of an asymmetrical encryption method is RSA.

Let's take another look at the example with Alice and Bob:



- For secure communications, Bob first of all generates a key pair with a private key and a public key that belong together. The method used for generating this key ensures that the private key cannot be backwardly computed with knowledge of the public key. Bob can now publicize the public key without worry. He can send it to Alice per e-mail or simply publish it on a web server.
- Alice now encrypts the message for Bob with his public key. This now illegible message can only be decrypted by using Bob's private key. Even if the data are intercepted on the way from Alice to Bob, no-one but Bob can regenerate the cleartext message.

The asymmetrical encryption offers the following advantages over symmetrical variants:

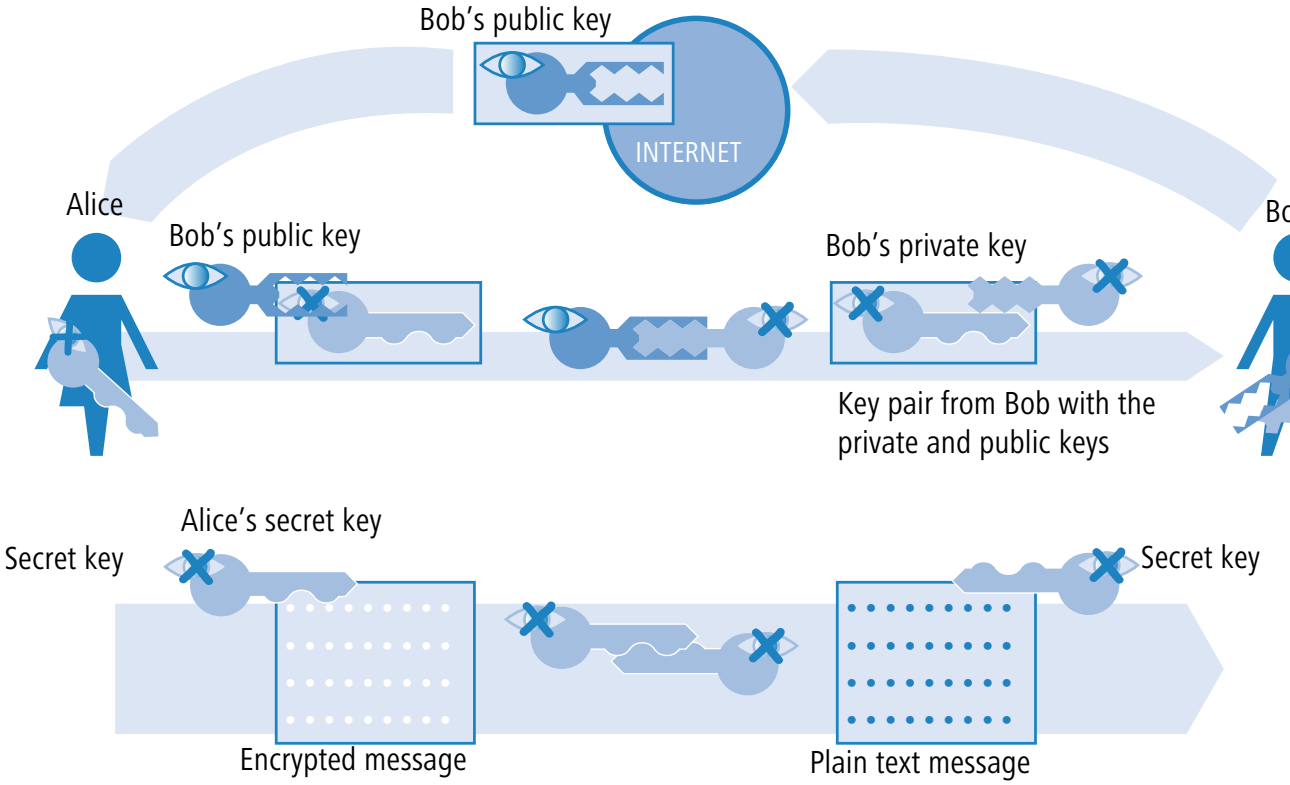
- A key pair is not required for every communications relationship, but for each participant only. Even with 1000 participants, each user needs only his/her personal key pair, of which only the public key is publicly available. Instead of 500,000 secret keys, the public key method requires just 1000 key pairs.
- The risky transmission of a secret key to the communications partner is simply not necessary as knowledge is only required of the public key on the other side of the communications relationship. This is the solution to a significant problem in the dynamic encryption of data between multiple participants.

11.6.1.3 Combination of symmetrical and asymmetrical encryption

Asymmetrical encryption methods have quickly become established due to the security they offer. However, security has its price: Asymmetrical encryption methods are slow. The mathematics involved in the encryption and decryption of

messages is far more complex that with symmetrical encryption methods and thus require more computing time--a critical factor when transmitting larger quantities of data.

The advantages of symmetrical and asymmetrical encryption can be used in suitable combinations of these methods. In this method, the higher security of the asymmetrical encryption is used to protect the transmission of the secret key. The actual data for transmission are then encrypted with the faster symmetrical method.



1. First of all, Bob generates a key pair and publicizes the public key.
2. Alice uses the public key to encrypt a secret symmetrical key and sends this to Bob. For each transmission, this secret key is newly defined according to a random procedure.
3. Bob is the only one who can decrypt this secret key by using his private key.
4. Alice and Bob then use this secret key to encrypt and decrypt the clearly much larger volume of the payload data.

11.6.1.4 Public key infrastructure

The combination of symmetrical and asymmetrical encryption methods enable initially unsecured connections to be used to establish secure data communications. Until now, the aspect of authenticity has been ignored. How should Alice know that the public key really does come from Bob? The use of public keys thus depends directly on the trust in the authenticity of the communications partner.

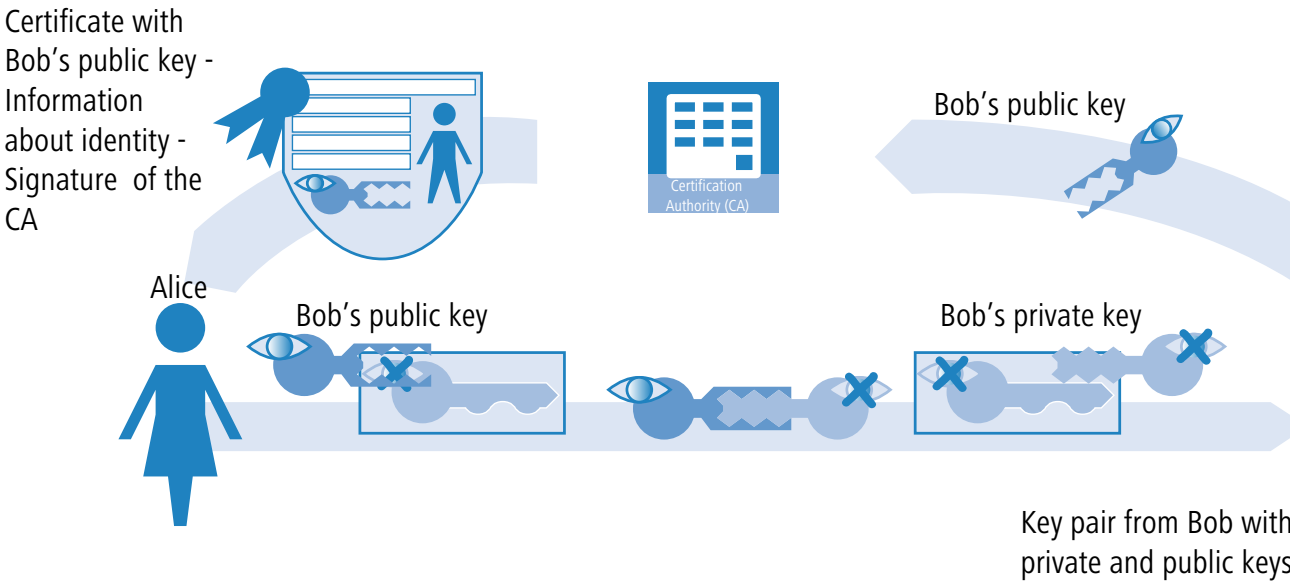
To secure this trust, a confirmation of the key pairs for use with asymmetrical encryption can be issued by publicly recognized and trustworthy authorities. In Germany, for example, the highest authority for the confirmation of digital keys is the Federal Network Agency for electricity, gas, telecommunications and railways (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen). This agency in turn issues accreditations to suitable service providers who are viewed as equally trustworthy.

The web site of the Federal Network Agency (*www.bundesnetzagentur.de*) features up-to-date lists of accredited certification service providers and notification of revoked accreditations. Accredited service providers include numerous tax advisers and legal associations.

The task of this organization is to attribute a public key to just one person or organization. This attribution is recorded and officially publicized in a certificate. Consequently these providers are known as "Certification Authorities", or CAs for short. The uppermost certification authority is known as the Root CA.

Bob can now approach a CA to have his public key certified as belonging to him. He submits his public key to the CA who then confirm that the key belongs to Bob.

The CA issues a certificate which lists the public key and further information about Bob, such as his identity, among others.



The certificate carries the signature of the CA to show that the confirmation itself is genuine. The certificate takes up just a small amount of data and is suitable for exchange with an asymmetric method. With a signature, however, the asymmetric method is used in the opposite direction:

1. The CA, too, has a key pair consisting of private and public keys. Since this is a trustworthy authority, their key pair can be considered as reliable.
2. The CA calculates a hash value for the certificate, encrypts this and uses it in the signature in Bob's certificate. This acts to confirm the attribution of Bob's public key to his identity.

   This procedure behaves in the opposite manner to the normal asymmetrical encryption. In this case, the encryption does not fulfill the task of protecting the data from unauthorized persons, but confirms the signature of the CA instead.
3. Any data communications participant anywhere in the world with the public key from the CA is now in a position to check the signed certificate.

   Only the CA is in a position to use their private key to generate signatures that can be decrypted again by using the CA's public key. This signature guarantees that the certificate is genuinely sourced from the issuing CA.

11.6.2 Advantages of certificates

In some cases the use of certificates for securing VPN connections can be an alternative to the otherwise widespread preshared key (PSK) method:

› Higher security for VPN client connections (with IKE Main Mode)

  When using PSK connections between peers that use dynamic IP addresses, the Main Mode cannot be used. In these cases, the aggressive mode must be used with it lesser degree of security. Using certificates allows peers with dynamic IP addresses, such as dial-in computers with the LANCOM Advanced VPN Client, to use the Main Mode and thus to increase the level of security.

- Higher security for keys and passwords

  Preshared keys are just as susceptible as other passwords, too. The way that users treat these passwords (the “human factor”) is a major factor in the securing of connections. With a certificate-based VPN establishment, the keys in the certificates are automatically generated with the desired key length. Furthermore, the random keys generated by computers offer more security from attack (e.g. dictionary attack) than the preshared keys of the same key length that are thought up by people.

- Peer authenticity can be checked

  The use of certificates allows both ends of the connection to be authenticated during VPN connection establishment. Certificates can contain additional information useful for checking the peers. Additional protection is provided by a time limitation of the certificates, e.g. for users receiving only temporary access to a network.

- Support of tokens and smartcards

  Certificates stored on external data media can be integrated into “strong security” environments which prevent passwords from being read from computers.

The advantages of certificates have to be considered in relation to the considerable increase in effort of introducing and maintaining a public key infrastructure (PKI).

11.6.3 Structure of certificates

11.6.3.1 Contents

A certificate contains a variety of information needed for it to fulfill its purpose. Some information is obligatory, some is optional. A certificate can also be stored in a variety of different formats. An X.509-standard certificate contains the following information, for example:

- Version: This is the relevant version of the X.509 standard. For example, 06/2005 version 'v3' was current.
- Serial number: This is a unique number that identifies the certificate.
- Signature algorithm: This identifies the algorithm that the issuer used to sign the certificate. The digital signature of the issuer is also to be found here.
- Validity: Certificates are valid for a limited period of time. This entry indicates the duration of the certificate's validity.
- Issuer: This identifies the issuer, for example by name, e-mail address, nationality, etc.
- Subject: This identifies the certificate's owner, for example by name, institution, e-mail address, nationality, city, etc.
- Subject public key: Information indicating the method used to generate the public key used by the certificate owner. The owner's public key is also to be found under this item.

11.6.3.2 Target application

When the certificates are generated, the possible uses of the certificate usually have to be selected. Some certificates are intentionally designed for transfer with web browsers or e-mails only, and others are more generally applicable to any use.



When you generate certificates, make sure that you enter its intended purpose.

11.6.3.3 Formats

The ITU standard X.509 is a wide spread format for certificates. When displayed as text, this type of certificate looks like the following:

```
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 1 (0x1)
 Signature Algorithm: md5WithRSAEncryption
 Issuer: CN=CA/Email=ca@trustme.dom, OU=Certificate Authority, O=TrustMe Ltd, ST=Austria, L=Graz, C=XY,
 Validity
 Not Before: Oct 29 17:39:10 2000 GMT
 Not After : Oct 29 17:39:10 2001 GMT
```

```
Subject: CN=anywhere.com/Email=xyz@anywhere.com, OU=Web Lab, O=Home, L=Vienna, ST=Austria, C=DE
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
f0:b4:95:f5:f9:34:9f:f8:43
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
email:xyz@anywhere.com
Netscape Comment:
mod_ssl generated test server certificate
Netscape Cert Type:
SSL Server
Signature Algorithm: md5WithRSAEncryption
12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
ff:8e
```

11.6.3.4 File types

Depending on the issuer, there are various file suffixes for digital certificates and private keys. The following types are common:

- *.pfx and *.p12: PKCS#12 files
- *.pem, *.cer and *.crt: BASE-64 encoded certificates
- *.cer, *.crt and *.der: DER-encoded certificates
- *.key: BASE64 or DER encoded keys
- *.pvk: Microsoft-specific key format

Along with actual certificates, the world of certificate-secured VPN connections has another important file type: PKCS#12 files can contain several components, including a certificate and a private key. To process the PKCS#12 file, a password has to be entered when the certificate is exported.



BASE64-coded certificates have a header that typically features the following lines:

```
----- BEGIN CERTIFICATE -----
```

11.6.3.5 Validity

A further option is to refer to a certificate revocation list (CRL). CRLs list certificates that have lost their validity, for example if an employee has left the company and his certificate has been withdrawn. This information allows those who are checking certificates to refer to the appropriate CRL.

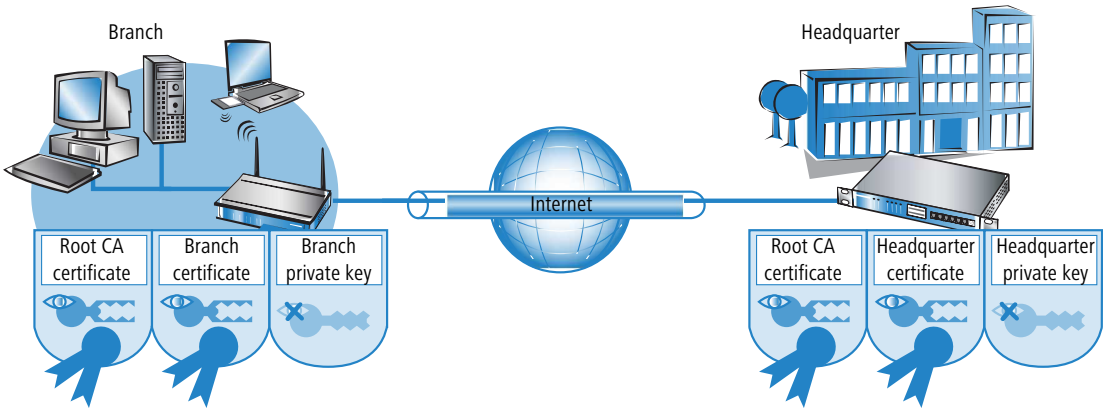
11.6.4 Security

Certain security aspects have to be observed even when dealing with certificates:

- Only ever transfer private keys via secure connections, e.g. with HTTPS.
- Only use passphrases that are long enough and secure as passwords to be used as keys or PKCS#12 files.

11.6.5 Certificates for establishing VPN connections

Along with basic information about certificates, this section now considers their concrete application in establishing VPN connections. For connection establishment with the support of certificates, certain information must be available at both ends of the connection (e.g. when connecting a branch office to the network at headquarters by means of a router):



- The branch office has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The check sum for this certificate is signed with the CA's private key.
  - Its own private key
- The headquarters has the following components:
  - The Root CA's certificate with the CA's public key
  - A certificate for its own device with its own public key and the confirmation of identity. The check sum for this certificate is signed with the CA's private key.
  - Its own private key

Put simply, the following procedures are carried out during the VPN connection exchange in Main Mode (symmetrical in both directions):

1. In an initial exchange of packets the peers negotiate, for example, the encryption methods and the authentication method that are to be used. At this phase, both ends are not fully certain about who they are negotiating with, although this is not yet critical.
2. At the next stage, common key material is negotiated for the continued communications, including among other things symmetrical keys and asymmetrical key pairs. At this phase, too, the two ends are not yet fully certain about who the keys are being negotiated with.
3. In the next stage, the certificate is used in a check to ensure that the peer involved in negotiating the key material really is the intended communication partner:
   - The branch office uses the current negotiation's key material to calculate a checksum (hash value) that can only be calculated by the two peers involved (branch office and headquarters) and only so long as the connection exists.
   - The branch office encrypts the hash with its own private key, generating a signature with it.
   - The branch office then transmits this signature together with its own certificate to the peer at headquarters.
   - The headquarters then checks the signature of the certificate received from the branch office. This can be done with the help of the public key at the Root CA, which is identical for both peers. If the signature in the branch office's certificate (generated with the CA's private key) can be decrypted with the CA's public key, then the signature is valid and the certificate is trustworthy.

- In the next stage, the headquarters checks the signature of the encrypted hash. The branch office's public key in the corresponding certificate was found to be valid at the previous stage. The headquarters can thus check if the signed hash can be decrypted with the branch office's public key. The headquarters can calculate the same hash as the branch office using the key material for the current connection. If this check is successful then the peer “branch office” can be considered as authentic.

11.6.6 Certificates from certificate service providers

Certificates on offer from public certifiers are available in various security classes. The higher security classes require more effort on behalf of the applicants to demonstrate the authenticity of their identity to the CA. The Trustcenter AG in Hamburg, for example, uses the following classes:

- Class 0: These certificates are issued without an identity check and serve only for customer tests.
- Class 1: For this class, the existence of an e-mail address is the only check. These certificates are useful for private users wishing to sign their e-mails, for example.
- Class 2: This level, too, does not involve any personal proof of identity. The submission of an application along with, for example, a certificate of company registration is sufficient. This level is suitable for communications between companies that already know each other.
- Class 3: This level involves a personal check of the person or company. The information in the issued certificates is compared with a passport or a notarized copy of the certificate of company registration. This level is suitable for advanced applications such as e-business or online banking.

In your dealings with public certificate service providers, be sure to check in detail the security class or the proof of identity. This is the only way to be sure that the certificates really do meet with your security requirements.

11.6.7 Establishing a proprietary CA

Referring to public CAs for secure enterprise communications can only be recommended under certain conditions.

- There is considerable effort involved in the issue of new certificates and this can be slow.
- The keys in use are transferred via connections which are inadequately secured.
- Communication is based upon the trust in the CA.

An alternative for company communications is to establish a proprietary CA. Suitable packages are the Microsoft CA on a Microsoft Windows server or, as an open source version, OpenSSL. A proprietary CA empowers you to issue and manage all of the necessary certificates for secure data exchange with complete independence from any external parties.

Companies are recommended to use a proprietary CA rather than public certifiers. There are, however, several important issues to be considered when planning a CA. For example, even as early as during the installation of a Windows CA, the validity period for the Root CAs has to be defined and cannot be altered subsequently. Other aspects of planning include:

- The certificate policy or the level of security that is to be achieved with certificates
- The available name space
- Key lengths
- The duration of certificate validity
- Managing blocking lists

Precise planning is strongly recommended since corrections at a later date often imply considerable amounts of effort.

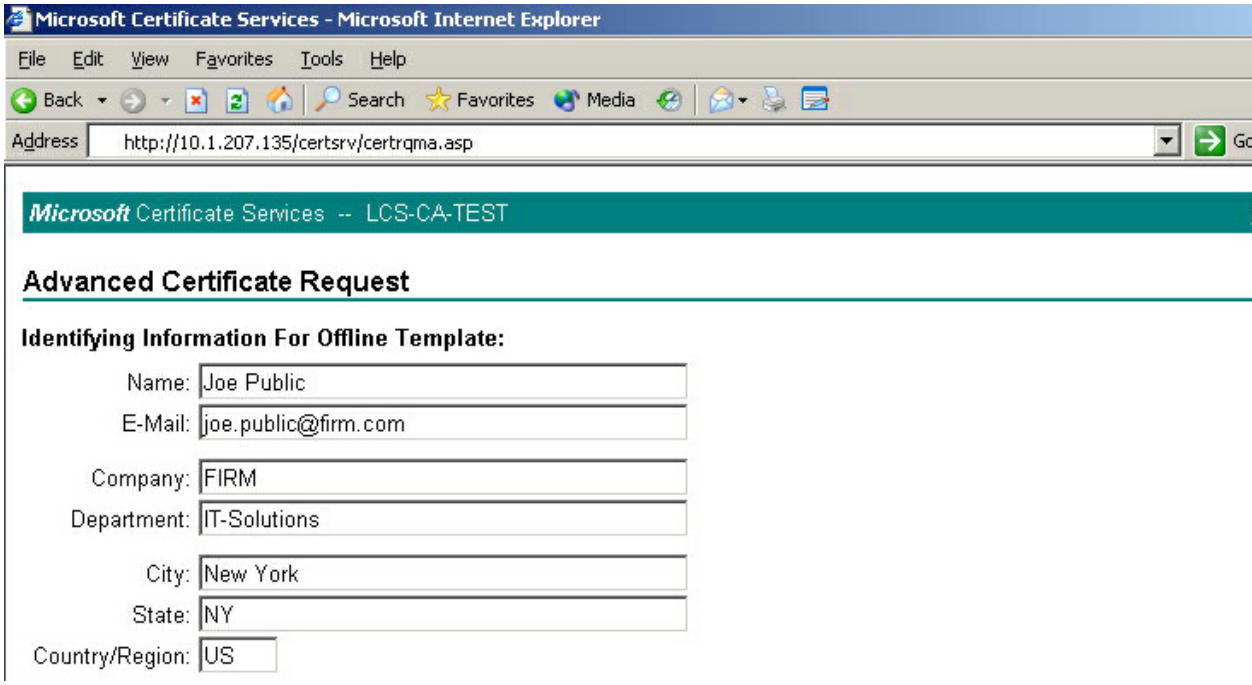
11.6.8 Requesting a certificate with Stand-alone Windows CA

For operations with a router, a combination of PKCS#12 file with root certificate, a proprietary device certificate and the device's public key offer the best services.

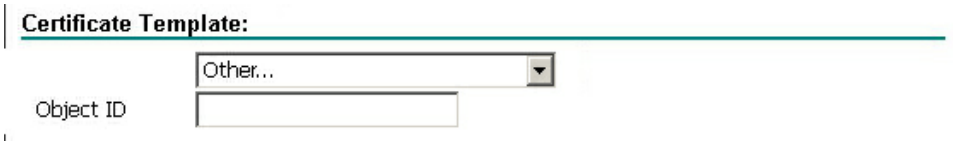
1. Using your browser, access the start page of the Microsoft Certificate Services.
2. For the certificate type, select 'Advance Certificate Request'.
3. The next step is to selection the option 'Generate and submit a certificate request '.

If, and only if, the root certificate is already available as a file, select the option 'BASE64'.

4. In the following step the information for identification is entered.



5. In the same dialog, select the certificate template as 'Other...' and then delete the value in 'Object ID'.



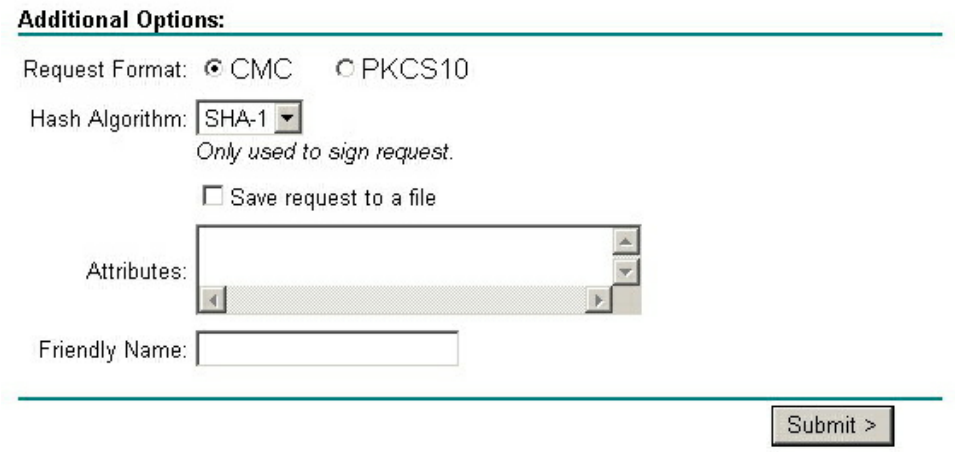
6. Mark 'Create new key set'. The public and private keys for the current user will now automatically be generated by the CA.



7. Select the key size according to certificate policy and activate the option to mark keys as exportable.

The key is not exported at this point and so a file name does not have to be specified. An export would create a Microsoft-specific *.pvk file, a format which is unsuitable for use with a LCOS.

8. Finally, select the hash algorithm 'SHA-1' and send your certificate request with a click on **Submit**.



You can check on the status of your certificate request at any time via the Windows CA start page. Certificate requests can only be viewed from the same computer used to submit the request.

9. The certificate can be installed on your computer once the CA administrator has checked the request and created the certificate.

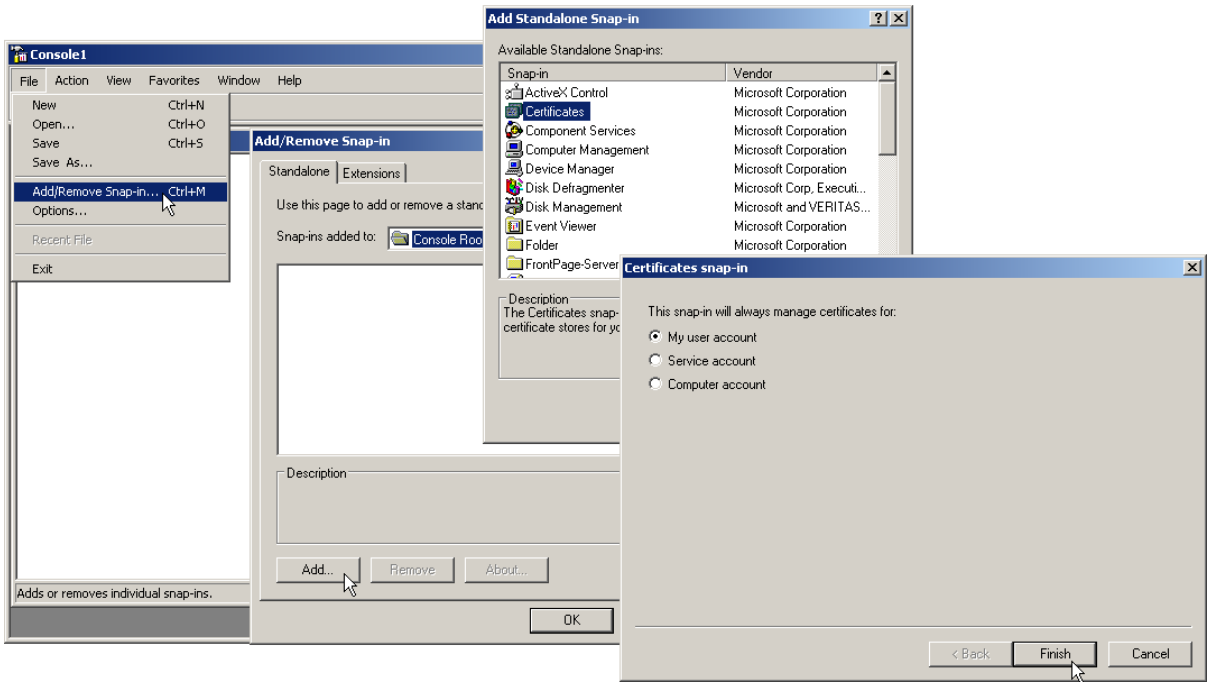
Certificates can only be installed on the same computer that was used for the request.

11.6.9 Export the certificate to a PKCS#12 file

The installation stores the certificate in your operating system but it is not yet available as a separate file. You will need this for installation to the device, though. For access to a certificate in file form, it has to be exported first.

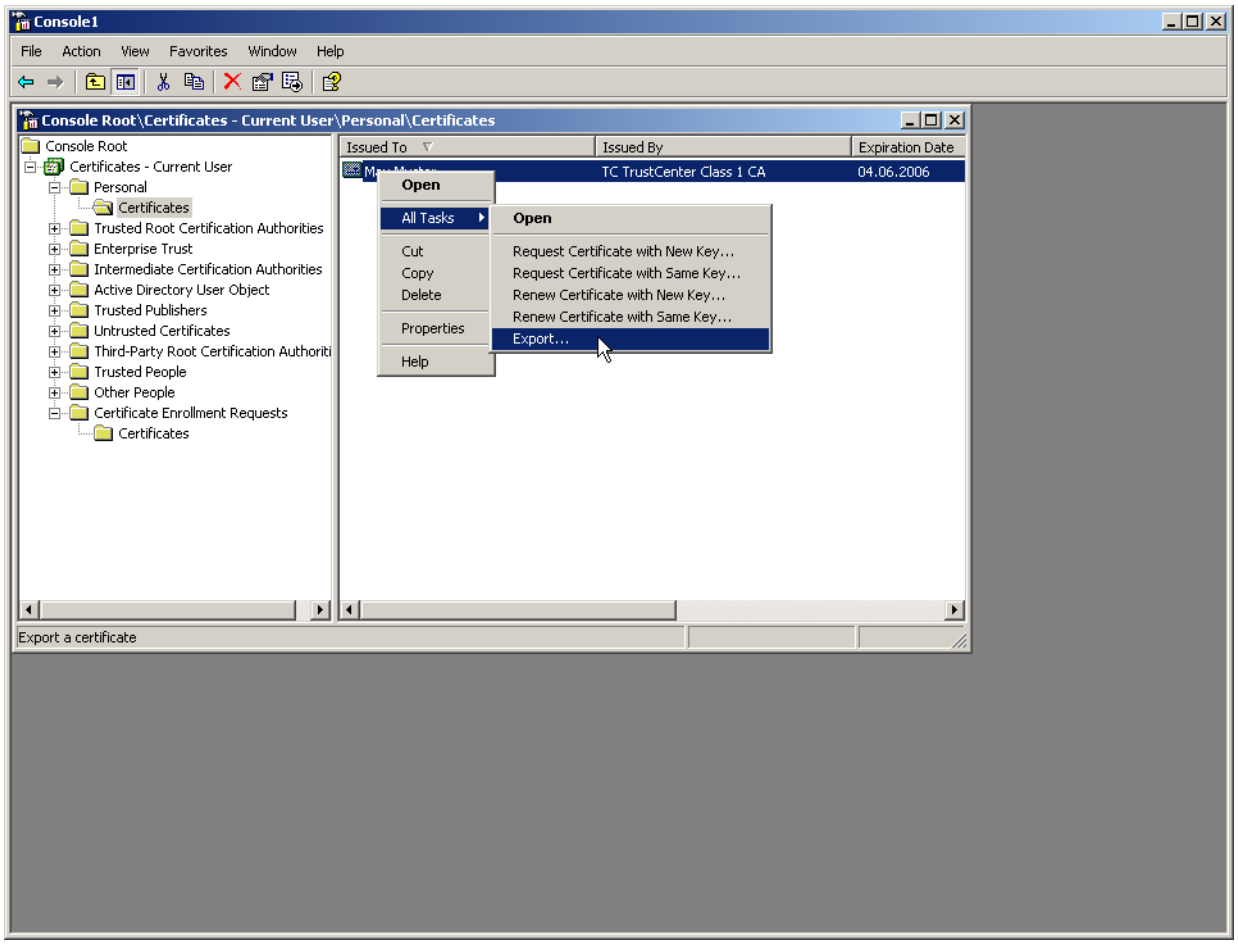
11.6.9.1 Export via the Windows CLI root

1. Open the Management CLI with the command `mmc` at the command line and select the menu item **File** > **Add/Remove Snap-In**.

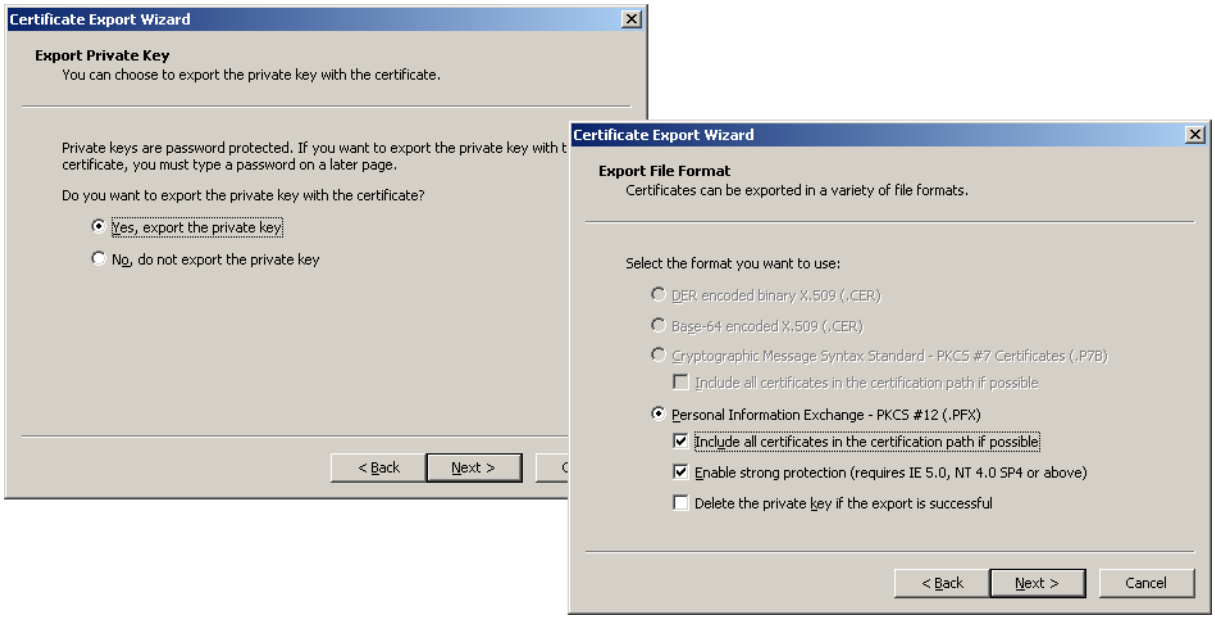


2. Click on **Add** and select “Certificates”. Confirm with **Add**, then mark “My user account” and click on **Finish**.

3. To export the desired certificate to a file, go to the Management CLI and click in the group **Certificates - current user** > **My certificates** > **Certificates** with the right mouse key and, from the context menu, select **All tasks** > **Export**.



4. In the Certificate Export Wizard, activate the option to export the private key. You can optionally delete the private key from the system after exporting.



The option "Include all certificates in the certification path" must be activated so that the root certificate is also exported to the PKCS#12 file.

5. You will be requested to enter a password to protect the private key. Ensure that you choose a secure password of sufficient length (passphrase). You will need this password later to install the certificated in the device.

The term "password" is synonymous with other terms used in the different environments, e.g. "PIN".

11.6.10 Create certificates with OpenSSL

OpenSSL is a further possibility for creating proprietary certificates and to test certified connections. OpenSSL is an open-source project available for Linux and Windows at no cost; as a command-line tool, however, it does not offer the user-friendliness of other CA variants.

The configuration file openssl.cnf must be adapted to your specific needs. Further information is available in the OpenSSL documentation.

11.6.10.1 Installing OpenSSL

1. Download the current version of OpenSSL from *https://www.slproweb.com/products/Win32OpenSSL.html*.

   Information about the download servers is available under *https://wiki.openssl.org/index.php/Binaries*.

2. Install the package and, in the directory `./bin/PEM/demoCA`, create the following subdirectories:
   - `/certs`
   - `/newcerts`
   - `/crl.`
3. In the file openssl.cnf, change the path in the `[CA_default]` group to: `dir=./PEM/demoCA`
4. OpenSSL is started with a double-click on `openssl.exe` in the `./bin` directory.

11.6.10.2 Issue a certificate for Root CA

1. Create a key for the CA with the command:

   ```
   genrsa -aes256 -out ca.key 2048
   ```

   Remember the password that you enter after the request for the CA key as you will need it again later!

   This command creates the file 'ca.key' in the current directory.

2. Create a certificate request for the CA with the command:

   ```
   req -key ca.key -new -subj /CN="Test_CA" -out ca.req
   ```

   You will be requested to enter the password for the CA key here.

   This command creates the file 'ca.req' in the current directory.

3. Create a certificate from the certificate request with the command:

   ```
   x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt
   ```

   Here, too, you will be requested to enter the password for the CA key.

   This command signs the certificate request 'ca.req' with the key 'ca.key' and then issues the certificate 'ca.crt'.

11.6.10.3 Issue certificates for users or devices

1. Create a key for the device or user with the command:

   ```
   genrsa -out device.key 2048
   ```

   This command creates the file 'device.key' in the current directory.

2. Create a certificate request for the device or user with the command:

   ```
   req -key device.key -new -subj /CN=DEVICE -out device.req
   ```

   This command creates the file 'device.req' in the current directory.

   In addition to this command, further changes to the file “openssl.cnf” are required to define an extension.

3. Create a certificate from the certificate request with the command:

   ```
   x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt
   -CAcreateserial -days 90 -out device.crt
   ```

   This command signs the certificate request 'device.req' with the key 'ca.key' and then issues the certificate 'device.cert'. The configuration file openssl.cnf is also involved in the procedure.

4. Export the certificate for the device or user with the command:

   ```
   pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt
   -out device.p12
   ```

   This command combines and saves the key 'device.key', the device certificate 'device.crt' and the root certificate 'ca.crt' to the file 'device.p12'. This PKCS#12 file can be uploaded directly to the required device.

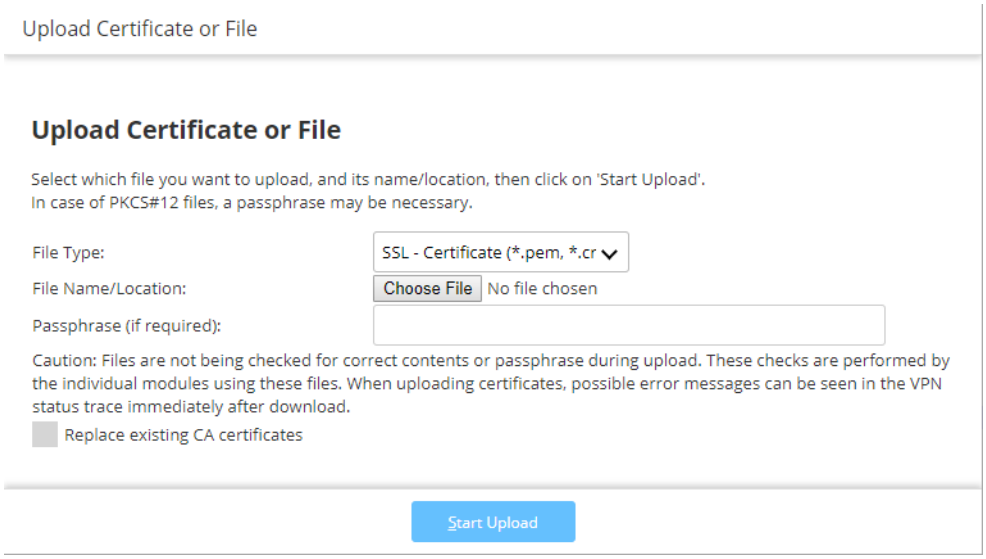
11.6.11 Uploading certificates to the device

The following components must be available in a device for the establishment of VPN connections that are secured by certificate.

- The Root CA's certificate with the CA's public key
- A certificate for its own device with its own public key and the confirmation of identity. The check sum for this certificate is signed with the CA's private key.
- Its own private key

If you have followed the instructions for issuing certificates with a Windows CA and their export, then this information will now be available in the form of a combined PKCS#12 file. Alternatively you have used a different method and the individual components are available as separate files.

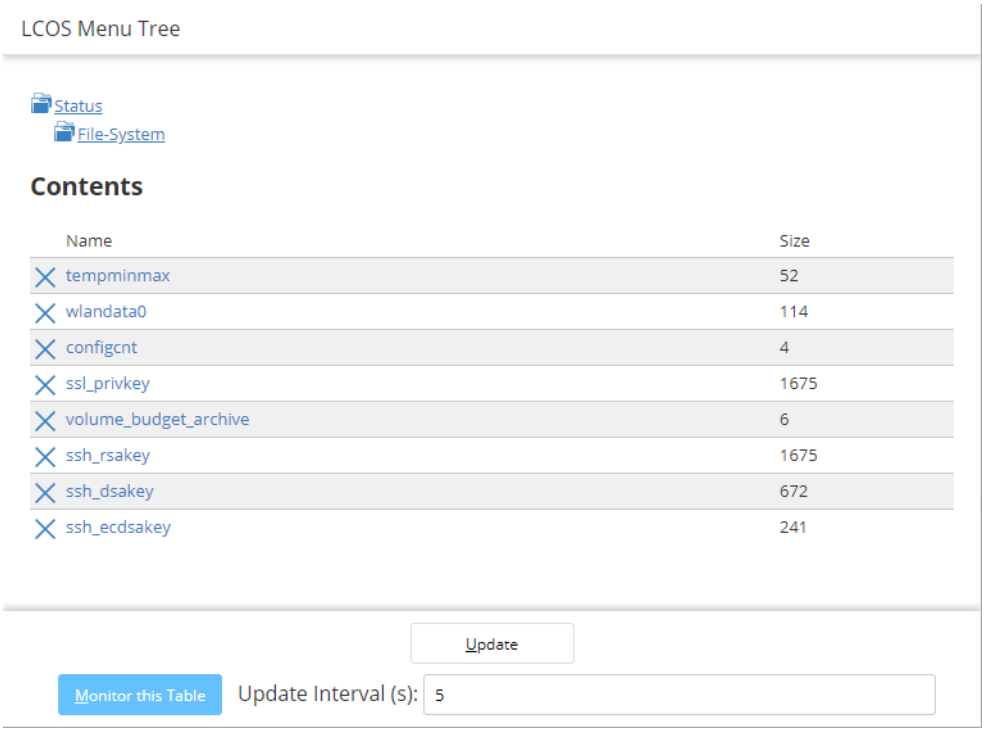
1. Use WEBconfig to log on to the required device; you will need administrator rights.
2. Select the entry **Extras** > **File management** > **Upload certificate or file**.



3. Select the components that you wish to upload to the device:
   - Root certificate
   - Device certificate
   - Private key for the device
   - PKC#12 file with a combination of root certificate, device certificate and private key

The relevant password must be entered depending on the type of file to be uploaded.

The uploaded files can then be inspected under **Extras** > **LCOS menu tree** > **Status** > **File system** > **Contents**.



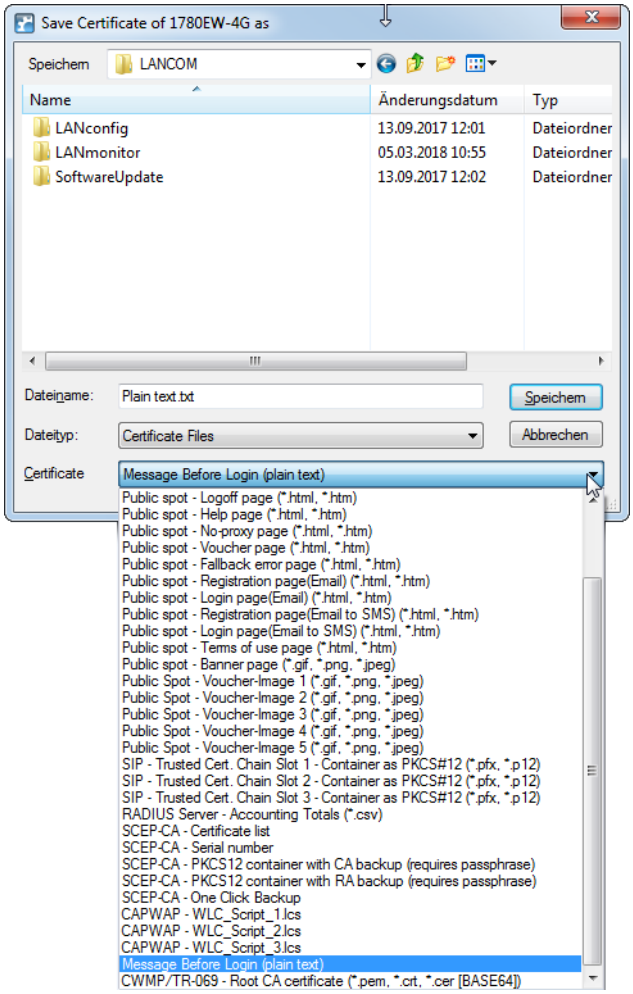
A combined PKCS#12 file is divided up into the necessary components upon upload.

11.6.12 Saving and uploading certificates with LANconfig

Various certificates can be used in a device for the encryption of certain services. These certificates can be uploaded to the devices by using LANconfig. Furthermore, the certificates in a device can also be read by LANconfig and stored to a file.

1. Select the device which you want to upload a certificate into, or from which you want to save a copy.

2. Click on the device with the right mouse key and from the context menu, select **Configuration management** and select either **Save certificate as file** or **Upload certificate from file**.



3. Select the storage location and the type of certificate to be saved or uploaded and confirm your selections with **Save** > **Open**.

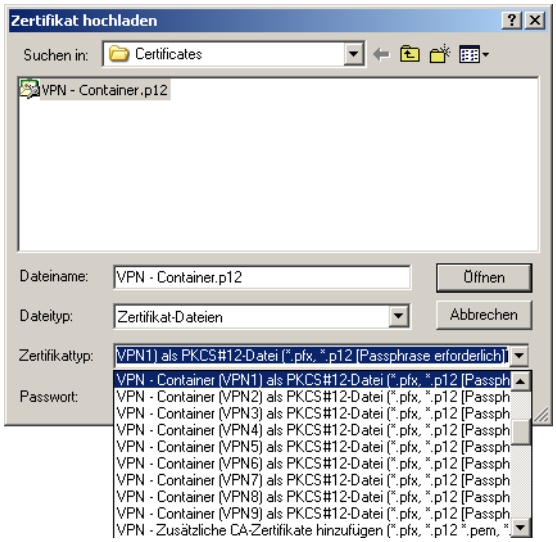
By selecting several devices, a certificate file can be uploaded to several devices at once. It is however not possible to simultaneously save the certificates from multiple devices. Depending on the type of certificate file, a passphrase may be necessary for uploading.

11.6.13 Extended certificate support

11.6.13.1 Multi-level certificate hierarchies

In order to support multiple certificate hierarchies, up to nine PKCS#12 files can be uploaded to the device. Also, further files with individual additional CA certificates can be uploaded, which enclose the certificates either individually or as PKCS#12 containers. All certificate hierarchies can be managed manually or with SCEP, and they can use CRLs.

LANconfig: **Device** > **Configuration management** > **Upload certificate from file**



The certificates in the device can be viewed in the status area:

WEBconfig: **Extras** > **LCOS menu tree** > **Status** > **Certificates** > **Device-Certificates**

The internal file system for the device classifies the device certificates as applications "VPN1" to "VPN9".

To use the certificate, either the certificate subject or this abbreviation can be used as “local identity” in the IKE keys of type ASN.1-Distinguished Name.

Using this abbreviation to reference the certificates allows subjects containing special characters to be used, such as German umlauts. This is not usually possible when working with the command-line interface configuration.

The abbreviation is entered as "Application" when configuring the certificates for the SCEP client.

11.6.13.2 Adjustable trace level for the SCEP client

The output of trace messages for the SCEP client trace can be restricted to contain certain content only. The specified value defines the amount of detail of the packets in the trace.

Command prompt: **Setup** > **Certificates** > **SCEP-Client** > **Trace-Level**

Trace level

Possible values:

All (default)

All trace messages, including information and debug messages.

Reduced

Error and alert messages only.

Only errors

Error messages only

11.6.14 Set up VPN connections to support certificates

VPN connections that support certificates are only established if the device has the correct time. Without the correct time, the device cannot correctly assess the validity of the certificates, which causes the certificates to be rejected: no connection will be established.

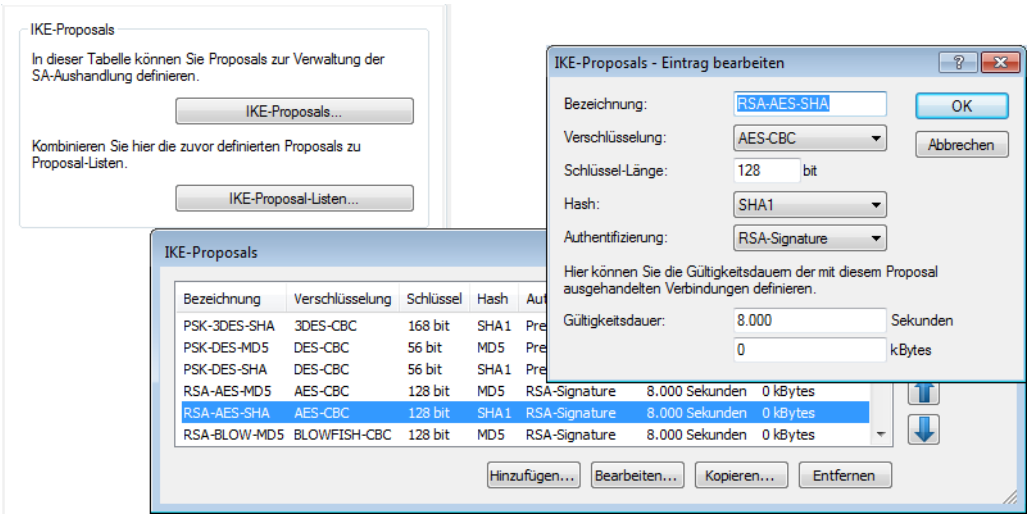
Several areas of the configuration have to be changed to set up VPN connections to support certificates.

- IKE proposals
- IKE proposal lists
- IKE keys
- VPN parameters
- Connection parameters

Some of the values may already be available in your device depending on its firmware version. In this case you just have to check that the values are set correctly.

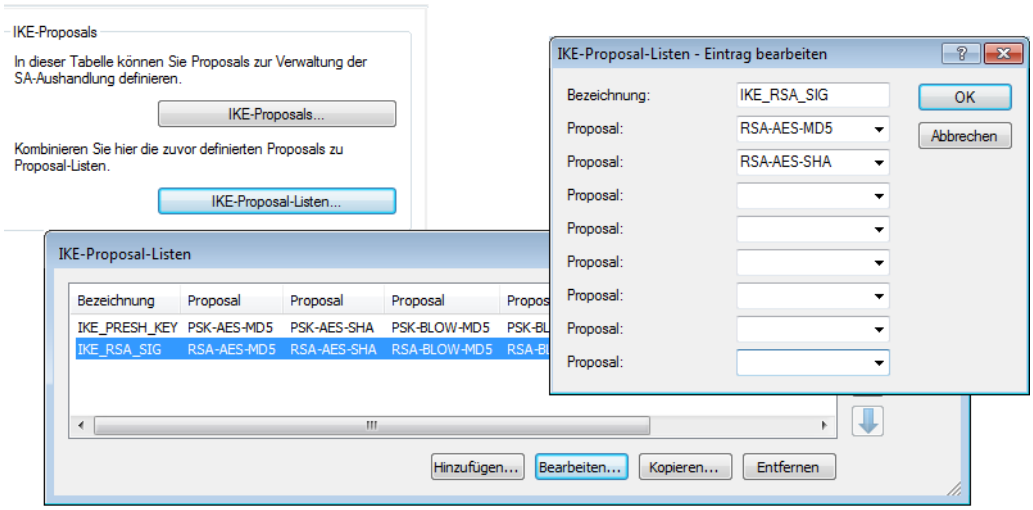
If you are reconfiguring a remote device for certificate support with the method described below, and that device can only be reached via a VPN tunnel, then it is imperative that you reconfigure the remote device first before adjusting the connection in the local device. Changing the local configuration first would make the remote device unattainable!

1. The proposals lists are to be supplemented with two new proposals with the exact description of 'RSA-AES-MD5' and 'RSA-AES-SHA', both of which use 'AES-CBC' for encryption and 'RSA signature' as the authentication mode, and which differ only in their hash method.



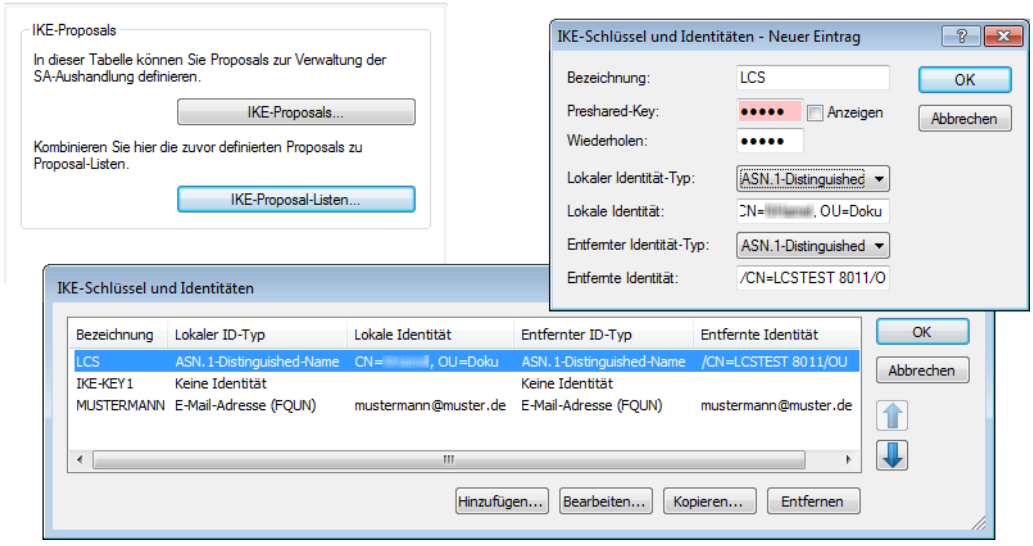
LANconfig: **VPN** > **IKE/IPSec** > **IKE proposals** > **IKE proposals**

2. A new list will be required in the proposals lists with the exact name 'IKE_RSA_SIG' which contains the two new proposals 'RSA-AES-MD5' and 'RSA-AES-SHA'.



LANconfig: **VPN** > **IKE/IPSec** > **IKE proposals** > **IKE proposal lists**

3. In the list of IKE keys, all certificate connections must be set up with the corresponding identities.



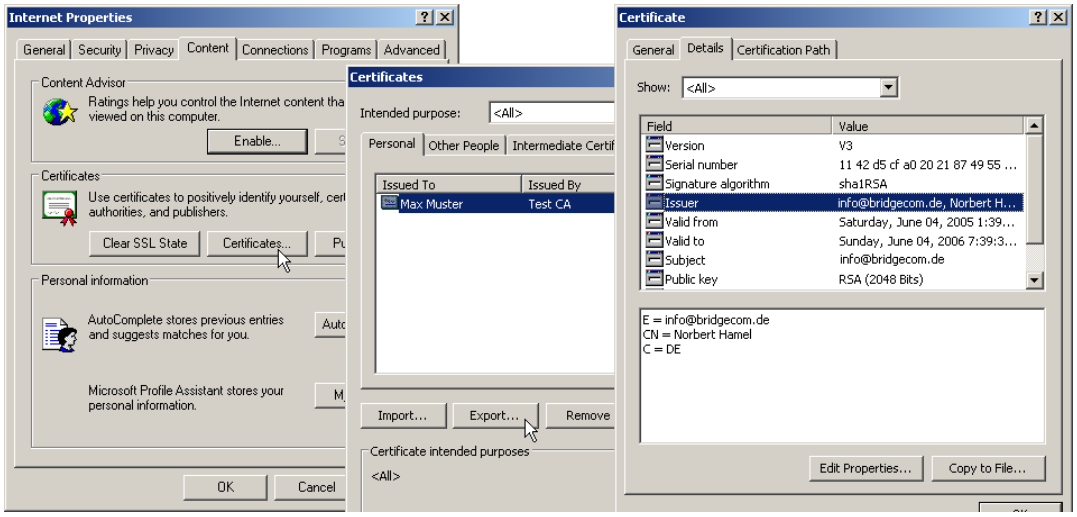
LANconfig: **VPN** > **IKE/IPSec** > **IKE keys & identities**

- Once it is no longer required, the preshared key can be deleted.
- The type of the identities is reset to ASN.1 Distinguished Names (local and remote).
- The identities are entered exactly as they stand in the certificates. The individual values such as 'CN', 'O' or 'OU' can be separated by commas or slashes.

All of the values entered in the certificates must be listed in the same order. If necessary, check the certificate contents by using the Control Panel. To do this, use the Windows search, enter **Internet options** and open it. Here, go to the **Content** tab and click the button **Certificates**.

Open the certificate and use the **Details** tab to select the corresponding value. For the applicant you will find, for example, the necessary ASN.1 Distinguished Names and their abbreviations here. The values listed from top

to bottom in the certificates must be entered into the IKE key from left to right. Observe the use of upper and lower case!

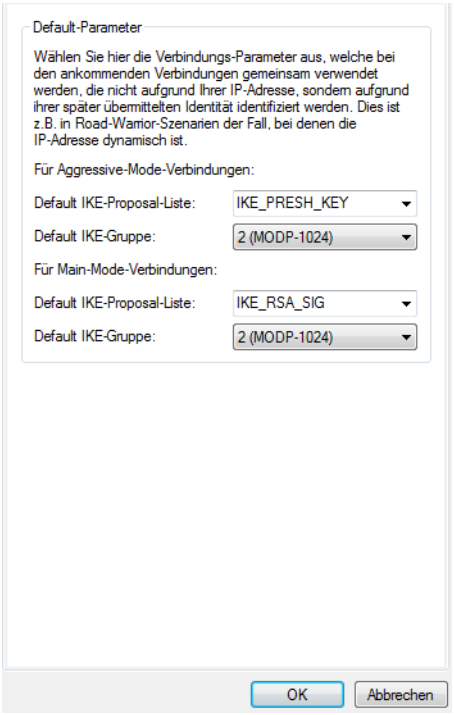


Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

Special characters in the ASN.1 Distinguished Names can be entered by typing in the hexadecimal ASCII codes after a leading backslash. For example, "\61" corresponds to a small "a".

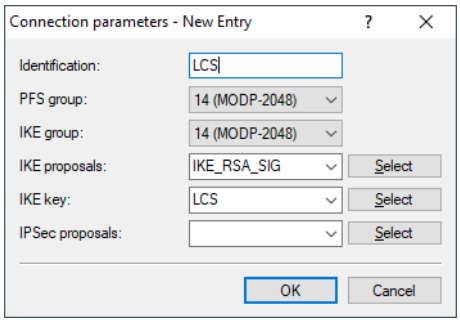
4. In the IKE connection parameters, the default IKE proposal lists for incoming aggressive-mode and main-mode connections must be set to the proposal list 'IKE_RSA_SIG'. Also observe the settings in the default IKE group which are adjusted in the following step as necessary.

The default IKE proposal lists and default IKE groups in LANconfig are located under **VPN** > **IKE/IPSec** > **Default parameters**:



Finally, the VPN connection parameters must be set up to use the correct IKE proposals ('IKE_RSA_SIG'). The values for 'PFS group' and 'IKE group' must agree with the values set in the IKE connection parameters.

The VPN connection parameters in LANconfig are located under **VPN** > **IKE/IPSec** > **VPN connections** > **Connection parameters**:



11.6.15 Set up certificate-based VPN connections with the Setup Wizard

LANconfig is equipped with Setup Wizards with which you can set up certificate-based LAN connectivity or RAS access via VPN.

VPN connections that support certificates can only be set up if the device is programmed with the correct time and if the corresponding certificates are loaded into the device.

11.6.15.1 LAN connectivity

1. Choose the Wizard "Connect two local area networks (VPN)" for connectivity between two local area networks over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature).
2. Enter the identities contained in the certificate for the local and remote devices. Enter the full information from the respective certificates in the correct order: The ASN.1 distinguished names listed in the certificates from top to bottom under Windows are entered into LANconfig from left to right.

   Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

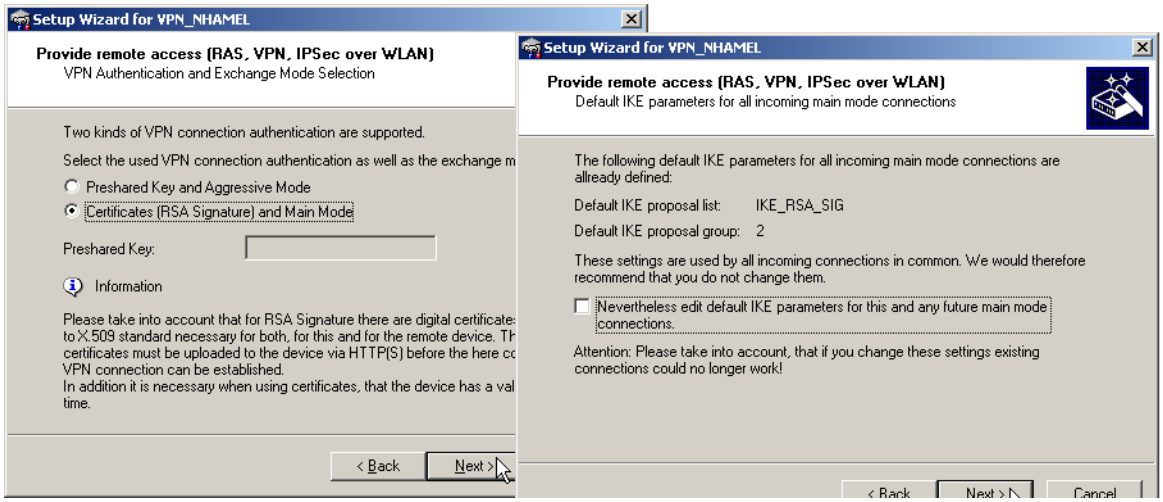
   The CLI command `show vpn cert` displays the content of the certificate in a device, including the entered Relative Distinguished Names (RDN) under "Subject".
3. If available choose the optimized connection establishment with IKE and PFS group 14. Only choose group 5 for IKE and PFS if this is required by the remote device.
4. Enter the names of the VPN remote site, the IP address, the netmask for the remote network and, if applicable, the domain for the DNS forwarding. If required, activate "Extranet" function.

11.6.15.2 RAS connections

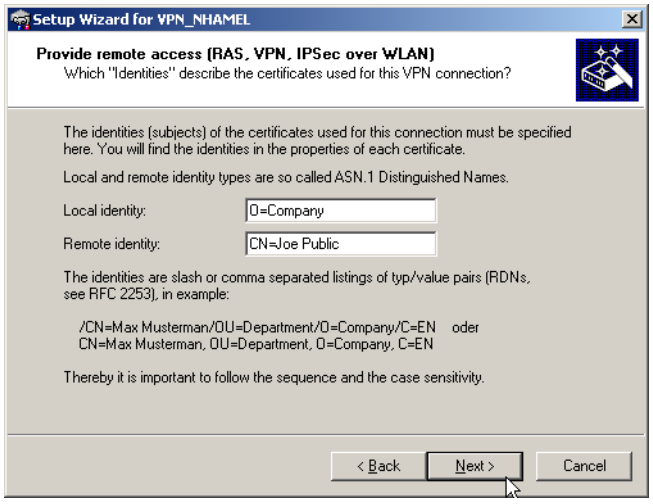
RAS connections that support certificates can be set up for the LANCOM Advanced VPN Client or for any other VPN client with user-defined parameters. The LANCOM Standard VPN Client does not support certificates.

Various parameters are requested depending on the choice of client or the options. This description shows all of the possible Wizard dialogs, some of which may not necessarily be relevant for your application.

1. Choose the Wizard that provides remote access over VPN. In the appropriate dialog, select VPN connection authentication with certificates (RSA signature). The default "Exchange Mode" is the Main Mode.



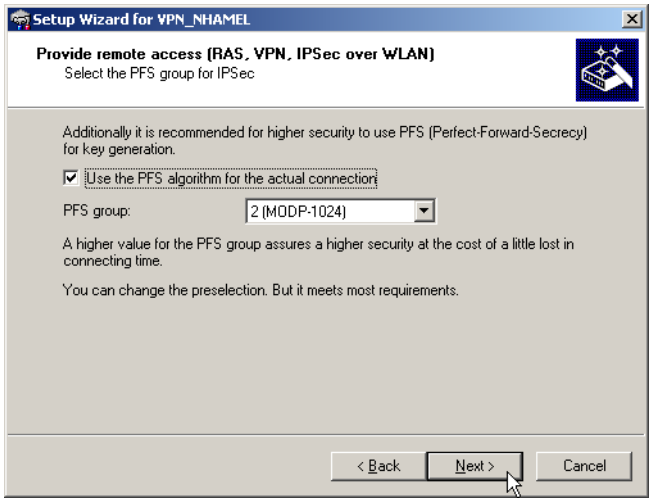
2. The configuration normally presents standard IKE parameters for incoming main mode connections in the standard IKE proposal list 'IKE_RSA_SIG'. If possible use the list of prepared IKE parameters.
3. If you wish to use different parameters for incoming main mode connections, you can adapt the standard IKE parameters to fit your requirements. You can either create a new list 'WIZ-IKE-MAIN-MODE' or you can select one of the existing IKE proposal lists as the new "Standard IKE proposal list". The list defined here will be used for all incoming main mode connections in the future. For a new IKE proposal list, you can select the encryption and authentication methods that are to be used by the client during the IKE negotiation.
4. Enter the identities contained in the certificates for the local and remote devices. Be sure to use the information from each certificate in full and in the right order: The ASN.1-Distinguished Names listed in Windows from top to bottom in the certificates must be entered into LANconfig from left to right.



Microsoft Windows displays some values in the certificates with outdated abbreviations, such as 'S' instead of 'ST' for 'stateOrProvinceName', or 'G' instead of 'GN' for 'givenName'. In these cases make sure that you use the current abbreviations 'ST' and 'GN'.

The Telnet command `show vpn cert` displays the content of the device certificate in a device, including the entered Distinguished Names (DN) under "Subject". The Distinguished Names are displayed in reverse order here until LCOS 6.00 and in the usual order as of LCOS 6.10!

5. If available choose the optimized connection establishment with IKE and PFS group 2. Only choose group 5 as the PFS group if this is required by the client.

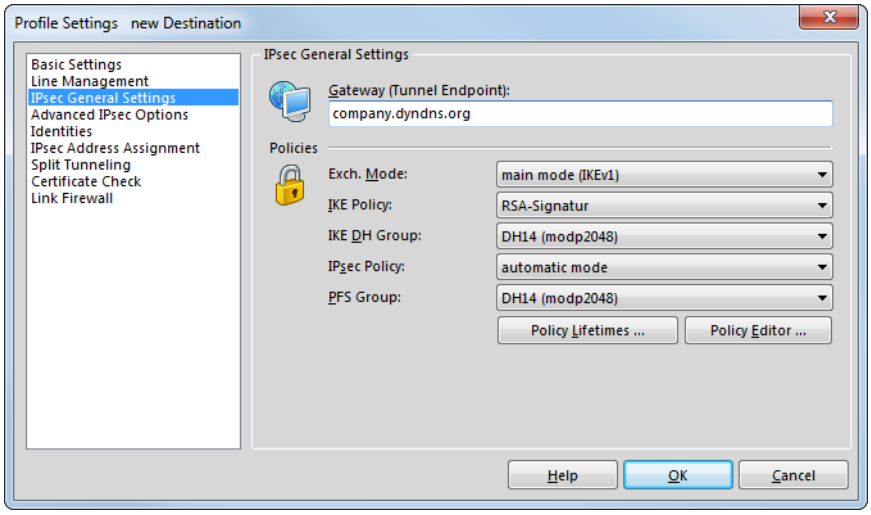


6. The following dialogs define the encryption and authentication methods, the authentication header and the data compression that the client will use for the transfer of the payload data with IPSec. Use the preset values as much as possible as long as the client does not demand different settings.
7. Enter the IP address of the client and for the address range that is to be accessible in the local network.

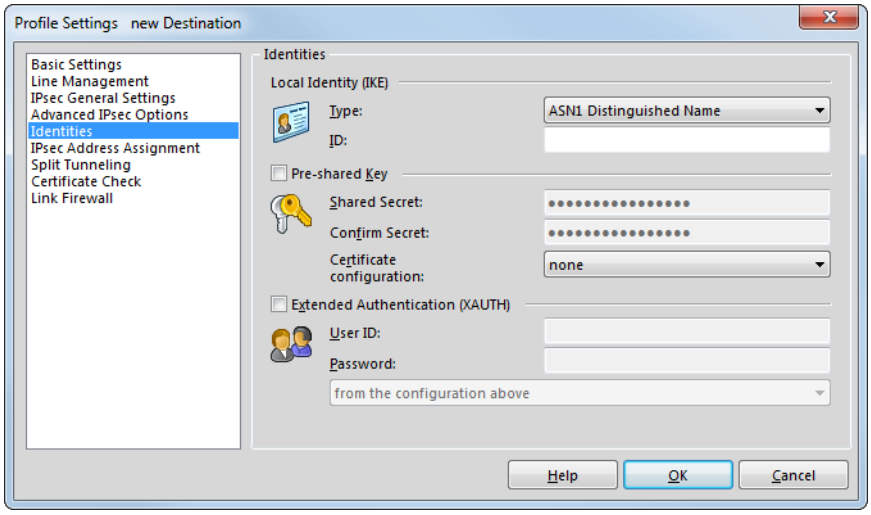
11.6.16 Setting up the LANCOM Advanced VPN Client for certificate connections

To use the LANCOM Advanced VPN Client to dial in to a router, the appropriate profile settings must be adjusted to allow for the use of certificates.

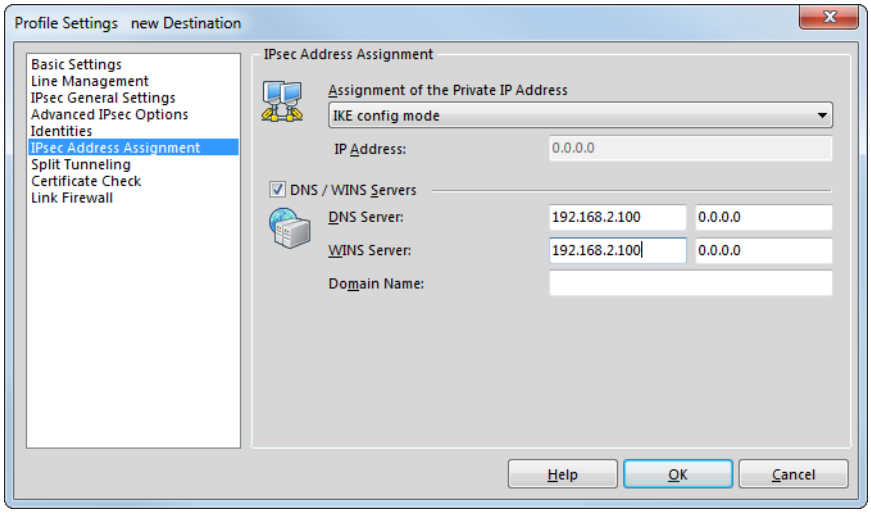
1. In the IPSec General Settings for the profile, change the IKE policy to 'RSA signature'.



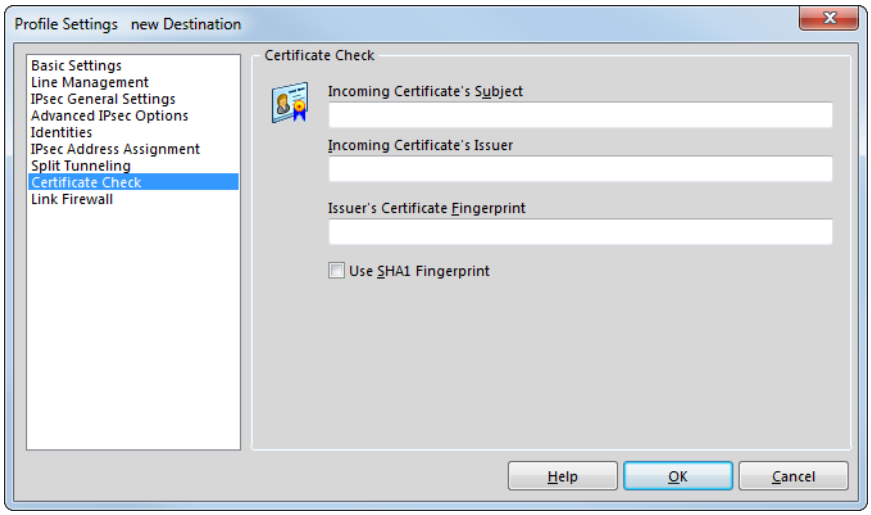
2. Switch the identity to 'ASN1 Distinguished Names'. The 'identity' can remain blank since this information is taken from the certificate.



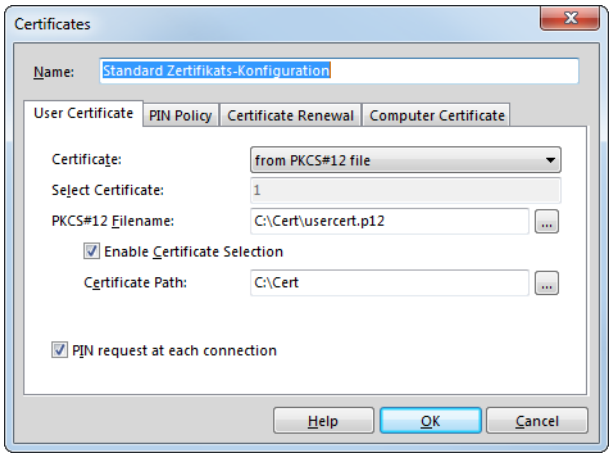
3. Use the 'IKE config mode' to assign the IP address.



4. For the certificate check, you can optionally restrict the certificates accepted by the LANCOM Advanced VPN Client. To do this, you define the user and/or the issuer of the incoming certificate and, if applicable, the associated "fingerprint".

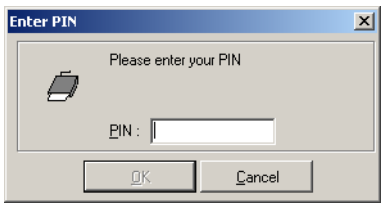


5. After storing the adapted connection profile, click on the menu item **Configuration / Certificates** to open the settings for the User Certificate.

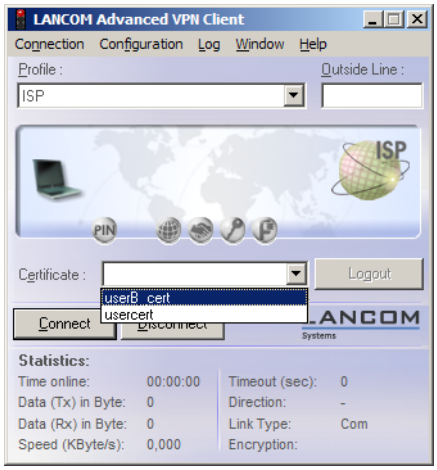


6. Select the certificate type 'from PKCS#12 file' and set the required certificate file.

   - To work with different certificates, activate the option 'Soft Certificate Selection' and enter the path for the folder where the certificate files are stored.
   - Specify whether the PIN (password) for the certificate should be requested for every connection. Alternatively, the PIN can be permanently stored in the LANCOM Advanced VPN Client under the menu item **Connection** > **Enter PIN**.



› If you have enabled certificate selection, when you initiate the connection you can select the required certificate in the main window of the LANCOM Advanced VPN Client according to the selected profile.



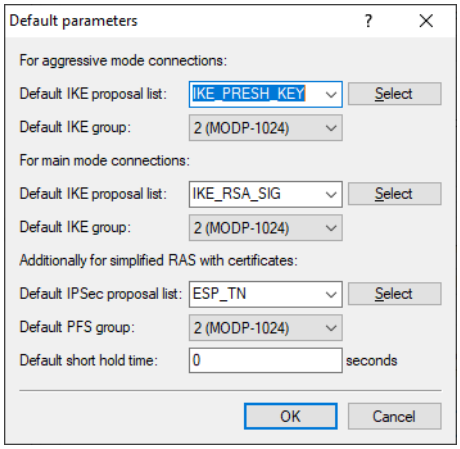
11.6.17 Simplified RAS with certificates

When computers with changing IP addresses dial in, the identity of the remote site is unknown when the IKE negotiation (phase 1) begins. The communication relies on default values for IKE proposal lists and IKE proposal groups. During negotiation, the identity is communicated and this is used to determine the parameters for phase 2 (IPsec proposal list and PFS group). For this to occur, every single user must be entered individually into the VPN router configuration.

With certificate-based RAS, the identity is communicated via the certificate. To avoid having to make individual user entries in the router configuration, common parameters for phase 2 can be defined for all users who are identified by certificate. All the user requires for simplified RAS is a valid certificate with a signature from the publisher of the root certificate in the device. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

Information about configuring the VPN client is available in the relevant documentation from the software manufacturer.

To configure the simplified dial-in in LANconfig, enable the option **VPN** > **General** > **Simplified RAS with certificates activated**. If necessary, the default parameters can be found under **VPN** > **IKE/IPSec** > **Default parameters**.



By activating the simplified RAS with certificates, **all** clients with a valid certificate signed by the issuer of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-in connections are then prevented exclusively by blocking the certificates and using a certificate revocation list (CRL).

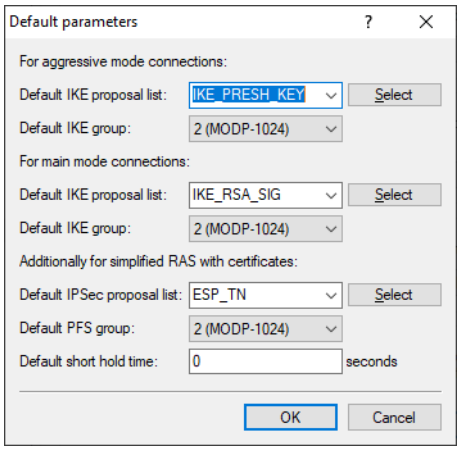
11.6.18 Simplified network connection with certificates – proadaptive VPN

In cases where large network infrastructures are coupled via VPN, it is advantageous for the costs and effort in configuring a new subnetwork to be confined to the local VPN router and for the central dial-in router configuration to remain unchanged. In order to achieve this simplified network connection, the dial-in devices transmit their identity with the help of a digital certificate.

If simplified dial-in with certificates is activated for the router at headquarters, then the remote routers can suggest a network to be used for the connection during the IKE negotiation in phase 2. This network is entered, for example, when setting up the VPN connection on the remote router. The router at the headquarters accepts the suggested network as long as the simplified dial-in is activated with **VPN** > **General** > **Simplified RAS with certificates activated** in addition to activating the option **VPN** > **General** > **Allow peer to select remote network**. Moreover, the parameters used by the client during dial in must agree with the default values in the VPN router.

When configuring the dial-in remote sites, be sure to note that each remote site requests a specific network so that no network address conflicts arise.

If necessary, the default parameters can be found under **VPN** > **IKE/IPSec** > **Default parameters**.



By activating the simplified RAS dial in, **all** remote routers that have a valid certificate signed by the publisher of the device's root certificate can dial in to the corresponding network. No further configuration of the router is necessary! Unwanted dial-in connections are then prevented exclusively by blocking the certificates and using a CRL. The simplified connection of networks with certificates is therefore limited to models that support certificate revocation lists (CRL).

11.6.19 Request certificates using CERTREQ

During IPsec negotiations authenticated with the use of RSA signatures, some VPN gateways expect the remote site to request the certificates to be exchanged via a "certificate request" (CERTREQ). Among other things, this allows the gateway to select the certificate to be used providing that the gateway trusts more than one CA.

In order to establish a connection to these VPN gateways, the VPN router sends a corresponding CERTREQ when the connection is initiated. This is received by the publisher of the root certificate stored in the router.

11.6.20 Certificate revocation list – CRL

Certificates for VPN connections have a validity period by a start date and an end date. During this period, the certificate can be used to establish a VPN connection. Should an employee leave the company, then it should be possible for certificates, for example that were used for mobile VPN access, to be declared as invalid. This prevents continued access to the company network and does not require any changes to the VPN router configuration.

The certificate is physically located with the ex-employee and cannot be changed, which is why a certificate revocation list is of use. Certificates which are no longer valid are entered into the CRL, which are supported by Microsoft CA and

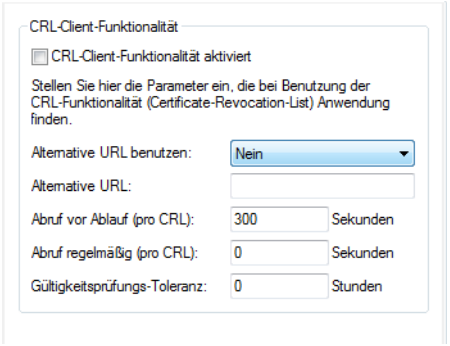
OpenSSL, for example. The CRL is available from a suitable server. The URL to be used by a router to download the CRL into its own memory is entered into the root certificate of the VPN router and/or into the configuration of the device itself.

The CRL is renewed by the CA on a regular basis, enabling changes in the CRL, such as withdrawn certificates, to be recognized by the VPN routers in good time. During the setup at the CA, a schedule is defined for the regular updating of the CRL. After an update to the CRL and its storage to the server (manual or automatic), the VPN router then has to update its information, too. To do this, the router reads out the validity period of the CRL and, briefly before expiry, attempts to load a current version. Alternatively, a regular update which depends on the validity period of the CRL can be set in the router.

When a connection is being established, the VPN router checks if the remote site's certificate is in the current CRL. Connections to remote sites without a valid certificate are rejected.

11.6.20.1 Configuring the CRL function

The address where a certificate revocation list (CRL) can be collected is normally defined in the certificate (as crlDistributionPoint). Configuration of the CRL function involves the definition of additional parameters such as the update interval.



Configuration tool	Request
LANconfig	**Certificates** > **CRL**
CLI	**Setup** > **Certificates** > **CRLs**

CRL client utilization activated

When checking the validity of a certificate, a CRL is referred to, if available.

With the CRL function activated, a newly started system will always block new (certificate-based) connections until the system has a valid CRL with a match for the certificate. With the CRL function activated, existing connections are maintained but subsequent phase 1 rekeying will fail.

Update before (per CRL)

This value is always increased by a random value from 0 to 59 seconds to prevent server overload from multiple simultaneous queries. At the beginning of this period, regular updating, if any, is stopped.

If CRL retrieval fails, a new attempt is made every 30 seconds.

Retrieve regularly (per CRL)

The interval between regular attempts to download a new CRL.

In the case that the CA spontaneously issues new CRLs (i.e. in the middle of the current CRL's validity period), an interval can be defined in which regular attempts are made to download a new CRL after the previous

download. This allows the new CRL to be used sooner than following the expiry of the current CRL. A interval of 0 switches this function off.

If with regular updates the CRL cannot be retrieved, no further attempts will be started until the next regular attempt.

Validity check tolerance

Even after expiry of the CRL, certificate-based connections will continue to be accepted for the period defined here. This tolerance period can prevent the unintentional rejection or interruption of connections if the CRL server should be temporarily unavailable.

Within the time period defined here, even certificates in the CRL which have expired can still be used to maintain or establish a connection.

Alternative URLs

The address where a certificate revocation list (CRL) can be collected is normally defined in the certificate (as crlDistributionPoint). Alternative CRLs can be specified in a table in the firmware. After a system start the CRLs are automatically collected from these URLs. These are used in addition to the lists offered by the certificates.

11.6.20.2 CRL status display in LANmonitor

Information about the validity period and the publisher of the current CRL in the device can be inspected in LANmonitor under **Certificates** > **CRLs**.

11.6.21 Wildcard matching of certificates

11.6.21.1 Introduction

Generally speaking, the local identity and remote identity for certificate-based VPN connections are the certificate subjects. In the VPN configuration, these are stored in the form of (often complex) ASN.1 Distinguished Names (DN). During VPN negotiation, the local identity is used to select the certificate which is to be transmitted to the remote station, whereas the local value for the remote identity is compared with the received identity of the remote station and the subject of the received certificate.

Until now, the local and the remote identities had to be entered in full into the VPN configuration. Not only is this prone to error, it is sometimes desirable to specify only a part of the certificate subject. This is practical where different certificates with similar subjects are to be accepted automatically, for example where certificates can change, or where multiple parallel certificate hierarchies operate simultaneously.

This is facilitated by flexible identity comparison. The certificate subjects have to contain the components of an ASN.1 Distinguished Name (DN) (Relative Distinguished Names – RDNs) as included in the configured identities. The RDNs can be in any order. Also, the RDN values can include the wildcards "?" and "*". If the RDNs are to include wildcards, these must be entered in the form "\?" or "*". Examples:

- Subject = '/CN=John Doe/O=*ACME*', DN = '/CN=John?Doe*'
- Subject = '/CN=John Doe/O=*ACME*', DN = '/O=*ACME*'

11.6.21.2 Configuration

This flexible method of identification comparison is activated or deactivated in the VPN configuration.

Command prompt: **Set up** > **VPN** > **Flexible-ID-Comparison**

Possible values:

- Yes, No
- Default: No

Flexible identity comparison is used when checking the (received) remote identity and also for selecting the certificate based on the local identity.

11.6.22 Diagnosis of VPN certificate connections

If the VPN connection establishment does not work as desired, then entering the following commands on the CLI can provide useful information.

- `trace + vpn-status`

  Displays a trace of the current VPN connections.

- `show vpn long`

  Displays the contents of the VPN configuration, including the entered Distinguished Names (DN).

- `show vpn ca`

  Displays the content of the root certificate.

- `show vpn cert`

  Displays the content of the device certificate.

  The relative distinguished names are shown in reverse order up to firmware version 6.00 and in the normal order as of firmware version 6.10!

11.6.23 OCSP client for certificate validation

11.6.23.1 Introduction

The Online Certificate Status Protocol (OCSP) provides a way to verify the status of certificates, for example when establishing VPN connections. The devices use this protocol to investigate whether the issuer has revoked the certificate before its expiry, so marking it as invalid.

Certificate issuers update the status of all issued certificates on a special server, the OCSP responder. The OCSP client (e.g. a VPN router that wants to establish a connection) uses the HTTP protocol to send an OCSP request to the responder to verify the certificate. The responder answers with a signed response, which the OCSP client uses to verify its validity. The message from the OCSP responder describes one of the following conditions:

- Good: The verified certificate has not been revoked.
- Revoked: The verified certificate has been revoked and may not be used to establish VPN connections.
- Unknown: The OCSP responder cannot determine the status of the certificate. This may be because the OCSP responder does not recognize the certificate issuer because the certificate has been faked and therefore has not been entered into the database of the OCSP responder.

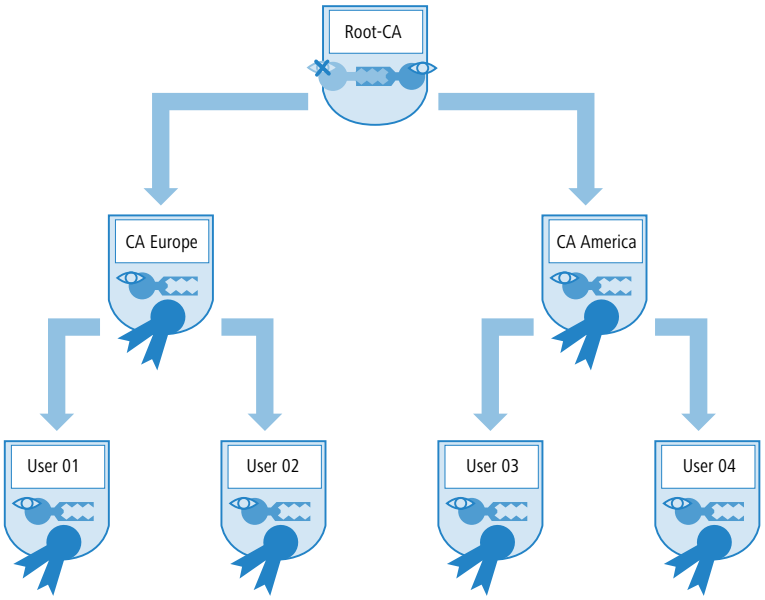
You can use the OCSP to complement or substitute certificate verification by certificate revocation lists (CRL). OCSP offers the following advantages when compared to CRLs:

- The issuers generate the CRLs at specific time intervals and, in the ideal case, distribute the CRLs to the devices which use the certificates for establishing VPN connections. The reliability of this check thus depends on the speed with which CRLs in the devices are updated. However, certificate verification through an OCSP responder is always "online", i.e. it is automatically updated. The operator of the OCSP responder can automatically synchronize their data with that of the CA or CAs, thus ensuring that they are up to date at all times.
- Using certificate revocation lists for certificate verification takes up a considerable amount of device memory, especially if the CRLs are large. Querying certificate status from an OCSP responder, on the other hand, is independent of the number of CAs and certificates being used, and is therefore more scalable.
- As the CRL method does not allow for unknown certificates, this method cannot detect fake certificates. The OCSP responder, depending on its configuration, responds to a request about an unknown certificate with a negative evaluation.

11.7 Multi-level certificates for SSL/TLS

11.7.1 Introduction

Larger or geographically dispersed organizations often make use of multi-level certificate hierarchies that rely on one or more intermediate CAs to issue certificates. The interim CAs themselves are certified by the Root CA.



To authenticate final certificates, it must be possible to check the entire certificate hierarchy.

11.7.2 SSL/TLS with multi-level certificates

For applications based on SSL/TLS (e.g. EAP/802.1X, HTTPS or RADSEC), the SSL (server) certificate together with the private key and intermediate level CA certificate(s) are loaded into the device as a PKCS#12 container.

The remote devices establishing a connection only have to send their own device certificates to the device. The certificate chain is checked for validity in the device.

11.7.3 VPN with multi-level certificates

For the certificate-based establishment of VPN connections, the following are stored to the file system in the device: A private key, a device certificate, and the CA certificate. With single-layer certificate solutions this can be handled with the individual files or with a PKCS#12 file. After uploading and entering the password, a container is separated into the three components indicated above.

In the case of a multi-level certificate hierarchy, however, a PKCS#12 container has to be used that includes the CA certificates from all levels in the certificate chain. After uploading and entering the password, the private key, the device certificate and the certificate from the next CA "above" the device are unpacked—the other certificates remain in the PKCS#12 container. The unpacked certificates and the certificates from the container are imported when the VPN configuration is updated. A remote station establishing a VPN connection transfers its own device certificate only and not the entire chain. The device then checks this certificate against the hierarchy available to it.

The certificate structures in the two peers must match to one another, i.e. the hierarchy in the VPN device making the request should not demand certificates that are not included in the other VPN device's hierarchy.

11.8 Certificate enrollment via SCEP

An increasing number of certificate-based VPN connections are being used to provide secure communications via public networks. The high levels of security provided by certificates comes at the price of significantly higher levels of effort in the administration and distribution of certificates. Most of this effort arises at branch offices or home offices within a geographically dispersed network structure.

A VPN router requires the following components to establish a certificate-based VPN connection from a remote site to the network at the headquarters:

- The Root CA's certificate with the CA's public key. The headquarters also requires a certificate issued by the same CA.
- The device's own certificate with its own public key. This certificate is signed with the CA's private key and serves identity confirmation.
- Own private key.

The SCEP client supports one certificate per usage type (VPN, WLAN controller). For the CAs, the setting "General" can be selected along with the usage type. If a general CA is entered, this CA is used for all certificates.

In the case of a conventionally structured VPN with certificates, the keys and certificates have to be loaded into each device manually and exchanged before they expire. The Simple Certificate Enrollment Protocol (SCEP) enables a secure and automatic distribution of certificates via a suitable server, so reducing the effort of roll-out and maintaining certificate-based network structures. There is no need for an external application to generate the key pair and subsequently transfer it to the device. Instead, the key pair is generated directly by the VPN router itself; the private portion of the key never has to leave the device, which results in a significant gain in security. A VPN router can automatically retrieve the CA root certificate and its own certificate from a central location.

11.8.1 SCEP server and SCEP client

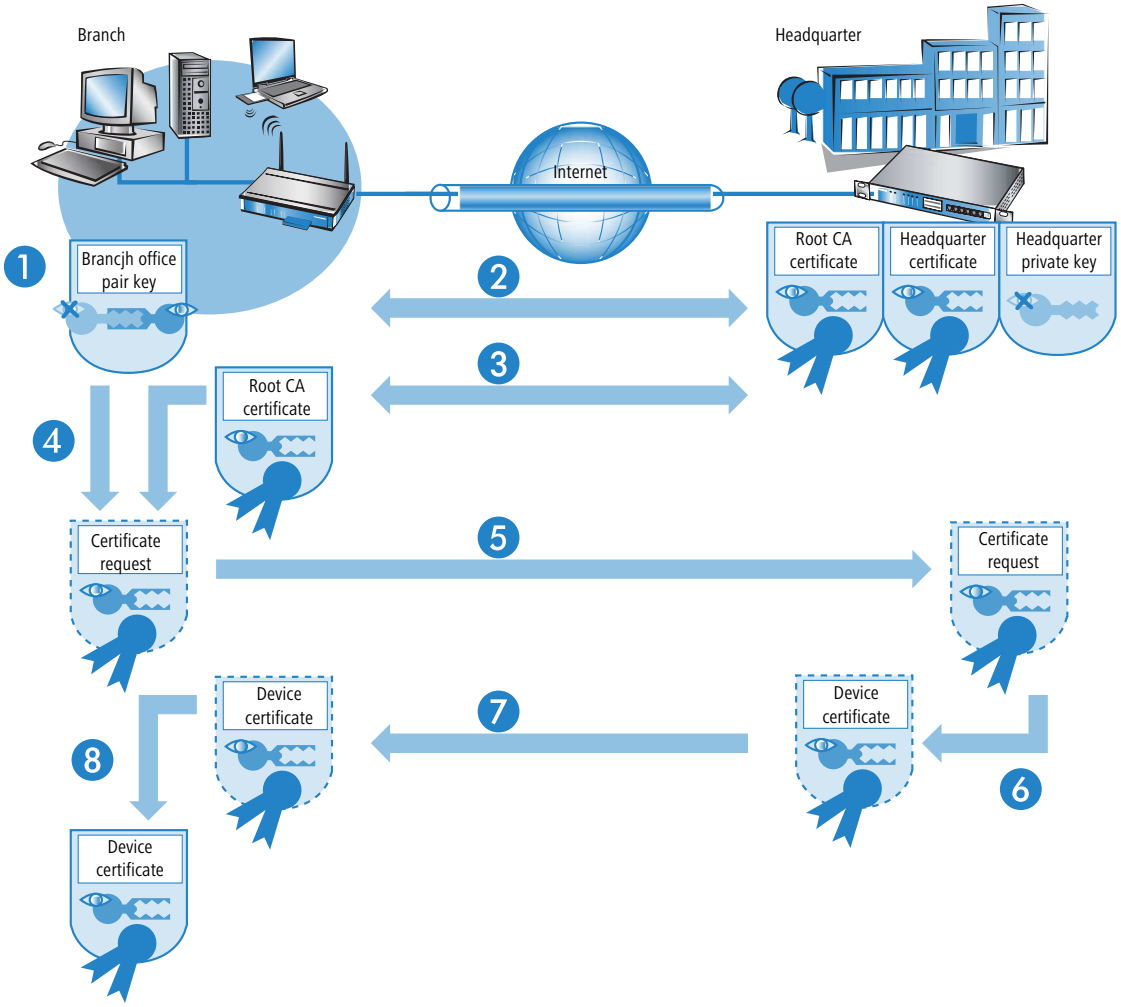
Provisioning and administration of the certificates is handled by an SCEP server that fulfills the usual function of a Certificate Authority (CA) as well as the SCEP functions. This server can, for example, be implemented as a Windows Server CA by using a special plug-in (mscep.dll). There are also a number of other CA solutions which work with SCEP, such as the OpenSource solution OpenCA (www.openca.org).

The SCEP extension such as with mscep.dll creates an additional instance on the server and processes requests from SCEP clients for forwarding to the actual CA. This entity is referred to as the Registration Authority (RA).

The VPN routers are SCEP clients that attempt to automatically retrieve the necessary certificates from the central server. Also generally required by the SCEP procedure are the RA (Registration Authority) certificates as signed by the CA. For VPN operations the VPN routers primarily require valid system certificates (device certificates). Any other certificates which may be in use only apply to the SCEP procedure.

11.8.2 Distributing certificates

In brief, the procedure for distributing certificates via SCEP is as follows:



1. Generate the key pair in the VPN router.

   A key pair is generated in the VPN router. The public part of this key pair is later sent together with the request to the SCEP server. The private key remains in the SCEP client (VPN router). The fact that the private key never has to leave the device is a major security gain over manual certificate distribution, for example with PKCS#12 containers.

2. Retrieve CA and RA certificates.

   For communication with the RA/CA, the appropriate RA and CA certificates must be available in the VPN router. To ensure that CA certificates retrieved via SCEP do genuinely originate from the CA, an automated check can be carried out with the use of a fingerprint which is defined in advance. SCEP itself has no mechanism for clients to conduct automated authentication of CA certificates. If the administrator of the VPN router does not have direct access to the CA then the fingerprint can be checked manually, for example with a telephone call to the CA admin.

3. Generate and encrypt the request for a device certificate.

   To place a request for a system or device certificate, the SCEP client collects all of the configured information such as the identity of the requester device and, if applicable, the "challenge phrase" or password for automatic request processing by the SCEP server. This request is signed with the private key.

4. Send the request to the SCEP.

   The SCEP client then sends the request along with its public key to the SCEP server.

5. Check the certificate request on the SCEP server and issue the device certificate.

The SCEP server can decrypt the request and subsequently issues a system or device certificate to the requester. SCEP has the following methods for request processing:

- Automatic processing requires the requester's authenticity to be assured by means of the challenge phrase. The challenge phrase can, for example, be generated automatically by a Windows CA server using mscep.dll. The phrase is valid for one hour. If the challenge phrase submitted with the certificate request agrees with the valid value, the system certificate is issued automatically.
- For manual processing, the SCEP server puts the certificate request "on hold" until the acceptance or rejection has been received from the CA administrator. While waiting, the SCEP client regularly checks with the SCEP server to see if the certificate has been issued yet.
- With RA-AutoApprove, the client is authenticated using a valid certificate issued by the CA.

6. Retrieve device certificate from the SCEP server

   Once the certificate has been issued, the client's regular polling informs it that the certificate is ready for retrieval.

7. Check the device certificate and present it for VPN operation

11.8.3 Configuration of SCEP

To configure SCEP, global parameters are defined for SCEP operations and for the CAs where the device certificates are to be retrieved.

In addition to the configuration of the SCEP parameters, it may be necessary to adapt the VPN configurations.

Configuration tool	Request
WEBconfig, CLI	LCOS Menu Tree > Setup > Certificates > SCEP-Client

11.8.3.1 Global SCEP parameters

- Active

  Turns the usage of SCEP on or off.

  - Possible values: Yes, No
  - Default: No

- Retry-After-Error-Interval

  Interval in seconds between retries after errors of any type.

  - Default: 22

- Check-Pending-Requests-Interval

  Interval in seconds for checks on outstanding certificate requests.

  - Default: 101

- Device-Certificate-Update-Before

  Preparation time in days for the timely request for new system certificates (device certificates).

  - Default: 2

- CA-Certificate-Update-Before

  Preparation time in days for the timely retrieval of new RA/CA certificates.

  - Default: 1

11.8.3.2 Actions

- Reinit

  Starts the manual reinitialization of the SCEP parameters. As with the standard SCEP initialization, the necessary RA and CA certificates are retrieved from the CA and stored within the file system in the VPN router in such a way that they are **not** yet ready for use in VPN operations.

  - If the available system certificate fits to the retrieved CA certificate, then the system certificate, CA certificate and the device's private key can be used for VPN operations.
  - If the existing system certificates do **not** fit to the retrieved CA certificate, then the next step is for the SCEP server to submit a new certificate request. Only once a new system certificate that fits to the retrieved CA certificate has been issued and retrieved can the system certificate, CA certificate and the device's private key can be used for VPN operations.

- Refresh display

  Manually triggers a request for a new system certificate, irrespective of the remaining validity period (lease). A new key pair is generated at the same time.

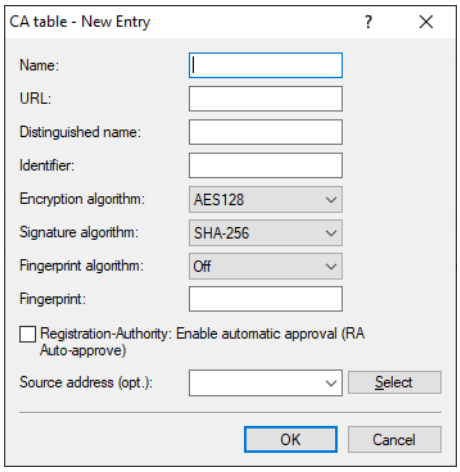
- Clear-SCEP-Filesystem

  Starts a clean-up of the SCEP file system.

  - Deleted are: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.
  - Retained are: System certificates currently in use for VPN operations, associated private keys, and the CA certificates currently in use for VPN operations.

11.8.3.3 Configuring the CAs

The configuration is carried out with LANconfig under **Certificates** > **SCEP client** with the button **CA table**.



Name

Configuration name of the CA.

URL

URL of the CA.

Distinguished name

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

- Comma (",")
- Slash ("/")
- Plus ("+")
- Semicolon (";")
- Equals ("=")

You can also use the following internal firmware variables:

- %% inserts a percent sign.
- %f inserts the version and the date of the firmware currently active in the device.
- %r inserts the hardware release of the device.
- %v inserts the version of the loader currently active in the device.
- %m inserts the MAC address of the device.
- %s inserts the serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

Identifier

CA identifier (as required by some web server to identify the CA).

Encryption algorithm

This algorithm encrypts the payload of the certificate request. Possible values are:

- 3-DES
- AES128 (default)
- AES192
- AES256

Signature algorithm

The certificate request is signed with this algorithm. Possible values are:

- MD5
- SHA1
- SHA256 (Default)
- SHA384
- SHA512

Fingerprint algorithm

Algorithm for signing the fingerprint. This determines whether the CA certificate is to be checked by means of fingerprint, and which algorithm is used for this. The CA fingerprint has to agree with the checksum which results when this algorithm is applied. Possible values are:

- Off (default)
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint

The authenticity of a received CA certificate can be checked by means of the the checksum (fingerprint) entered here (corresponding to the set CA fingerprint algorithm).

RA autoapprove

Some CAs provide the option of using an earlier certificate issued by this CA as proof of authenticity for future requests. This option defines whether an existing system certificate should be used to sign new requests. Possible values are:

- Yes
- No (Default)

Source address

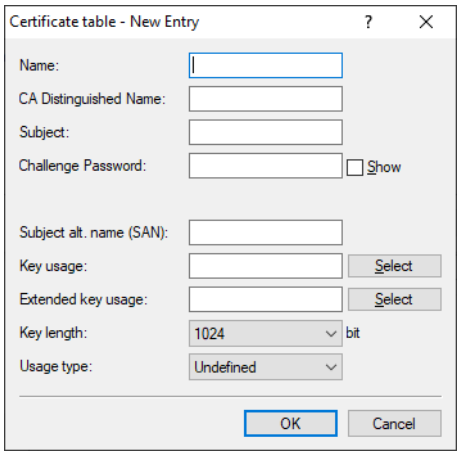
This is where you configure an optional source address to be used instead of the one otherwise automatically selected for the source address. If you have configured loopback addresses, you can specify them here as source address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

11.8.3.4 Configuring the certificate table

The configuration is carried out with LANconfig under **Certificates** > **SCEP client** with the button **Certificate table**.



Name

The certificate's configuration name.

CA distinguished name

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

- Comma (",")
- Slash ("/")

- Plus (“+”)
- Semicolon (“;”)
- Equals (“=”)

You can also use the following internal firmware variables:

- %% inserts a percent sign.
- %f inserts the version and the date of the firmware currently active in the device.
- %r inserts the hardware release of the device.
- %v inserts the version of the loader currently active in the device.
- %m inserts the MAC address of the device.
- %s inserts the serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

Subject

Distinguished name of the subject of the requester.

Challenge password

Password (for the automatic issue of device certificates on the SCEP server).

Subject alt. name (SAN)

Further information about the requester, e.g. domain or IP address.

Key usage

Any comma-separated combination of:

- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly
- critical (possible but not recommended)

Extended key usage

Any comma-separated combination of:

- critical
- serverAuth
- clientAuth
- codeSigning
- emailProtection
- timeStamping
- msCodeInd
- msCodeCom
- msCTLSign
- msSGC
- msEFS
- nsSGC

- 1.3.6.1.5.5.7.3.18 for WLAN controllers
- 1.3.6.1.5.5.7.3.19 for access points in managed mode

Key length

The key length in bits. Possible values:

- 1024
- 2048
- 4096
- 8192

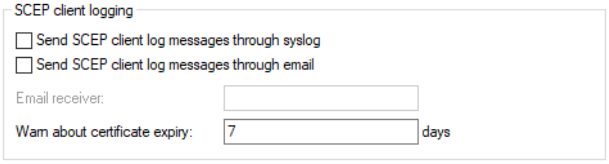
Usage type

Indicates the intended application of the specified certificates. The certificates entered here are only queried for the corresponding application. Possible values:

- VPN
- WLAN controller
- EAP/TLS
- CA
- Default certificate

11.8.3.5 SCEP client logging

LANconfig: **Certificates** > **SCEP Client** > **SCEP client logging**



Send SCEP client log messages through syslog

Enables/disables log message transmission via SYSLOG.

Send SCEP client log messages through email

Enables/disables log message transmission via e-mail.

This requires that you enter an e-mail address in the corresponding input box.

Email receiver

E-mail address to receive the log message.

To make an entry, you first have to activate the option **Send SCEP client log messages through email**.

Warn about certificate expiry

Time interval in days before certificate expiry.

11.8.4 Using smart certificates

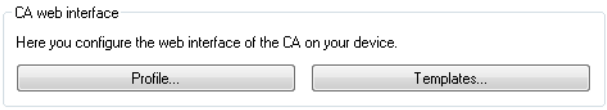
The configuration of the SCEP client for the generation and distribution of certificates can quickly become a complex and laborious task in extensive network infrastructures. This work required for this task can be reduced with the help of predefined, selectable profiles and access via a web interface.

A LANCOM router enables you to create and issue highly secure certificates. It is easy to manage the certificates via the WEBconfig interface of the corresponding device. An external CA is no longer required, which is particularly advantageous for small-scale infrastructures.

Using the Certificate Wizard from LANCOM, even users without certificate know-how can create certificates in just a few steps.

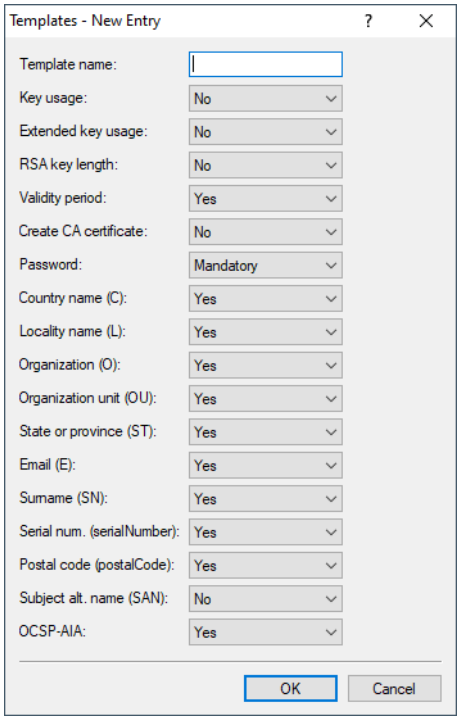
The devices administrator creates the profile as a collection of certificate properties. It contains the configuration of the certificate and also a unique certificate ID. From this point on, all you need to do to create and distribute a certificate is to select one of the profiles.

Profiles can also be managed in LANconfig under **Certificates** > **Certificate handling** in the section **CA web interface**.



11.8.4.1 Creating templates for certificate profiles

In LANconfig, profiles are created under **Certificates** > **Certificate handling** > **Templates**.



A “DEFAULT” a template is already available.

The administrators specifies which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.

These permissions apply to the following profile and ID fields:

Profile fields

- Key usage
- Key usage (extended)
- RSA key length
- Validity period
- Create CA certificate
- Password

Identifier

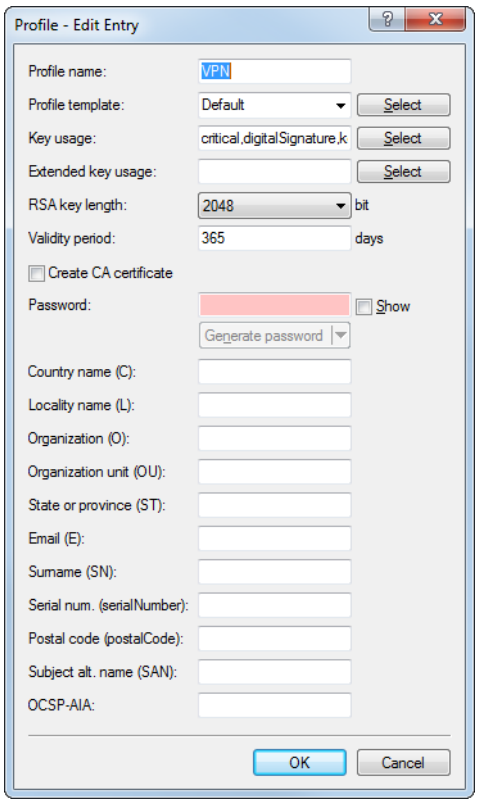
- Country code (C)
- Locality name (L)
- Organization (O)
- Organization unit (OU)
- State or province (ST)
- E-mail (E)
- Surname (SN)
- Serial no. (serialNumber)
- Postal code (postalCode)
- Subject alt. name
- OCSP-AIA

If the Templates table is empty, the user can only see the input fields for the profile name, the common name (CN), and the password. The other profile fields retain the default values as set by the device administrator.

11.8.4.2 Creating a profile in LANconfig

The user needs the appropriate access rights to create, select, modify and assign profiles.

In LANconfig, profiles are created under **Certificates** > **Certificate handling** > **Profile**.



By default three profiles are already available for common application scenarios.

Profile name

The unique name of the profile.

Profile template

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Certificates** > **Certificate handling** > **Templates**.

Key usage

Specifies for which application the profile is to be used. The following usages are available using the **Select** button:

Table 26: The available key usages

Value	Meaning
critical	This restriction requires the extended key usage to be considered. If the extension is not supported, the certificate is rejected as invalid.
digitalSignature	Is this option is used, the public key is used for digital signatures.
nonRepudiation	With this option set, the key is used for digital signatures of a non-repudiation service, i.e. one with a rather long-term character such as notary public service.
keyEncipherment	If this option is set, the key is used for encrypting other keys or security information. It is possible to restrict the use of **encipher only** and **decipher only**.
dataEncipherment	If this option is set, the key is used for encrypting user data (but not other keys).

Value	Meaning
keyAgreement	If this option is used, the "Diffie-Hellman" algorithm is used for key agreement.
keyCertSign	If this option is set, the key is applied to certificates for signature verification. This is useful for CA certificates, for example.
cRLSign	If this option is set, the key is applied to CRLs for signature verification. This is useful for CA certificates, for example.
encipherOnly	This is only useful with the Diffie-Hellman keyAgreement.
decipherOnly	This is only useful with the Diffie-Hellman keyAgreement.

Multiple comma-separated entries can be selected.

Ext. key usage

Specifies the extended application for which the profile is to be used. The following usages are available using the **Select** button:

Table 27: Extended usages

Value	Meaning
critical	
serverAuth	SSL/TLS Web server authentication
clientAuth	SSL/TLS Web client authentication
codeSigning	Signing of program code
emailProtection	E-mail protection (S/MIME)
timeStamping	Furnishing data with reliable time stamps
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto
msEFS	Microsoft Encrypted File System
nsSGC	Netscape Server Gated Crypto

Multiple comma-separated entries can be selected.

RSA key length

Sets the length of the key.

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

Create CA certificate

Indicates whether this is a CA certificate.

Password

Password to protect the PKCS12 certificate file.

The following input creates a certificate ID. The following options are available:

Country code (C)

Enter the country identifier (e.g. "DE" for Germany).

This entry appears in the subject or issuer of the certificate under `C=` (**C**ountry).

Locality name (L)

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under `L=` (**L**ocality).

Organization (O)

Specify the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `O=` (**O**rganization).

Organization unit (OU)

Specify the unit within the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `OU=` (**O**rganization **U**nit).

State or province (ST)

Enter the State or province.

This entry appears in the subject or issuer of the certificate under `ST=` (**ST**ate).

E-mail (E)

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

Surname (SN)

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN=` (**S**ur**N**ame).

Serial no. (serialNumber)

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

Postal code (postalCode)

Enter the location post code.

This entry appears in the subject or issuer of the certificate under `postalCode=`.

Subject alt. name (SAN)

The "Subject Alternative Name" (SAN) links additional data with this certificate. The following data are allowed:

- E-mail addresses
- IPv4 or IPv6 addresses
- URIs
- DNS names
- Directory names
- Any names

This entry appears in the subject or issuer of the certificate under `subjectAltName=` (e.g. `subjectAltName=IP:192.168.7.1`).

OCSP-AIA

This field is required for the OCSP server. It contains the name or IP address where OCSP clients can reach the OCSP server. See *OCSP server* on page 815.

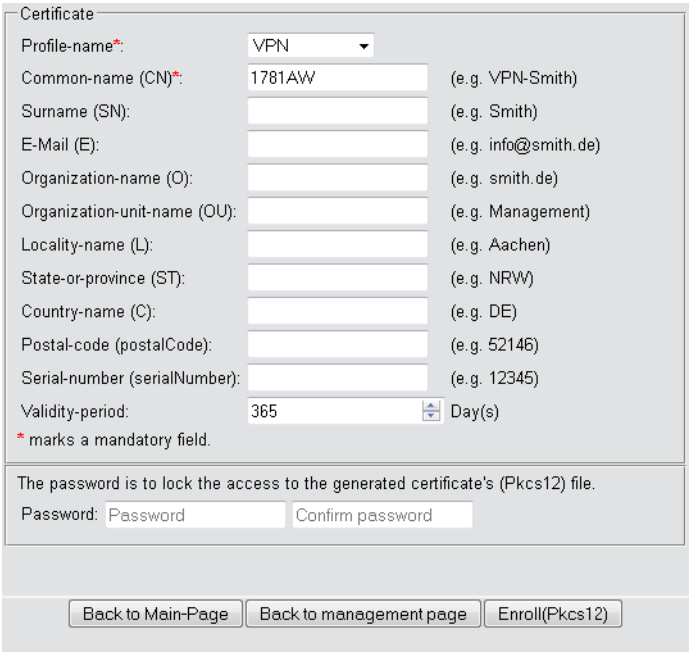
The certificate issuer assigns the general name "CN". The "CN" is required as a minimum.

11.8.4.3 Certificate creation with WEBconfig

You need the appropriate access rights to select, modify and assign profiles.

To create your certificates, navigate to the WEBconfig of the LANCOM device.

1. To create a certificate using the web interface, navigate to the view **Setup Wizards** > **Manage certificates** and select **Create new certificate**.



2. From the **Profile name** drop-down menu, select the profile to be used as the basis for the certificate.

   Empty templates only contain fields with the selection “No”. If the user selects a profile based on an empty template, the input mask displays only the common name. The other profile fields retain the default values as set by the device administrator.

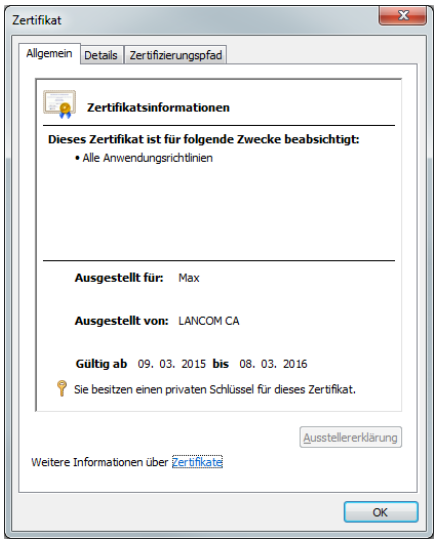
3. Fill out the **common name (CN)** field. Set a validity period for the certificate and give it a secure password (PIN). The other fields such as **Email** and **Organization name** are optional information. However, under certain circumstance this information can help to find the certificate recipient if there are problems with the certificate.

   The following characters are allowed in the password: [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

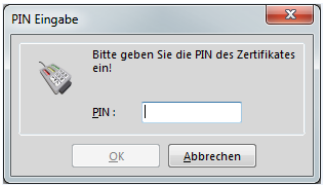
4. To complete of the changes, click the **Enroll (PKCS12)** button. In the following dialog box, you can set the name and location of the file.

The newly created certificates appear in the certificate status table under **Status** > **Certificates** > **SCEP-CA** > **Certificates**.

5. Issue the newly enrolled certificate to the recipient together with the access password set in step 3.



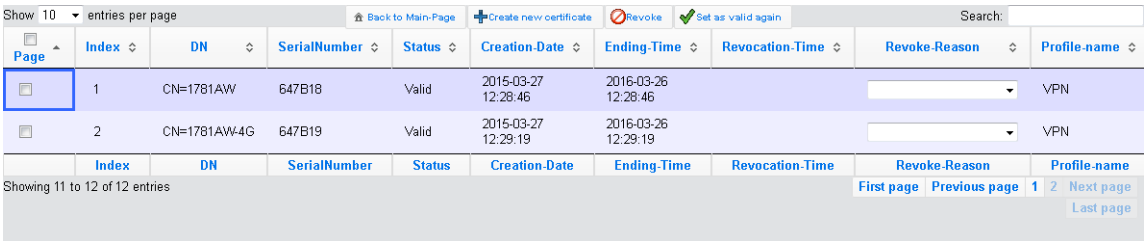
6. The recipient is now able to use a secure VPN dial-in. For the dial-in to succeed, the user must enter the password (PIN) set in step 3.



11.8.4.4 Certificate management with WEBconfig

You need the appropriate permissions to be able to manage the certificates.

To manage a certificate via the web interface, navigate to the view **Setup Wizards** > **Manage certificates**. This gives you an overview of the enrolled certificates, which you can revoke if necessary.



The column headers have the following meanings:

Page

This column is used to mark the entry.

Index

Displays the sequential index of the entry.

Name

Displays the name the certificate.

Serial number

Contains the serial number of the certificate.

Status

Displays the current status of the certificate. Possible values are:

- V: Valid
- R: Revoked
- P: Pending

Creation date

Displays the date of the certificate's creation (date, time).

Ending time

Indicates the date and time of (regular) certificate expiry.

Revocation time

Indicates the date and time of (premature) certificate revocation.

Revoke reason

Indicates the cause of the premature revocation. The selection is made via a drop-down selection list.

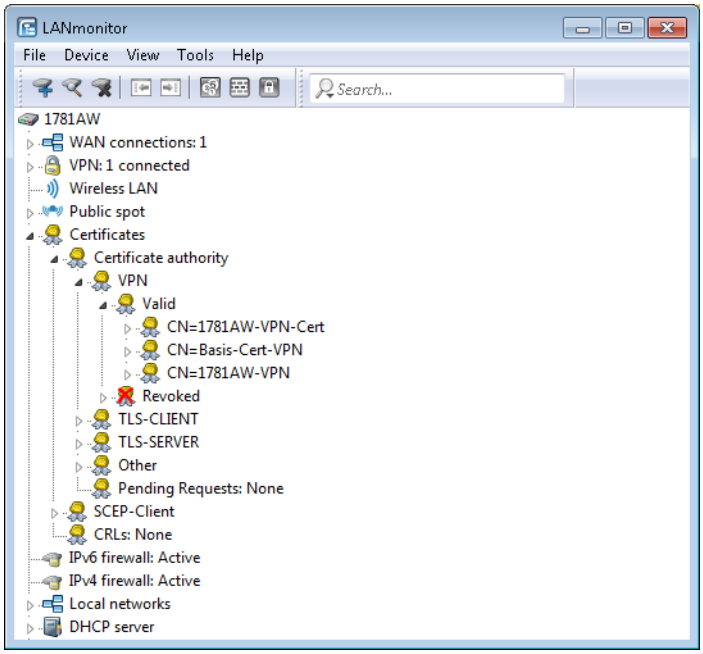
To revoke a certificate, select it in the **Page** column, in the **Revoke reason** column you select why you are revoking the certificate, and then click the **Revoke** button.

The column entries for **Status**, **Revocation time** and **Revoke reason** change accordingly.

To reverse a revocation, highlight the certificate again in the first column and click **Set as valid again**.

11.8.4.5 Managing certificates in LANmonitor

LANmonitor displays the active and revoked certificates, as well as the certificate requests from the SCEP clients.



To revoke a certificate, right-click on the corresponding certificate and select **Revoke certificate** from the context menu.

An overview of all revoked certificates is located in the **Revoked** section.

Certificate requests from SCEP clients can be seen in the **Pending requests** section. Right-click on the corresponding request and select either **Reject** or **Accept** in the context menu.

11.8.4.6 Creating certificates via URL-API

A special API can greatly simplify the creation of certificates for a complex and extensive network infrastructure.

For example, you can use a script to automate the process by sending a call to a URL with parameters attached. The following parameters are possible:

- `a`: Specifies the profile name.
- `b`: Specifies the common name.
- `c`: Specifies the surname.
- `d`: Specifies the email.
- `e`: Specifies the organization.
- `f`: Specifies the organization unit.
- `g`: Specifies the locality.
- `h`: Specifies the State or province.
- `i`: Specifies the country.
- `j`: Specifies the postal code.
- `k`: Specifies the serial number.
- `l`: Specifies the subject alternative name.
- `m`: Specifies the key usage.

- `n`: Specifies the extended key usage.
- `o`: Specifies the key length
- `p`: Specifies the validity period in days.
- `q`: Specifies the password for the PKCS12 file.
- `r`: Indicates whether this is a CA certificate.
  - 1: CA certificate
  - 0: No CA certificate

The Wizard only processes the parameters set with the appropriate permissions in the presets table.

The call to the URL with the appropriate parameters looks like this:

```
192.168.10.74/scepwiz/a=VPN&b=iPhone&q=company
```

11.8.4.7 OCSP server

The Online Certificate Status Protocol (OCSP) is a procedure defined in RFC 6960 for checking the validity of a certificate at a central instance. Unlike certificate revocation lists (CRLs), the full CRL does not need to be downloaded periodically; instead, an on-demand OCSP request is made to the OCSP server when the connection is established, which ensures that the information about the validity of the certificate is always up-to-date. Only a small amount of data is transmitted since only the validity information for a certificate is sent. Compared to the CRL-based method, the validity information is always up-to-date and verification is faster.

The OCSP server can only be used in conjunction with a certification authority (CA) on the same device (LANCOM Smart Certificate). The OCSP server is not able to provide validity information for certificates from other CAs.

In order for the OCSP server to be used to generate certificates per LANCOM Smart Certificate, it must be assigned a certificate and a new entry is required in the profile for certificate creation in order to identify the OCSP server.

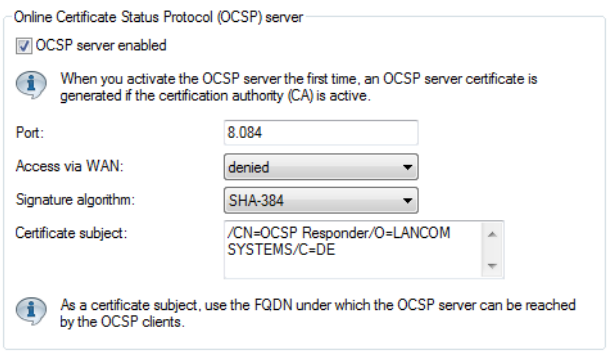
Configuring the OCSP server

Take the following steps to configure the OCSP server:

1. Enable the OCSP server under **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** > **OCSP server enabled**.
2. Assign a certificate to the OCSP server.

   Operating the OCSP server requires it to receive a certificate from the CA whose certificates it should provide information about. This certificate is used to sign the OCSP responses.

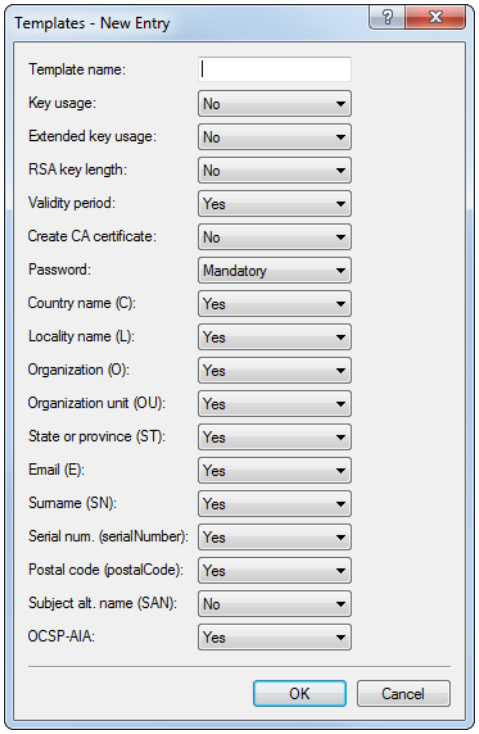
   For this purpose, go to **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** and configure the **Certificate subject** for the OCSP server. When the server is activated for the first time, this information is used to automatically generate the certificate for the OCSP server.



In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

3. Provide information about the OCSP server to the Smart Certificate preconfiguration

   a) Under **Certificates** > **Certificate handling** > **CA web interface** > **Templates**, you can specify that when Smart Certificate CA generates a certificate, the field "OCSP-AIA" (Authority Information Access) is available for configuration. If you use the "Default" template, this is automatically the case. If you use a custom template, then set the field “OCSP-AIA” to Yes.

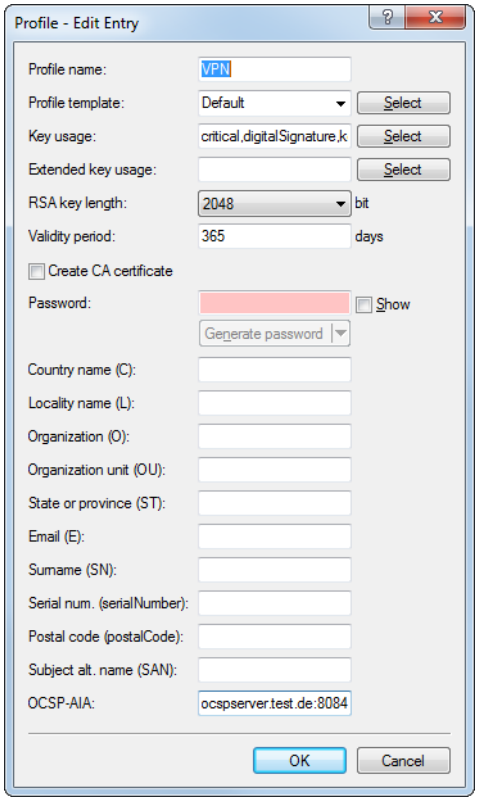


   b) Under **Certificates** > **Certificate handling** > **CA web interface** > **Profile** you set a default value for the field OCSP-AIA in the desired Smart Certificate profile.

This step is optional. If you do not specify a default value here, you must manually specify a value when creating a certificate.

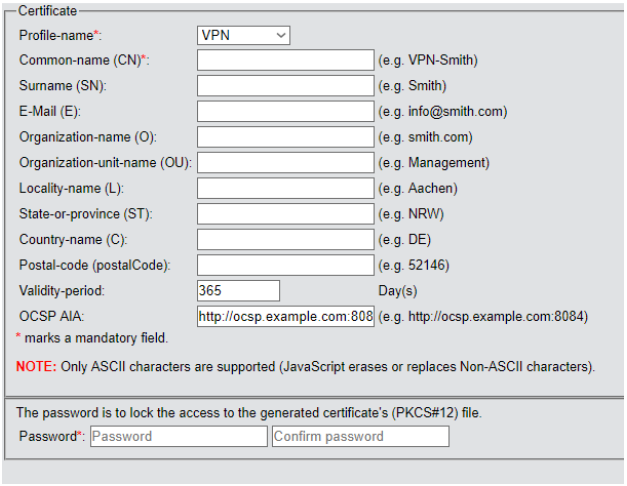
Configure the name or IP address where the OCSP server is available to the OCSP clients. This was already used earlier when generating the OCSP server certificate. Also add the port number where the OCSP server can be reached. The default setting is port 8084.

In the example, the default value for the profile “VPN” is adapted to “ocspserver.test.de:8084”:



This concludes the configuration of the OCSP server.

If you now use Smart Certificate in WEBconfig to generate a certificate as described in *Certificate creation with WEBconfig* on page 811, the OCSP AIA is automatically added to it, so enabling the client to contact the OCSP server for a validity check during connection establishment.



The OCSP server refers to its internal certificate list to check the validity. All in all, the Smart Certificate web interface offers a convenient way to withdraw or validate the certificates.

11.9 NAT Traversal (NAT-T)

The insufficient number of publicly valid IP addresses has lead to the development of procedures such as IP masquerading or NAT (Network Address Translation), where a whole local network is masked by a single, publicly valid IP address. In this way, all clients in a LAN use the same IP address to exchange data with public networks such as the Internet. The assignment of the incoming and outgoing data packets to the different participants in the network is ensured by connecting the internal IP addresses to corresponding port numbers.

This process has proven its worth and has since become the standard in almost all Internet routers. However, new difficulties arise when the hidden data packets are processed using VPN. As data connections over VPN are highly secured, mechanisms such as authentication and encryption are of great importance here.

Converting internal IP addresses to the gateway's central, publicly valid IP address and converting source and target ports can lead to problems in many applications, for example where the UDP port 500 that is usually used during the IKE negotiation has been changed and the IKE can no longer be successfully completed as a result. The address change using NAT is therefore assessed by a VPN gateway as a security-critical data packet change, the VPN negotiation fails and no connection is made. In fact these problems occur, for example, when you dial in using some mobile telephone networks where the network operator's servers do not support the address conversion in combination with IPsec-based VPNs.

So you can successfully create a VPN connection even in such cases, NAT-T (NAT Traversal) provides a process that can overcome the problems described when handling data packets with changed addresses.

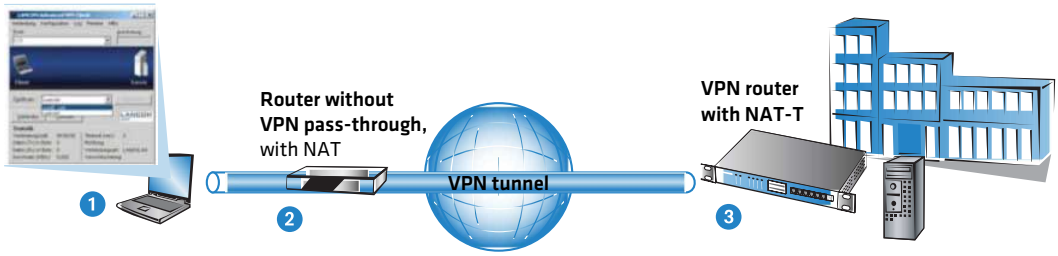
NAT-T can only be used with VPN connections that use ESP (Encapsulating Security Payload) for authentication. Unlike AH (Authentication Header), ESP does not consider the IP header of the data packets when determining the hash value for authentication. The hash value calculated by the receiver is therefore also equivalent to the hash value entered in the packets.

If the VPN uses AH for authentication, then in principle no connection can be established over sections with Network Access Translation, as the AH hash values similarly change when the IP addresses change, and the recipient would classify the data packets as untrustworthy.

The NAT Traversal process eliminates the problems that occur when establishing a VPN connection at the end points of the VPN tunnel. The following scenarios can be distinguished from one another:

- A member of the field staff uses the LANCOMAdvanced VPN Client to dial into the company VPN router **without** "VPN pass-through" support (i.e. IPsec masking) but **with** Network Address Translation.

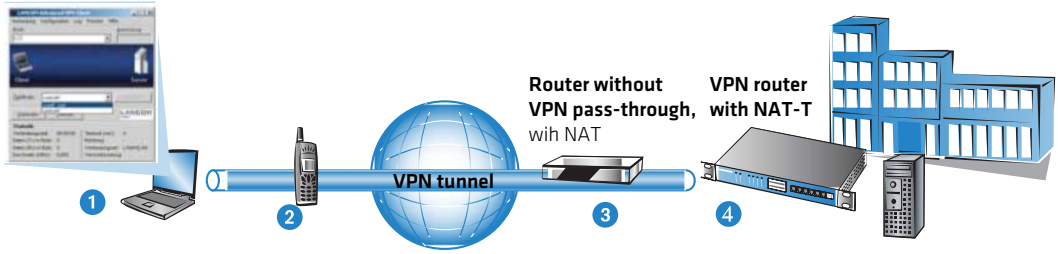
LANCOM Advanced VPN Client with NAT-T



- The two tunnel end points LANCOMAdvanced VPN Client **1** and VPN router **3** support NAT-T and can therefore also establish a VPN connection through the intermediary router.
- Router **2** as a NAT device between the VPN end points performs straight forward NAT address conversion. This router does not require NAT but firewall ports 500 and 4500 must be open in order to enable NAT communication between both tunnel end points.

› In the second example application, the travelling field worker dials in to the network at the headquarters with his notebook **1** and a mobile telephone or modem **2**.

LANCOM Advanced VPN Client with NAT-T

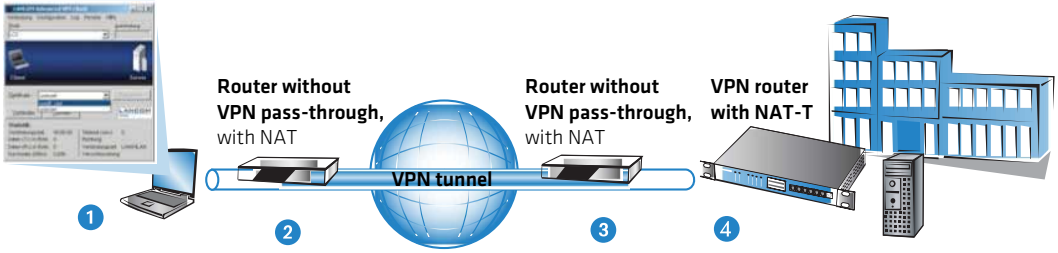


› At the headquarters, the VPN router **4** is located behind a terminating router **3**, which only provides Internet access with the address conversion.

› The two tunnel end points LANCOMAdvanced VPN Client **1** and VPN router **4** support NAT-T and can therefore establish a VPN connection, as in the first example.

› In the terminating router **2**, the firewall ports 500 and 4500 have to be activated, as does port forwarding.

› In both of these cases, the two ends of the connection are the straight-forward NAT routers **2** and **3**. The VPN connection is established between the LANCOM Advanced VPN Client **1** and VPN router **4**.



The two routers **2** and **3** have to permit the NAT-T connection between the two tunnel endpoints in that the firewall ports 500 and 4500 are activated, and port forwarding has to be activated in the terminating router at the headquarters, as well.

To enable this process, both ends of the VPN connection have to work with NAT-T. The process of establishing the VPN connection (reduced to the NAT-T-relevant operations) appears as follows:

1. At an early stage of the IKE negotiation, there is a check to see if both ends of the VPN connection are NAT-T-compatible.
2. In the second step, there is a check to see if the address is converted to NAT on the section between the two tunnel end points, and at what point in the connection the NAT devices are located.
3. To deal with problems with ports that may have changed, all negotiation and data packets are subsequently sent only via UDP port 4500 when a NAT device has been detected.

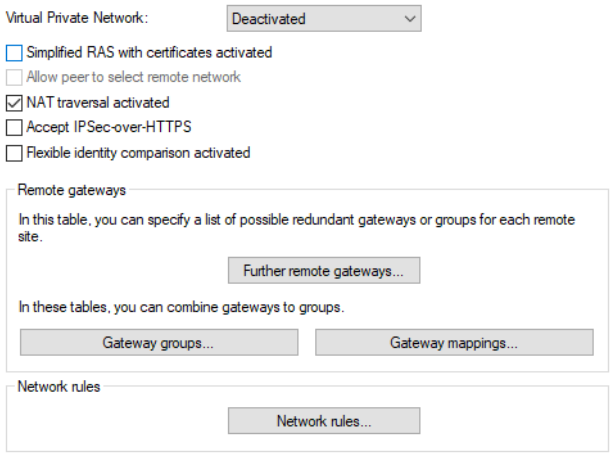
   If the device functions as a NAT router between the VPN end points, ensure that UDP ports 500 and 4500 are enabled in the firewall when you use NAT-T! This port is activated automatically if you use the firewall assistant in LANconfig.

   If the VPN connections are first created on devices with firmware version 5.20 or above using the VPN assistant and later with the firewall assistant from LANconfig, then no additional firewall settings are required for the NAT router.

4. In the diagram below, the data packets are packed again into UDP packets (UDP encapsulation) and are also sent using port 4500. As a result of this additional encapsulation, changing the IP addresses for the VPN negotiation is no longer relevant and the VPN tunnel can be established without any problems. At the other end of the connection, the IP data is released again by the additional UDP header and can be processed by the router without further action.

In order to use this process, both ends of the VPN connection have to use NAT-T.

You will find the button for activating NAT-T in LANconfig under **VPN** > **General**.



Under Telnet or SSH client you will find the settings for activating NAT-T under **Setup** > **VPN** > **NAT-T-Operating**.

11.10 Extended Authentication Protocol (XAUTH)

11.10.1 Introduction

RADIUS servers are often used to authenticate users for remote sites dialing-in over WAN connections (such as via PPP). Over time, conventional WAN connections increasingly gave way to secure (encrypted) and more cost-effective VPN connections. However, the structure of VPN connections over IPsec with IKE does not permit unidirectional authentication of users by RADIUS or similar technologies.

The Extended Authentication Protocol (XAUTH) provides the ability to extend authentication in the negotiation of IPsec connections by an additional level in which user data can be authenticated. An additional authentication with XAUTH user name and XAUTH password is performed between the first and second IKE negotiation phases. This authentication is protected by the encryption negotiated in advance. A RADIUS server can be used for this authentication, enabling existing RADIUS databases to continue to be used in the migration of dial-in clients to use VPN connections. Alternatively, authentication can use an internal user table of the device.

In order make XAUTH particularly secure, dial-in via RSA-SIG (certificates) was to be used instead of the preshared key method (PSK) whenever possible. Here it is important to ensure that the VPN gateway accepts only the certificate of the correct remote site (and not all certificates issued by the same CA).

11.10.2 XAUTH in the firmware

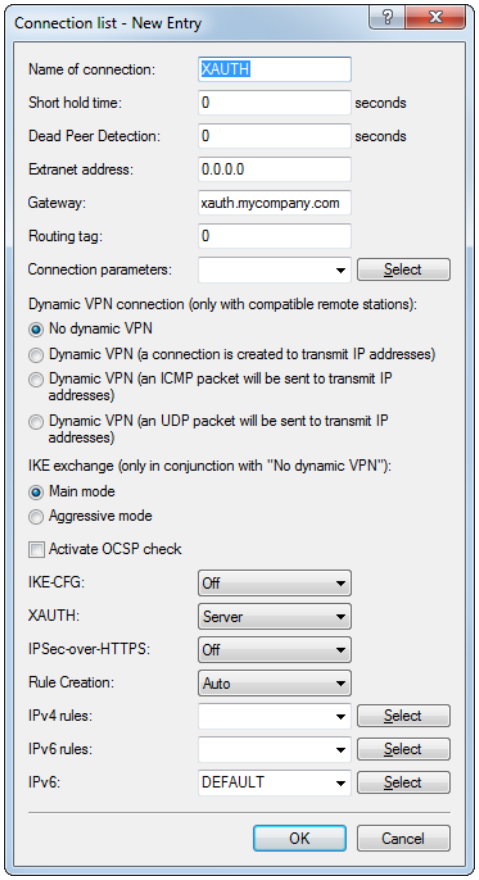
In the device, the XAUTH protocol uses entries in the PPP table for remote site authentication. Use of the entries in the PPP table is dependent on which direction the connection is established, i.e. on the XAUTH operating mode:

XAUTH operating mode	Server	Client
XAUTH user name	Remote site from the PPP table. The PPP-table entry is selected for which the PPP remote site corresponds to the transferred XAUTH user name. The PPP remote site must also match the VPN remote site used.	User name from the PPP table. The entry selected from the PPP table is that for which the PPP remote site corresponds to the VPN remote site used.
XAUTH password	Password from the PPP table.	Password from the PPP table.

11.10.3 Configuration of XAUTH

The application of the XAUTH protocol is set up separately for each VPN remote site. Only the XAUTH operating mode is specified.

LANconfig: **VPN** > **IKE/IPSec** > **Connection list**



CLI: **Setup** > **VPN** > **VPN-Peers**

› XAUTH

Enables the use of XAUTH for the VPN remote site selected.

Possible values:

Client

In the XAUTH client operating mode, the device starts the initial phase of IKE negotiation (Main mode or Aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the user name and password from the PPP table entry in which the PPP remote site corresponds to the VPN remote site defined here. There must therefore be a PPP remote site of the same name for the VPN remote site. The user name defined in the PPP table normally differs from the remote site name.

Server

In the XAUTH server operating mode, the device (after successful negotiation of the initial IKE negotiation) starts authentication with a request to the XAUTH client, which then responds with its user name and password. The XAUTH server searches for the user name in the PPP table and, if a match is found, it checks the password. The user name for this entry in the PPP table is not used.

Off (Default)

No XAUTH authentication is performed for the connection to this remote site.

If XAUTH authentication is enabled for a VPN remote site, the IKE-CFG option must be set to the same value.

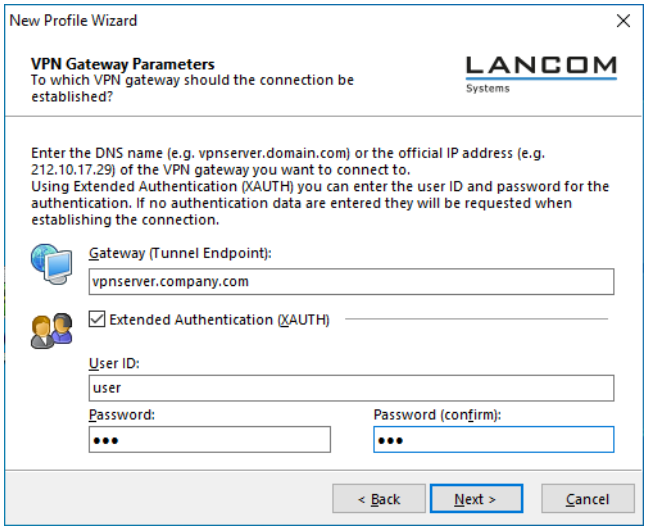
11.10.4 XAUTH with external RADIUS servers

As of firmware version 7.60, a router can identify and authenticate remote stations with the Extended Authentication Protocol (XAUTH). Authentication referred to the user data in the PPP list.

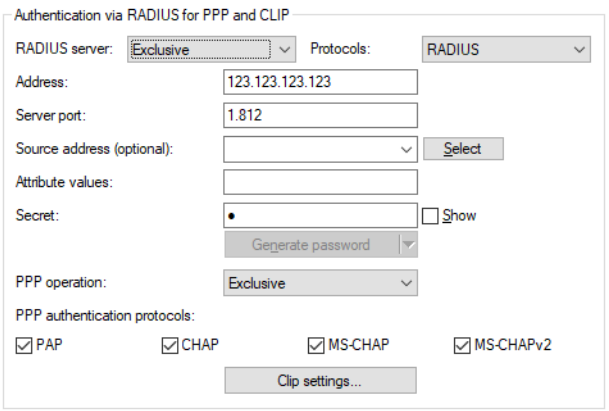
As of firmware version 7.80, XAUTH authentication can also be handled by an (external) RADIUS server. For example, this allows reference to existing RAS user data on the RADIUS server, assuming that RADIUS-authenticated dial-in via PPP has been set up for VPN with XAUTH.

To supplement VPN dial-in with XUTH for authentication, please proceed as follows:

1. Set up a VPN dial-in account, for example with the LANconfig Setup Wizard.
2. Activate XAUTH in the VPN client at the station which is to dial in. The user name and password are the same as those stored on the RADIUS server.



3. Activate the authentication of dial-in remote stations via the XAUTH protocol on an external RADIUS server. In LANconfig, access the configuration area **Communication** > **RADIUS** to activate the "Exclusive" operating mode for the RADIUS server. With this setting, all incoming XAUTH requests are authenticated by the RADIUS server.



4. You should also specify the IP address, the port, and the key for the external RADIUS server.

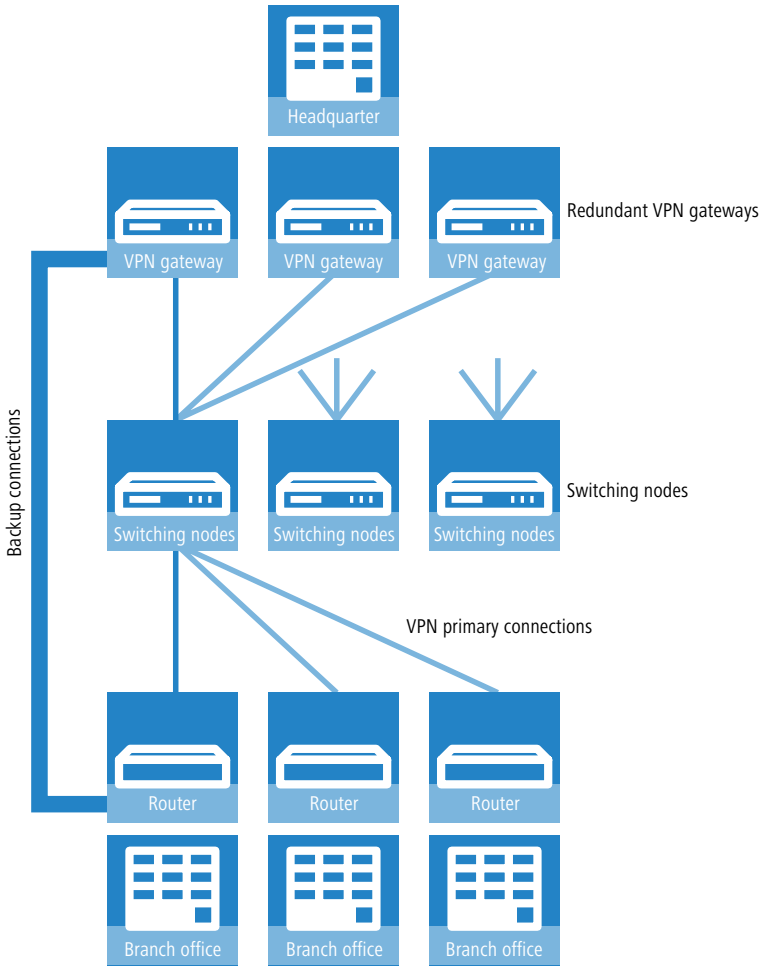
5. Also set PPP operation to "Exclusive" so that incoming XAUTH requests are authenticated by the RADIUS server only.

11.11 Backup via alternative VPN connection

11.11.1 Introduction

The subject of backup connections is vital to the availability of business-critical applications, especially at distributed sites with several branch offices connected via VPN to the main office. The subject of backups is easy to resolve where routers at the branch offices relate directly to redundant routers at the main office: If a router at the main office can be not reached over the Internet, the branch office simply dials-in to another router at the main office. RIP ensures that the devices can communicate over the available routes.

However, in very large networks branch offices are rarely connected directly to the main office. Instead, several sites initially merge at switching nodes, and these in turn are connected to the main office. If the branch office temporarily loses contact to the switching node, the branch office could establish a direct backup connection to main office.



However, this only works via a cellular connection, often an undesirable solution due to the costs and limited bandwidth. A parallel backup connection directly over VPN does not achieve the objective for the following reasons:

› Only the switching nodes are defined as VPN remote sites in the main office – all routes to the branch offices pass through these switching nodes. If a branch office attempts to establish a direct connection to the main office, the

attempt is rejected. And even if this connection were successful, the routes to the branch offices via the switching nodes remain in place at the main office because the switching node is, from the viewpoint of the main office, still accessible.

- The switching node knows nothing about any potential direct connection from branch office to main office. It therefore cannot access the destinations in the network at the branch office by detouring via the main office.
- Both the network of the switching node and the network of the branch office are accessible from the main office via the standard VPN connection. However, a direct VPN connection of the branch office to the main office only provides access to the branch-office network. It is because of these different characteristics that the router at the main office cannot accept the direct connection as a backup for the standard connection.
- The branch office can no longer establish the standard connection to the switching node because the principle of unambiguousness in IPsec rules does not permit a second connection with the same set of rules. Along with the specifications on encryption, IPsec rules also contain "network relationships", i.e. the IP addresses of the networks at both ends of the connection. These network relationships may only appear once in the VPN rule set. For a backup, however, two rules would have to exist for the same network relationship – once for the backup connection and once for the newly established primary connection.

11.11.2 Backup-capable network infrastructure

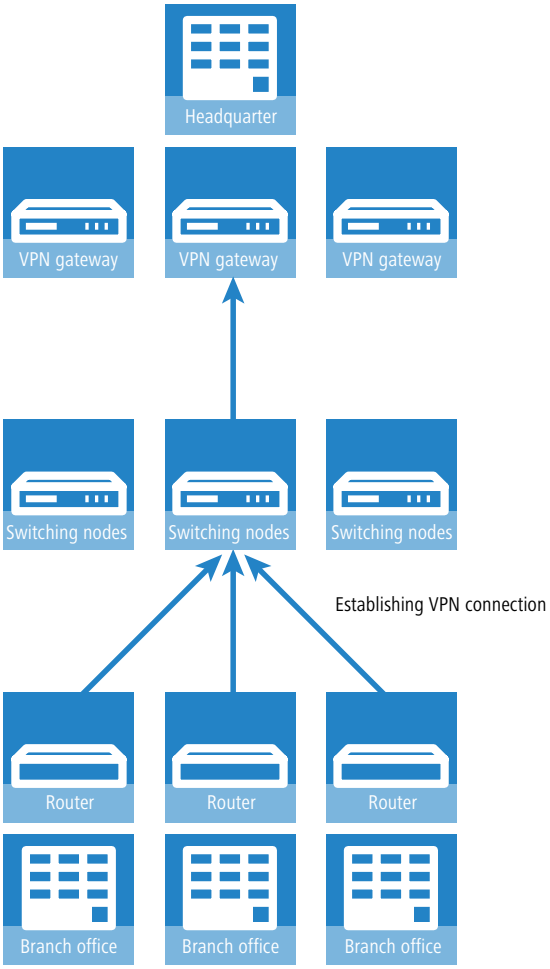
In order to also build up an operational backup solution for these applications, the points described in the following sections must be satisfied.

11.11.2.1 Basic prerequisites

The basic prerequisite for the backup function described here are; the configuration of a “Dynamic VPN” connection between branch offices and switching nodes; and the functions “Simplified RAS with certificates” and “Allow remote site to select the remote network” must be enabled in the VPN gateways at the main office.

11.11.2.2 Hierarchy for establishing VPN connections

In order for branch offices to connect to the network at the main office for backup purposes, a defined hierarchy must be observed when establishing the connection. Connections are only established from the "lower" to the "upper" networks, i.e. from the branch office to the switching node, from the switching node to the main office.



Thus connections only have to be accepted passively at the main office. The switching nodes also accept the branch office connections passively, but establish the connections to the main office actively. This hierarchy is a prerequisite for the later definition of VPN rules.

11.11.2.3 Network definitions

The branch offices establish network relationships with the switching nodes and with the main office - this must be allowed by the appropriate rules. In addition, either all conceivable network relationships must be stored individually or the networks have to be defined such that all required network relationships can be allowed with a single rule. This is possible if, for example, the IP addresses in the networks have the following structure:

- Central network 10.1.1.0/255.255.255.0
- Switching nodes 10.x.1.0/255.255.255.0
- Branch offices 10.x.y.0/255.255.255.0

Using the following VPN rule in the VPN gateways at the main office permits all required network relationships, i.e. all remote sites from the 10.x... range of addresses can establish connections to all gateways:

- Source 10.0.0.0/255.0.0.0
- Destination 10.0.0.0/255.0.0.0

Because branch offices communicate with the main office via the intermediate level of the switching nodes, corresponding VPN rules must also be created in the switching nodes. If communication with other sub-nodes and branch offices is also to be made possible, all of the required network relationships are permitted with the following VPN rule in the switching nodes:

- Source 10.x.0.0/255.255.0.0
- Destination 10.0.0.0/255.0.0.0

11.11.2.4 Routing information

During normal operation, the routes from main office to individual branch offices run via the switching nodes. These routes must be adapted for backup situations. For this adaptation to be performed automatically, "Simplified RAS with certificates" is enabled in the VPN gateways at the main office. This allows a shared configuration to apply for all incoming connections (using default settings) if the certificates of the remote sites have been signed with the root certificate of the VPN gateways in the main office. This also allows remote sites to select the remote network. The routers at the branch offices can then suggest a network (during IKE negotiations in phase 2) to be used for the connection.

Enabling the two functions "Simplified RAS with certificates" and "Allow remote site to select the remote network" is a necessary condition for the backup function described here.

The routing information at the switching nodes must also be adapted in backup situations. The switching nodes are normally accessed directly from the branch offices. In backup situations, the switching nodes must be able to receive the data from the branch offices via the main office detour. This is made possible with a route that transmits the entire combined network (10.x.0.0/255.255.0.0 in the example or, if communication with other nodes is to be possible: 10.0.0.0/255.0.0.0) to the main office.

In order for the routes to be switched automatically, "Allow remote site to select the remote network" must also be activated at the switching nodes.

This results in the following sequence of events when establishing VPN connections:

- The switching node establishes the connection to the main office and requests all network relationships to the branch offices (i.e. it requests the 10.x.0.0/255.255.0.0 network).
- The branch office establishes the connection to the switching node and requests its network (10.x.y.0/255.255.255.0).

  Data can now be transferred from the branch office to the main office via the switching node.

The following happens if the VPN connection between branch office and main office now fails:

- The switching node detects the loss by polling (DPD) and removes the route to the branch office.
- At some point the branch office establishes the backup connection to the main office and requests its network (10.x.y.0/255.255.255.0).

  Data can now be transferred from the branch office to the main office.

  If the networks have been combined and the switching nodes always route the combined network (as in the example, network 10.x.0.0/255.255.0.0 or 10.0.0.0/255.0.0.0) to the main office, data can be transmitted from the branch office to the switching node via the main office.

Once the backup event is over, the branch office reestablishes the primary connection to the switching node:

- The branch office tears down the backup connection and the main office deletes the route to the branch office.
- The branch office again requests its network (10.x.y.0/255.255.255.0) from the switching node.

  Smooth communication between branch office and switching node now exists again.

  Because the branch office network is a sub-network of the network in the switching node, immediate communication between branch office and main office via the switching node is also possible again. The main office no longer has its own route to the branch office and therefore resumes transfers data for the branch office via the switching node again.

If network addresses cannot be structured as described above, the route to the branch office must be configured statically at the main office and point to the switching node. If the branch office then establishes the backup connection, the statically registered route is overwritten by the dynamically registered route. If the backup connection is torn down again, the dynamic route is deleted and the static route re-enabled. If, in this case, communication between branch offices and switching node is to be guaranteed for backup as well, the routes to the branch offices must also be configured statically in the switching nodes.

11.11.2.5 Establishing a backup connection

In order to conform to the basic principle of unambiguous IPsec rules, backup situations require VPN rules for the primary connection to be deleted first, and then new rules for the backup connection are created.

If the backup connection fails, the backup module selects the next backup connection if several have been configured.

11.11.2.6 Re-establishing the primary connection

The device attempts to restore the primary connection while the backup connection is being established. During this attempt to connect, the VPN rule set must not be recreated again – otherwise the backup connection would fail or an existing VPN connection would simply be torn down.

To prevent this, initial "Dynamic VPN" negotiations with the primary connection's remote site are performed. If these negotiations are successful, the primary connection can be reestablished. To this end, the backup connection is disconnected and the backup status is reset. This prevents the backup connection from being reestablished immediately. Only after this is the primary connection reestablished with the original VPN rules.

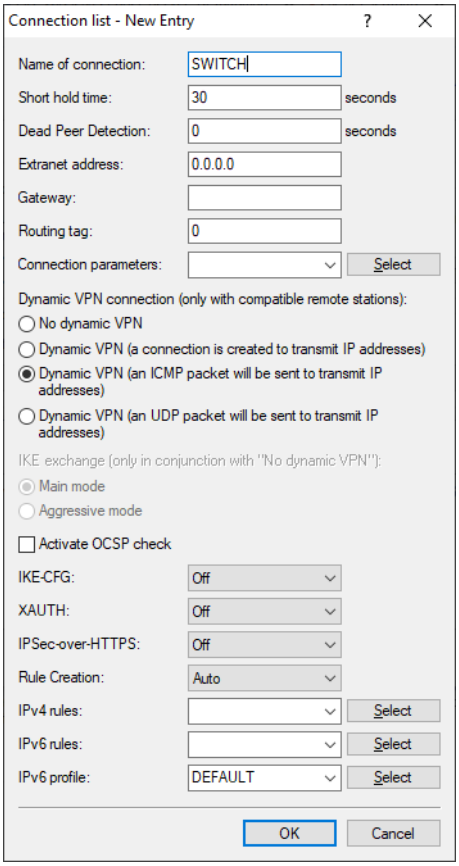
The use of the "Dynamic VPN" connection between branch office and switching node is a necessary condition for the backup function described here.

11.11.3 Configuring the VPN backup

For configuring the VPN backup, the devices at the branch offices, main office and switching nodes must be considered separately.

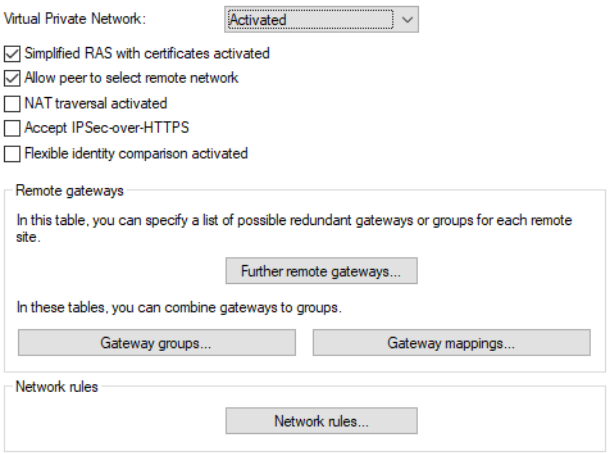
› Branch

- "Dynamic VPN" over ICMP/UDP must be configured for the primary connection.



- The backup connection has no requirement for "Dynamic VPN".
- At the branch office, the main office must be configured as a backup remote site.

- Head office
  - Simplified RAS with certificates must be enabled.
  - Selection of the remote network by the remote site must be enabled.
  - A configuration in the backup table is not necessary here.



- Switching nodes
  - The VPN connection to the main office must be completely configured.
  - Simplified RAS with certificates must be enabled.

› Selection of the remote network by the remote site must be enabled.

If the system does not have “combined networks” (i.e.the branch office network is a sub-network of the switching node and the switching node network is a sub-network of the central network), then the switching node's route to the branch office must point to the main office in order for the branch office to be able to reach the switching node in backup situations. In normal operation, this route is overwritten by the route passed by the branch office in the VPN (because remote sites may provide network relationships) and is therefore only used when the direct connection is torn down and the branch office establishes the backup connection.

11.12 Automatic configuration synchronization (Config Sync) with the LANCOM VPN High Availability Clustering XL option

Example application, VPN:

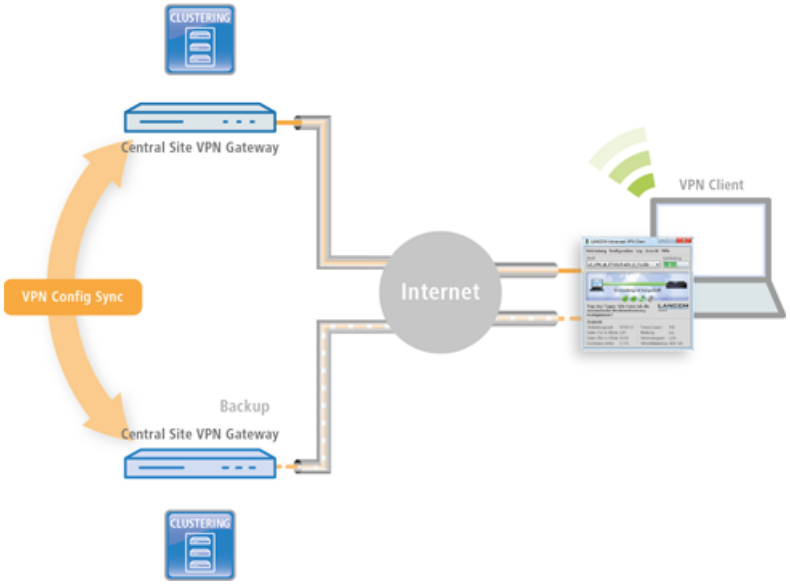
VPN infrastructures have been a part of corporate networks for a long time now. The demands on the availability of VPN gateways have increased sharply in recent years. Whereas VPN solutions in professional scenarios were mainly temporary in the past, e.g. for sales representatives with VPN clients, these days home or branch offices are often permanently linked to the main office via a VPN tunnel. They support voice services (VoIP), database applications, or file services, for example. With increasing dependence on VoIP services or critical business applications, the need for reliable backup and high-availability of the VPN solution has increased.

In order for VPN services in larger-scale critical network infrastructures to remain highly available, it is advisable that you operate one or more backup VPN gateways in addition to the primary VPN gateway. In this case, the failure or downtime of a central-site VPN gateway causes another device to operate as a backup. The VPN connection is automatically established via the accessible backup central-site VPN gateway.

For this purpose the backup central-site VPN gateway needs to have the same configuration as the primary central-site VPN gateway. In particular VPN user data and the firewall configuration must be present on both devices in order for a user to be authenticated and the services to be provided correctly. This requires a manual setup of each individual device—in other words, a huge amount of work for the administrator.

New with the LANCOM VPN High Availability Clustering XL option: This option allows multiple central-site VPN gateways to be grouped into a cluster. In this way, configuration changes, features and enhancements made on one central-site VPN gateway are automatically transferred between the cluster devices, without having to make manual

changes on each individual device. Common parameters in a cluster (e.g. VPN user database, firewall) remain synchronized, individual parameters (such as the IP address) are not exchanged.



The prerequisites for a device to be a valid member of a cluster are:

- The LANCOM VPN High Availability Clustering XL option must be available.
- IP communications must be available to all other devices, e.g. via LAN, WAN, or VPN.
- It must be in the list of group members that is stored in each device.
- A valid certificate must be available
- It needs to authenticate itself by certificate as a member of the cluster.

11.13 IPSec over HTTPS

11.13.1 Introduction

In some environments it is impossible to establish a secure VPN connection over an existing Internet connection due to an interim firewall that blocks the ports used by IPsec. To be able to set up an IPsec-secured VPN connection in such a situation, VPN routers support the technology known as IPsec-over-HTTPS.

The first attempt always tries to establish data communications with standard IPsec. If the connection cannot be established (e.g. because IKE port 500 is blocked by a cellular network), then an attempt is then automatically made to establish a connection that encapsulates the IPsec VPN in an additional SSL header (port 443, like https).

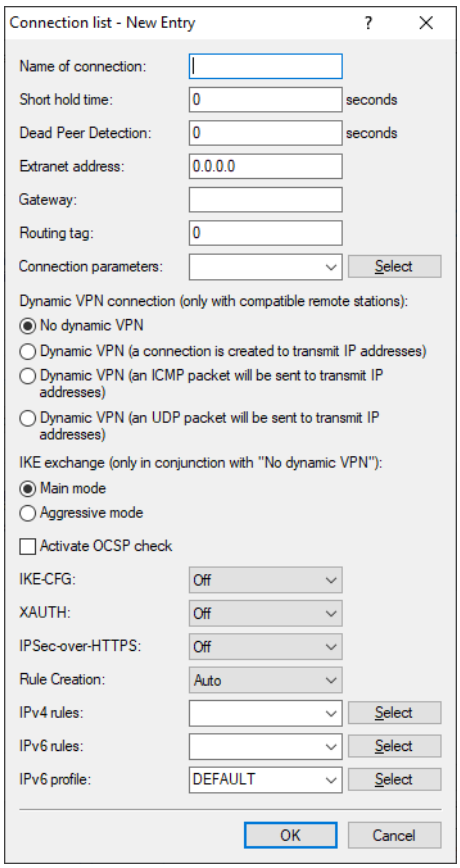
Note that IPsec-over-HTTPS technology only works when both ends of the connection support this function and the corresponding options are activated. IPsec-over-HTTPS is available from LCOS 8.0 as well as in LANCOM Advanced VPN Client 2.22 or higher.

11.13.2 Configuring IPsec-over-HTTPS technology

For the active establishment of a connection from one VPN device to another VPN remote by using IPsec-over-HTTPS technology, activate the option in the VPN name-list entry that corresponds to the remote site.

LANconfig: **VPN** > **IKE/IPSec** > **Connection list**

CLI: **Setup** > **VPN** > **VPN-Peers**



IPsec-over-HTTPS

With this option you activate IPsec-over-HTTPS technology when actively establishing a connection to this remote site.

Possible values:

- On, off

Default:

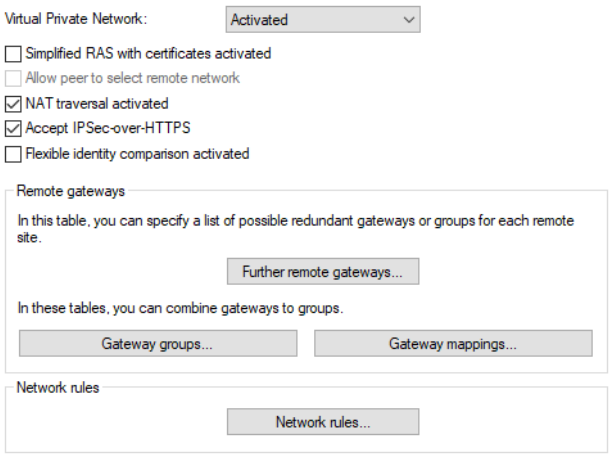
- Off

Please note that when the IPsec-over-HTTPS option is activated, the VPN connection can only be established when the remote site also supports this technology and when the remote site is set up to receive passive VPN connections that use IPsec over HTTPS.

To enable passive connection establishment to a VPN device from another VPN remote device using IPsec-over-HTTPS technology (VPN device or LANCOM Advanced VPN Client), activate the option in the general VPN settings.

LANconfig: **VPN** > **General**

CLI: **Setup** > **VPN**



Accept IPsec-over-HTTPS

With this option your system accepts passive attempts to connect when the remote site supports IPsec-over-HTTPS technology.

Possible values:

- On, off

Default:

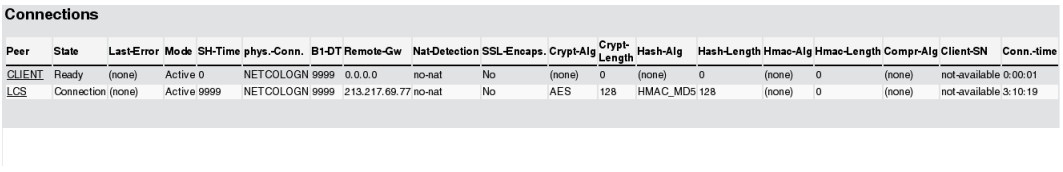
- Off

The LANCOM Advanced VPN Client supports automatic fallback to IPsec over HTTPS. With this setting, the VPN client initially attempts to establish a connection **without** using the additional SSL encapsulation. If the connection cannot be made, the device then tries to connect **with** the additional SSL encapsulation.

11.13.3 Status displays of the IPsec-over-HTTPS technology

The status displays show whether IPsec-over-HTTPS (SSL encapsulation) is being used on each of the active VPN connections.

WEBconfig: **LCOS menu tree** > **Status** > **VPN** > **Connections**



11.14 MPPE for PPTP tunnels

The encryption protocol MPPE (Microsoft Point-To-Point Encryption) secures data transmission over PPP and VPN connections with key lengths of up to 128 bit.

MPPE uses the "stateless mode" for encryption to ensure that both communication partners are synchronized. In this mode, the session key changes with each transmitted data packet. The two stations also synchronize their encryption tables (where the keys are stored for data encryption) each time.

VPN-capable devices use MPPE to encrypt data transfer by PPTP tunnel.

In LANconfig you find this setting under **Communication** > **Remote sites** > **PPTP** > **PPTP list**.

If you have enabled the MPPE encryption protocol, connections to clients are established only under the following conditions:

- The client establishes a connection secured with MPPE. The router rejects the request for other protocols.
- The client uses as a minimum the key length specified in the router. With shorter key lengths the router refuses to connect and, with stronger encryption, the router switches to the appropriate key length.

11.15 Layer-2 tunneling protocol (L2TP)

LCOS supports L2TP of versions 2 and 3.

With L2TPv2, an L2TP access concentrator (LAC) tunnels the PPP request from a client arriving on a public connection (e.g. Internet, ATM, frame relay) to an L2TP network server (LNS). The LNS serves as a gateway to the remote network. There, a connected RADIUS server initially authenticates the client, if necessary. The LNS then sends the IP address to the LAC and starts the L2TP tunnel. The LAC communicates the IP address to the client. As of this moment, the client has joined the remote network via an L2TP connection.

Within the firmware, the LAC and the PPP client are collected in a role. Thus a device operating as a LAC starts the control channel and the PPP session. For network virtualization, multiple PPP sessions are supported in an L2TP tunnel. An L2TP-enabled device is able to operate as an LAC and also as an LNS.

With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

L2TP uses two types of data:

Control data

The control data are used to establish, maintain and tear down the tunnel connections. The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

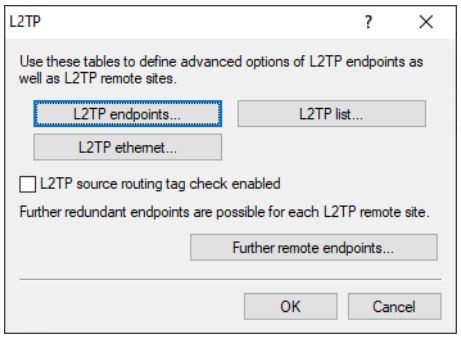
Payload data

The payload data are encapsulated in PPP frames, which are exchanged between the LAC and the LNS via the tunnel. In contrast to the control data, payload data contains no data flow control. Thus there is no guarantee that the sender and receiver are exchanging data correctly.

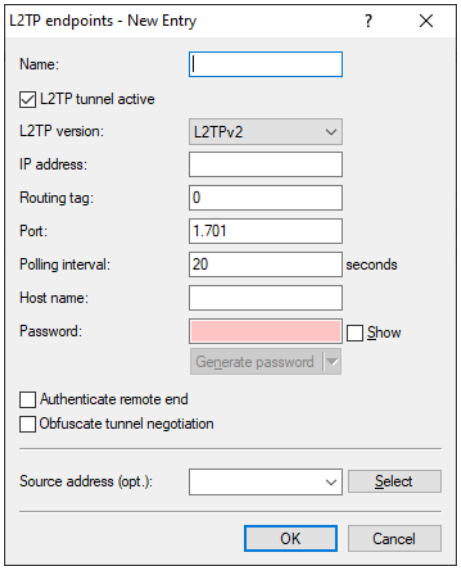
Unlike PPTP, which transfers control and payload data via different protocols (TCP and GRE), L2TP only uses UDP for both data types. You also have the option to operate multiple logical payload-data channels on each control-data channel.

11.15.1 Configuring the L2TP tunnel

With LANconfig, you configure L2TP under **Communication** > **Remote sites** > **L2TP**.



The tunnel configuration for the control data of an L2TP tunnel to a tunnel endpoint is located under **L2TP endpoints**.



Name

Name of the tunnel endpoint.

L2TP tunnel active

Enables the configured L2TP tunnel.

L2TP version

The L2TP protocol version used, either version 2 or 3.

Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

L2TPv3 in the LCOS is always encapsulated in UDP. This allows transmissions to pass through NAT gateways without problem.

IP address

IP address of the tunnel endpoint (IPv4, IPv6, FQDN).

Leaving this field blank when the L2TPv3 protocol is selected makes this field into a “wildcard” entry that can accept connections from any remote site.

Routing tag

The routing tag of the route to the tunnel endpoint.

If a loopback address is entered as the source address and the routing tag has a value of "0", the device uses the routing tag of the loopback address.

Port

UDP port

Polling interval

Polling interval in seconds

Host name

Name used by the device to authenticate at the tunnel endpoint

Password

Password used by the device to authenticate at the tunnel endpoint

Authenticate remote end

Enable this option if two tunnel endpoints (LAC and LNS) are required to mutually authenticate one another before establishing a tunnel. In this case, the tunnel endpoint name and password for this device are configured as the tunnel endpoint and the option to **Authenticate remote end** is similarly enabled.

Obfuscate tunnel negotiation

If the tunnel negotiations between the LAC and the LNS are to be encrypted, you enable this option. The two L2TP partners encrypt and decrypt the L2TP messages with the help certain AVPs (attribute value pairs) of a common preshared secret.

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

If the list of IP networks or loopback addresses contains an entry named “DMZ” then the associated IP address will be used.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

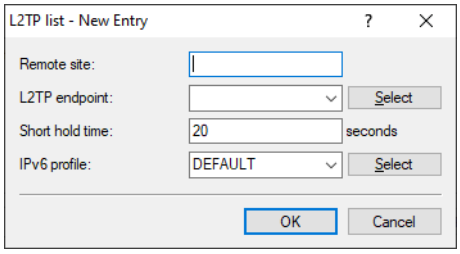
From LCOS 10.20, layer-3 Ethernet tunnels can be configured to use L2TPv3. The configuration is done in the L2TP endpoint table described above and in the L2TP Ethernet table described below. For a corresponding scenario, see *Configuring a WLAN scenario for bridging payload data to the central site* on page 845. If you specify an IP address or a host name, an attempt is made to establish a connection. If the corresponding field is left blank, no connection is established, but connections can be accepted. Configured properties such as the station name or password are checked by the remote site when the connection is established.

A number of implicit dependencies during the connection establishment and authentication are not directly apparent, so we will enlarge on these here:

- The host name transmitted by the remote site is checked to see whether it corresponds to a configured L2TP endpoint. The host name is configured in the L2TP endpoint table of the remote site under **Host name**. If this field is left blank, the device name is used for authentication instead.
- If this is the case, the connection is established using the configuration for the corresponding L2TP endpoint.

- If not, the L2TP endpoints table is checked to see if it contains a “wildcard” entry. This is an entry that contains no host/station name or routing tag. The connection is established using the configuration of the “wildcard” entry.
- If authentication is activated for the corresponding entry in the L2TP endpoints table, authentication is carried out based on the configured password.
- If the password field is empty and authentication is switched on, a RADIUS authentication is carried out. See *Authentication via RADIUS* on page 838.
- If authentication is turned off, a “wildcard” entry accepts any incoming tunnel accordingly.

Under **L2TP list**, you make the link between the L2TP remote sites and a previously configured tunnel endpoint.



An entry in this table is necessary only under the following conditions:

- Outgoing connections
- Incoming connections with an idle timeout not equal to “20” or
- If incoming links specify the use of a specific tunnel only.

Remote site

Name of the L2TP remote device

L2TP endpoint

Name of the tunnel endpoint used by this remote site.

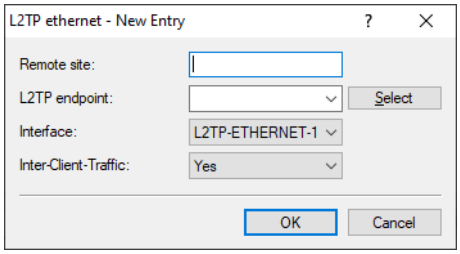
Short hold time

Determines how long the L2TP tunnel endpoint keeps the tunnel open when inactive.

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **WAN interfaces**.

Under **L2TP Ethernet** you link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.



Remote site

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

L2TP endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need "to run" via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

Interface

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

Inter-Client-Traffic

This toggle determines whether traffic between clients bound to the same L2TP Ethernet interface is allowed.

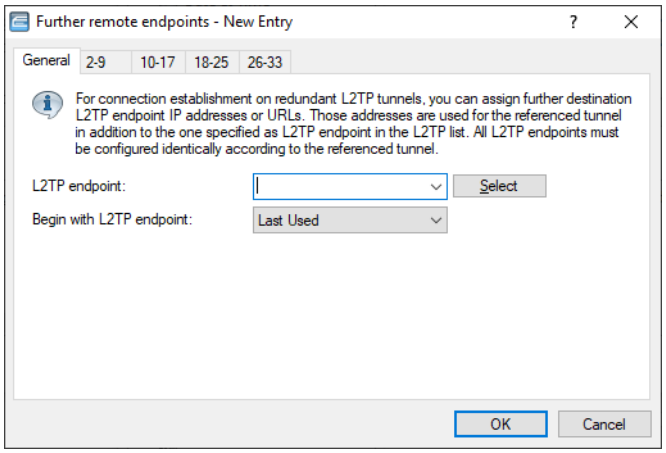
When updating from a LCOS version earlier than 10.92, the configuration is automatically adjusted based on the default:

If multiple sessions are actually bound to the same L2TP Ethernet interface, the first appearance of the interface determines how the inter-client traffic option is set: If it is changed on its first occurrence, the same setting will be applied to all other sessions bound to the interface. Any changes on subsequent occurrences will be rejected. This prevents conflicting entries in the configuration.

In the case of incoming tunnel requests, a check is performed either by RADIUS or by means of an entry for the requesting host in the L2TP endpoints table. If the table contains an entry with the same IP address (or no IP address is specified for this entry), the device permits tunnel establishment to this host.

For additional protection, for example to enable encryption of the L2TP sessions via IPSec, the device can additionally check the routing tag of the remote site from which it received the data. This option is enabled with **L2TP source routing tag check enabled**.

You have the option to configure up to 32 additional gateways per tunnel endpoint by clicking on **Further remote endpoints**.



Ensure that all additionally specified L2TP endpoints are configured identically to the referenced tunnel endpoint.

L2TP endpoint

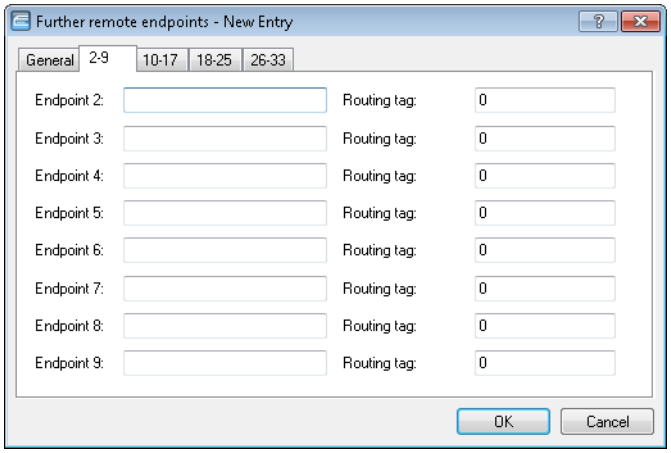
Name of the tunnel endpoint, as configured in the table of **L2TP endpoints**.

Begin with L2TP endpoint

Option for selecting the next gateway. The following options are available:

- **Last used**: Select the last successful address
- **First**: Select the first gateway in the list
- **Random**: Random selection from the gateways in the list

On the following tabs you configure the names and the respective routing tags of the alternative gateways.



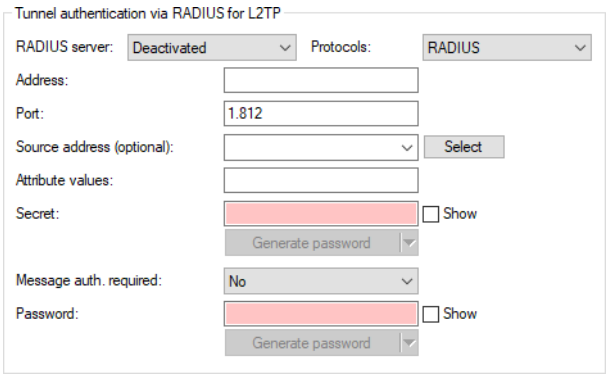
11.15.2 Authentication via RADIUS

RADIUS authentication for L2TP is possible in two cases:

- Tunnel authentication: The RADIUS server checks to see whether a LAC is allowed to establish a L2TP connection.
- PPP session: The RADIUS server checks the user data of the corresponding PPP session.

For this reason, the configuration of the RADIUS server for L2TP-tunnel authentication and the PPP user data are carried out independently of one another.

In the case of tunnel authentication by RADIUS, the settings in LANconfig are configured under **Communication** > **RADIUS** in the section **Tunnel authentication via RADIUS for L2TP**.



RADIUS server

Enables or disables the RADIUS server for the authentication of the tunnel endpoint, regardless of a PPP-session authentication. The following options are possible:

- **Deactivated**: The RADIUS server is not enabled for the authentication of tunnel endpoints.
- **Activated**: The RADIUS server handles the authentication of tunnel endpoints.

- **Exclusive**: Enables the use of the external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Protocols

Protocol for communication between the internal RADIUS server and the tunnel endpoint.

Address

IP address or DNS name of the RADIUS server.

Port

The port the RADIUS server

Source address

Optional sender address of the device. If you have configured loopback addresses, these can also be specified here.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

Attribute values

LCOS allows the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified by means of a semicolon-separated list of attribute numbers or names and a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Secret

Shared secret between the RADIUS server and the device

Password

Dummy password for tunnel authentication

If an L2TP tunnel request arrives from a remote host (Start Control Connection Request), the device sends a request to the RADIUS server that has been enabled for L2TP. This request contains among other things the name of the host, the dummy password, the IP address of the device, and also the service type "Outbound User". The RADIUS server authenticates the host and sends a "RADIUS accept" to the device together with; the tunnel password to be used; the tunnel type "L2TP" with the tag "0"; and also the Tunnel-Client-Auth-ID, which must match with the host name transmitted earlier by the device. The device checks this data and, if the result is positive, it takes the tunnel password to authenticate the dial-in client and, if applicable, to obfuscate the L2TP tunnel negotiations.

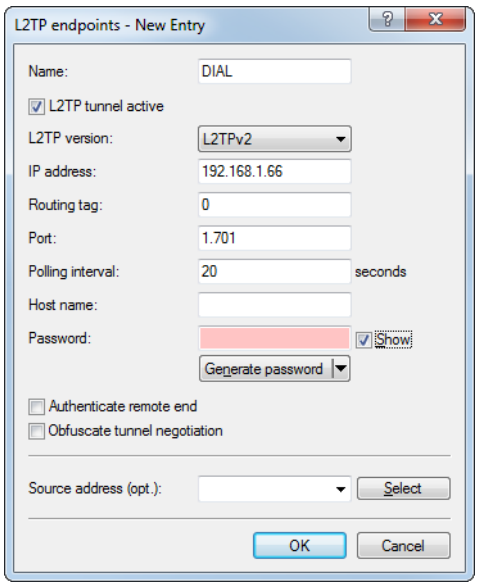
Configuring the RADIUS server to authenticate PPP sessions is conducted as described in the section **Other services** > **RADIUS** > **Configuration of RADIUS as authenticator or NAS** > **Dial-in using PPP and RADIUS**.

11.15.3 Operation as an L2TP access concentrator (LAC)

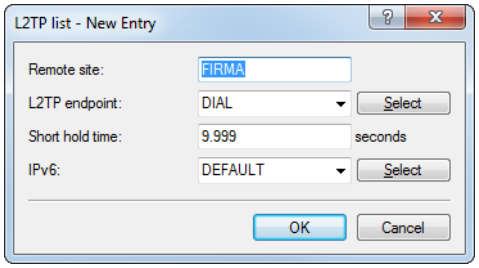
In the following example, the device operating as a L2TP access concentrator (LAC) establishes an L2TP tunnel to an L2TP network server (LNS) with the IP address 192.168.1.66.

Proceed as follows to configure the device as a LAC:

1. Under **Communication** > **Remote sites** > **L2TP** in the table **L2TP endpoints** create an entry for an LNS as the remote L2TP gateway.

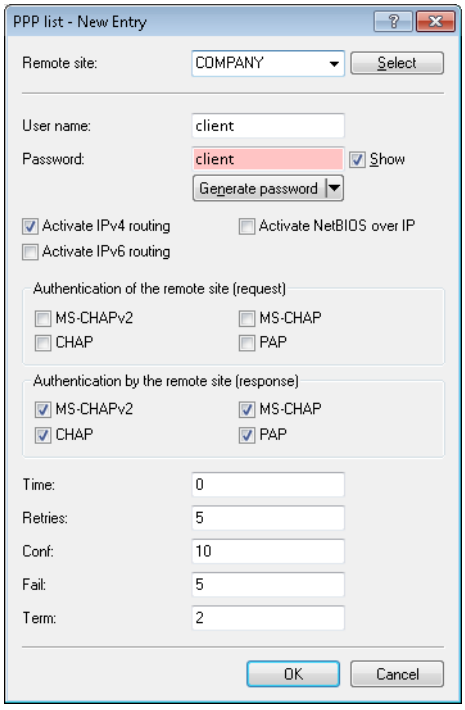


2. Enter a name for this site under **Communication** > **Remote sites** > **L2TP** in the table **L2TP list** and connect it with the L2TP endpoint you created previously.

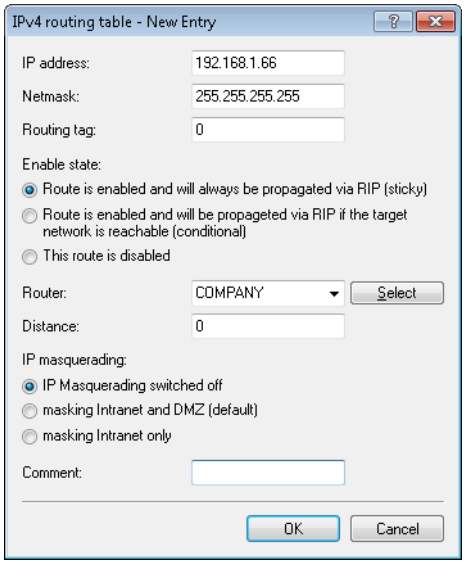


It is possible to connect several remote sites with an L2TP tunnel. This allows multiple PPP sessions to be transported through an L2TP tunnel. For this purpose, configure in this table several remote sites with the same L2TP endpoint.

3. Under **Communication** > **Protocols** in the table **PPP list** create an entry for the L2TP tunnel.



4. For this site, go to **Configuration** > **IP router** > **Routing** and create an entry in the corresponding IPv4 or IPv6 routing table.

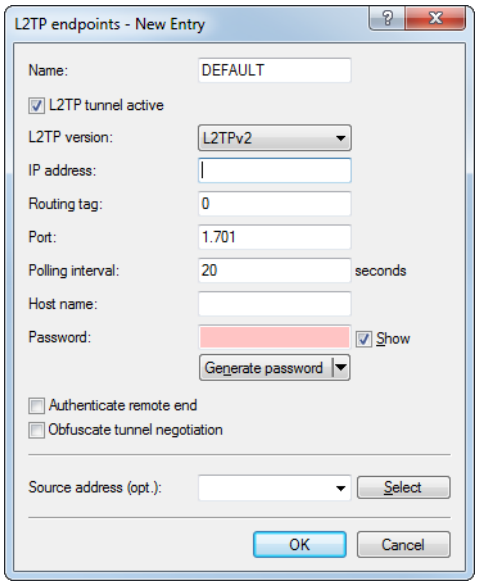


11.15.4 Operation as an L2TP network server (LNS) with authentication via RADIUS

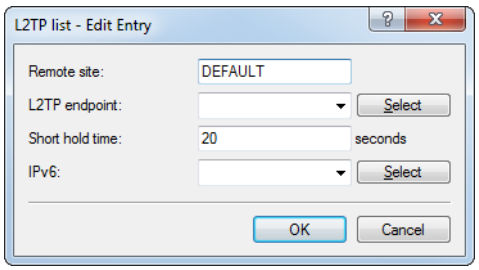
In the following example, the device functions as an L2TP network server (LNS). RADIUS is used to authenticate the incoming L2TP tunnel and the PPP sessions.

Proceed as follows to configure the device as an LNS:

1. Under **Communication** > **Remote sites** > **L2TP** in the table **L2TP endpoints**, create an entry "DEFAULT".

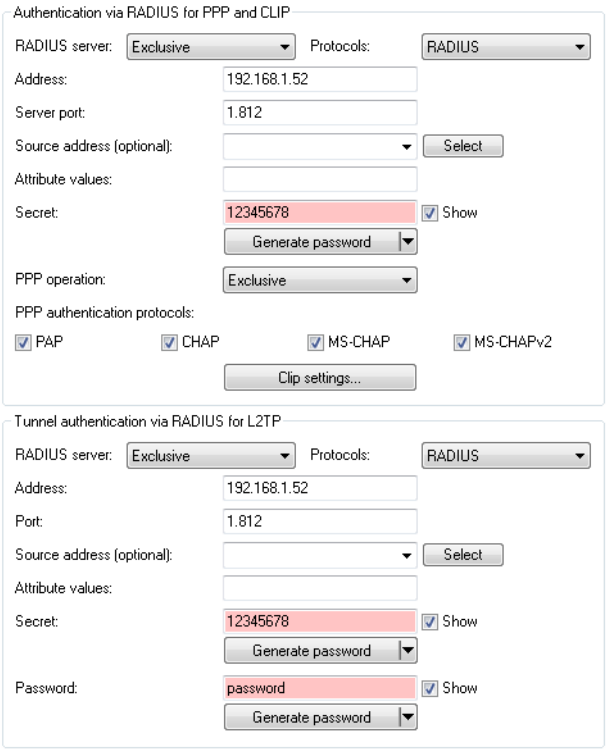


2. Then, under **Communication** > **Remote sites** > **L2TP** in the table **L2TP list**, configure a "DEFAULT" entry.



If the L2TP tunnel is to be connected permanently, set the short hold time to "9999".

3. Configure the RADIUS server under **Communication** > **RADIUS**.



You only configure the lower section **Tunnel authentication via RADIUS for L2TP** if L2TP tunnel authentication should be done via the RADIUS server.

4. Configure the RADIUS server in order for it to be able to authenticate the L2TP tunnel and the PPP sessions.

   If a LAC needs to authenticate itself at the L2TP tunnel with the station name "router1" and the password "abcde", you configure the appropriate entry in the RADIUS server (e.g. FreeRADIUS) as follows:

```
router1 Cleartext-Password := "password"
        Service-Type := Outbound-User,
        Tunnel-Type  := L2TP,
        Tunnel-Password := "abcde",
        Tunnel-Client-Auth-ID := "router1"
```

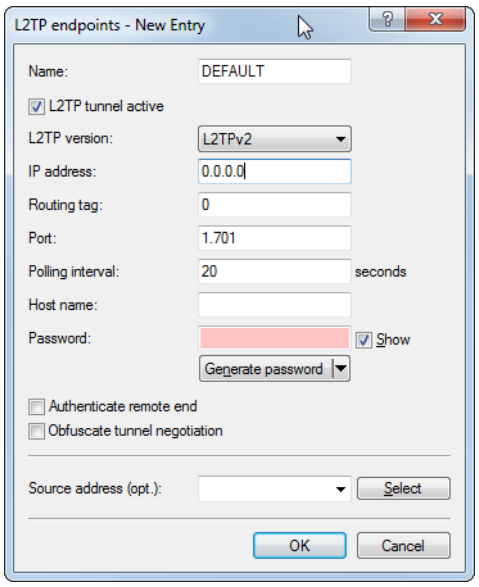
   For the authentication of the PPP session of a user with the username "test" and the password "1234", you configure the appropriate entry in the RADIUS server as follows:

```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP
```

11.15.5 Operation as the L2TP network server (LNS) for RAS clients

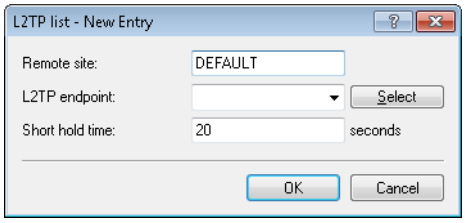
In order to configure the device as the L2TP network server (LNS) for authenticating RAS clients without configuring a RADIUS server in the device, you have two options:

1. Under **Communication** > **Remote sites** > **L2TP** in the table **L2TP endpoints**, create an entry "DEFAULT".



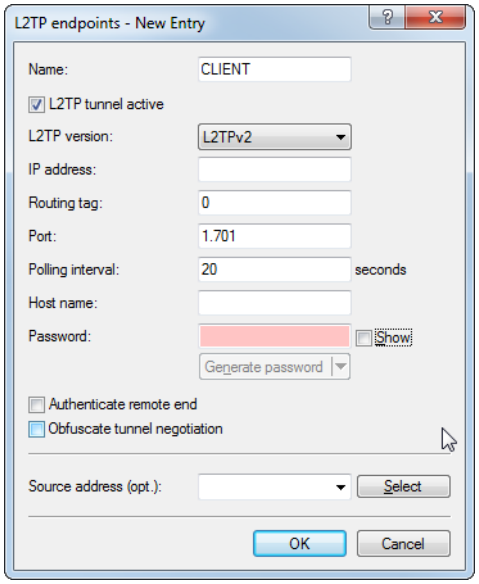
The entry for the IP address is "0.0.0.0", because the IP address of the L2TP-LAC is unknown to the device.

2. Then, under **Communication** > **Remote sites** > **L2TP** in the table **L2TP list**, configure a "DEFAULT" entry.

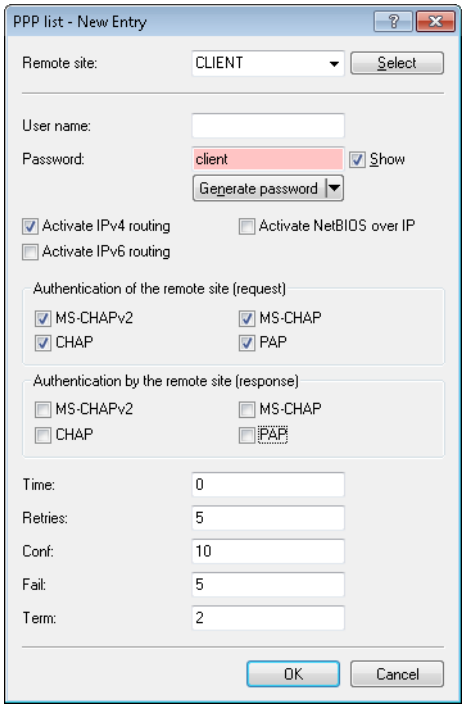


If the L2TP tunnel is to be connected permanently, set the short hold time to "9999".

3. Alternatively, you make a separate entry for the RAS client (e.g., "CLIENT") under **Communication** > **Remote sites** > **L2TP** in the **L2TP endpoints** table.



4. You then configure a new entry for the client under **Communication** > **Protocols** in the **PPP list**.

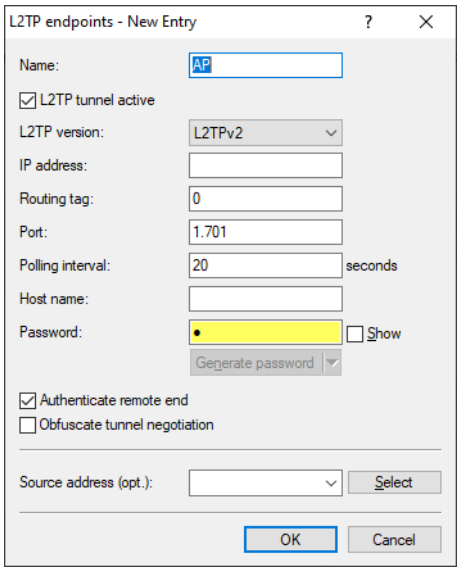


11.15.6 Configuring a WLAN scenario for bridging payload data to the central site

This is an example of how L2TPv3 is used in a scenario where several access points use bridging to transfer their payload data to a central router (referred to here as the "concentrator"), where the data are made available via a separate Ethernet port.

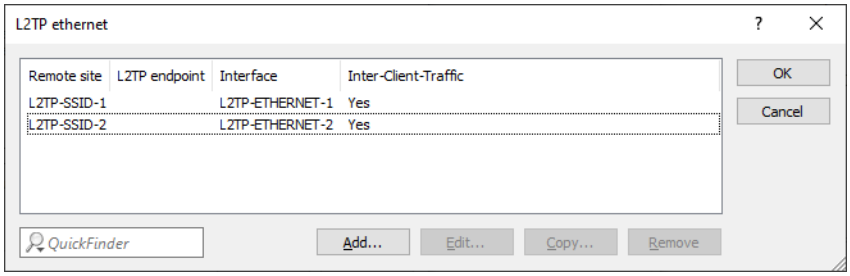
Before LCOS 10.20, this scenario would have required a WLAN controller.

1. Prepare the WLAN configuration on the access points. To enable roaming, SSID names and encryption settings should be configured identically on each AP.
2. Now configure the concentrator, which is to accept the L2TPv3 Ethernet sessions from the individual access points.
   a) Under **Communication** > **Remote sites** > **L2TP** in the L2TP endpoints table, create an entry "DEFAULT". Enter a descriptive name for the new entry. Set the **L2TP version** to "L2TPv3". Do not specify an **IP address**. Set a password to increase security and enable the "Authenticate remote end" option to use the password for authentication during connection establishment. Leave the remaining settings at their default values.



   The **IP address** is empty. This is then a "wildcard" entry that can accept connections from any remote site.

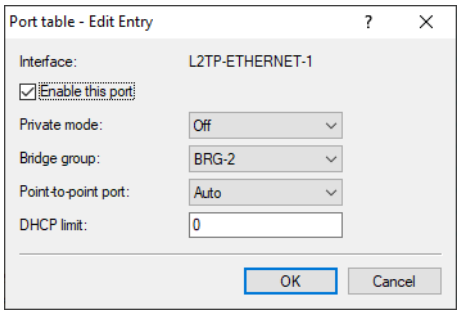
   b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Use **Remote site** to set a name for the Ethernet tunnel, e.g. the name of the SSID to which the tunnel on the access points is to be linked. Leave the field **L2TP endpoint** empty so that any (authenticated) sessions can be accepted. This method avoids having to create an entry for each individual access point in the L2TP endpoint table: The wildcard entry created in the previous step is used instead. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected. If the access points operate multiple SSIDs that are to be bridged to the central site, use this table to create an entry for each SSID, each with a unique name under **Remote site**.





In our scenario, the payload data of all connected access points are routed to the virtual interface configured here. Furthermore, the payload data of all access points connected to this virtual interface are bridged to one another—rather like the WLAN controller-based layer-3 tunneling technique.

c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a LAN interface where you set the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.

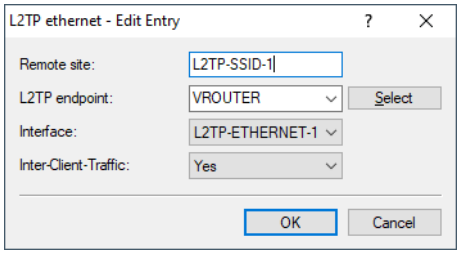


d) This concludes the configuration of the concentrator.

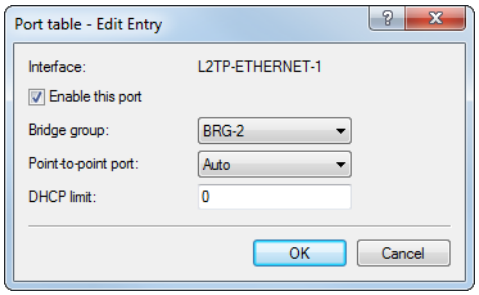
3. The following example shows how to configure an access point to transfer payload data to the concentrator.

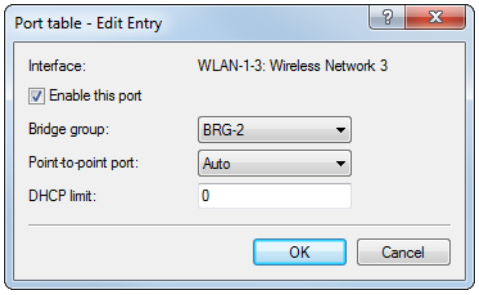
a) Under **Communication** > **Remote sites** > **L2TP**, create a new entry in the L2TP endpoints table. Enter a descriptive name for the new entry. Set the **L2TP version** to "L2TPv3". Enter the IP address or host name where the access point contacts the concentrator. Enter the password you set when configuring the concentrator and select "Authenticate remote end" to use the password for authentication. Leave the remaining settings at their default values.

b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Under **Remote site**, enter a name that identifies the Ethernet tunnel. This must be the same as the name given to this Ethernet tunnel on the concentrator. In the field **L2TP endpoint**, select the L2TP endpoint table entry that was created in the previous step. This endpoint is then used to establish the Ethernet tunnel. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected.



c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a WLAN interface by setting the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.



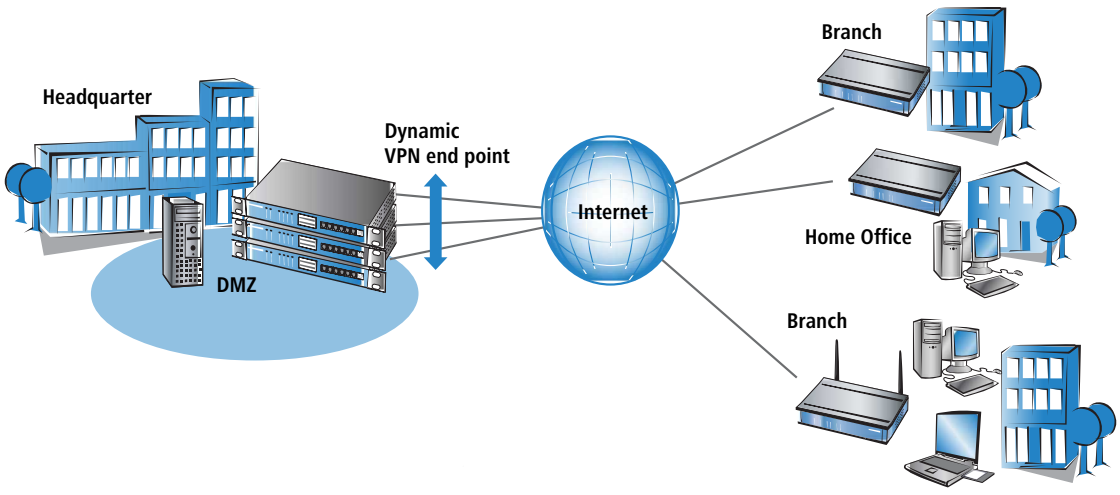


d) Carry out the configuration described here for the other access points. Once the configuration has been completed in this way, the identical configuration can be used on all of the access points and no further adaptations are necessary for the individual APs.

11.16 VPN connections: High availability with “load balancing”

11.16.1 Multiple VPN gateway addresses

In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.



With the option of configuring several "remote gateway" addresses as the "dynamic VPN end point" for a VPN connection, VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the branch sites, all of these available gateways are entered as possible remote sites for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular branch site, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

High availability thanks to "load balancing" between the VPN gateways at the headquarters is attained with the configuration of the branch sites to select the remote site for VPN connection on a random basis.

11.16.2 Grouping and prioritization of alternative gateways

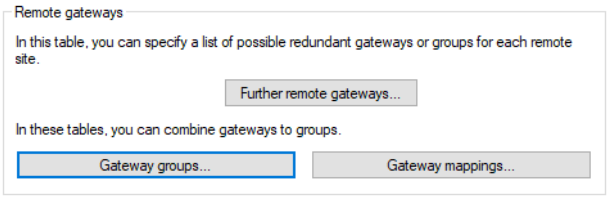
This enhances the existing ability to configure up to 32 additional gateways, which can be selected according to a configurable scheme (first, last used, random) as soon as the primary VPN gateway becomes unreachable.

Now gateways can optionally be collected into groups with equal priority. The highest priority is 0, the lowest 65535. The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the level of priority 0, regardless of its configured priority. All gateways in the table of **Further remote gateways** that do not reference a group name are also added to the group of primary gateways. The selection strategy in the group of primary gateways is defined by the following rules:

- If there are further gateways, the selection strategy is set by the column **Begin with gateway** in the table of **Further remote gateways**.
- If there are no further gateways:
  - If there is only one primary gateway, then the selection strategy is "first".
  - If the primary gateway is a gateway group, the selection strategy of that group is used.

All defined groups are then added to the structure of levels in the order of the gateways from the **Further remote gateways** table with their priority as stored in the **Gateway groups** table. The strategy used to select from groups of the same priority is decided by the column **Begin with gateway** in the **Further remote gateways** table, and the selection strategy within a group is decided by the column **Begin with** in the **Gateway groups** table. The different levels are always used in ascending order of priority beginning with 0.

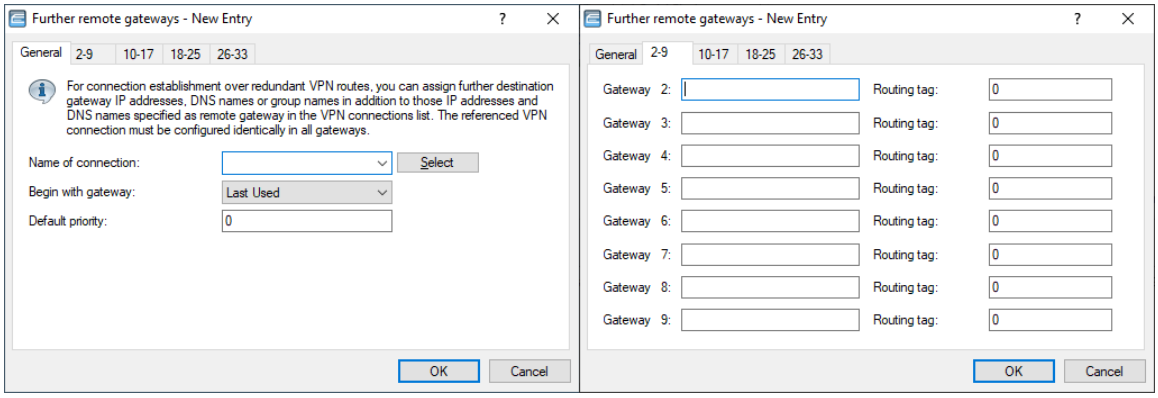
The configuration is performed under **VPN** > **General** > **Remote gateways**.



11.16.2.1 Further remote gateways

The table **Further remote gateways** is used to specify redundant VPN routes by entering further destinations (as an IP address, DNS name or group name for the referenced connection) in addition to the IP address or DNS name specified

as the remote gateway in the VPN connection list. All gateways have to be configured identically with respect to the referenced connection.



Name of connection

From the list of defined VPN connections, select here the name of the VPN connection that the additional gateways defined here apply to.

Begin with gateway

Here you select the first gateway that is to be used for establishing the VPN connection. Possible values:

Last used

Selects the gateway that was most recently used to connect successfully.

First

Start with the first entry in the list.

Random

Selects a random entry from the list.

Default priority

This is the default priority for all gateways specified here. The highest priority is 0, the lowest 65535. All gateways are grouped together, with groups of equal priority placed next to each other on one level.

The primary gateway is automatically placed in its own group with a priority of 0. If the primary gateway references a gateway group, this group is added to the level of priority 0, regardless of its configured priority. If alternative gateways specified here do not reference a gateway group, these will also be added to the group of primary gateways.

Gateway 2-33

You can make three possible entries for each of the up to 32 alternative gateways:

1. The name of a gateway group
2. The DNS name of a gateway
3. The IP address of a gateway

When the table is processed, the first check is to see whether the entry matches with the name of a group specified in the **Gateway groups** table. In this case, all gateways that are mapped to this group in the **Gateway mappings** table are added to the gateway list.

Routing tag

Enter the respective routing tag which is used to set the route to the associated remote gateway.

If you do not specify a routing tag here (i.e. routing tag is 0), then the routing tag configured for this remote station in the VPN connection list is used for the associated gateway.

Example of an alternative gateway

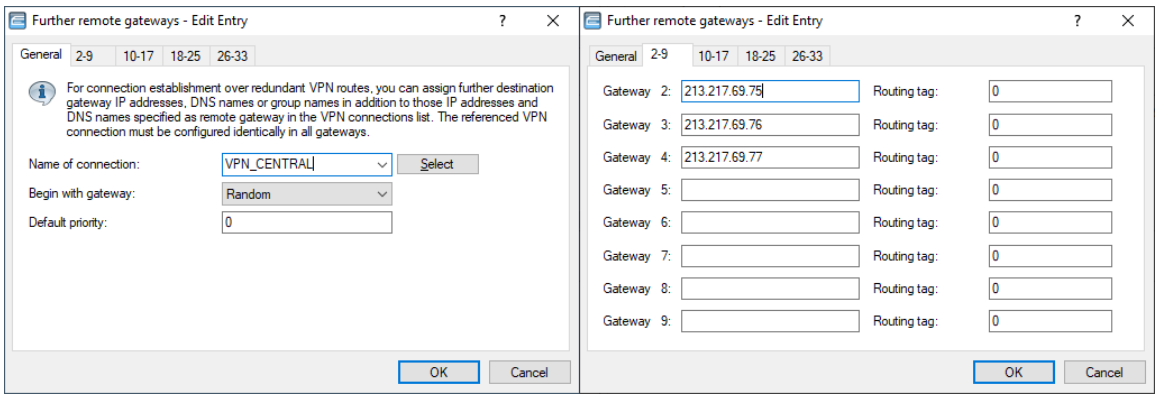
Use the list of **Further remote gateways** to enter additional targets for a VPN connection. The list consists of the following entries:

- Name of the remote site from the VPN connection list, the “targets” of the VPN connection.
- Gateway 2 to gateway 23, the addresses of the alternative gateways, as an IP address or DNS-resolvable address.
- Definition of the order in which the gateway addresses are tried.

The entry for the gateway in the VPN connection list can be left blank if all of the possible gateways are entered into the list of **Further remote gateways**.

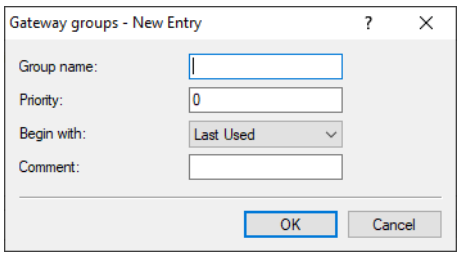
Example:

The following entries specify three gateways (213.217.69.75, 213.217.69.76, 213.217.69.77) as target at the headquarters, one of which is to be selected at random:



11.16.2.2 Gateway groups

The **Gateway groups** table is used to enter gateway groups that you can reference in *Further remote gateways*.



Group name

Give this gateway group a unique name so that you can reference the group later.

Priority

The priority of this group. The highest priority is 0, the lowest 65535.

Begin with

Selection strategy within the group. Possible values:

Last used

Selects the gateway in the group which successfully connected most recently.

First

Start with the first entry in the list.

Random

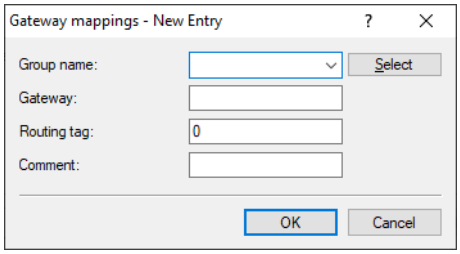
Selects a random entry from the list.

Comment

Optionally enter a meaningful comment as a description.

11.16.2.3 Gateway mappings

The **Gateway mappings** table is used to enter gateway groups that you can reference in *Further remote gateways*. **Gateway** and **Group name** together form the primary key of the table, i.e. the combination of the two must be unique within the table. This allows a single gateway to be mapped to multiple groups, if desired.



Group name

Name of the group that the gateway belongs to.

Gateway

DNS name or IP address of a gateway.

Routing tag

Routing tag of the gateway.

Comment

Optionally enter a meaningful comment as a description.

11.16.2.4 Example of an alternative gateway with prioritized groups

The customer "Telekom" uses the primary gateway 1.1.1.1 and the further gateway 1.1.1.2 without any particular group associations. Also, the further gateways, gateway groups and gateway mappings are specified under **VPN** > **General** > **Remote gateways** as follows:

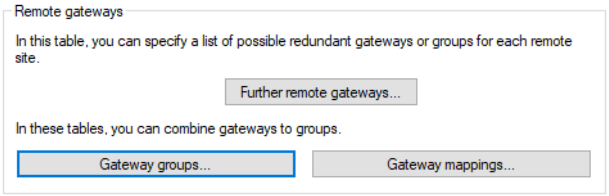


Figure 2: Remote gateways

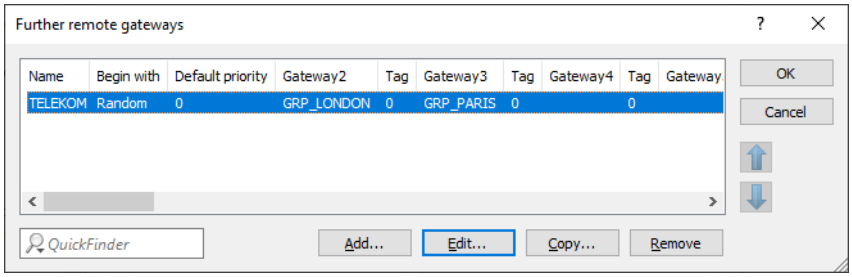


Figure 3: Further remote gateways

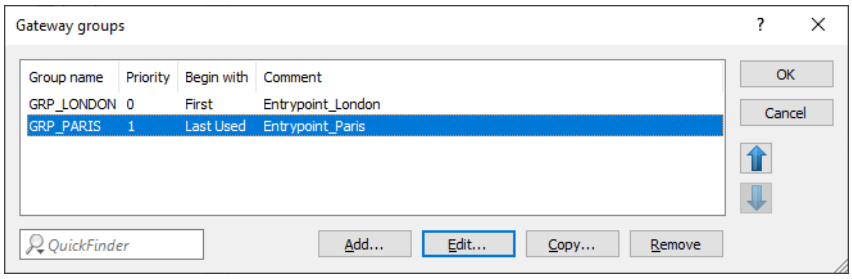


Figure 4: Gateway groups

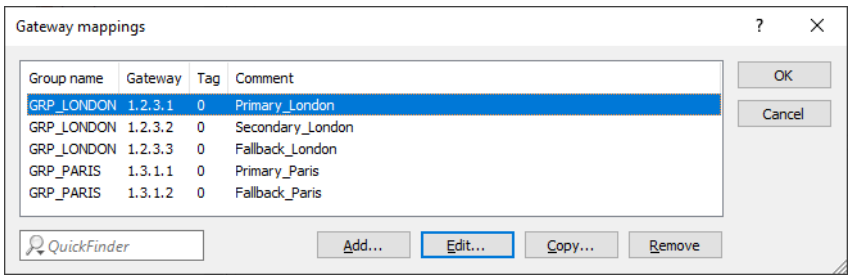


Figure 5: Gateway mappings

This results in the following levels:

Priority	Group 1	Group 2
0	1.1.1.1, 1.1.1.2	GRP_LONDON
1	GRP_PARIS	

This addresses the gateways in the following order:

1. Priority 0: A group is selected at random because in the table **Further remote gateways**, the column **Begin with** is set to "Random":
   - 1.1.1.1, 1.1.1.2 (primary gateway and additional gateway, which does not belong to any group)
   - 1.2.3.1, 1.2.3.2, 1.2.3.3 (GRP_LONDON) beginning with the first gateway in this group
2. Priority 1: A group is selected randomly because in the table **Further remote gateways**, the column **Begin with** is set to "Random":
   - 1.3.1.1, 1.3.1.2 (GRP_PARIS) beginning with the last gateway in this group to be reached successfully.

11.17 How does VPN operate?

In practice, a VPN must fulfill a number of requirements:

- Unauthorized third parties must not be able to read the data (encryption)
- It should not be possible to manipulate the data (data integrity)
- Unambiguous identification of the sender of data (authentication)
- Simple key management
- Compatibility to VPN devices from a variety of manufacturers

VPN achieves these five major goals by applying the widely used IPsec standard.

11.17.1 IPsec – the foundation of VPN

The original IP protocol does not contain any provisions for security. Security problems are compounded by the fact that IP packets do not go directly to a specific recipient, but are sent scattershot to all computers on a given network segment. Anyone can help themselves and read the packets. This leaves the door open to the misuse of data.

IP has been developed further for this reason. A secure version is now available: IPsec. VPN is based on IPsec.

IPsec stands for "**IPsec**urity Protocol" and was originally the name used by a working group of the IETF, the **I**nternet **E**ngineering **T**ask **F**orce. Over the years, this group has developed a framework for a secure IP protocol that today is generally referred to as IPsec.

It is important to note that IPsec itself is not a protocol, but merely the standard for a protocol framework. IPsec actually consists of a variety of protocols and algorithms for encryption, authentication and key management. These standards will be introduced in the following sections.

11.17.1.1 Security in an IP environment

IPsec has been implemented almost completely within level 3 of the OSI model, i.e. in the network layer. The transfer of data packets using the IP protocol is realized on level 3 of IP networks.

IPsec thus replaces the IP protocol. Under IPsec, the packets have a different internal structure than IP packets. Their external structure remains fully compatible to IP, however. IPsec packets can therefore be transported without problems by existing IP networks. The devices in the network responsible for the transport of the packets cannot distinguish IPsec packets from IP packets on the basis of their exterior structure.

The exceptions in this case are certain firewalls and proxy servers that access the contents of the packets. Problems can arise from the (often function dependent) incompatibilities of these devices to the existing IP standard. These devices must therefore be adapted to IPsec.

IPsec will be firmly implemented in the next generation of the IP standard (IPv6). For this reason, we can assume that IPsec will remain the most important standard for virtual private networks in the future.

11.17.2 Alternatives to IPsec

IPsec is an open standard. It is not dependent on individual manufacturers and is being developed by the IETF with input from the interested public. The IETF is a nonprofit organization that is open to everyone. The broad acceptance of IPsec is the result of this open structure which unites a variety of technical approaches.

Nevertheless, there are other approaches for the realization of VPNs. We will only mention the two most important of these here. They are not realized at the network level like IPsec, but at the connection and application levels.

11.17.2.1 Security at the connection level – PPTP, L2F, L2TP

Tunnels can already be set up at the connection level (level 2 of the OSI model). Microsoft and Ascend developed the **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP) early on. Cisco presented a similar protocol with **L**ayer **2** **F**orwarding (L2F). Both manufacturers agreed on a joint effort and the IETF produced the **L**ayer **2** **T**unnel **P**rotocol (L2TP).

Their main advantage over IPsec is that any network protocol can be used with such a network connection, especially NetBEUI.

A major disadvantage of the described protocols is the lack of security at the packet level. What's more, these protocols were designed specifically for dial-up connections.

11.17.2.2 Security at higher levels – SSL, S/MIME, PGP

Communications can also be secured with encryption at higher levels of the OSI model. Well known examples of this type of protocol are SSL (**S**ecure **S**ocket **L**ayer) mainly used for web browser connections, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) for e-mails and PGP (**P**retty **G**ood **P**rivacy) for e-mails and files.

In all of the above protocols, an application handles the encryption of the data, for example the Web browser on one end and the HTTP server on the other.

A disadvantage of these protocols in the limitation to specific applications. In addition, a variety of keys is generally required for the different applications. The configuration must be managed on the individual computers and can not be administered conveniently on the gateways only, as is the case with IPsec. Security protocols at the application level tend to be more intelligent as they know the significance of the data being transferred: This of course makes them much more complex, however.

All of these layer-2 protocols only support end-to-end connections; they are therefore not suitable for connectivity entire networks.

On the other hand, these mechanisms do not require the slightest changes to the network devices or access software. And unlike protocols in lower network levels, they are still effective when the data content is already in the computer.

11.17.2.3 Combinations are possible

All of the alternatives listed above are compatible to IPsec and can therefore be used parallel to it. This permits a further increase of the security level. It would be possible, for example, to dial into the Internet using an L2TP connection, set up an IPsec tunnel to a Web server and exchange HTTP data between the Web server and the browser in secure SSL mode.

Each additional encryption would reduce the data throughput, however. Users can decide on a case-by-case basis whether the security offered by IPsec alone is sufficient. Only in rare cases is a higher level of security really necessary. Particularly as the degree of security can be adjusted within IPsec.

11.18 The standards behind IPsec

IPsec is based on a variety of protocols for the individual functions. These protocols are based on, and complement one another. The modularity achieved with this concept is an important advantage of IPsec over other standards. IPsec is

not restricted to specific protocols but can be supplemented at any time by future developments. The protocols integrated to date also offer such a high degree of flexibility that IPsec can be perfectly adapted to virtually any requirements.

11.18.1 IPsec modules and their tasks

IPsec has to perform a number of tasks. One or more protocols have been defined for each of these tasks.

- Authentication of packets
- Encryption of packets
- Transfer and management of keys

11.18.2 Security Associations – numbered tunnels

A logical connection (tunnel) between two IPSec devices is known as a **S**ecurity **A**ssociation (SA). SAs are managed independently by the IPSec device. An SA consists of three values:

- **Security parameter index (SPI)**

  ID to distinguish multiple logical connections to the same target device with the same protocols
- **IP target address**
- **Security protocol used**

  Designates the security protocol used for the connection, normally ESP:

An SA applies only to one communication direction of the connection (simplex). A complete send and receive connection requires two SAs. In addition, an SA only applies for one used protocol.

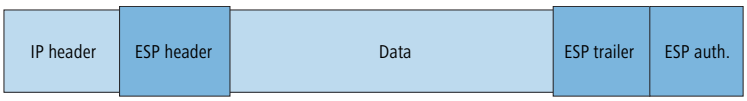
The SAs are managed in an internal database of the IPSec device that also contains the advanced connection parameters. These parameters include the algorithms and keys used, for example.

11.18.3 Encryption of the packets – the ESP protocol

The ESP protocol (**E**ncapsulating **S**ecurity **P**ayload) encrypts the packets as protection against unauthorized access. This was once the only function of ESP, but in the course of the further development of the protocol it was expanded with options for the protection of integrity and verification of authenticity. In addition, ESP also features effective protection against replayed packets.

11.18.3.1 How ESP works

ESP inserts a header behind the IP header as well as its own trailer and a block of ESP authentication data.



11.18.3.2 Transport and tunnel mode

ESP can be used in two modes: transport and tunnel mode.

In transport mode, the IP header of the original packet is left unchanged and the ESP header, encrypted data and both trailers are inserted.

The IP header contains the unchanged IP address. Transport mode can therefore only be used between two end points, for example for the remote configuration of a router. It cannot be used for the connectivity of networks via the Internet—this would require a new IP header with the public IP address of the recipient. In such cases, ESP can be used in tunnel mode.

In tunnel mode, the entire packet including the original IP header is encrypted and authenticated and the ESP header and trailers are added at the entrance of the tunnel. A new IP header is added to this new packet, this time with the public IP address of the recipient at the end of the tunnel.

11.18.3.3 Encryption algorithms

As a higher-level protocol, IPSec does not require any specific encryption algorithms. The manufacturers of IPSec products are thus free in their choice of the processes used. The following standards are common:

- AES – Advanced Encryption Standard

  AES is the official encryption standard for use by US authorities, and therefore one of the most important standards worldwide. Following a worldwide competition in the year 2000 to find the best of the numerous encryption algorithms, the **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) selected the Rijndael algorithm (pronounced: "Rinedoll") and declared it as the AES in 2001.

  AES is a symmetric key algorithm with variable block and encryption lengths. It has been developed by the Belgian scientists Joan Daemen and Vincent Rijmen, and features outstanding security, flexibility and efficiency.
- Triple DES (a.k.a. 3-DES)

  A further development of DES. The conventional DES algorithm is applied three times consecutively. Two or three different keys, each with a length of 56 bits are used. The key for the first run is reused for the third DES run. The result is a nominal key length of 168 bit, with an effective key length of 112 bits.

  Triple-DES combines the sophisticated DES technology with a sufficiently long key and is therefore considered to be secure. Triple-DES is slower than other processes, however.

The encryption can be adapted from the command line. Modifications of this sort are generally only required when setting up VPN connections between devices from different manufacturers.

11.18.4 Key management – IKE

The **I**nternet **K**ey **E**xchange protocol (IKE) can include subprotocols for establishing the SAs (Security Associations) and for key management.

IKE uses two subprotocols: Oakley for the authentication of partners and key administration, and ISAKMP for managing the SAs.

11.18.4.1 Establishing an SA with ISAKMP/Oakley

Establishing an SA involves a sequence of steps (with dynamic Internet connections, these steps follow the exchange of the public IP addresses):

1. The initiator sends a plain-text message to the remote site via ISAKMP with the request to set up an SA and with proposals for the security parameters of the SA.
2. The remote site replies with the acceptance of a proposal.
3. Both devices now generate key pairs, each consisting of a public and private key, for Diffie-Hellman encryption.
4. In two further messages, the devices exchange their public keys for Diffie-Hellman. The further communication is encrypted with Diffie-Hellman.
5. Both ends use numbers that have been transferred (with the Diffie-Hellman method) and the Shared Secret to generate a common secret key that is used to encrypt the subsequent communication. Both sides additionally authenticate their Shared Secrets by using hash codes. Phase 1 of the SA setup is thus completed.
6. Phase 2 is based on the encrypted and authenticated connection established in Phase 1. In Phase 2, the session keys for the authentication and symmetrical encryption of the actual data transfer are generated at random and transferred.

Symmetrical processes are used for the encryption of the actual data transfer. Asymmetrical processes (also known as public-key encryption) are more secure as they do not require the exchange of secret keys. However, they require considerable processing resources and are thus significantly slower than symmetrical processes. In practice, public-key encryption is generally only used for the exchange of key material. The actual data encryption is then performed using the fast symmetrical process.

11.18.4.2 The regular exchange of new keys

ISAKMP ensures that new key material is regularly exchanged between the two devices during the SA. This takes place automatically and can be configured with the Lifetime setting in LANconfig.

11.18.5 Replay detection

Replay detection is a feature of the IPSec standard for the detection of so-called replay attacks. In a replay attack, an unauthorized station logs data and sends this, either repeatedly or with a delay, to a remote site to simulate a different identity.

Replay detection defines a certain number of consecutive packets (a "window" with the length of "n"). Because the IPSec standard provides the packets with a continuous sequence number, the receiving VPN device can determine whether a packet contains a sequence number from the permitted window. If, for example, the current highest received sequence number is 10,000 and the window width is 100, then a sequence number of 9,888 is outside the permitted window.

Replay detection discards received packets if:

- they contain a sequence number before the current window, in which case they are seen as being too old, or if
- they contain a sequence number which has already been received by the VPN device, in which case replay detection evaluates this packet as part of a replay attack

Please consider the following aspects when configuring the replay-detection window:

- If you select too large a window, then replay detection may overlook a replay attack
- If you make the window too small, replay detection may drop legitimate packets that became reordered during data transfer, so generating errors on the VPN connection



You have to weigh-up the application of replay detection for your particular case. Only activate replay detection if the security of the VPN connection is more important to you than interference-free data transfer.

11.19 IKEv2

LANCOM devices are capable of operating VPN with IKEv1 and IKEv2.

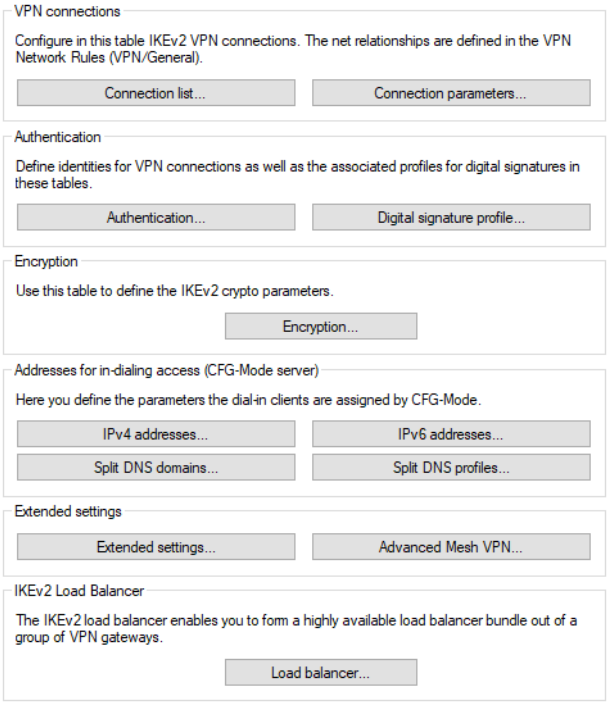
IKEv2 facilitates a fast and secure establishment of VPN tunnels. For the first time it is now possible to operate encrypted networking between IPv6-based sites and IPv4-based sites by means of the mixed mode.

Manually configuring a VPN connection that uses IKEv1 is complex and error prone. Consequently, many IPSec implementations have incompatible configurations, which causes the VPN connections between the devices to fail. The IKEv2 configuration in LCOS gives administrators a reliable method of setting up a configuration that matches that of the remote station. For example, administrators have a choice of several Diffie-Hellman groups. At the same time, the revised user interface presents recommended default values for many of the configuration parameters. The simplified configuration with IKEv2 eliminates sources of error, which results in a lower administrative overhead. Further, VPN connection establishment with IKEv2 offers better performance, because IKEv2 only exchanges 4 packets when negotiating a VPN tunnel (one `REQUEST` per VPN partner and one `REPLY`), rather than the 6 required by IKEv1 in the "aggressive/quick mode" or 12 in "main mode". The standard of security is just as high with IKEv2 as with IKEv1.

Operating IKEv2 supports *RFC 7296*, *RFC 7427* and, in the IKEv2 client mode, *RFC 5685*.

11.19.1 Configuring IKEv2 with LANconfig

IKEv2 is configured under **VPN** > **IKEv2/IPSec**.



VPN connections

In this section, you configure the IKEv2 VPN connections and the connection parameters.

Authentication

This table is used to define the identities for your VPN connections.

Digital signature profile

This table is used to specify the authentication methods for your VPN connections.

Encryption

This table is used to set the encryption parameters.

Addresses for dial-in access (CFG mode server)

Use these tables to specify the parameters that the device CFG mode assigns to the dial-in clients.

IKEv2 supports Split DNS. This is configured under **Split DNS domains** and **Split DNS profiles**.

Extended settings

This section is used to configure the settings for the authentication of other remote identities, the IKEv2 rekeying parameters, and the prefixes for IKEv2 routing.

Load balancer

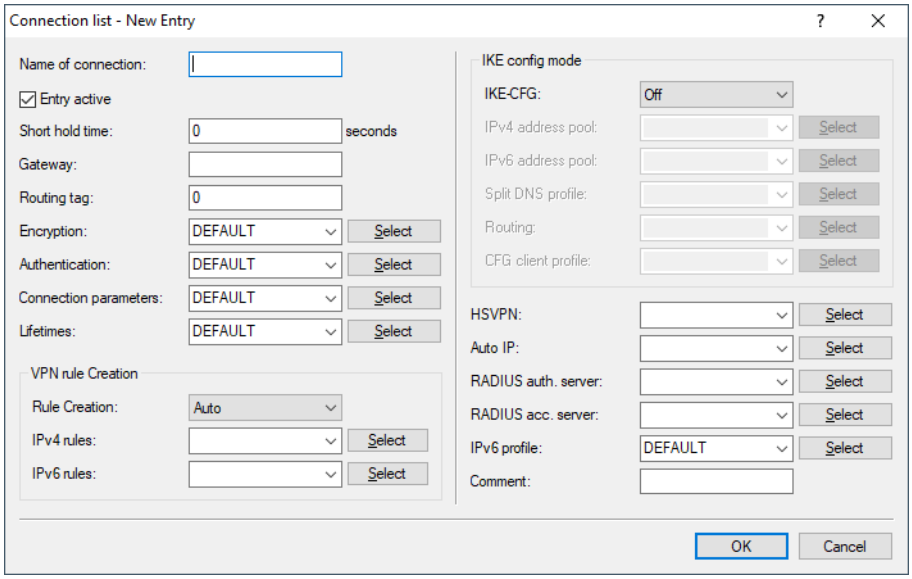
Use this section to configure the settings for the IKEv2 load balancer.

In order to configure an IKEv2 connection, you first need to make an entry in the **Connection list**. LCOS contains default entries in order to minimize the effort of configuration. Most of these entries contain default parameters with common settings for strong encryption algorithms, dead-peer-detection, and lifetimes. All you need to do is specify the address of the VPN remote peer, the authentication parameters (under **Authentication**), and the VPN rules (under **VPN** > **General** > **Network rules**).

The CLI command `show vpn` displays whether the VPN connection was established successfully.

11.19.1.1 Connection list

In this table, you configure the IKEv2 connections to VPN partners.



Name of connection

Contains the name of the connection to the remote station.

Entry active

Enables or disables the connection to this VPN peer.

Short hold time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

Gateway

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner. If the value is left blank, there is no additional check of the IP address of the other party. This is required if the remote site has a dynamic IP address, for example.

If you specify a FQDN, you can use a suffix to control the DNS resolution. See also *Configuration option for IPv4/IPv6 resolution with DNS resolutions* on page 171.

Routing tag

Contains the routing tag for this VPN connection.

Encryption

Specifies the encryption used for the VPN connection. The corresponding entry is located in the **Encryption** table.

Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the **Authentication** table.

Connection parameters

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the **Connection parameters** table.

Validity period

Specifies the lifetime of the key used for the VPN connection. The corresponding entry is located in the table **VPN** > **IKEv2/IPsec** > **Extended settings** > **Lifetimes**.

VPN rule creation

Rule creation

Specifies how VPN rules are created.

Possible values:

Automatic

The local intranet serves as the source network (private IP address range that the local VPN gateway itself belongs to). For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

When two simple local networks are connected, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.

Manual

Rules are created for the network relationships in the same way as rules are defined manually for IPv4 or IPv6.

IPv4-Rules

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table **VPN** > **General** > **Network rules**.

IPv6-Rules

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table **VPN** > **General** > **Network rules**.

IKE config mode

IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

Possible values are:

- Off: IKEv2 config mode is disabled
- Server: The router distributes configuration parameters (such as addresses or the DNS server) to VPN clients. The parameters to be distributed are configured in the IPv4 or IPv6 address pool.
- Client: The router requests the server for configuration parameters (e.g. addresses or the DNS server).

IPv4 address pool

IPv4 addresses and DNS server for dial-in access in the IKE CFG mode Server.

IPv6 address pool

IPv6 addresses and DNS server for dial-in access in the IKE CFG mode Server.

Split DNS profile

Name of the Split DNS profile. The split DNS profile is only active if **IKE-CFG** is set to the value **Server**.

Routing

Specifies the routes that the remote site should transmit dynamically via IKE-CFG mode. This function is only available in the IKEv2 CFG mode for the client and server.

The routes for IPv4 and IPv6 connections are located in the tables **VPN** > **IKEv2/IPsec** > **Extended settings** > **IPv4 routing/IPv6 routing**.

CFG client profile

Select a CFG client profile that you created under *CFG client profile* on page 885. This profiles specifies whether the device in the role CFG-Mode client should request an address from the CFG-Mode server.

HSVPN

High Scalability VPN (HSVPN)

In SD-WAN scenarios where branches connect to one or more central sites, there are usually several logical networks that need to be securely separated from one another (e.g. for payment transactions, inventory management, or a hotspot) by means of VLAN and ARF. These local networks were previously connected to the central site either as "stacked" tunnels, i.e. PPTP or L2TP within a VPN tunnel, or as individual IPsec VPN tunnels. However, these architectures do not scale well with large numbers of branches and ARF networks. For example, in an architecture with one tunnel per ARF network, 1,000 branches and 8 ARF networks results in a total of 8,000 tunnels. Stacked tunnels have performance and MTU restrictions due to the protocol overhead.

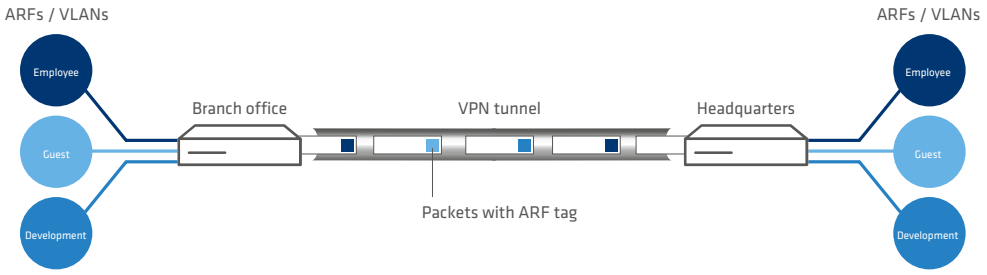


Figure 6: LANCOM HSVPN scenario for SD-WAN

The new architecture LANCOM HSVPN ("LANCOMHigh Scalability VPN") solves these challenges. With HSVPN, packets from ARF networks within an IPsec tunnel are marked with an ARF tag and transported in the VPN tunnel without overhead. This layer-2 based tagging method corresponds to the VLAN layer-3 approach and provides the same level of security. As fewer tunnels are required overall, tunnel establishment times are improved, especially in case of failover. Also, no major restrictions apply with regard to MTU.

The following configuration steps are necessary:

1. Creating the individual ARF networks
2. Creating an IKEv2 tunnel
3. The allowed ARF networks are configured as a tag list in the HSVPN configuration profile of the IKEv2 tunnel (*HSVPN profiles* on page 880)
4. For the desired ARF networks, corresponding routes must be created through the HSVPN tunnels.

LANCOM HSVPN supports two modes:

› Classic site-to-site VPN

- CFG mode with IKEv2 routing, where routes and routing tags are transmitted

Current restrictions:

- Multicast routing is currently not supported over HSVPN. This requires a separate VPN tunnel for multicast.
- OSPF over HSVPN is not supported

Here you set the name of the HSVPN profile from the table *HSVPN profiles* on page 880.

Auto-IP

Using the Auto-IP parameter, a VPN central site can transmit the IP address of the *Dynamic Path Selection* measurement target to a VPN branch. For this purpose, the Auto-IP parameter is configured at the central site. At the branch, the measurement target has to be set (IPv4 as 0.0.0.0 or IPv6 as ::) in order for the branch to automatically take over the measurement target from the central site.

Refers to the relevant Auto-IP profile, which you set up under *IKEv2-Auto-IP-Profile* on page 886.

RADIUS auth. server

Specifies the RADIUS server for the VPN peer authorization. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPsec** under **Extended settings**.

RADIUS acc. server

Specifies the RADIUS server for the VPN peer accounting. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPsec** under **Extended settings**.

IPv6 profile

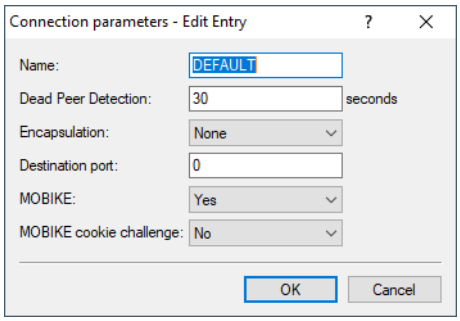
This entry specifies the name of the IPv6 WAN profile. Leaving this entry blank causes IPv6 to be disabled for this interface. The IPv6 remote sites are configured under **IPv6** > **General** > **IPv6 interfaces** > **WAN profiles**.

Comment

Enter a descriptive comment here.

11.19.1.2 Connection parameters

Use this table to specify the parameters of IKEv2 VPN connections that are not included in the SA negotiation. An entry named "DEFAULT" is provided with common settings.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Connection parameters" field.

Dead peer detection

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. SSL or UDP can be set here. Use this in combination to configure any **Destination port**. The IKEv2 tunnel is established either with port 4500 for UDP or with the port set for the **Destination port**. If the destination port is set to 500, this will be ignored and port 4500 is used instead. For SSL, the tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead. If set to "None", the port 500 is taken and the setting in **Destination port** is ignored.

The configurable port can be used for scenarios where a LANCOM router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

Destination port

Here you can specify that the destination port depends on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

MOBIKE

Defines whether MOBIKE as per *RFC 4555* should be supported.

MOBIKE according to RFC 4555 for IKEv2 optionally allows mobile clients to roam between different networks without disconnecting the VPN tunnel. For example, a VPN client can roam seamlessly from cellular to Wi-Fi, whereby an IKEv2 update message updates the external IP address on the VPN gateway. The advantage is that the VPN tunnel or the Security Associations (SAs) do not have to be terminated and setup again.

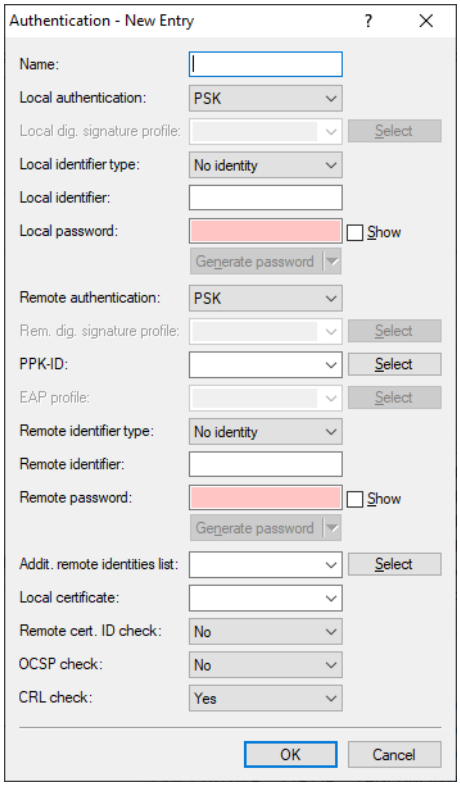
MOBIKE is only supported as a responder role, i.e. when VPN clients establish connections to the LANCOM VPN router. The establishment of VPN tunnels with the MOBIKE extension is not supported.

MOBIKE cookie challenge

Defines whether the device should send a cookie challenge to determine whether the VPN client can actually receive packets at the new address ("Return Routability Check").

11.19.1.3 Authentication

In this table, you configure the parameters for IKEv2 authentication of the local and at least one remote identifier.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Authentication" field.

Local authentication

Sets the authentication method for the local identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per RFC 7427. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.
- ECDSA-256, ECDSA-384, ECDSA-521: Use of Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 for authentication.

  ECDSA signatures are generally smaller than RSA signatures with comparable cryptographic strength. ECDSA keys and certificates also have significantly smaller file sizes than RSA-based keys and certificates. Furthermore, ECDSA operations are generally faster on most devices. The following methods are supported in IKEv2.

  - ECDSA with SHA-256 on the P-256 curve
  - ECDSA with SHA-384 on the P-384 curve
  - ECDSA with SHA-512 on the P-521 curve

  When using OpenSSL, the following predefined curves must be used as parameters for ECDSA in IKEv2:

- prime256v1 with ECDSA-256
- secp384r1 with ECDSA-384
- secp521r1 with ECDSA-512

The following restrictions apply when using ECDSA:

- ECDSA-based certificates currently cannot be generated by the LCOS's own CA. Similarly, it is not possible to obtain certificates automatically by means of SCEP. ECDSA certificates must be generated using an external application such as OpenSSL or XCA and then loaded into the device.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

Local digital signature profile

The profile name of the local digital signature profile that is used.

Local identifier type

Defines the ID type of the local identity. The device interprets the entry under "Local identifier" accordingly. Possible entries are:

- No identity: No identity is transmitted.
- IPv4 address: The device uses an IPv4 address as a local ID.
- IPv6 address: The device uses an IPv6 address as a local ID.
- Domain name (FQDN): The device uses a domain name as a local ID.
- E-mail address (FQUN): The device uses an e-mail address as a local ID.
- ASN.1 Distinguished Name: The device uses a distinguished name as a local ID (e.g. "CN=client01.example.com,O=test,C=DE").
- Key ID (group name): The device uses the group name as a local ID. You can set any group name.

Local identifier

Contains the local identity. The significance of this entry depends on the setting under "Local identifier type".

Local password

Contains the password of the local identity. The device uses this password to authenticate at the remote site. The local and remote password can be identical or different.

Remote authentication

Sets the authentication method for the remote identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per RFC 7427. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.
- ECDSA-256, ECDSA-384, ECDSA-521: Use of Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 for authentication.

  ECDSA signatures are generally smaller than RSA signatures with comparable cryptographic strength. ECDSA keys and certificates also have significantly smaller file sizes than RSA-based keys and certificates. Furthermore, ECDSA operations are generally faster on most devices. The following methods are supported in IKEv2.

- ECDSA with SHA-256 on the P-256 curve
- ECDSA with SHA-384 on the P-384 curve
- ECDSA with SHA-512 on the P-521 curve

When using OpenSSL, the following predefined curves must be used as parameters for ECDSA in IKEv2:

- prime256v1 with ECDSA-256
- secp384r1 with ECDSA-384
- secp521r1 with ECDSA-512

The following restrictions apply when using ECDSA:

- ECDSA-based certificates currently cannot be generated by the LCOS's own CA. Similarly, it is not possible to obtain certificates automatically by means of SCEP. ECDSA certificates must be generated using an external application such as OpenSSL or XCA and then loaded into the device.

- EAP: Extensible Authentication Protocol

  EAP is not a specific authentication mechanism, but rather a framework for various authentication methods such as TLS (authentication by certificate) or MSCHAP (authentication by username/password).

  EAP authentication is handled by an external RADIUS server, such as the LANCOM RADIUS server, FreeRADIUS, or Microsoft Network Policy Server (NPS). The VPN gateway merely acts as a mediator between the client and the RADIUS server. The VPN gateway must authenticate itself to the client using a certificate with a valid RSA signature. The RADIUS server must also have a valid certificate. The necessary certificates can be generated, for example, with the LANCOM SCEP CA in the router. After generation, the appropriate certificate containers are imported into the VPN gateway and into the RADIUS server.

  To use the IKEv2 EAP authentication feature on LANCOM routers, you will need the VPN-25 Option or a router with 25 or more VPN tunnels. Check whether the router supports IKEv2 EAP in the LCOS Status menu under **Status** > **Software-Info** > **IKEv2-EAP-License**.

  See also *EAP and IEEE 802.1X* on page 959.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

Remote digital signature profile

The profile name of the remote digital signature profile.

PPK ID

Enter the name of the PPK-ID (Post-quantum Preshared Keys as per *RFC 8784*) from the table of *PPKs (Post-quantum Preshared Keys)* on page 877.

EAP profile

Specify an EAP profile if the method for the **Remote authentication** was set to EAP. The EAP profiles are specified under *EAP profiles* on page 878.

Remote identifier type

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under "Remote identifier" accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the "Remote identifier" field.

- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as a remote ID (e.g. “CN=client01.example.com,O=test,C=DE”).
- Key ID (group name): The device expects the group name as the remote ID.

Remote identifier

Contains the remote identity. The significance of this entry depends on the setting under “Remote identifier type”.

Remote password

Contains the password of the remote identity.

Addit. remote identities list

Redundant VPN scenarios allow the use of alternative remote identities.

Here you configure additional remote identities from the table **Extended settings** > **Identity list**.

Local certificate

Specify the local VPN certificate used by the device for outbound connections.

The corresponding VPN certificates “VPN1” to “VPN9” have to be configured under **Certificates** > **SCEP client** in the **Certificate table**.

Remote certificate check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

OCSP check

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

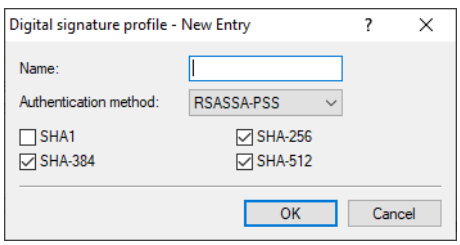
CRL check

This setting enables the checking of an X.509 certificate by certificate revocation list (CRL), which checks the validity of the remote station's certificate.

You should only switch this off if you are checking by other means, e.g. with OCSP.

11.19.1.4 Digital signature profile

Use this table to configure the parameters for the IKEv2 authentication.



Name

Contains the unique name of this entry. You can assign this name in three different places. In the **Authentication** section in the fields **Local dig. signature profile**, **Rem. dig. Signature profile** and under **Extended Settings** > **Authentication** > **Identities** > **Rem. dig. signature profile**.

Authentication method

Sets the authentication method for the digital signature. Possible values are:

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)
- ECDSA: Elliptic Curve Digital Signature Algorithm (ECDSA)
- EdDSA25519: Edwards Curve 2551 (EdDSA25519) as per *RFC 8420*
- EdDSA448: Edwards Curve 448 (EdDSA448) as per *RFC 8420*

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

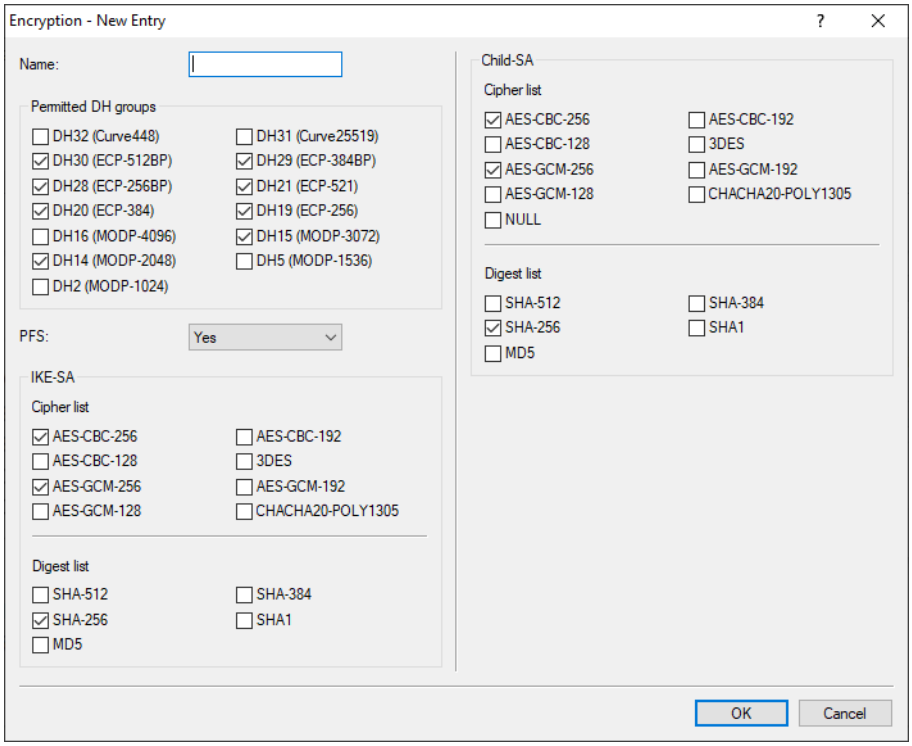
You also specify the secure hash algorithms (SHA) to be used.

11.19.1.5 Encryption

This table is used to configure the encryption parameters. An entry named "DEFAULT" is provided with common settings.

Multiple parameters can be selected. The device propagates these parameter lists in the IKE protocol and in CHILD SAs. The two VPN partners agree to use one of the algorithms in the propagated lists. While they are establishing the first IKE SA, the VPN partners agree to use the highest of the mutually propagated DH groups. The VPN partners use this DH group when they renew the IKE SAs, or when they create or renew the CHILD SAs (if PFS is enabled).

A connection will be established between the VPN partners if there are sets of encryption parameters that agree at both ends. If none of the parameters match, no connection can be established.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** by selecting it from the "Encryption" field.

Permitted DH groups

Contains the selection of Diffie-Hellman groups used by the VPN partners to create a key for exchanging data. The higher the DH group selected, the more complex is the key that is generated. The following groups are currently supported:

- DH-2 (1024-bit modulus)
- DH-5 (1536-bit modulus)
- DH-14 (2048-bit modulus)
- DH-15 (3072-bit modulus)
- DH-16 (4096-bit modulus)
- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)
- DH-31 (Curve25519)
- DH-32 (Curve448)

PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

Cipher list

Specifies which encryption algorithms are enabled. The following encryption algorithms are available:

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- 3DES
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256
- Chacha20-Poly1305

  ChaCha20 data stream encryption in conjunction with the Poly1305 Authenticator, see *RFC 7634*.

  Please note that ChaCha20-Poly1305 is currently not accelerated by hardware and is therefore not recommended for VPN scenarios where high encryption performance is required.

- NULL

  The data packets are no longer encrypted here. This function is only required in special scenarios and is generally not recommended.

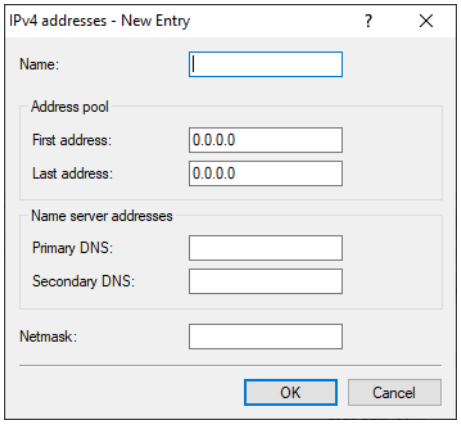
Digest list

Specifies which hash algorithms are enabled. The following hash algorithms are available:

- SHA1
- SHA-256
- SHA-384
- SHA-512
- MD5

11.19.1.6 IPv4 addresses

Use this table to configure the IPv4 parameters that the device CFG mode assigns to the VPN clients.



Name

Contains the name of the IPv4 address pool.

Address pool

First address

Here you enter the first IPv4 address of the pool of addresses that you want to provide to VPN clients.

Last address

Here you enter the last IPv4 address of the pool of addresses that you want to provide to VPN clients.

The address pool specified here should be outside the defined networks. Otherwise, you have to enable proxy ARP.

Name server addresses

DNS default

Contains the primary DNS address.

DNS backup

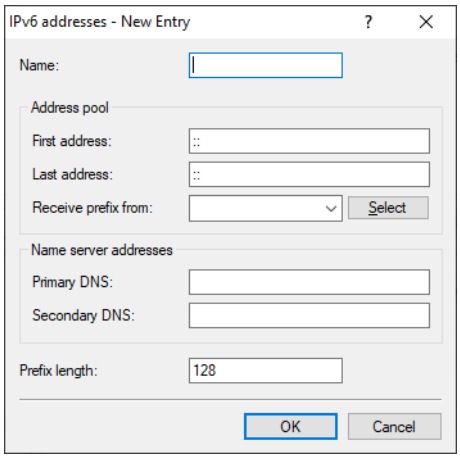
Contains the secondary DNS address.

Netmask

Optional netmask sent along with the negotiated IP address.

11.19.1.7 IPv6 addresses

Use this table to configure the IPv6 parameters that the device CFG mode assigns to the VPN clients.



Name

Contains the name of the IPv6 address pool.

Address pool

First address

Here you enter the first IPv6 address of the pool of addresses that you want to provide to VPN clients.

Last address

Here you enter the last IPv6 address of the pool of addresses that you want to provide to VPN clients.

Receive prefix from

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter **First address** to the value "::1" in the **Last address** to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- First address: 0:0:0:0001::1
- Last address: 0:0:0:0001::9

Currently no Neighbor Discovery Proxy is supported for IPv6. For this reason, the address range of the pool must not overlap with address ranges or prefixes that are already used for other networks on the router.

Name server addresses

DNS default

Contains the primary DNS address.

DNS backup

Contains the secondary DNS address.

Prefix length

Optional prefix length sent for the negotiated IP address.

11.19.1.8 Split DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. "*.company.com") to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

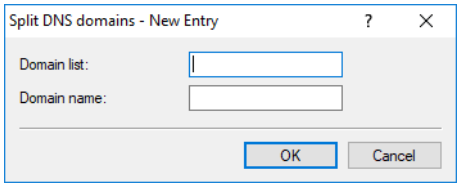
Split DNS for IKEv2 is supported by LANCOM VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

The split-DNS configuration is assigned in the IKEv2 connection list when the CFG mode is set to "Server" and the split DNS profile has been selected.

In LANconfig you first specify the required domains under **VPN** > **IKEv2/IPSec** > **Split DNS domains** and assign these to a profile under **VPN** > **IKEv2/IPSec** > **Split DNS profiles**. This profile can then be selected in the **Connection list** under IKE config mode when **IKE-CFG** is set to **Server**.

Split DNS domains

In LANconfig, the split DNS domains are configured under **VPN** > **IKEv2/IPSec** > **Split DNS domains**.



Domain list

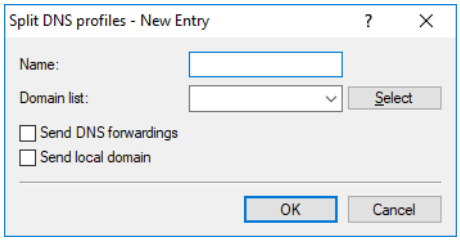
Enter a name for the domain lists.

Domain name

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. “company.internal”. Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

Split DNS profile

In LANconfig, the split DNS profiles are configured under **VPN** > **IKEv2/IPSec** > **Split DNS profiles**.



Name

Enter a name for this profile.

Domain list

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

Send DNS forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

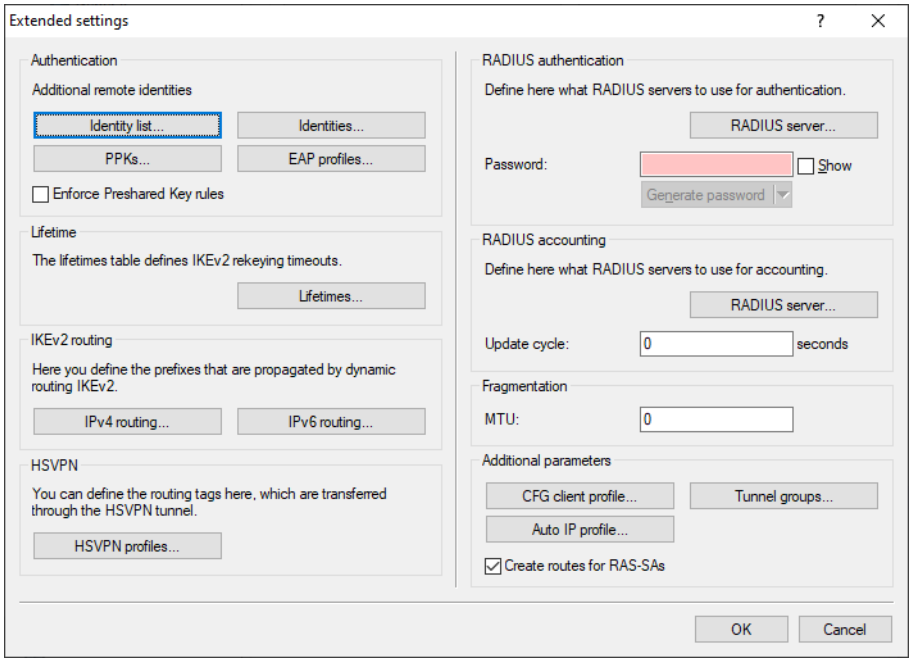
Send local domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

11.19.1.9 Extended settings

Use this dialog to configure the following: The settings for the authentication of other remote identities; the IKEv2 rekeying parameters; the prefixes for IKEv2 routing; the routing tags for High Scalability VPN (HSVPN), which are

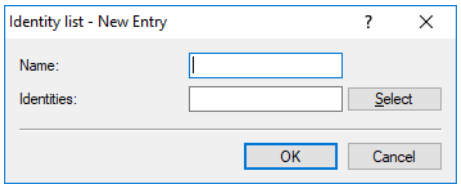
transmitted through the HSVPN tunnel; the RADIUS servers for IKEv2; IKEv2 fragmentation; client profiles used in the role CFG-Mode Client to control whether a request should be made to the CFG-Mode server; and the IKEv2 tunnel groups.



Authentication

Identity list

Use this table to collect other remote identities into a group.



Name

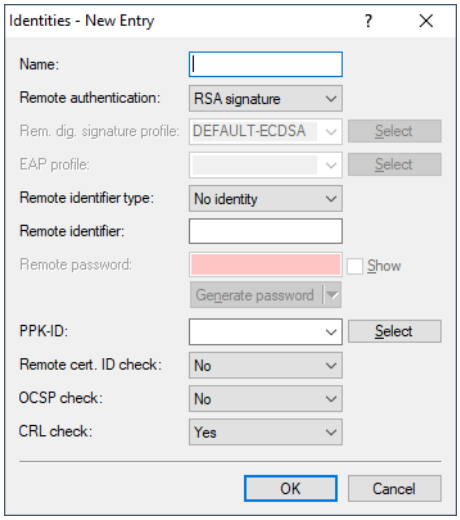
Contains the unique name of this entry.

Identity

Lists the other identities that are collected into this group. Configure the identities under **Identities**.

Identities

Use this table to configure additional remote identities. You select this name when grouping remote identities in the **Identity list**.



Name

Contains the unique name of this entry.

Remote authentication

Sets the authentication method for the remote identity.

Rem. dig. signature profile

If the **Remote authentication** is set to “Digital signature”, enter the name of the remote digital signature profile here.

Remote identifier type

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under “Remote identifier” accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the “Remote identifier” field.
- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as the remote ID.
- Key ID (group name): The device expects the group name as the remote ID.

Remote identifier

Contains the remote identity. The significance of this entry depends on the setting under “Remote identifier type”.

Remote password

Contains the password of the remote identity.

PPK ID

Enter the name of the PPK-ID (Post-quantum Preshared Keys as per *RFC 8784*) from the table of *PPKs (Post-quantum Preshared Keys)* on page 877.

Remote certificate ID check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

OCSP check

With this setting you enable the Online Certificate Status Protocol (OCSP), which checks the validity of the remote station's certificate in real time. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

Please note that the check via OCSP only checks the locking status of a certificate, but it does not check the mathematical correctness of its signature, validity period, or other usage restrictions.

CRL check

This setting enables the checking of an X.509 certificate by certificate revocation list (CRL), which checks the validity of the remote station's certificate.

You should only switch this off if you are checking by other means, e.g. with OCSP.

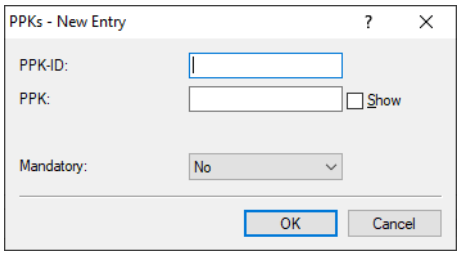
PPKs (Post-quantum Preshared Keys)

Quantum computers pose a potential challenge to current cryptographic algorithms, such as those used in IKEv2 VPN. Current algorithms are considered to be very robust, but the challenge is that an attacker can record encrypted data today and decrypt it using quantum computers in the future.

The *RFC 8784* "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security" offers a way to resist quantum computers when passwords (PSKs) are used. The extension works by "mixing" the standard IKEv2 password key (PSK) with another key in the form of a Post-quantum Preshared Key (PPK) to increase resistance.

Existing IKEv2 PSK tunnels can easily be supplemented with PPKs. The PPK is independent of the existing PSK.

LCOS supports manual configuration of PPKs. Automatic procedures for changing PPKs are not supported.



PPK-ID

Set a unique name for this entry. The input format can be a string or hexadecimal number (identified by a leading 0x).

PPK

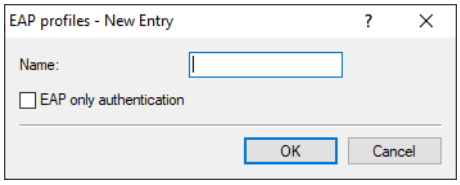
Enter the post-quantum preshared key here as a character string or hexadecimal number (identified by a leading 0x).

Required

If the use of PPKs is configured as required, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

EAP profiles

This table is used to configure EAP profiles. You select this during **authentication** if you set the **remote authentication** method to EAP.



Name

Give this EAP profile a name that can be used to reference it.

EAP-only authentication

Optionally allows mutual authentication of remote sites within the EAP. Authentication outside the EAP is then not required. See also *RFC 5998*

Password rules

Enforce preshared key rules

This entry gives you the option to disable or enable password-rule enforcement. The following rules apply to the preshared keys (PSK) for IKEv2:

- The length of the password must be at least 32 characters.
- The password must contain at least 3 of the 4 character classes, i.e. lowercase letters, uppercase letters, numbers, and special characters.

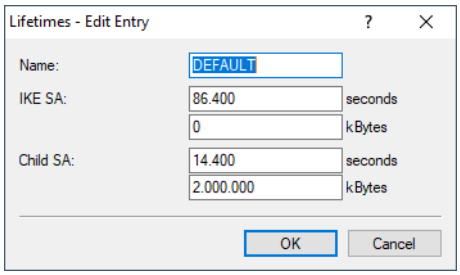
These rules do not apply to PSKs managed and sourced from a RADIUS server.

Lifetimes

Use this table to specify the IKEv2 rekeying parameters. An entry named "DEFAULT" is provided with common settings.

Depending on the phase, the device discriminates according to time or the amount of transmitting data. The parameter that reaches its limit first triggers the renewal of the corresponding IKEv2 key.

The value "0" means that the device sets no limit on the corresponding key.



Name

Contains the unique name of this entry.

IKE SA

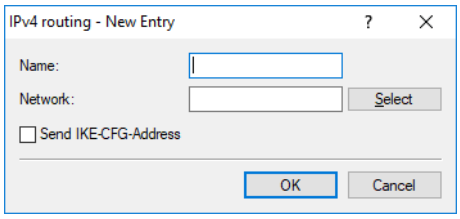
Contains the time in seconds and/or the data volume in kilobytes until the IKE SA key is renewed.

Child SA

Contains the time in seconds and/or the data volume in kilobytes until the CHILD SA key is renewed.

IPv4 routing

Use this table to configure the IPv4 networks that the device propagates via dynamic routing as per IKEv2.



Name

Contains the unique name of this entry.

Network

Contains the comma-separated list of IP subnets.

Networks are entered in the following available formats:

- IP address
- IP address/netmask
- IP address/netmask@tag
- IP address/prefix length
- IP address/prefix length@tag
- IP interface name
- IP interface name@tag

The specification with routing tag is used for HSVPN. See also HSVPN in section *Connection list* on page 860.

The IP subnets are configured under **IPv4** > **General** in the section **Own addresses**.

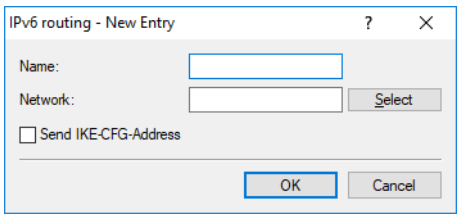
Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

IPv6 routing

Use this table to configure the IPv6 networks that the device propagates via dynamic routing as per IKEv2.



Name

Contains the unique name of this entry.

Network

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 address/prefix length@tag
- IPv6 interface name
- IPv6 interface name@tag

The specification with routing tag is used for HSVPN. See also HSVPN in section *Connection list* on page 860.

The IP subnets are configured under **IPv6** > **General** in the section **IPv6 networks**.

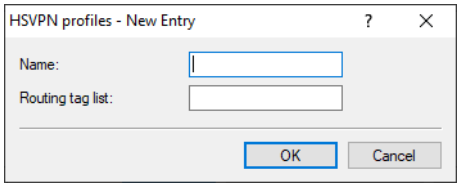
Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

HSVPN profiles

This table is used to configure the HSVPN profiles. In LANconfig, navigate through the configuration to **VPN** > **IKEv2/IPSec** > **Extended settings** and, in the section**HSVPN**, configure the **HSVPN profiles**.



Name

Here you set a name for the HSVPN profile.

Routing tag list

Here you define the routing tags as a comma separated list (e.g. 1,2,3) that are to be transmitted via HSVPN. The Rtg-Tag list must be identical on both VPN partners in order for all of the desired ARF networks to be transported.

RADIUS authentication

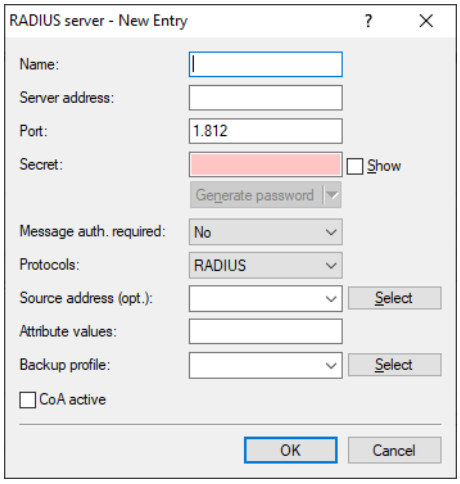
In the **RADIUS authentication** section you configure the settings for the RADIUS server used for VPN client authentication.

In the **Password** field you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the LANCOM gateway after this receives the corresponding authorization in the `access-accept` message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.



Name

Specify an identifier for this entry.

Server address

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Port

Specify the UDP port of the RADIUS server. The value "1812" is preset as the default value.

Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Source address (optional)

Enter the loopback address of the device, where applicable.

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the following form:

```
<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>
```

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

CoA active

Here you enable/disable **CoA**.

The disconnect message is supported as a CoA message in order to disconnect a connected VPN user or a VPN peer. The CoA-disconnect message must include the username as a RADIUS attribute “User-Name” as well as the attribute “NAS-IP-Address”. Activating the function also requires *Dynamic Authorization* to be activated globally, and access for CoA clients must be configured.

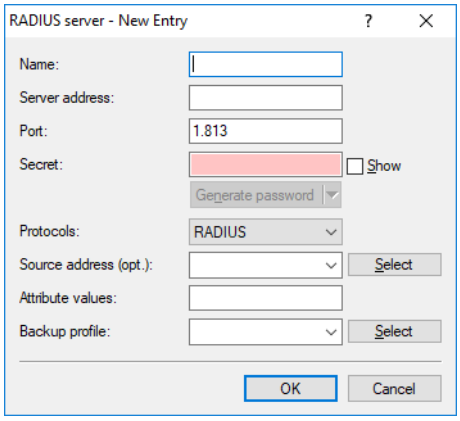
The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPsec** > **Connection list** in the **RADIUS auth. server** field.

RADIUS accounting

In the **RADIUS accounting** section you configure the settings for the RADIUS server used for VPN client accounting.

The **Update cycle** field is used to set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of ±10% to keep the update messages of parallel accounting sessions separate from one another.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.



Name

Specify an identifier for this entry.

Server address

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Port

Specify the UDP port of the RADIUS server. The value "1813" is preset as the default value.

Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Source address (optional)

Enter the loopback address of the device, where applicable.

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the following form:

`<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPSec** > **Connection list** in the **RADIUS acc. server** field.

IKEv2 fragmentation

The fragmentation of data packets is controlled by the maximum transmission unit (MTU). The MTU is the maximum size that a packet may have in order to be sent as payload over a channel. The two communication partners negotiate this during connection establishment in order to optimize data transmission by avoiding any additional fragmentation of the data packets.

In LCOS, IKEv2 fragmentation is enabled automatically. You can manually specify a maximum MTU if you wish.

To do this in LANconfig, go to **VPN** > **IKEv2/IPSec** > **Extended settings**.



Enter the maximum IP packet length/size in bytes into the **MTU** field in the **Fragmentation** section. Smaller values lead to greater fragmentation of the payload data.

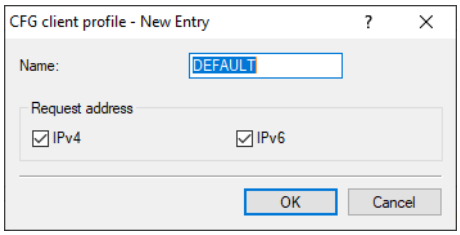
IKEv2 fragmentation as per RFC 7383 enables the VPN router to fragment IKEv2 messages by itself, which is more efficient than having IKE-packet fragmentation performed by the transport network. Two methods of IKEv2 fragmentation are supported:

- Manufacturer-specific fragmentation, compatible with third-party manufacturers
- Fragmentation as per RFC 7383

The device sets the best method automatically. If a VPN remote site supports both methods, fragmentation as per RFC 7383 is preferred.

CFG client profile

In LANconfig, navigate through the configuration to **VPN** > **IKEv2/IPSec** > **Extended settings** and, in the section **Additional parameters**, configure the **CFG client profile**. This profiles can be selected under *Connection list* on page 860 so as to specify whether the device in the role CFG-Mode client should request an address from the CFG-Mode server.



Name

Unique name for the CFG client profile.

Request address

Specify whether addresses for IPv4 and / or IPv6 should be requested for this profile.

IKEv2 tunnel groups

Some VPN scenarios require that a given group of VPN tunnels of a device terminates on, or establishes to, a common VPN gateway. This is necessary, for example, where VPN tunnels are configured on a cluster of load balancers and VPN tunnels use the alternative gateway list and maybe even different paths or outbound Internet connections (DSL, LTE, Ethernet) to reach the destination.

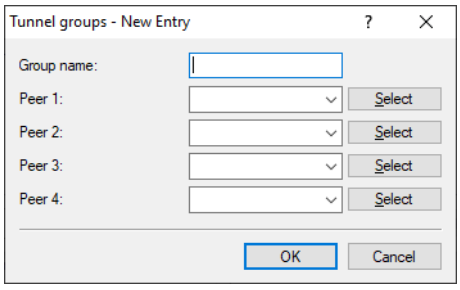
A VPN load balancer requires that the various VPN tunnels always terminate on a common VPN gateway.

IKEv2 tunnel groups is a feature that ensures that all VPN tunnels in a group always terminate on a common VPN gateway. The first VPN tunnel to be established in a group determines the common VPN gateway, and the VPN remote gateways for all of the other members of the tunnel group are transferred to this destination. Usually, this is the VPN tunnel that is established the fastest. The selection of a gateway is only performed again if all tunnel group members are unable to reach the gateway.

The function of the IKEv2 tunnel groups can basically be used independently of a load balancer.

Tunnel groups are not supported in conjunction with IKEv2 Redirect and the IKEv2 Redirect Load Balancer.

In LANconfig, navigate through the configuration to **VPN** > **IKEv2/IPSec** > **Extended settings** and, in the section **Additional parameters**, configure the **Tunnel groups**.



Group name

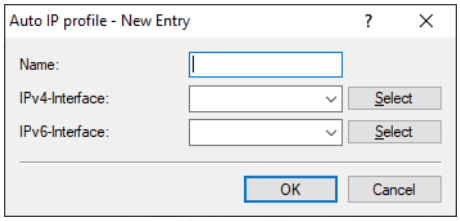
Unique name for the tunnel group.

Peer 1-4

The name of each remote site of the IKEv2 VPN tunnel terminating in the tunnel group.

IKEv2-Auto-IP-Profile

In LANconfig, this is configured under **VPN** > **IKEv2/IPSec** > **Extended settings** in the section **Additional parameters** under **Auto IP profile**.



Name

Unique name of the Auto-IP profile. This is referenced under *Auto-IP* on page 863.

IPv4-Interface

IPv4 network used to send the IPv4 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv4 networks

IPv6-Interface

IPv6 network used to send the IPv6 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv6-LAN-Interfaces

11.19.1.10 LANCOM Advanced Mesh VPN (AMVPN)

Classic VPN scenarios in site connectivity are usually star-shaped (hub & spoke). The connected branches (spokes) set up VPN tunnels to one or more hubs. In such traditional scenarios, a hub & spoke network design is a logical topology

decision, because data flows mainly between the branch and the headquarters, since central servers are located there, such as the ERP system, databases or web servers.

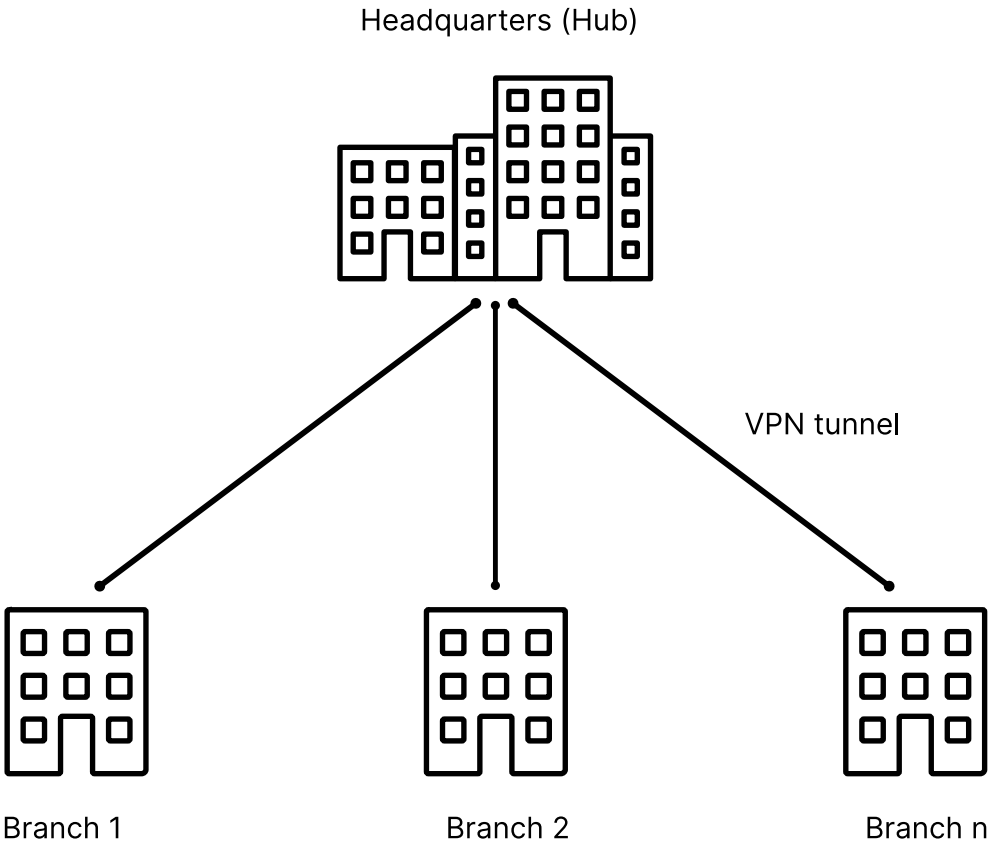


Figure 7: Classic site networking (hub & spoke)

The advantages of this star-shaped network design are the simple structure and the central control in the headquarters. The disadvantage, however, is that all data traffic—including that between individual branches, such as telephony or file exchange via a file server—always takes place indirectly via the headquarters'. As a result, the headquarters Internet

connection is burdened with data traffic between the branches and thus becomes the bottleneck of the entire communication.

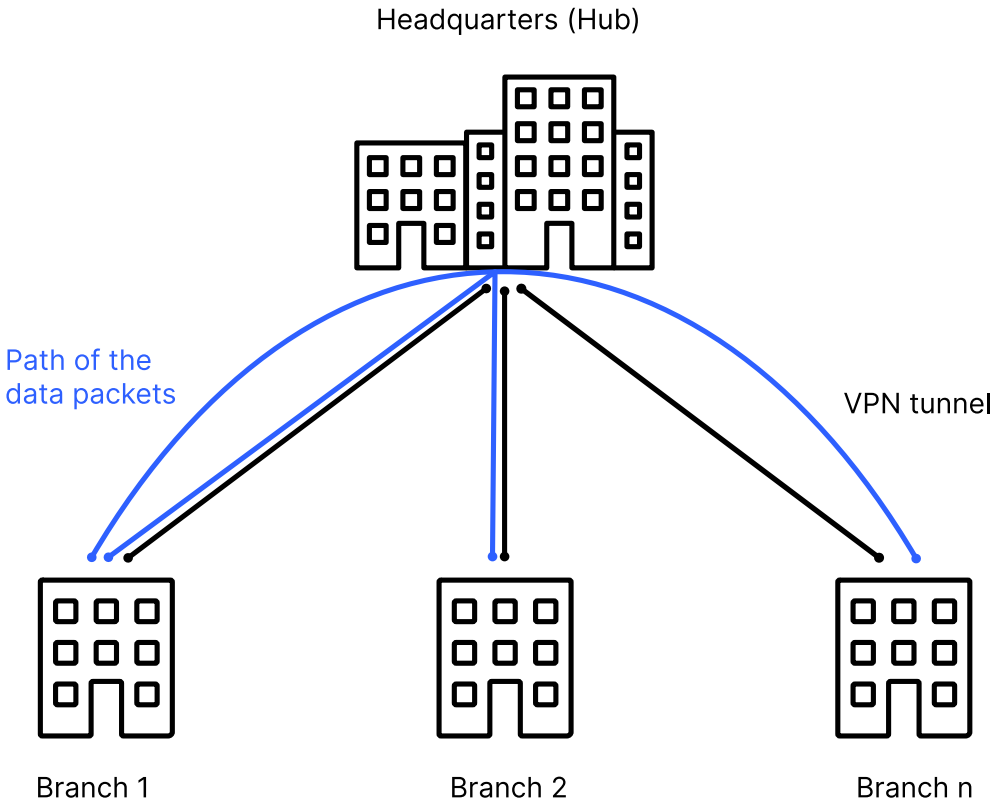


Figure 8: Data exchange between branches with classic site networking (hub & spoke)

If inter-branch traffic is the largest portion of the traffic relationship, a practical approach is to manually configure direct VPN tunnels between branches. This case is referred to as a VPN mesh scenario. In simple scenarios, the manual approach works well. However, if there are many branches and many possible VPN tunnels, this rigid, individual, and fixed configuration approach no longer scales.

LANCOM offers the "Advanced Mesh VPN" as a solution in this scenario. The starting point is a classic star-shaped VPN structure, where each of the branches connects to the headquarters via VPN tunnel. In the event of data traffic between two branches, a VPN tunnel is dynamically established directly between them. The data now flows directly through a VPN tunnel between the branches without the data going via the headquarters.

The initial data packets have to take the long route from branch A via the headquarters to the second branch B. Only when the first data packets are received at the target branch does the target branch initiate a dynamic VPN tunnel to the branch that was the origin of the initial data packet. If no data flows for a time, the tunnel is dynamically terminated again.

The advantage: Significantly less traffic in the headquarters and, as a result, higher performance throughout the entire corporate network.

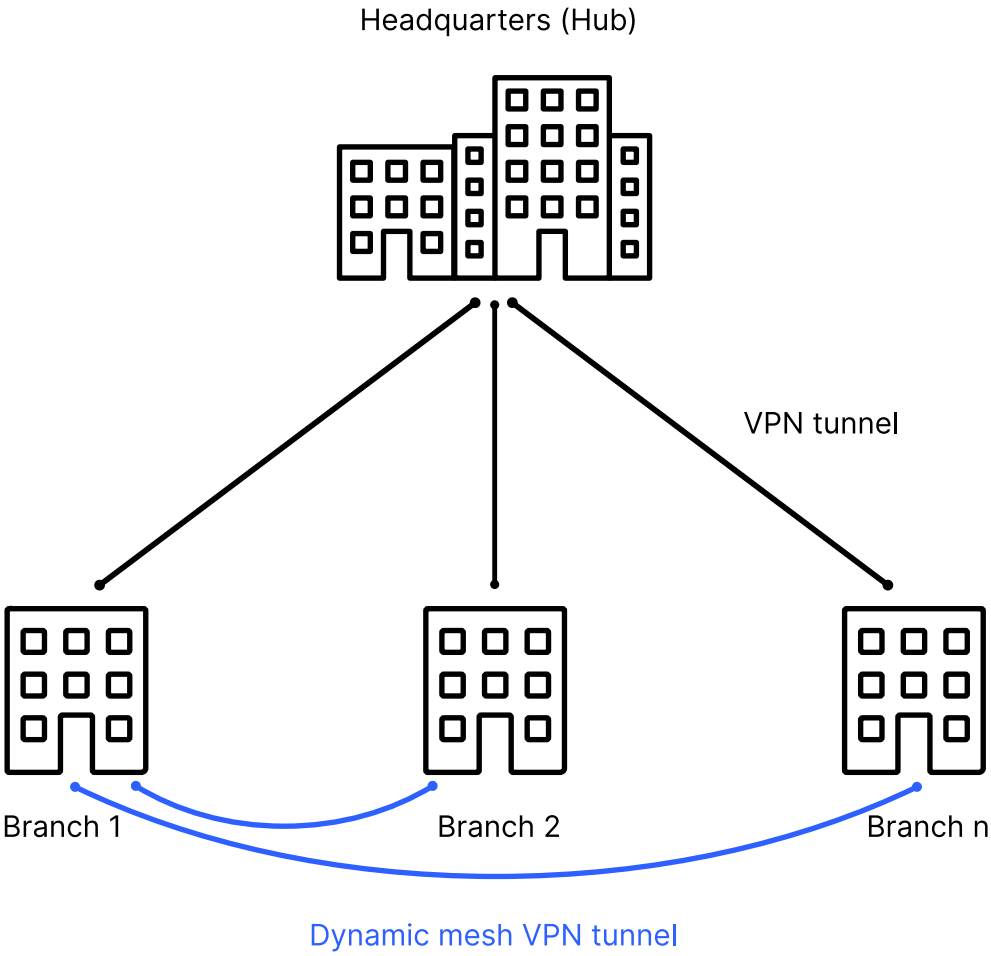


Figure 9: Site networking via Advanced Mesh VPN

The following basic steps are necessary to configure Advanced Mesh VPN:

1. Configuring the VPN tunnel between the branch office and headquarters.
2. Creating a Mesh VPN tunnel template in the IKEv2 peer table that contains the shared VPN properties such as encryption method, PSK, or certificate for the dynamic Mesh VPN tunnel.
3. Activation of the Mesh VPN feature and configuration of the global mesh parameters on all relevant VPN routers.

How is the dynamic setup of a Mesh VPN done?

1. Branch A sends data packets over the existing static VPN tunnel via the main office to branch B.
2. The router at branch B detects a new session because data packets from an unknown subnet arrive via the VPN tunnel from the headquarters.
3. Branch B sends an encrypted manufacturer-specific IKEv2 message to the headquarters. The message contains the private subnets or IP addresses of the desired communication relationship and the public IP address of branch office B.
4. The headquarters receives the vendor specific IKEv2 message in the VPN tunnel from branch B and forwards it to branch A via the VPN tunnel to branch A.
5. Branch A receives the headquarters' vendor specific IKEv2 message.
6. Branch A creates a dynamic Mesh VPN tunnel and establishes it directly to the IP address of branch B. The router takes the necessary information from the vendor specific IKEv2 message (gateway IP address, subnet, etc.).

7. Branch B accepts the tunnel setup by branch A and updates its local routing table to include the subnet at branch A with the destination gateway that is the public IP address at branch A. The private subnet of branch A is used by IKEv2 routing as an IKEv2 message during VPN tunnel establishment and is more specific than the route to the headquarters.
8. Data now flows directly between branches A and B, since the routes at both ends now point to the dynamic VPN tunnel.
9. If no further data is transmitted after the timeout, the Mesh VPN tunnel is terminated.

- The first data packets initially flow via the tunnel to the main office and then trigger the establishment of a dynamic tunnel.
- A ping to the LAN IP address of the router at the peer does not trigger the establishment of a Mesh VPN tunnel. Only data packets to endpoints in the LAN will trigger tunnel establishment, as only these can be correctly identified by the router-firewall. However, a ping to a (possibly non-existent) IP address in the LAN does however trigger the establishment of a VPN mesh tunnel.
- Ongoing firewall sessions relating to the data packets first sent via the headquarters are moved to the newly established mesh tunnel after the Mesh VPN tunnel was set up successfully (session switchover).
- The branch that is to accept a dynamic Mesh VPN tunnel must have a public IP address (IPv4 or IPv6) and be reachable from the outside. Routers with a cellular connection usually do not have a public IP address.
- LANCOM Advanced Mesh VPN is a vendor-specific implementation based on IKEv2 and only works between LCOS-based LANCOM VPN routers. The LANCOM Advanced VPN Client does not support this.
- The security is based entirely on IKEv2/IPsec and can handle all settings such as PSK, certificates, encryption algorithms, or LANCOM HSVPN from IKEv2.
- All routers involved (branch office, main office) require LCOS 10.70 or higher.

Traces on LANCOM Advanced Mesh VPN have been facilitated by the parameter `VPN-Mesh`. See also *Trace information* on page 305.

Licensing

Mesh VPN tunnels are counted separate from and in addition to normal VPN tunnels. If the licenses for Mesh VPN tunnels are exhausted, no mesh tunnel is set up and the data continues to travel the longer route via the main office. Central-site devices are limited to a maximum of 200 mesh tunnels, whatever their configuration.

The following Mesh VPN licenses apply (depending on the number of normal VPN tunnels):

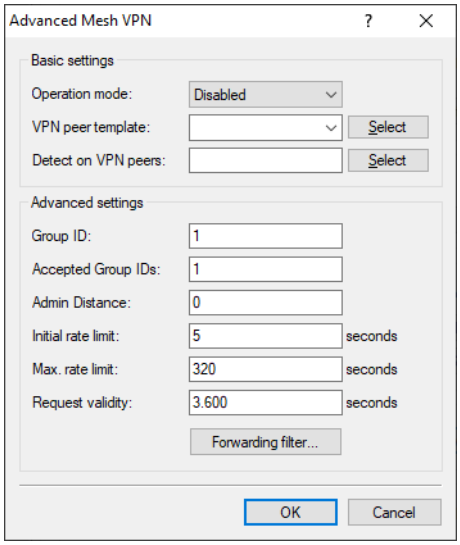
Table 28: Mesh VPN tunnel licenses

Category	Devices	Number of licenses	
		VPN tunnel	Mesh VPN tunnel
CPE	R88x, 88x VoIP, 1640E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx with VPN 25	25	50
CPE	19xx	25	50
CPE	19xx with VPN 50	50	100
CPE	19xx with VPN 100	100	200
Central-site	ISG-1000	100	200
Central-site	ISG-4000	200	200
Central-site	ISG-5000	100	200
Central-site	ISG-8000	250	200

Configuring Advanced Mesh VPN

Now configure the Advanced Mesh VPN in LANconfig under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Advanced Mesh VPN**.





Operation-Mode

This control affects the way the Mesh VPNs works and enables behavior as a spoke or hub, or even both roles at the same time. Possible values:

Deactivated

The Mesh VPN feature is disabled, Mesh VPN messages are not sent, forwarded, or processed. Mesh VPN tunnels are neither established nor accepted.

Hub

The device assumes the role of the central-site VPN gateway. Mesh VPN messages are forwarded between the tunnels. The device itself does not establish or accept any Mesh VPN tunnels.

Spoke

The device assumes the function of a branch office and establishes and accepts Mesh VPN tunnels.

Hub&Spoke

The device takes on the role of the central-site VPN gateway, and also establishes Mesh VPN tunnels to other spokes and accepts Mesh VPN tunnels.

VPN peer template

This parameter refers to an entry in the IKEv2 peer table. This entry is used as a configuration template for the Mesh VPN tunnels.

Detect on VPN peers

A comma-separated list of VPN peers that the (firewall) detector should react to. This entry is required for branches to detect incoming sessions. This can be left empty, e.g. for branches behind a NAT (without port forwarding) and therefore unable to act as responders for a mesh tunnel.

Group-ID

Each device can be assigned to a group that is used to send its requests. One option of this is to divide the mesh into smaller groups, e.g. regional mesh structures.

Accepted group IDs

A comma-separated list specifying the mesh group IDs that are accepted. A request from a group ID not listed here will be discarded.

Admin distance

The distance set in the IP router for routes received via the mesh tunnel. The special value "0" is equivalent to the internal default of "15".

Initial rate limit

Requested networks (addresses) are temporarily blocked in order to protect the network. The initial lockout period is specified here in seconds.

Max. rate limit

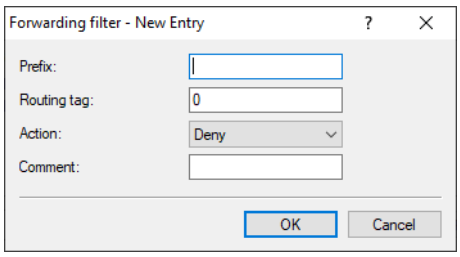
The lockout period from the **Initial rate limit** is doubled each time until the **Maximum rate limit** is reached.

Request validity

After the lockout period has expired, networks (addresses) that were previously requested will still be available. This validity always begins when the blocking expires and ends when the device sends or receives a request for this network (this address).

Forwarding filter

This filter list can be used to filter requests to specific networks on the hub. If the network request in a Mesh message does not match any row in the table, the request is allowed through (allow-all).



Prefix

Defines the prefix for which a rule should apply, e.g. 10.0.0.0/24 or 2001:db8::/32.

Day

Defines the routing tag or routing context associated with the filter rule.

Action

Defines the action for this filter entry. Possible values: Allow, Deny.

Comment

Enter a descriptive comment here.

Tutorial: Setting up Advanced Mesh VPN

Initial situation: The scenario consists of two branches (A and B) with public IPv4 addresses and a main office, also with a public IPv4 address. The two branches have already set up a static IKEv2 VPN tunnel to the main office, and this

is running. The VPN peer at the branches is called “MAIN”. Branch A has the subnet 192.168.1.0/24 and branch B has the subnet 192.168.2.0/24 with the name “INTRANET”.

Configuration at branch A

1. Create a new entry, e.g. “MESH-TEMPLATE”, in the IKEv2 connection list under **VPN** > **IKEv2/IPSec** > **Connection list**.

   This entry serves as a template used by the dynamic mesh tunnels take to read their parameters.

2. The **Short hold time** is the time of data inactivity after which Mesh VPN tunnels disconnect, e.g. 300 seconds.

   Deactivating the short hold time by setting it to the value 0 is not recommended, otherwise dynamic Mesh VPN tunnels will never terminate after inactivity, and this will consume licenses.

3. Leave the remote **Gateway** blank as it is set dynamically.
4. The **Routing** parameter transmits the local network to the opposite branch, in this case the “INTRANET” network. To do this, create a new entry in the **IPv4 routing** table under **VPN** > **IKEv2 / IPSec** > **Extended settings**. For example, select “INTRANET-ROUTING” as the name and, in the **Network** field, select the local network to be used for Mesh VPN, e.g. “INTRANET”.

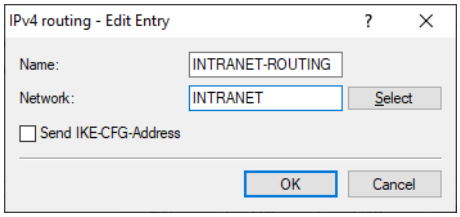


Figure 10: Example of the IPv4 routing entry

5. Under **Authentication**, set the option **Manage source**. Create a new entry, e.g. “MESH”. Enter the **Local identifier** of the branch and the **PSK** used for all dynamic mesh tunnels. The PSK must be identical on all branches involved in the mesh VPN tunnel. This is then entered in the **Remote password** field. Leave the field **Remote identifier**

blank and select the option "No identity" for **Remote identifier type**, so that all incoming identities with the correct PSK are accepted as mesh tunnels.

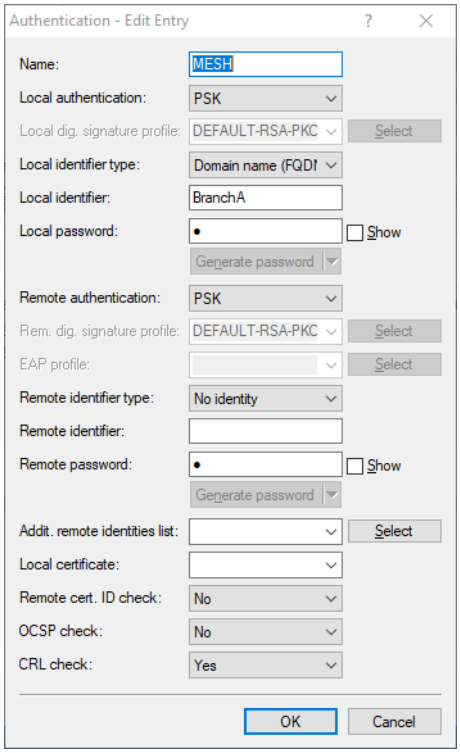


Figure 11: Example authentication settings

6. Set the **VPN rule** to "ANY" or select "RAS-WITH-NETWORK-SELECTION" for **IPv4 rules**. Thus uses 0.0.0.0/0 <=> 0.0.0.0/0.
7. Set **Rule creation** to "Manual".

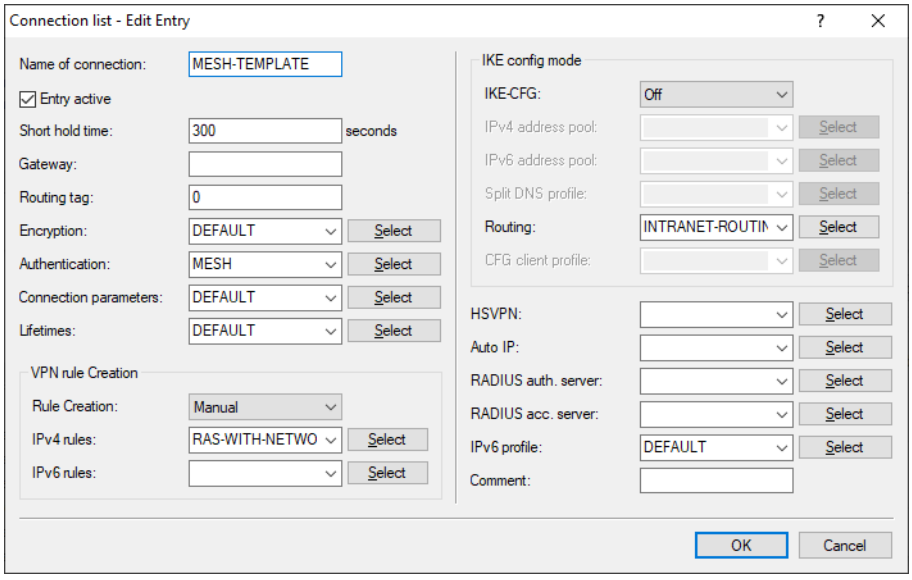


Figure 12: Example of the Mesh VPN template in the connection list

8. Now configure the Mesh VPN parameters under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Advanced Mesh VPN**.

9. Set **Operation mode** to "Spoke".
10. Under **VPN peer template** select the previously created IKEv2 peer as a template for the Mesh VPN tunnel.
11. Under **Detect on VPN peers**, select the name of the VPN peer that corresponds to the name of the tunnel to the main office.

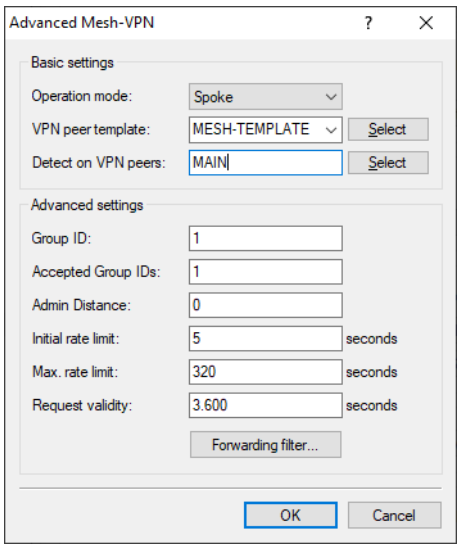


Figure 13: Example of Advanced Mesh VPN settings in the branch office

Configuration at branch B

12. The configuration is performed similar to branch A. Change the **Local identifier** for the **Authentication** to the name of branch B.

Configuring the main office

13. Since the main office itself does not set up a dynamic mesh tunnel, there is no need to create a template for the peer. Set the **Operation mode** for the Advanced Mesh VPN to "Hub".

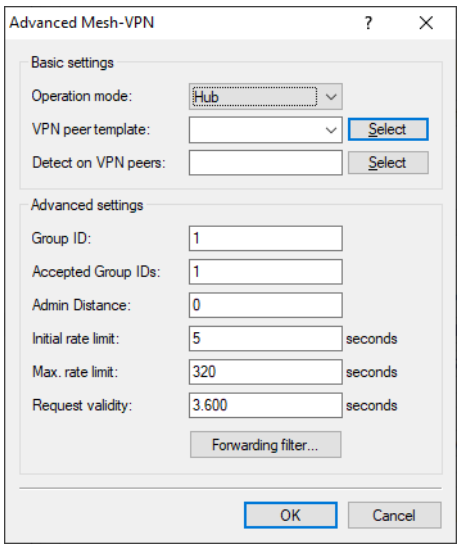


Figure 14: Example of Advanced Mesh VPN settings in the main office

If you now transfer data from branch A to branch B, the first packets take the detour via the main office. After that, the dynamic mesh tunnel is set up between the branches.

A ping to the router's IP address at the other end will not establish a mesh tunnel. A (possibly non-existent) station in the LAN at the other end must be used as the destination.

11.19.1.11 IKEv2 load balancer

The IKEv2 load balancer allows the distribution of incoming IKEv2 connections to other gateways depending on the current load or number of VPN tunnels. The IKEv2 redirect mechanism is used to achieve this.

Larger-scale VPN scenarios generally operate with redundant VPN gateways. Often, the gateways are are not used evenly, and some gateways are reserved for backup events. The result is a non-uniform resource load across the installation.

With multiple VPN gateways in operation, all of them need to be configured on all of the clients. Particularly when a new VPN gateway is installed, it has to be subsequently configured on all of the clients. With the redirect mechanism (RFC 5685), IKEv2 offers an enhancement that enables a VPN gateway to redirect a client to another gateway.

The IKEv2 redirect mechanism in combination with VRRP provides a highly available IKEv2 load balancer that is suitable for enterprise scenarios.

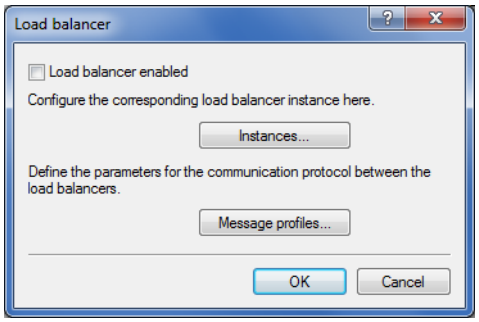
In the first step, a VRRP group is activated on all participating VPN gateways. The virtual VRRP IP address is at the same time the master IP address of the IKEv2 load balancer cluster. The VPN gateways now exchange information about their load and their availability by means of regular status messages via multicast. If the master goes down, another VPN gateway is automatically set as the master.

The only information the clients need is the master IP address. If a client establishes a VPN connection to this IP address, the master gateway checks the load of the VPN gateways and redirects the client to the gateway with the least load. The master gateway sends a redirect either in the IKE_SA_INIT response or in the IKE Auth phase. The redirect depends on the availability of free VPN tunnels of the participating gateways. The VPN client is directed to the VPN gateway with the lowest number of active tunnels.

The virtual gateway address is only used for the initial contact before the subsequent redirect. The client then establishes the actual VPN tunnel to a different gateway address.

The following limiting conditions must be observed:

- VRRP is required for the automatic selection of the master gateway.
- The VPN gateways involved must have a common layer-2 connection for the VRRP and the exchange of status messages via multicast.
- VRRP is currently supported on LAN interfaces only.
- An upstream router (redundant, if necessary) is required for WAN access.
- The client must support IKEv2 gateway redirect as per RFC 5685 (currently applies to LANCOM routers and the LANCOM Advanced VPN Client on Windows).

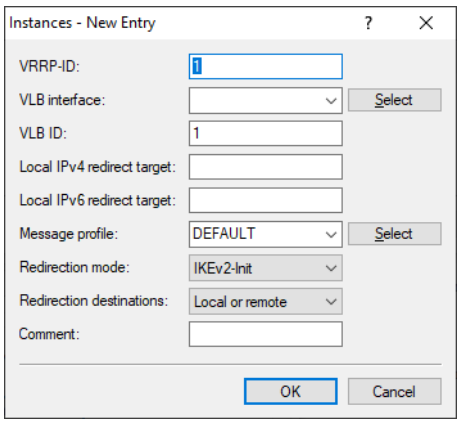


Load balancer enabled

activates the IKEv2 load balancer.

Instances

Configure IKEv2 load balancer instances in the **Instances** table.



VRRP-ID

VRRP-ID (Router ID) to be used for this IKEv2 load balancer instance. VRRP must be enabled and configured for this VRRP-ID on this device.

Possible values:

0 to 255

Default: 1

VLB Interface

Defines the interface or logical network on which the IKEv2 load balancer should accept VPN tunnels. VRRP must also be configured and active on this interface.

VLB ID

Defines the unique identifier of the load balancer instance. Default: 1

Local IPv4 redirect target

IPv4 address or FQDN where the device should accept VPN tunnels. A VPN client will be redirected to this address by the master in the load balancer group.

This is not the virtual VRRP IP address.

Local IPv6 redirect target

Global IPv6 address or FQDN where the device should accept VPN tunnels. A VPN client will be redirected to this address by the master in the load balancer group. Link-local addresses are not supported.

This is not the virtual VRRP IP address.

Message profile

Message profile used for this instance. The message profile includes the parameters for the status protocol, which the device uses to communicate its status information to the load balancer group.

Default: DEFAULT.

If an IPv6 address is configured here, the IPv6 firewall rule ALLOW_VLB must also be enabled.

Redirection mode

Defines the phase during the IKEv2 negotiation in which the VPN gateway redirects clients to another gateway.

This parameter is only effective if the device is the VRRP master.

Possible values:

IKEv2-Init (Default)

The redirect message is sent within the IKE_SA_INIT response of the VPN gateway.

IKEv2-Auth

The redirect message is sent during the IKE_AUTH phase after the client has authenticated with the VPN gateway.

Redirection destinations

Defines the redirection target to which VPN clients are forwarded.

This parameter is only effective if the device is the VRRP master.

Possible values:

Local or remote

Clients are redirected to both the device's own IP address and other remote gateways in the group.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed among all other gateways except the master gateway.

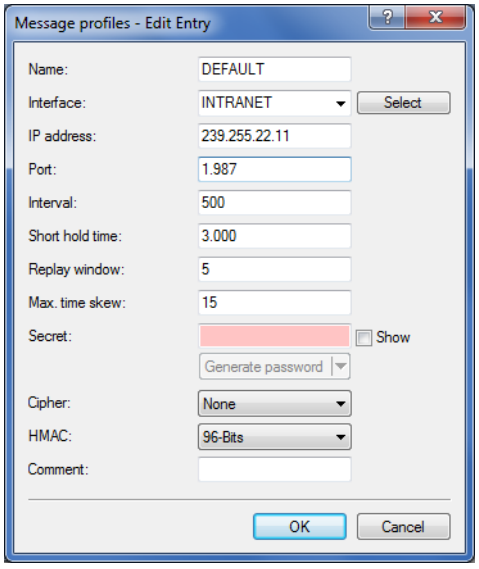
This configuration is suitable for scenarios where the load balancer master only distributes clients but does not terminate VPN tunnels itself.

Comment

Provide a meaningful description for this entry.

Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.



Name

Unique name for this profile

Interface

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

Possible values:

Entries from the IPv4 networks table

IP address

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

Default: 239.255.22.11

Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

Default: 1987

Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

Possible values:

0 to 65535

Default: 500

Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.

The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

Possible values:

0 to 65535

Default: 3000

Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

Possible values:

1 to 9

Default: 5

0

Disables the replay detection.

Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

Possible values:

0 to 255

Default: 15

Secret

Shared secret for the load balancer communication log.



The secret must be the same on all of the VPN gateways in a cluster.

Possible values:

Up to 32 random characters

Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None (default)

AES-128-GCM

AES-192-GCM

AES-256-GCM

HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None

96 bits (default)

128 bits

Comment

Enter a descriptive comment for this entry.

11.19.2 Two-factor authentication in the VPN

As of LCOS 10.70, LCOS supports VPN two-factor authentication (EAP-OTP) with the LANCOM Advanced VPN Client. For this purpose, the internal RADIUS server can manage OTP users.

In addition to his normal VPN user name and password (EAP-MSCHAPv2), the VPN user has an authenticator app, e.g., on his smartphone, on which a second factor is generated and used in addition to the user name / password. Two-factor authentication is only possible with EAP in IKEv2 according to the RFC, so simple PSK or RSA signature methods cannot be used. LCOS supports a vendor-specific implementation together with the LANCOM Advanced VPN Client.

Any apps can be used as authenticators, e.g. from Google, Microsoft or NCP. You can find these apps in the app store of your mobile device.

The setup procedure is as follows: First, EAP-VPN with IKEv2 must be configured in the LANCOM device. The internal RADIUS server with its user accounts is used for this purpose. In addition to a RADIUS user account, an OTP user must be created. Subsequently, a QR code can be retrieved in WEBConfig under **Extras** > **EAP-OTP users** , which must be scanned by the Authenticator app. This QR code applies per user and must be used each time an Authenticator app is

to be set up. WEBconfig generates a QR code per user from the parameters of the **OTP user accounts** table that can be scanned by Authenticator apps. Alternatively, the key can be added manually in most apps.

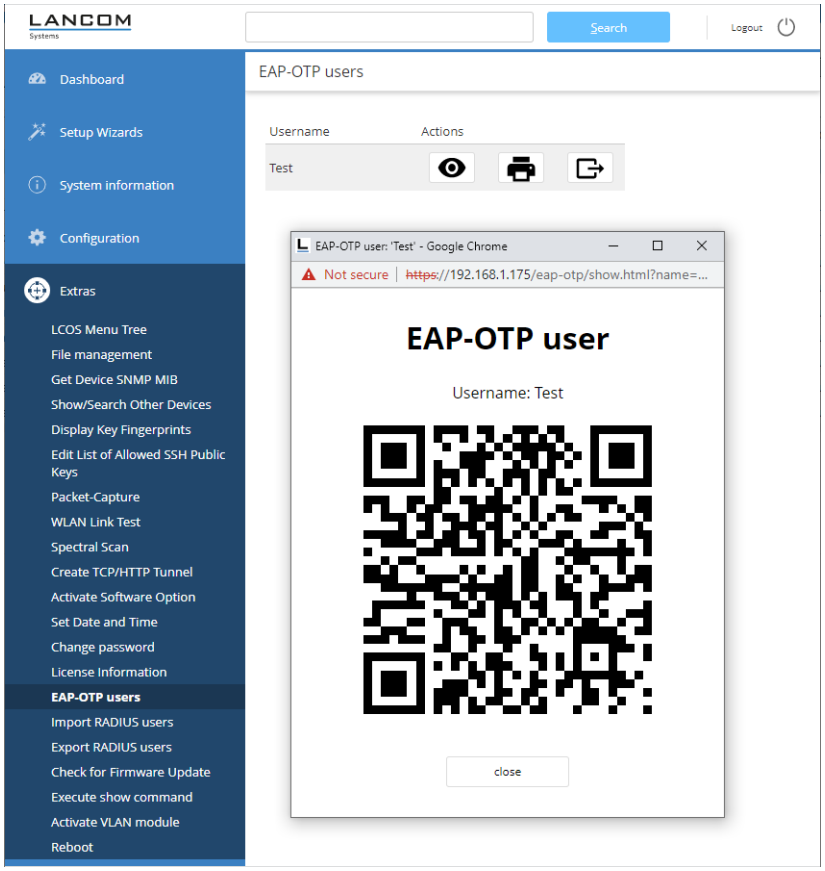


Figure 15: WEBconfig: Extras > EAP-OTP users

Instructions for setting up the entire scenario can be found in the *LANCOM Support Knowledge Base*.

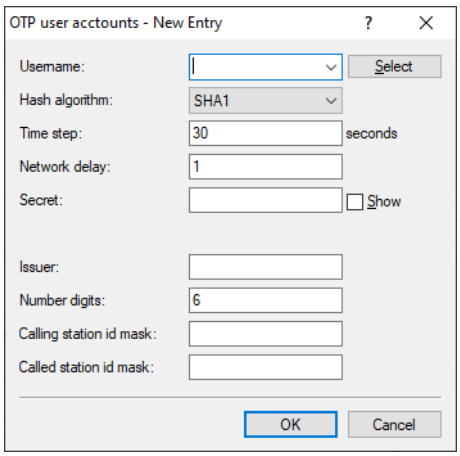
Please note that for correct time synchronization with the Authenticator, the router must have the current time. To do this, enable the NTP client in the router under **Date & Time** > **Synchronization** > **NTP client settings**.

11.19.2.1 Configuration with LANconfig

OTP user accounts

The OTP users are defined in the OTP user accounts table. For EAP-OTP, the user must be created with his normal password in the table of *RADIUS user accounts*, as well as additionally created in this table with the OTP secret.

The configuration of the OTP user accounts is done via **RADIUS** > **Server** > **User database** > **OTP user accounts**.



Username

Enter the name of the OTP user here. This must already be contained in the RADIUS user accounts table with the same name.

Hash algorithm

Defines the hash algorithm used.

Note that the Authenticator app supports the maximum possible hash algorithm. For example, Google Authenticator currently supports only SHA1 on certain Android platforms.

Time step

Defines the interval in seconds after which a new OTP is calculated. Default: 30 seconds

Network delay

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Secret

Defines the actual shared secret that must be shared with the Authenticator app. The secret must be different for each user. There are currently three possible entries in the table:

Base32 (Default)

Prefix "base32:" followed by the base32 encoded secret. The prefix "base32:" may also be omitted.

Hexadezimal

Prefix "hex:" followed by an even number of hex digits.

Plain text passphrase

Prefix "ascii:" and then the characters.

For Google Authenticator, the secret must be 16 characters long (80 bit, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G

Issuer

Freely definable text used in Authenticator to keep multiple keys apart when the same username is used. Must not contain a colon.

Number digits

Length of OTPs. Default: 6.

For Google Authenticator, the value 6 should be used.

Calling station id mask

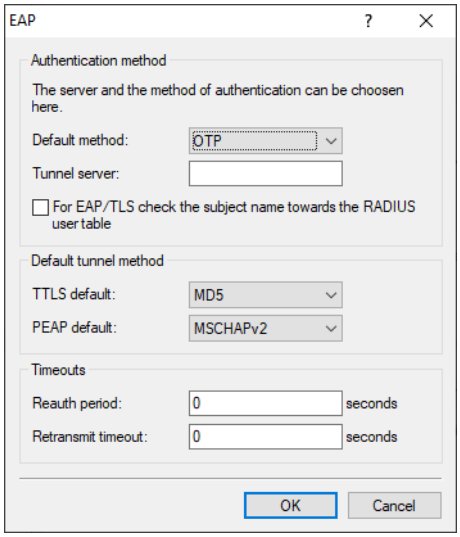
This mask restricts the validity of the entry to certain IDs transmitted by the calling station.

Called station id mask

This mask restricts the validity of the entry to certain IDs transmitted by the called station.

EAP-OTP

RADIUS > **Server** > **Extended configuration** > **EAP**



The **Default method** has been extended by the value OTP.

OTP

One Time Password. This value must be used with EAP-OTP for *two-factor authentication in the VPN*, because with the LANCOM Advanced VPN Client the EAP method is specified by the EAP server.

11.19.3 RADIUS support for IKEv2

LCOS enables the IKEv2 for authorization and accounting of VPN peers to be configured by an external RADIUS server. Also, the management of the VPN clients for dynamic IKEv2 load balancing is implemented via RADIUS.

In medium- to large-scale VPN scenarios, the tables for VPN configurations are generally rather large and complex. If multiple VPN gateways are operated for redundancy, it is important to ensure that the configuration is identical on all VPN gateways.

Operating a central RADIUS server allows the configuration of the VPN parameters on the VPN gateways to be almost completely outsourced to one or more RADIUS servers. When a device receives an incoming connection from a VPN peer, the device attempts to authenticate the incoming connection via RADIUS and to retrieve other necessary connection parameters, such as VPN network relationships, CFG-mode address or DNS server, from the RADIUS server. In this case, the user is not authenticated by the RADIUS server using the user name/password; instead, it sends the correct password for the requested user to the VPN gateway, which then authenticates the user. The VPN gateway then sets up the tunnel, and the RADIUS server can supply further attributes to the VPN tunnel.

The VPN configuration may be either completely or only partially retrieved from the RADIUS server, in which case it is combined with parameters stored locally. This mechanism works for incoming connections only.

Optional RADIUS accounting allows information about VPN connections to be stored centrally on a RADIUS server. This information may consist of the duration of the connection to the client, the time when the connection is established, or the transmitted data volume.

The RADIUS server is configured in LANconfig under **VPN** > **IKEv2/IPsec** > **Extended settings**.

RADIUS authentication

When authenticating a VPN peer, the LANCOM gateway transmits the following RADIUS attributes to the RADIUS server in the `Access-Request`:

ID	Name	Meaning
1	User name	The remote ID of the VPN peers sent in the `AUTH` negotiation with the LANCOM gateway.
2	User password	The dummy password is configured in LANconfig under **VPN** > **IKEv2/IPsec** > **Extended settings** > **Password**.
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute “95” instead (see below).
6	Service type	The service type is always “Outbound (5)” or “Dialout-Framed-User”.
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv4 connection, the gateway transmits the attribute “4” instead (see above).

Of the attributes contained in the `Access-Accept` response from the RADIUS server, the LANCOM gateway evaluates the following, in part vendor-specific attributes:

ID	Name	Meaning
8	Framed-IP-Address	IPv4 address for the client (in IKE CFG-mode “Server”).
9	Framed IP netmask	Specifies the IP netmask to be configured for the client (in IKE-CFG mode “Server”). This attribute value causes a static route to be added for the framed IP address with the specified mask.
22	Framed-Route	IPv4 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client). Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv4 address + '/' + prefix length or netmask **ifc=<destination interface>** Name of the IP interface or a load balancer to which the route should point, or “#Ifc”. If no destination interface is specified or it is “#Ifc”, the route points to the VPN interface for the respective

ID	Name	Meaning
		dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
69	Tunnel-Password	Sets the passwords on the local and remote identity to the same value when using synchronous PSKs.
88	Framed-Pool	Name of the IPv4 address pool from which the client retrieves its IP address and the DNS server. The values in "Framed-IP-Address" and "LCS-DNS-Server-IPv4-Address" take precedence over this attribute.
99	Framed-IPv6-Route	IPv6 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client). Format (string): <Prefix> [ifc=<destination interface>] [rtg_tag=<routing tag>] [admin_distance=<distance>] **<Prefix>** IPv6 address + '/' + prefix length **ifc=<destination interface>** Name of the IP interface or a load balancer to which the route should point, or "#Ifc". If no destination interface is specified or it is "#Ifc", the route points to the VPN interface for the respective dial-in client. The interface name can contain up to 16 characters. **rtg_tag=<routing tag>** Routing tag for the route. If this is not specified, the route is given the tag of the dial-in interface. **admin_distance=<distance>** Administrative distance of the route as a number from 0 to 255. If not specified, the route is given the default distance for VPN routes.
168	Framed-IPv6-Address	IPv6 address for the client (in IKE CFG-mode "Server").
169	DNS-Server-IPv6-Address	IPv6 DNS server for the client (in IKE CFG-mode "Server").
172	Stateful-IPv6-Address-Pool	Name of the IPv6 address pool (in IKE CFG-mode "Server").

ID	Name	Meaning
LANCOM 19	LCS-IKEv2-Local-Password	Local IKEv2 PSK
LANCOM 20	LCS-IKEv2-Remote-Password	Remote IKEv2 PSK
LANCOM 21	LCS-DNS-Server-IPv4-Address	IPv4 DNS server for the client (in IKE CFG-mode “Server”).
LANCOM 22	LCS-VPN-IPv4-Rule	Contains the IPv4 network rules (examples below)
LANCOM 23	LCS-VPN-IPv6-Rule	Contains the IPv6 network rules (examples below)
LANCOM 24	LCS-Routing-Tag	Routing tag to be configured for the client (IPv4/IPv6).
LANCOM 25	LCS-IKEv2-IPv4-Route	Routes in prefix notation (e.g. “192.168.1.0/24”) that the LANCOM gateway transfers to the client via `INTERNAL_IP4_SUBNET`. Multiple attributes can be analyzed.
LANCOM 26	LCS-IKEv2-IPv6-Route	Routes in prefix notation (e.g. “2001:db8::/64”) that the LANCOM gateway transfers to the client via `INTERNAL_IP6_SUBNET`. Multiple attributes can be analyzed.
LANCOM 27	LCS-IKEv2-DNS domain	Split DNS domains (list) that the gateway transfers to the client by means of the attribute `INTERNAL_DNS_DOMAIN` in the IKE-CFG mode “Server”, e.g. `mydomain.internal, example.com`,
LANCOM 28	LCS load balancer	Format (string): <Load balancer name> [client_binding={no|yes}] The <load balancer name> can be up to 16 characters long and specifies a load-balancing remote site on the LANCOM routers. This remote site is used for dynamic IKEv2-VPN load balancing and therefore must not be already used for static load balancing under **IP router** > **Load balancing**. The option “client_binding” turns the client binding (see *Client binding* on page 431) on or off. Unless otherwise specified, client binding is off. The first IKEv2-VPN client to connect specifies this setting. Any subsequent settings for the client binding in connection with this load-balancing remote site are ignored.
LANCOM 29	LCS-IKEv2-Routing-Tag-List	Format (string): #, e.g. `0,3,7` Contains the routing tags to be transmitted via HSVPN.
LANCOM 30	LCS-IKEv2-IPv4-Tagged-Route	Format (string): <Prefix> rtg_tag=<routing tag> **<Prefix>** HSVPN IPv4 route that the CFG mode server transmits to the client as part of IKEv2 routing. **rtg_tag=<routing tag>** The routing tag used here. For example, `192.168.1.0/24 rtg_tag = 1` A prefix with a routing tag can appear multiple times in the attribute and is separated by a comma.

ID	Name	Meaning
LANCOM 31	LCS-IKEv2-IPv6-Tagged-Route	Format (String), <Prefix> rtg_tag=<Routing-Tag> **<Prefix>** HSVPN IPv6 route that the CFG mode server transmits to the client as part of IKEv2 routing. **rtg_tag=<routing tag>** The routing tag used here. For example, `2001:db8::/64 rtg_tag=1` A prefix with a routing tag can appear multiple times in the attribute and is separated by a comma.
LANCOM 32	LCS-IPv6-Prefix-Length	Specifies the IPv6 prefix length to be configured for the client (in IKE-CFG mode "Server").
LANCOM 33	LCS-IKEv2-PPK	Specifies the post-quantum preshared key as a string or hexadecimal number (identified by a leading 0x).
LANCOM 34	LCS-IKEv2-PPK-MANDATORY	Specifies whether the use of the passed post-quantum preshared key (PPK) is required. If yes, the corresponding VPN connection will be rejected if the remote site does not support or has not configured a PPK. If the use of PPKs is configured as optional, both PPK and non-PPK connections are accepted.

Example: RADIUS attributes for a simple load balancer made up of IKEv2 VPN tunnels to the central site

```
LCS-Load-Balancer=LB1
Framed-Route=192.168.45.0/24 ifc=LB1;
```

Examples of network rules

The format for a network rule on the RADIUS server takes the form `<local networks> * <remote networks>`.

The entries for `<local networks>` and `<remote networks>`are comma-separated lists.

Example 1: `10.1.1.0/24,10.2.0.0/16 * 172.32.0.0/12`

The result is the following network rules:

- `10.2.0.0/255.255.0.0` <-> `172.16.200.0/255.255.255.255`
- `10.1.1.0/255.255.255.0` <-> `172.16.200.0/255.255.255.255`

Example 2: `10.1.1.0/24 * 0.0.0.0/0`

This results in the following network rule:

- `10.1.1.0/255.255.255.0` <-> `0.0.0.0/0.0.0.0`

Here, `0.0.0.0/0` means "ANY", i.e. any network. `0.0.0.0/32` can be used to restrict a CFG-mode client to its own (as yet unknown) config-mode address. This address could come from an address pool on the device or from the RADIUS server.

Example 3: `2001:db8:1::/48 * 2001:db8:6::/48`

RADIUS accounting

The LANCOM gateway counts the transmitted data packets and octets and sends this information as regular `Accounting-Request` messages to the RADIUS accounting server. The RADIUS server answers this message with an `Accounting-Response` message.

The `Accounting-Request` messages have the following status types:

Home

As soon as a VPN peer contacts the LANCOM gateway, the gateway starts an accounting session via IKEv2 and sends a `Start` status message with the appropriate RADIUS attributes to the RADIUS accounting server.

Interim-Update

During an ongoing accounting session, the gateway sends `Interim-Update` status messages at specified time intervals to that RADIUS accounting server, which gave a valid response to the `Start` status message. The gateway ignores any backup servers that may have been configured.

Stop

After the end of a session, the LANCOM gateway sends a `Stop` status message to the RADIUS accounting server. This message is also sent only to that RADIUS accounting server, which gave a valid response to the `Start` status message. The gateway ignores any backup servers that may have been configured.

In the `Access-Request` message, the gateway transmits the following RADIUS attributes to the RADIUS server:

ID	Name	Meaning	Status-Type
1	User name	The remote ID of the VPN peers sent in the `AUTH` negotiation with the LANCOM gateway.	› Home › Interim-Update › Stop
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute “95” instead (see below).	› Home › Interim-Update › Stop
8	Framed-IP-Address	IP4 address of the VPN client.	› Home › Interim-Update › Stop
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).	› Home › Interim-Update › Stop
32	NAS identifier	The device name of the gateway.	› Home › Interim-Update › Stop
40	Acct-Status-Type	Contains the status type “Start” (1).	› Home
40	Acct-Status-Type	Contains the status type “Interim-Update” (3).	› Interim-Update
40	Acct-Status-Type	Contains the status type “Stop” (2).	› Stop

ID	Name	Meaning	Status-Type
42	Acct-Input-Octets	Contains the number of octets received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	› Interim-Update › Stop
43	Acct-Output-Octets	Contains the number of octets sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	› Interim-Update › Stop
44	Acct-Session-Id	The name of the VPN peer and the timestamp at the start of the session form the unique session ID.	› Home › Interim-Update › Stop
46	Acct-Session-Time	Contains the elapsed time in seconds since the start of the session.	› Interim-Update › Stop
47	Acct-Input-Packets	Contains the current number of data packets received from the direction of the VPN peer.	› Interim-Update › Stop
48	Acct-Output-Packets	Contains the current number of data packets sent to the VPN peer.	› Interim-Update › Stop
49	Acct-Terminate-Cause	Contains the reason for terminating the session.	› Stop
52	Acct-Input-Gigawords	Contains the number of gigawords received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	› Interim-Update › Stop
53	Acct-Input-Gigawords	Contains the number of gigawords sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	› Interim-Update › Stop
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute “4” instead (see above).	› Home › Interim-Update › Stop
168	Framed-IPv6-Address	IP6 address of the VPN client.	› Home › Interim-Update › Stop

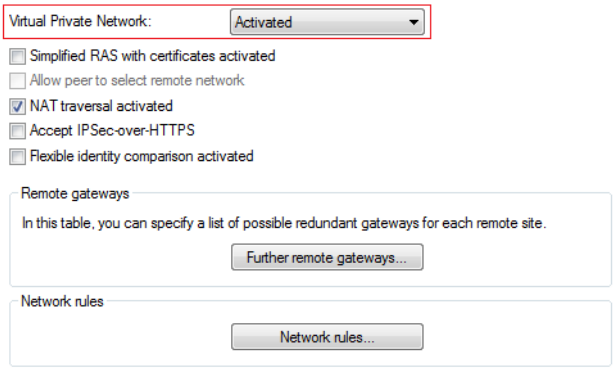
11.19.4 Tutorial: Setting up IKEv2 under LANconfig

Initial situation: Two LANCOM routers are connected via a WAN link. The requirement is to establish a secure VPN connection between them by means of IKEv2/IPSec VPN. The routers are a LANCOM 1800VAW at the main office and a LANCOM 1800VA-4G at the branch office.

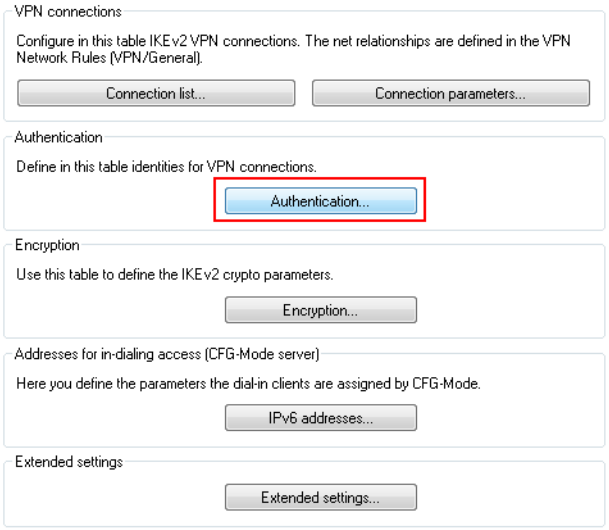


We assume that a WAN connection exists between the two devices.

1. **Enabling VPN**: For both of the routers, open the menu item **VPN** > **General** and, under **Virtual Private Network**, select the option **Activated**. This enables VPN on that specific device.

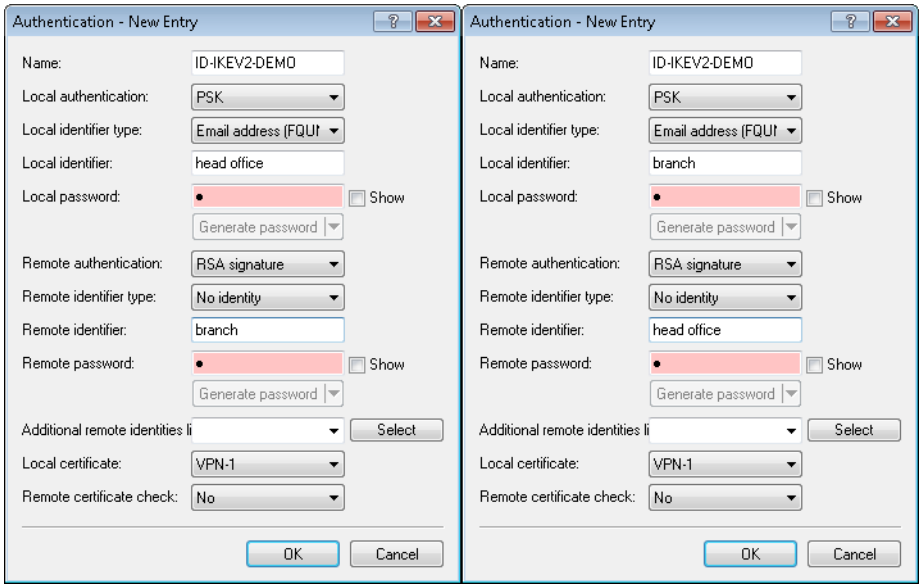


2. **Configuring the authentication**: Specify the type of authentication for the VPN connection. To do this, open the menu item **VPN** > **IKEv2/IPSec** and click the button **Authentication**.



3. Click on the **Add** button to configure a new authentication type. Enter the information for the authentication of the VPN connection into the configuration window.

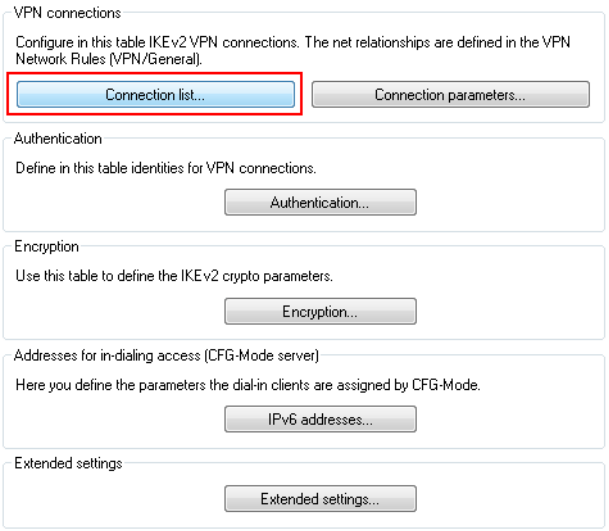
The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



The left half of the images shows the LANCOM 1800VAW, and the right half shows the parameters of the LANCOM 1800VA-4G.

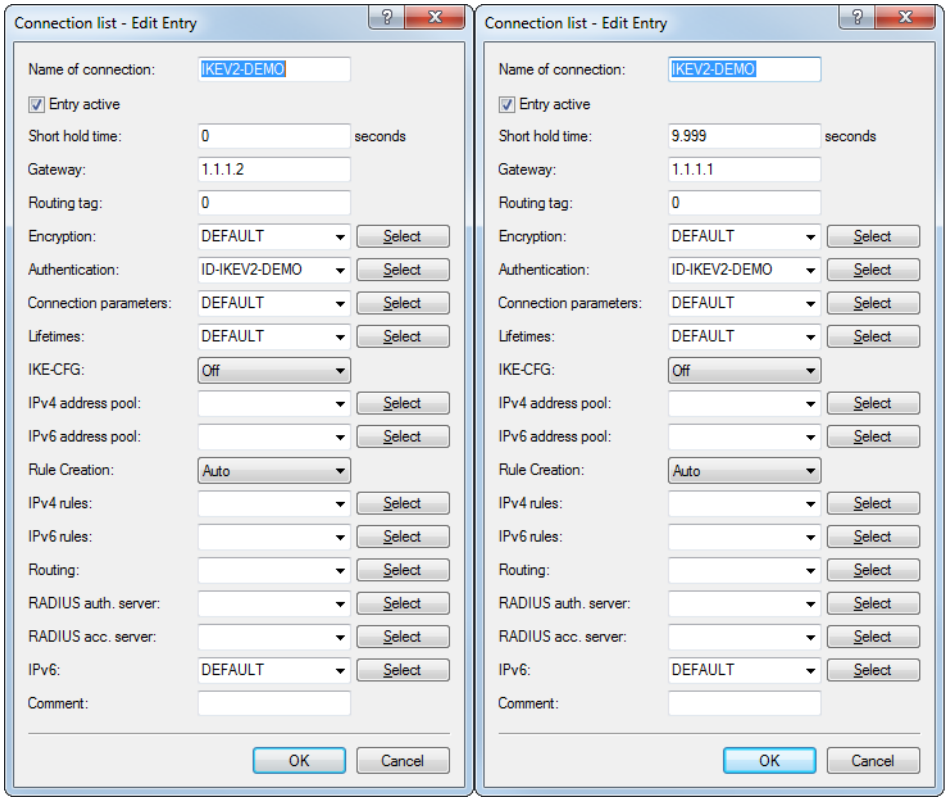
Parameter	Description
Name	Enter the name for the authentication here. In this example, **ID-IKEV2-DEMO** was entered on both devices. This entry is used later in the VPN connection list.
Local authentication	Select the authentication type used on this router. This example uses authentication by pre-shared key (PSK).
Local identifier type	Select the identifier type used on this router. In this example, the identity type was set to **E-mail address (FQUN)**.
Local identifier	Set the local identifier. In this example, the local identifier was set to **Main** on the 1800VAW and **Branch** on the 1800VA-4G.
Local password	The pre-shared key required to successfully authenticate at this router.
Remote authentication	Select the authentication type used by the remote router. On the 1800VAW, this entry corresponds to the entry for “Local authentication” on the 1800VA-4G.
Remote identifier type	Select the type of the remote identifier (used by the remote router). On the 1781AW, this entry corresponds to the entry for Local identifier on the 1800VA-4G.
Remote identifier	Enter the identifier of the remote station. On the 1781AW, this entry corresponds to the entry for “Local identifier” on the 1800VA-4G.
Remote password	The pre-shared key required to successfully authenticate at the remote station. On the 1781AW, this entry corresponds to the entry for Local password on the 1800VA-4G.

4. **Configuring the Connection list:** Configure the connection lists on each individual router. To carry out the configuration, open the menu item **VPN** > **IKEv2/IPSec** and click the button **Connection list**.



5. Create a new VPN connection by clicking the button **Add**.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

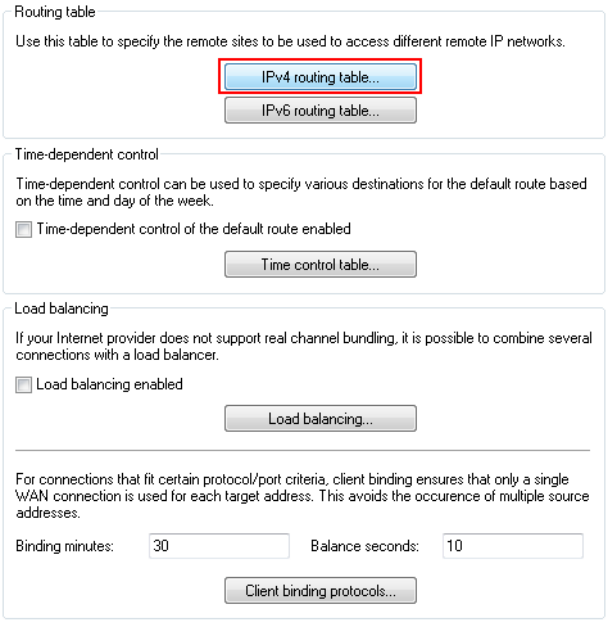


The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1800VA-4G.

Parameter	Description
Entry active	Set a check mark in the check box to activate the connection.

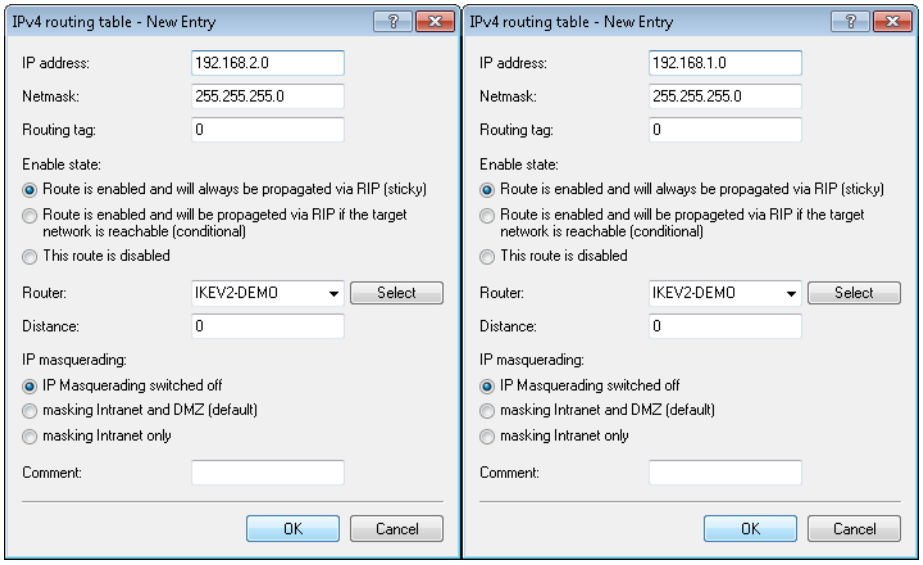
Parameter	Description
Name of connection	Enter a name for the VPN connection. This name is used later in the routing table.
Short hold time	Specify the short-hold time in seconds for the VPN connection. In this example, the value for the 1781AW is set to **0**. This means that this router will not actively establish the VPN connection. The value for the 1800VA-4G is set to **9999**. This value means that the router will not actively disconnect and, in case the connection is lost, it reconnects immediately.
Gateway	Specify the IP address of the remote station. In this example, the IP address of the WAN interface of the 1781AW is `1.1.1.1` and that of the 1800VA-4G is `1.1.1.2`. If the 1800VA-4G has a dynamic IP address, then the value for the **remote gateway** on the 1781AW needs to be set to `0.0.0.0` instead of `1.1.1.2`.
Authentication	Select the authentication. The entry here corresponds to the name of the authentication that you set in **step 3**.

6. **Configuring the Routing table:** Configuring the routes here ensures that packets can be sent from the router through the VPN tunnel to the VPN remote station. To do this, open the menu item **IP router** > **Routing** and click the button **IPv4 routing table**.



7. Create an additional route by clicking the button **Add**. Information about the route is entered into the configuration window for each router.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1800VA-4G.

Parameter	Description
IP address	Enter the IP network to be accessed via the VPN tunnel. In this example, the IP network `192.168.2.0` should be accessed from the 1781AW and the IP network `192.168.1.0` should be accessed from the 1800VA-4G.
Netmask	Specify the netmask of the IP network named above.
Enable state	Select the option **Route is enabled and will always be propagated by RIP**. This activates the entry and makes it available for use.
Router	For the router, enter the name of the VPN connection that you entered in **step 4**.
IP masquerading	Select **IP masquerading switched off** so that the router does not conceal the other network behind its own IP address.

8. Write the respective configurations back to the two devices.
9. Use LANmonitor to check the VPN connection. LANmonitor displays the status of the VPN connection.

11.19.5 Tutorial: Setting up a certificate-based IKEv2 VPN connection (RSA)

Initial situation: Two LANCOM routers connect to each other over a WAN connection. You want them to communicate securely with one another using a certificate-based IKEv2 VPN connection. Routers suitable for this purpose include LANCOM central-site gateways, WLAN controllers or LANCOM routers with an activated VPN 25 Option (when using the Smart Certificate feature).

We assume that a WAN connection exists between the two devices.

Certificates have already been created for the LANCOM routers.

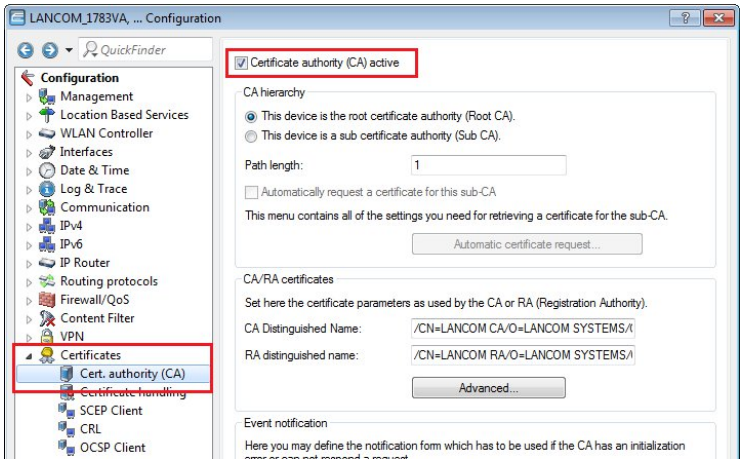
1. Enable the CA function in the LANCOM router at the headquarters:

In this example configuration, the LANCOM router at the headquarters acts as the CA for creating the certificates (Smart Certificate feature). If you wish to use certificates from another CA, you do not have to use the CA in the LANCOM router and you can skip this step of the configuration.

a) In LANconfig, open the configuration dialog for the LANCOM router at the headquarters and switch to the menu item **Certificates** > **Cert. authority (CA)**.

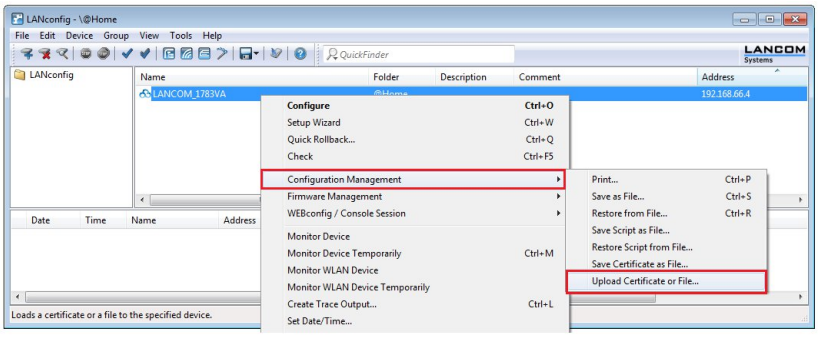
b) Set a check mark for the option **Certificate authority (CA) active**. The LANCOM router functions as the root certificate authority (root CA).

For this configuration example we leave all of the other parameters with their preset values.



2. Uploading certificates to the LANCOM routers:

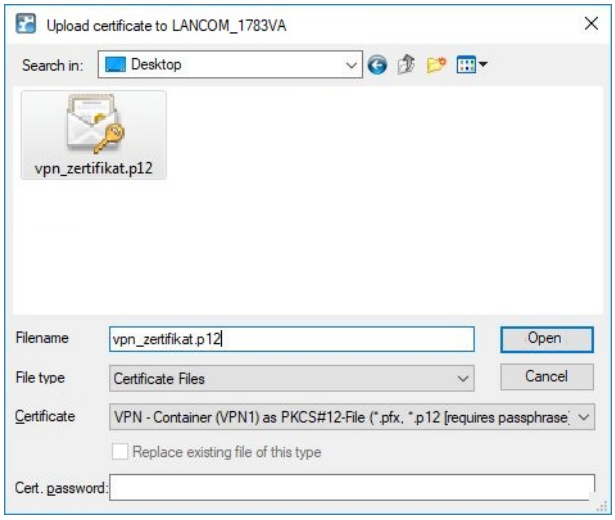
a) Right-click on each of the LANCOM routers in LANconfig and select the option **Configuration management** > **Upload certificate or file**.



b) In the following dialog select the certificate file intended for LANCOM router.

c) In the **certificate type** field, select a VPN container.

d) In the **Cert. password** box enter the password for the certificate file. Click on **Open** to start the upload.

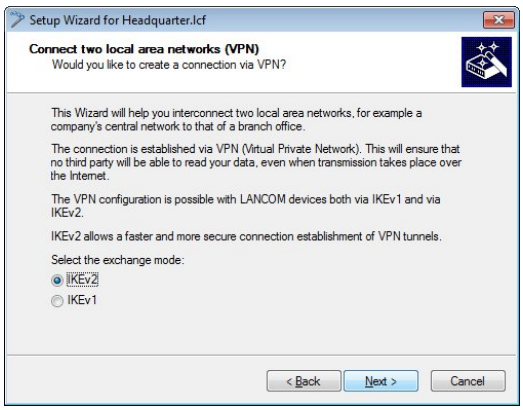


3. Configure the certificate-based VPN connection on the LANCOM router at the headquarters:

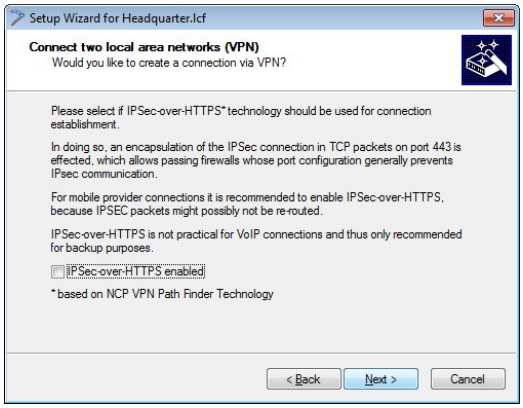
a) Start the Setup Wizard in LANconfig and select the option **Connect two local area networks (VPN)**.



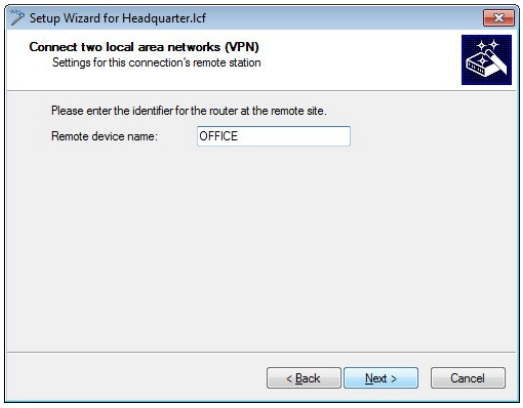
b) Now create an **IKEv2**-VPN connection.



c) In this example, we **do not use** IPSec-over-HTTPS.

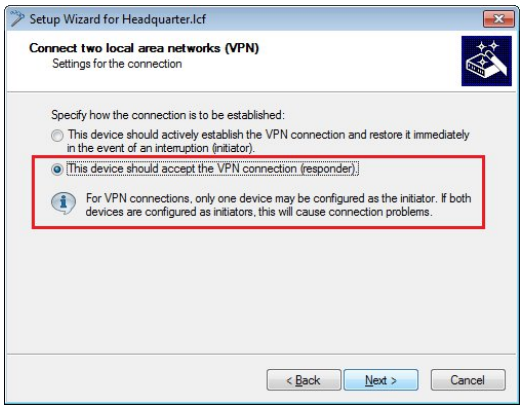


d) Enter a **name for LANCOM router at the remote site**.

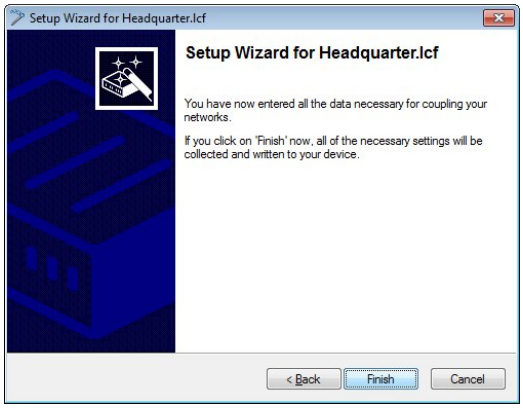


e) Enter any values into the following two dialogs, as they will later be manually replaced in the configuration of the LANCOM router by the certificate authentication parameters.

f) Since LANCOM router at the headquarters receives the VPN connection, no gateway address is required. Specify the local network to be accessed at the remote site.



g) Click on **Finish** to exit the setup wizard and write the configuration back to the LANCOM router.



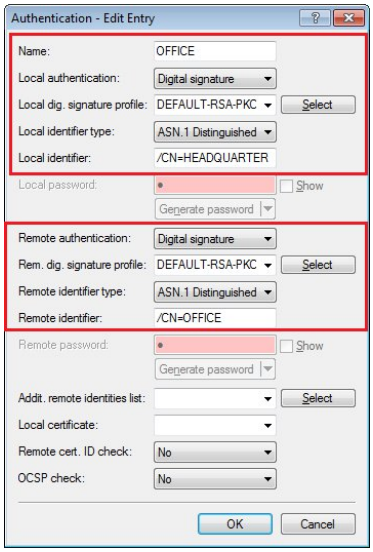
h) Open the the LANCOM router configuration in LANconfig and navigate to **VPN** > **IKEv2/IPSec** > **Authentication**.

i) Select the available entry for the certificate-based VPN client connection (in this case: OFFICE).

j) Set the **parameters for local and remote authentication** for each entry to the values **RSA signature** and **ASN.1 Distinguished Name**.

k) As the **local identity**, enter the name of the certificate in the LANCOM router at the headquarters.

l) As the **remote identity**, enter the name of the certificate in the LANCOM router at the branch office.



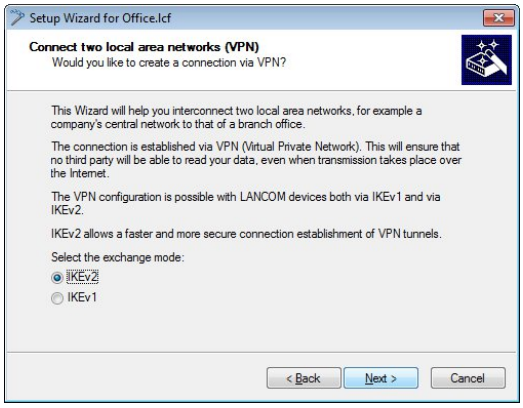
m) Write the configuration back to the LANCOM router at the headquarters.

4. Configure the certificate-based VPN connection on the LANCOM router at the branch office

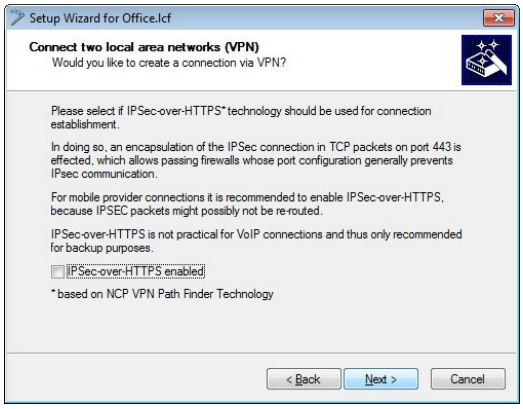
a) Start the Setup Wizard in LANconfig and select the option **Connect two local area networks (VPN)**.



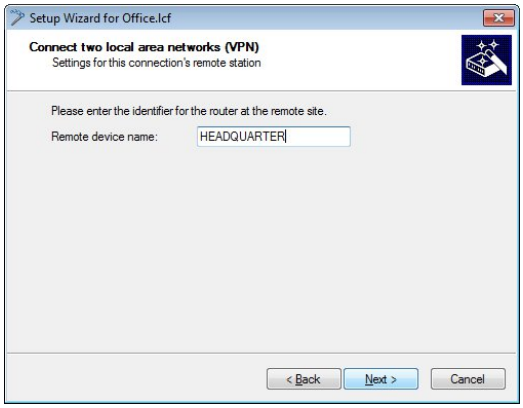
b) Now create an **IKEv2**-VPN connection.



c) In this example, we **do not use** IPSec-over-HTTPS.

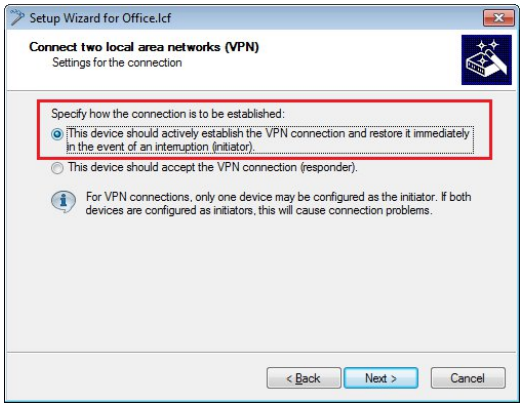


d) Enter a **name for LANCOM router at the remote site**.



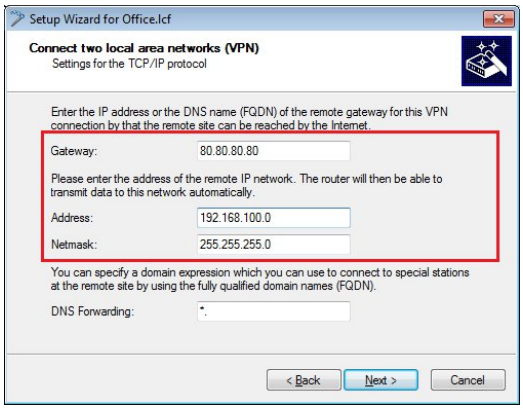
e) Enter any values into the following two dialogs, as they will later be manually replaced in the configuration of the LANCOM router by the certificate authentication parameters.

f) The LANCOM router at the branch office should establish the VPN connection.

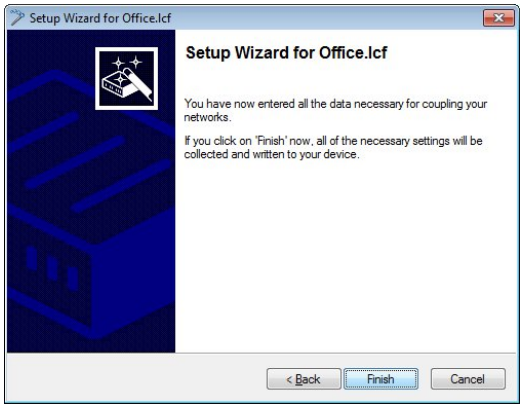


g) Since the LANCOM router at the branch office establishes the VPN connection, enter the gateway address of the headquarters.

h) Specify the local network to be accessed at the remote site.



i) Click on **Finish** to exit the setup wizard and write the configuration back to the LANCOM router.



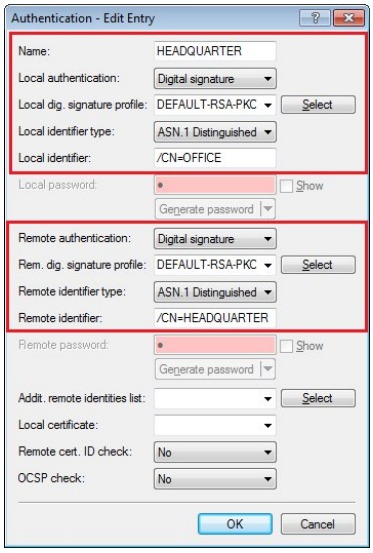
j) Open the the LANCOM router configuration in LANconfig and navigate to **VPN** > **IKEv2/IPSec** > **Authentication**.

k) Select the available entry for the certificate-based VPN connection (in this case: HEADQUARTERS).

l) Set the **parameters for local and remote authentication** for each entry to the values **RSA signature** and **ASN.1 Distinguished Name**.

m) As the **local identity**, enter the name of the certificate in the LANCOM router at the branch office.

n) As the **remote identity**, enter the name of the certificate in the LANCOM router at the headquarters.



o) Write the configuration back to the LANCOM router at the branch office.

The certificate-based IKEv2 VPN connection to the headquarters will now be established.

11.19.6 Tutorial: Setting up a certificate-based IKEv2 VPN connection (digital signature)

Initial situation: Two LANCOM routers connect to each other over a WAN connection. You want them to communicate securely with one another using a certificate-based IKEv2 VPN connection. Routers suitable for this purpose include LANCOM central-site gateways, WLAN controllers or LANCOM routers with an activated VPN 25 Option (when using the Smart Certificate feature).

We assume that a WAN connection exists between the two devices.

Certificates have already been created for the LANCOM routers.

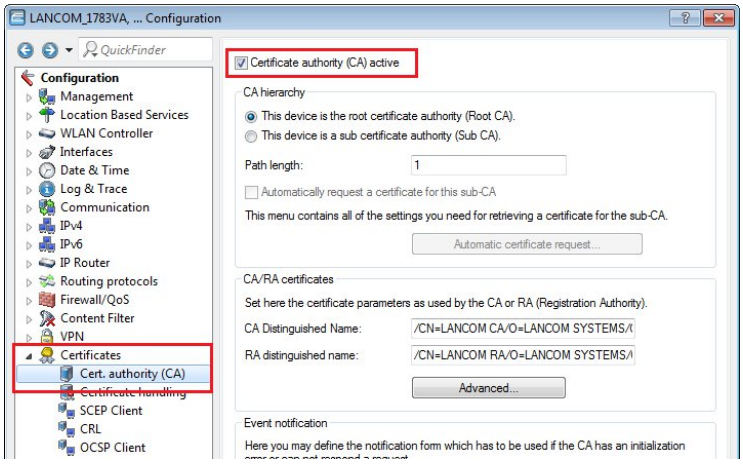
1. Enable the CA function in the LANCOM router at the headquarters:

In this example configuration, the LANCOM router at the headquarters acts as the CA for creating the certificates (Smart Certificate feature). If you wish to use certificates from another CA, you do not have to use the CA in the LANCOM router and you can skip this step of the configuration.

a) In LANconfig, open the configuration dialog for the LANCOM router at the headquarters and switch to the menu item **Certificates** > **Cert. authority (CA)**.

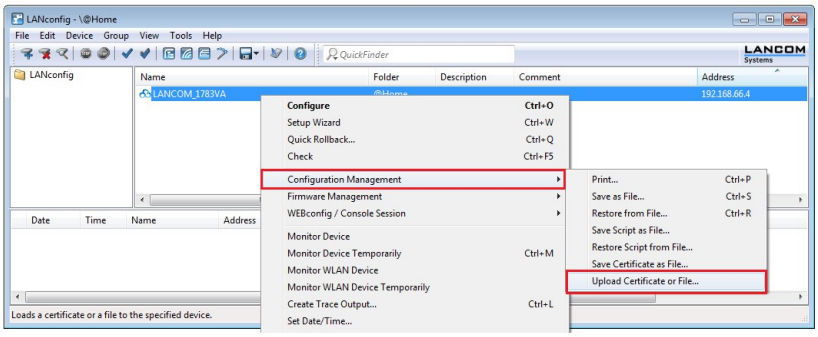
b) Set a check mark for the option **Certificate authority (CA) active**. The LANCOM router functions as the root certificate authority (root CA).

For this configuration example we leave all of the other parameters with their preset values.



2. Uploading certificates to the LANCOM routers:

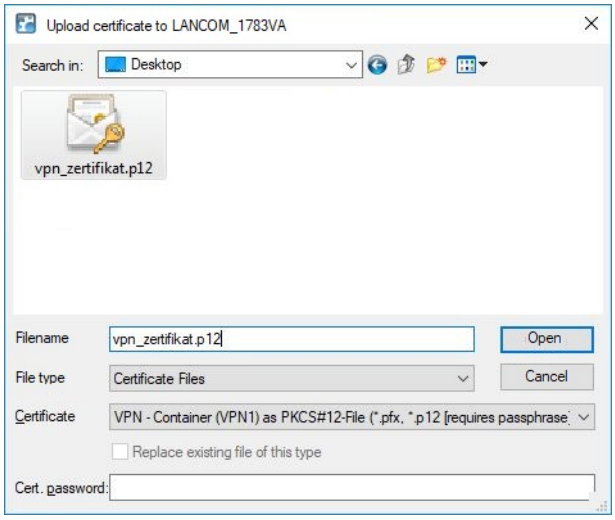
a) Right-click on each of the LANCOM routers in LANconfig and select the option **Configuration management** > **Upload certificate or file**.



b) In the following dialog select the certificate file intended for LANCOM router.

c) In the **certificate type** field, select a VPN container.

d) In the **Cert. password** box enter the password for the certificate file. Click on **Open** to start the upload.

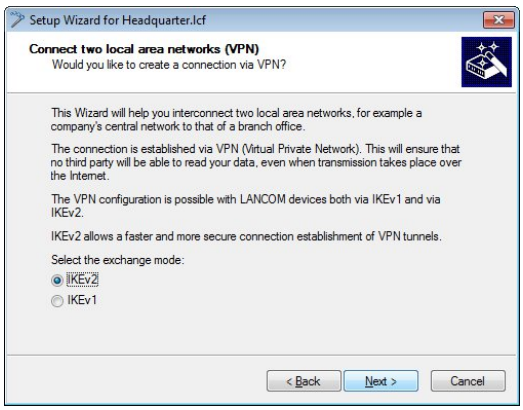


3. Configure the certificate-based VPN connection on the LANCOM router at the headquarters:

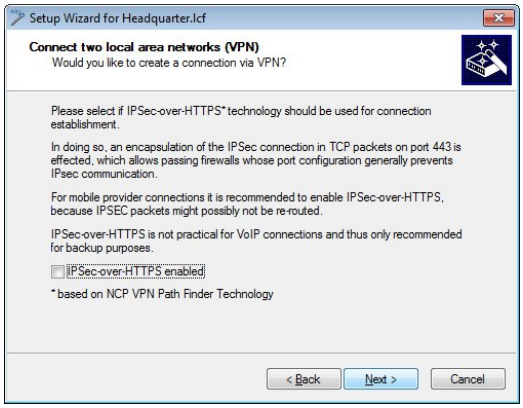
a) Start the Setup Wizard in LANconfig and select the option **Connect two local area networks (VPN)**.



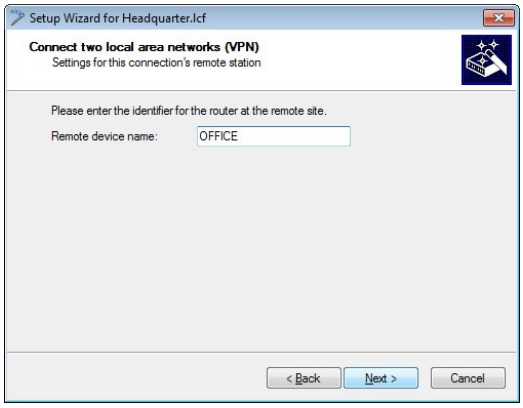
b) Now create an **IKEv2**-VPN connection.



c) In this example, we **do not use** IPSec-over-HTTPS.

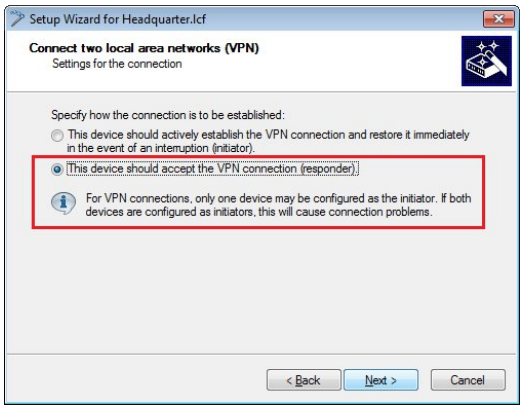


d) Enter a **name for LANCOM router at the remote site**.

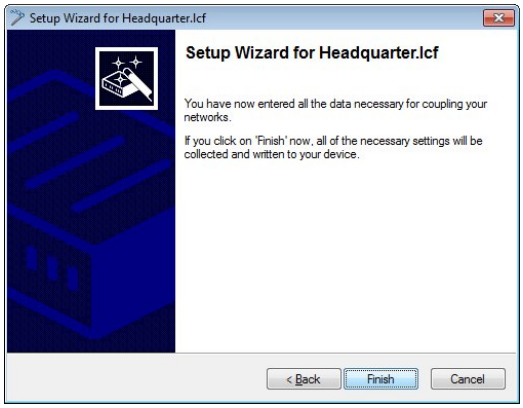


e) Enter any values into the following two dialogs, as they will later be manually replaced in the configuration of the LANCOM router by the certificate authentication parameters.

f) Since LANCOM router at the headquarters receives the VPN connection, no gateway address is required. Specify the local network to be accessed at the remote site.



g) Click on **Finish** to exit the setup wizard and write the configuration back to the LANCOM router.



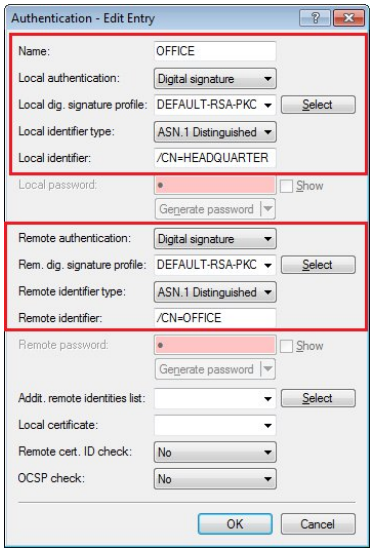
h) Open the the LANCOM router configuration in LANconfig and navigate to **VPN** > **IKEv2/IPSec** > **Authentication**.

i) Select the available entry for the certificate-based VPN client connection (in this case: OFFICE).

j) Set the parameters for **local and remote authentication** for each entry to the values **Digital signature** and **ASN.1 Distinguished Name**.

k) As the **local identity**, enter the name of the certificate in the LANCOM router at the headquarters.

l) As the **remote identity**, enter the name of the certificate in the LANCOM router at the branch office.



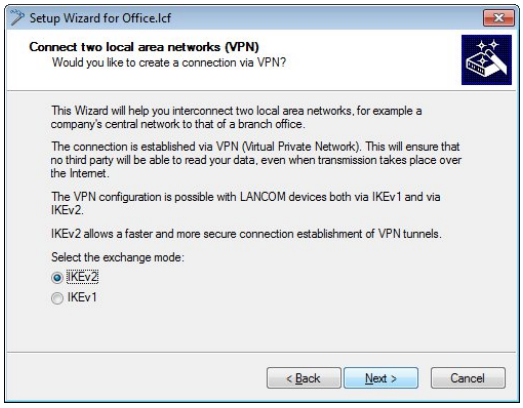
m) Write the configuration back to the LANCOM router at the headquarters.

4. Configure the certificate-based VPN connection on the LANCOM router at the branch office

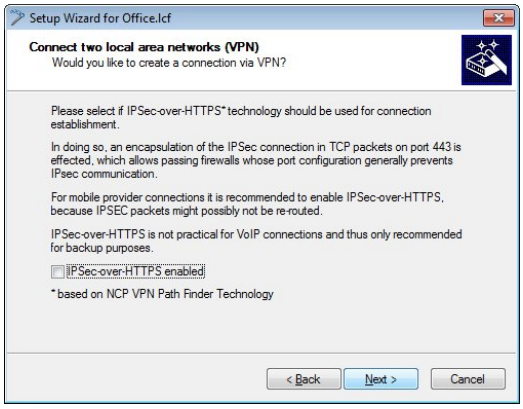
a) Start the Setup Wizard in LANconfig and select the option **Connect two local area networks (VPN)**.



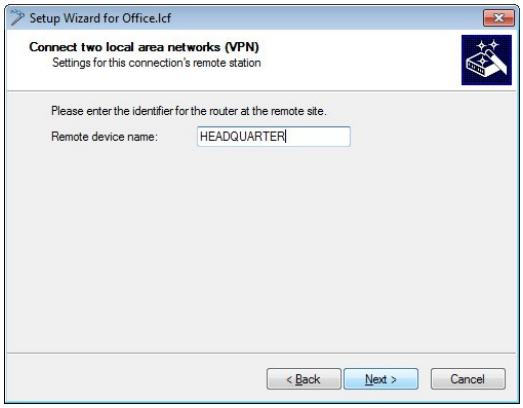
b) Now create an **IKEv2**-VPN connection.



c) In this example, we **do not use** IPSec-over-HTTPS.

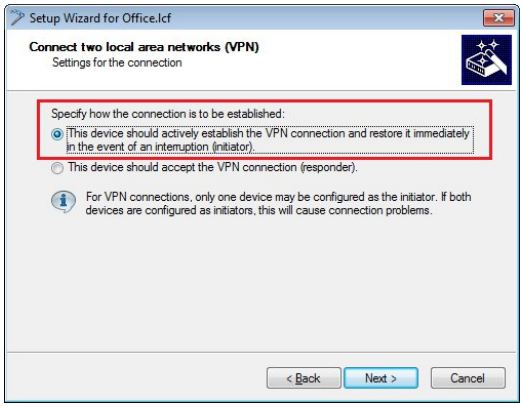


d) Enter a **name for LANCOM router at the remote site**.



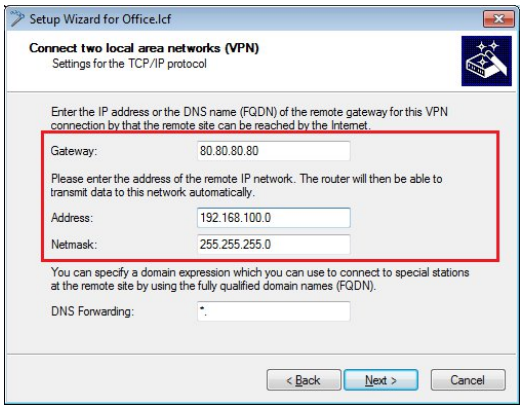
e) Enter any values into the following two dialogs, as they will later be manually replaced in the configuration of the LANCOM router by the certificate authentication parameters.

f) The LANCOM router at the branch office should establish the VPN connection.

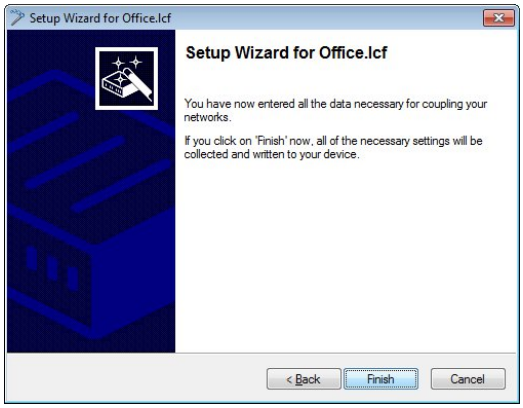


g) Since the LANCOM router at the branch office establishes the VPN connection, enter the gateway address of the headquarters.

h) Specify the local network to be accessed at the remote site.



i) Click on **Finish** to exit the setup wizard and write the configuration back to the LANCOM router.



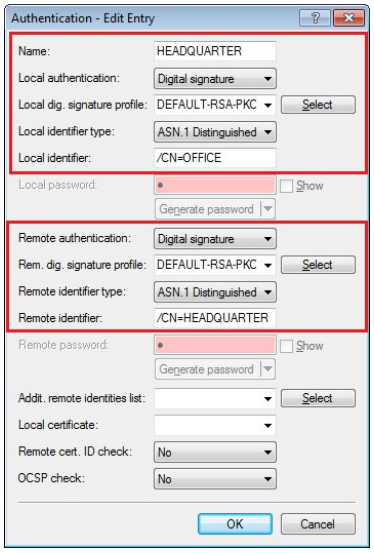
j) Open the the LANCOM router configuration in LANconfig and navigate to **VPN** > **IKEv2/IPSec** > **Authentication**.

k) Select the available entry for the certificate-based VPN connection (in this case: HEADQUARTERS).

l) Set the **parameters for local and remote authentication** for each entry to the values **RSA signature** and **ASN.1 Distinguished Name**.

m) As the **local identity**, enter the name of the certificate in the LANCOM router at the branch office.

n) As the **remote identity**, enter the name of the certificate in the LANCOM router at the headquarters.



o) Write the configuration back to the LANCOM router at the branch office.

The certificate-based IKEv2 VPN connection to the headquarters will now be established.

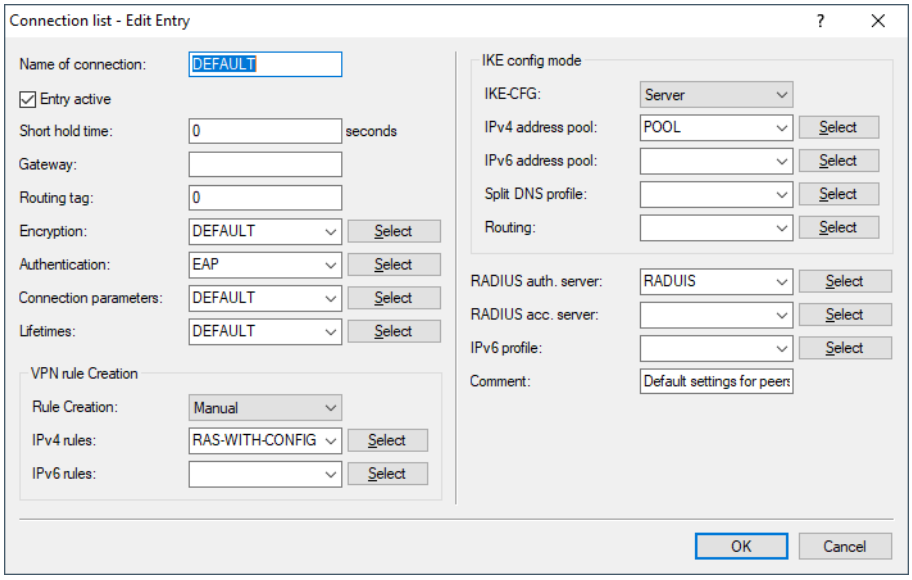
11.19.7 Tutorial – EAP client at an EAP server

The following tutorial will configure an EAP client against an EAP server.

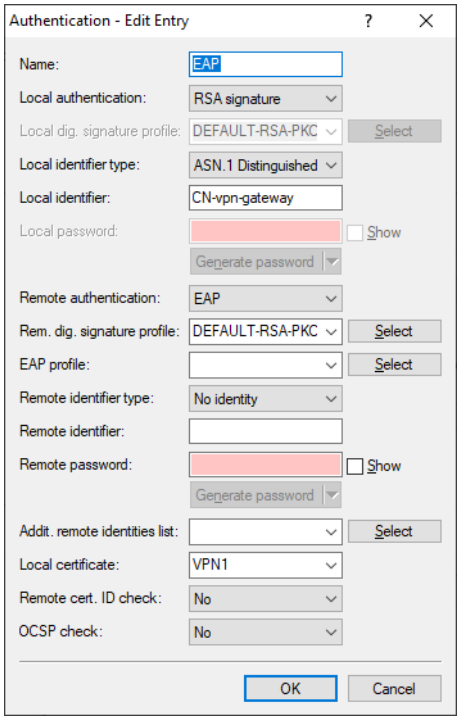
1. Create two certificates or certificate containers, for example with the LANCOM SCEP CA or OpenSSL.
2. Import a certificate into the VPN gateway and a certificate into the RADIUS server.

   Make sure the Subject Alternative Name (SAN) matches the valid DNS name of the VPN gateway and that the VPN client contacts the gateway under this DNS name.
3. Establish the trust relationship by importing the valid CA certificate into the IKEv2 EAP client.

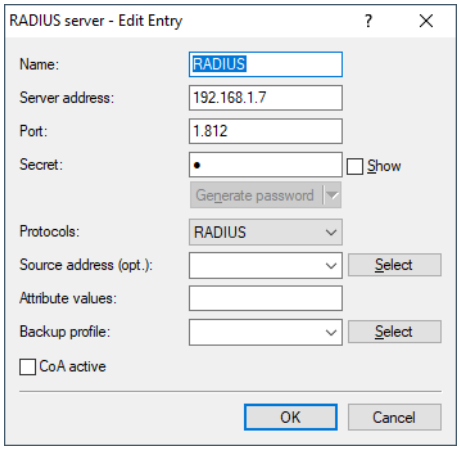
4. Modify the DEFAULT entry of the IKEv2 remotes table under **VPN** > **IKEv2/IPSec** > **VPN connections** > **Connection list** as follows:



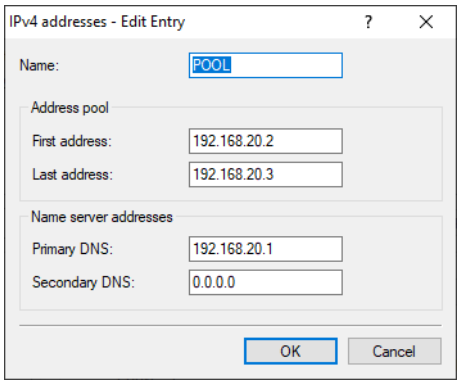
5. Insert a new row in the IKEv2 Authentication table under **VPN** > **IKEv2/IPSec** > **Authentication**. Local authentication of the VPN gateway uses a certificate (RSA signature), and remote authentication of the clients is done by EAP.



6. Configure the RADIUS server under **VPN** > **IKEv2/IPSec** > **Extended settings** > **RADIUS authentication** > **RADIUS server**.



7. Configure an address pool under **VPN** > **IKEv2/IPSec** > **IPv4 addresses**.



11.20 LANconfig application concepts

This section describes various applications of LANconfig.

11.20.1 1-Click-VPN for networks (site-to-site)

The site-to-site-to-site connectivity of networks is now very simple with the help of the 1-Click-VPN wizard. It is even possible to simultaneously couple multiple routers to a central network.

1. In LANconfig, mark the routers to be used to set up VPN site-to-site connectivity to a central router.
2. Use drag&drop by mouse to place the devices onto the entry for the central router.
3. The 1-Click VPN Site-to-Site Wizard opens. Enter a name for this access and select the address under which the router is accessible from the Internet.
4. Select whether connection establishment is to take place via the name or IP address of the central router. Enter the address or name of the central router.
5. The final step is to define how the networks are to intercommunicate:
   - The INTRANET at headquarters only is to be provided to the branch offices.
   - All private networks at the branch offices can also be connected to one another via headquarters.

All entries for the central device are made just once and are then stored to the device properties.

11.20.2 1-Click-VPN for the Advanced VPN Client

VPN accesses for employees who dial into the network with the LANCOM Advanced VPN Client are very easy to set up with the Setup Wizard and exported to a file. This file can then be imported as a profile by the LANCOM Advanced VPN Client. All of the information about the VPN router's configuration is also included, and then supplemented with randomly generated values (e.g. for the preshared key).

1. In LANconfig, use **Device** > **Setup Wizard** to start the **Provide remote access (RAS, VPN)** setup wizard.
2. In the subsequent dialog, select **VPN connection over the Internet** as the connection type and click **Next**.
3. From the list, select the entry **LANCOM Advanced VPN Client [...]** and activate the option **Speed up configuration with 1-Click-VPN**.
4. Next, enter a name for this access and select the address under which the router is accessible from the Internet.
5. In the final step you can select how the access data is to be entered:
   - Save profile as an import file for the LANCOM Advanced VPN Client
   - Send profile via e-mail
   - Print out profile

Sending a profile via e-mail could be a security risk should the e-mail be intercepted. To send the profile via e-mail, the device configuration must be set up with an SMTP account with the necessary access data. Further, the configuration computer requires an e-mail program that is set up as the standard e-mail application and that can be used by other applications to send e-mails.

When setting up the VPN access, certain settings are made to optimize operations with the LANCOM Advanced VPN Client, including:

- Gateway: If defined in the VPN router, a DynDNS name is used here, or alternatively the IP address
- FQDN: Combination of the name of the connection, a sequential number and the internal domain in the VPN router
- Domain: If defined in the VPN router, the internal domain is used here, or alternatively a DynDNS name or IP address
- VPN IP networks: All IP networks defined in the device as type 'Intranet'.
- Pre-shared key: Randomly generated key 16 ASCII characters long.
- Connection medium: The LAN is used to establish connections.
- VoIP prioritization: VoIP prioritization is activated as standard.
- Exchange mode: The exchange mode to be used is 'Aggressive Mode'.
- IKE config mode: The IKE config mode is activated, the IP address information for the LANCOM Advanced VPN Client is automatically assigned by the VPN router.

11.21 WireGuard

WireGuard is a simple and lightweight VPN protocol. Unlike IKEv2/IPSec, WireGuard focuses on simplicity, speed, and ease of use. It is also a protocol with a very compact code base and functionality, making it ideal for use on IoT and embedded devices.

IKEv2 is an IETF-standardized protocol offering many extensions and high flexibility, but also significant complexity. While IKEv2, for example, supports crypto agility—meaning encryption algorithms can be exchanged or negotiated between endpoints—WireGuard uses a fixed key exchange (Curve25519) and a fixed encryption protocol (ChaCha20/Poly1305). In WireGuard, authentication is only possible via public/private keys, whereas IKEv2 allows flexible authentication methods such as PSK, certificates, or EAP. IKEv2 also supports many extensions, such as RADIUS or two-factor authentication, which are not available in WireGuard. Furthermore, WireGuard only supports transmission over UDP but includes built-in roaming functionality similar to MOBIKE in IKEv2.

IKEv2/IPSec continues to be the recommended standard protocol for branch connectivity and SD-WAN due to its wide range of configuration and deployment scenarios in LCOS. WireGuard on LANCOM router platforms does not provide hardware acceleration for ChaChaPoly1305, meaning encryption is handled in software. For scenarios requiring high VPN throughput, IKEv2/IPSec remains the preferred option.

Within LCOS, IKEv2/IPSec is based on many years of practical use in VPN site connectivity and numerous protocol and feature extensions for medium, large, and complex VPN or SD-WAN scenarios. WireGuard in LCOS is therefore an ideal addition for simpler use cases where only basic encrypted connections are needed. Another scenario for WireGuard use is when the VPN protocol is specified by a service provider or VPN vendor.

Conceptually, WireGuard is a "silent" protocol—no control or negotiation packets are exchanged until user data needs to be transmitted. In contrast, IKE tunnels can be configured to initiate immediately. WireGuard supports both IPv4 and IPv6, as transport protocols and for data transmission within the tunnel.

For IPv6, the inbound UDP ports used for the tunnel must be configured manually in the IPv6 firewall inbound table, since the ports in WireGuard are freely configurable.

WireGuard tunnels in LCOS can be defined as either "Unnumbered"—i.e., without a configured IP address—or with assigned IP addresses under **Communication** > **Protocols** > **IP parameters**.

In LCOS, WireGuard is classified as an interface type "VPN". This classification is relevant, for example, in connection with the access list for management protocols to the device itself under **Management** > **Admin** > **Access settings**.

If WireGuard is used to connect to a VPN provider that, for example, routes public IP addresses or subnets to the router via WireGuard, the classification as a secure interface type "VPN" applies.

In this case, the ports of management protocols or the Voice Call Manager (VCM) that allow access "only via VPN" will be open and reachable via the public IP address of the WireGuard tunnel. If this is not desired, additional rules must be configured for access stations (for management protocols) or the setting must be changed to "from WAN denied".

This behavior also applies when an IPSec / IKE / IKEv2 interface has a public IP address.



The features "Additional remote or alternative gateways" and "Gateway groups" are not supported with WireGuard.



If dynamic routing protocols such as BGP are to be used over WireGuard tunnels, the configuration parameter **Connect automatically** must be set to "Yes", because for technical reasons BGP cannot initiate the establishment of the WireGuard tunnel.

11.21.1 Licensing

In LCOS, WireGuard counts as a VPN tunnel and is included in the device's VPN license count, sharing the same license pool with other VPN tunnels such as IKE/IPSec or PPTP-MPPE. A WireGuard license is consumed as soon as data is transmitted through the WireGuard tunnel. Any number of WireGuard tunnels can be configured.

Additional WireGuard licenses can be added through the VPN option upgrade.

Example:

If a device is licensed for 5 VPN tunnels and 3 IPSec tunnels are already active, two additional WireGuard tunnels can still be used.

11.21.2 Configuration

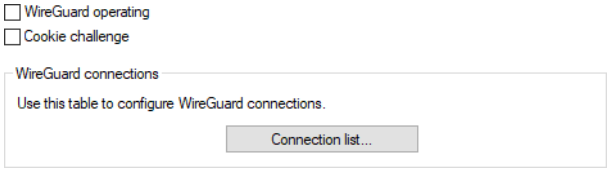
A WireGuard configuration in LCOS consists of at least two configuration elements, as well as additional optional elements:

1. An entry in the WireGuard tunnel configuration table.
2. An entry in the IPv4 and/or IPv6 routing table. This entry corresponds to the concept of "Allowed IP Addresses" in WireGuard on other platforms.
3. (Optional) Configure local IP addresses for the WireGuard peer via the IP Parameters table in LANconfig under **Communication** > **Protocols** > **IP Parameters**.

4. (Optional) Firewall configuration for granular control of network access rights.

11.21.3 Configuration with LANconfig

WireGuard is configured in LANconfig under **VPN** > **WireGuard**.



WireGuard operating

Enables or disables the WireGuard function on the device.

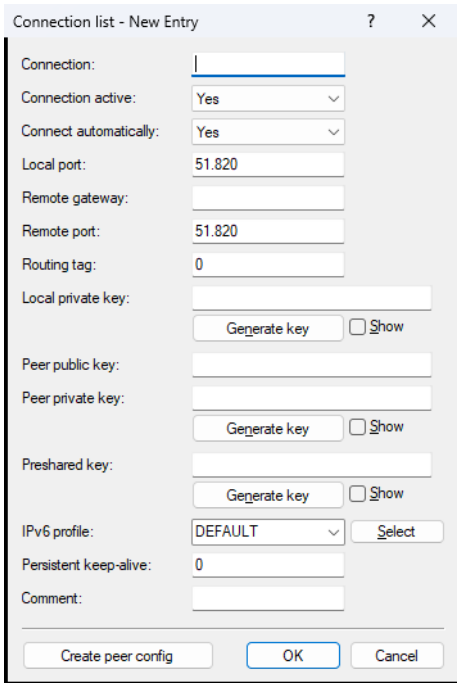
Cookie challenge

The cookie challenge is a protection mechanism against CPU exhaustion attacks during the handshake process. The computation of the Diffie-Hellman (DH) function during the WireGuard handshake is inherently CPU-intensive. An attacker could attempt to overload the router by sending a large number of handshake requests to crash it or severely impact its performance (CPU exhaustion attack). This mechanism forces the attacker to perform an additional network round trip and respond to the cookie for each handshake attempt. This significantly increases the cost of the attack, making it much less effective, while allowing the server to limit the number of DH computations it must perform, thus protecting its resources.

When the cookie challenge is enabled, the device always sends a cookie-reply message during the handshake.

Connection list

This section defines the WireGuard connections.



Connection

Name of the WireGuard connection or WireGuard peer.

Connection active

Enables or disables this connection.

Connect automatically

Defines whether the WireGuard tunnel should be established automatically—e.g., after the device starts or after the WAN connection has been established—or only when actual user data is being transmitted. This switch must be configured together with the "Persistent-Keepalive" option so that the WireGuard peer behaves like other peers that are intended to remain permanently active.

If set to "Yes", the WireGuard connection is established permanently, regardless of whether user data is transmitted. If set to "No", the connection is established only when user data is present.

Local port

Defines the local (UDP) port on which this connection should be accepted by the device. The configured local private key must be identical for all connections using the same port. Multiple configured connections using the same local port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created. If the value "0" is entered for the local port, a dynamic port is created.

For a WireGuard tunnel using IPv6 as a transport protocol, the incoming UDP ports for the tunnel must be manually configured or allowed in the IPv6 firewall's inbound table.

Remote gateway

IPv4, IPv6, or DNS address of the remote gateway or client. If the IP address of the remote side is unknown or dynamic, the field can be left blank. In this case, the connection must be initiated from the remote side.

Allowed values: IPv4 address, IPv6 address, 0.0.0.0, ::, or empty. The values 0.0.0.0 and :: for IPv6 have the same effect as an empty entry.

Remote port

Port number on the remote gateway side. If the remote port for incoming connections is dynamic or unknown, it can be left empty or set to 0. If an explicit port is configured, it must exactly match during connection setup; otherwise, the connection will be rejected or discarded.

Allowed values: Port, 0, or empty entry.

Routing tag

Defines the routing tag through which the WireGuard connection is established.

Local private key

Local private key for the WireGuard connection in Base64 format. Hex-formatted keys are not supported. The device automatically derives its public key from the local private key.

The configured local private key must be identical for all connections using the same local port. Multiple configured connections using the same port but different private keys are not supported and will prevent connections from being established or the internal configuration from being created.

The local private key is confidential and is generally not shared with the remote side—unless an administrator generates key pairs for managed devices. In this case, the administrator knows all device key pairs.

Peer public key

Public key of the remote gateway in Base64 format. Hex-formatted entries are not supported.

Each communication partner in the WireGuard connection must generate its own unique public/private key pair and share its public key with the remote side.

Peer private key

The peer private key is optional and only configured when LANconfig is used to generate a configuration or QR code for the remote side. It is not required for LCOS functionality and is only stored so that the configuration for the remote side can be displayed or regenerated later.

Preshared key

An optional additional key used alongside the public/private key pair for the connection. The key must be configured identically on both communication partners.

IPv6 profile

This entry defines the IPv6 WAN profile. An empty entry disables IPv6 for this interface.

IPv6 WAN profiles are configured under **IPv6** > **General** > **IPv6 interfaces** > **WAN profiles**.

Persistent Keepalive

Defines the time in seconds in which the remote device (peer) should send WireGuard keepalive packets. A value of 0 disables the sending of keepalive packets.

The "Persistent Keepalive" function in WireGuard ensures that the connection remains active even when no data is being transmitted. By regularly sending keepalive packets, the connection is kept alive across intermediate NAT gateways, for example, and this helps prevent unintentional connection drops.

Comment

Enter a comment for this entry.

11.21.3.1 Configuration Profiles for Clients

Within the WireGuard configuration page, LANconfig can generate minimal configuration profiles for remote WireGuard clients in the WireGuard configuration format, either as plain text or as a QR code. This configuration can be imported into compatible WireGuard clients via copy & paste or scanned directly from a mobile app using the QR code.

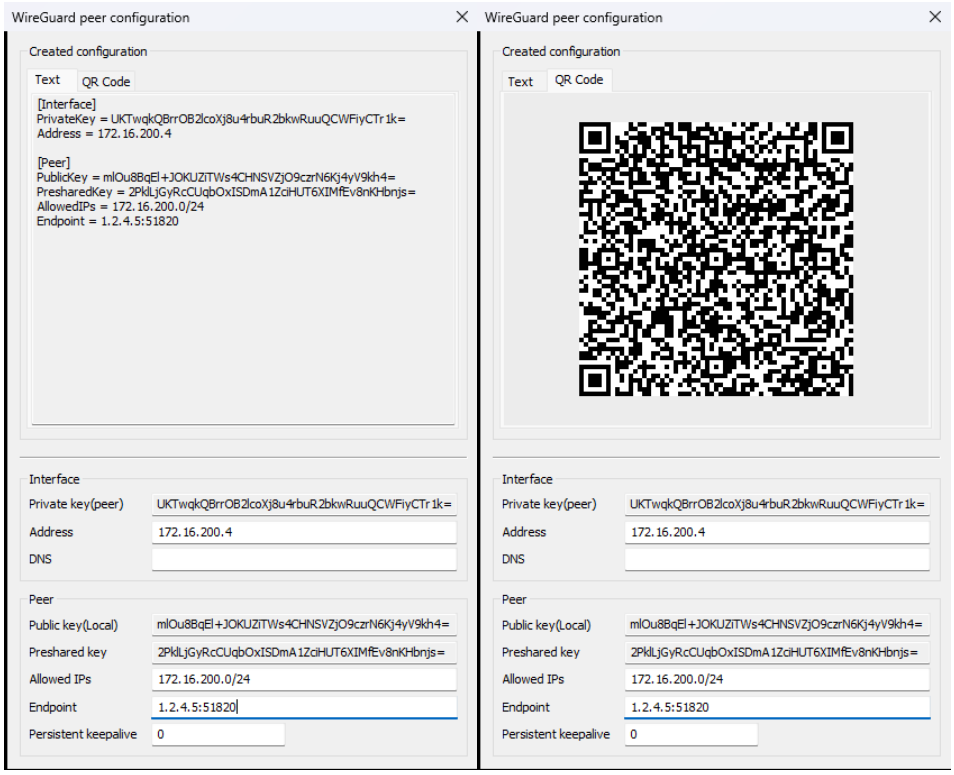
This function works similarly to a wizard, but with the advantage that the generated configuration can be recalled and displayed again at any time.

However, for this to work, the router or LANconfig must store the private key of the remote side — something that is typically undesirable when WireGuard peers belong to different administrative domains. Normally, each communication partner generates its own private/public key pair and shares only the public key with the remote side. The private key remains secret and is only known to the respective partner. This function is ideally suited for administrators who want to generate configurations for devices under their own control.

The parameters DNS and Pre-Shared Key are optional. All other parameters must be entered in order to generate a minimal configuration.

The parameters **Address**, **Allowed IPs**, and **Endpoint** are not stored by LANconfig and must be re-entered when the configuration is reopened.

To access this function in LANconfig for the respective WireGuard connection, go to **VPN** > **WireGuard** > **Connection list** > **Create peer config**.



Supported configuration parameters for the remote side:

Interface

Private key (peer)

Defines the client's private key.

Addresses

Local IP address of the WireGuard interface on the client side.

DNS

DNS server that the client should use for name resolution (optional).

Peer

From the perspective of the remote client, the LCOS device acts as the peer.

Public key (local)

Public key of the LCOS device.

Preshared key

Optional additional key used alongside the public/private key pair for the connection. The key must be configured identically on both communication partners.

Allowed IPs

IP addresses that the client should route into or allow through the WireGuard tunnel. The local networks of the router that the client should access must be specified here.

Endpoint

Public IP address including port in the format <IP address>:<Port> of the LCOS device to which the client should establish the connection.

Persistent Keepalive

Defines the time in seconds in which the remote device (peer) should send WireGuard keepalive packets. A value of 0 disables the sending of keepalive packets.

The "Persistent Keepalive" function in WireGuard ensures that the connection remains active even when no data is being transmitted. By regularly sending keepalive packets, the connection is kept alive across intermediate NAT gateways, for example, and this helps prevent unintentional connection drops.

QR Code

Using the displayed QR code, you can import the configuration into a WireGuard app. Open the WireGuard app and add a new peer via QR code. Additional parameters can then be modified or added if necessary.

12 Virtual LANs (VLAN)

12.1 What is a virtual LAN?

The increasing availability of inexpensive layer-2 switches enables the installation of much larger LANs than in the past. Until now, smaller parts of a network had been combined with hubs. These individual segments (collision domains) had been collected into larger sections by routers. A router always represents a border between two LANs, so several LANs with their own IP-address ranges arise from this structure.

By using switches, it is possible to combine many more stations into one large LAN. They specifically control the data flow on the individual ports, so the available bandwidth can be much better utilized than with hubs, and there is no need to configure and maintain routers within the network.

But even a network structure based on switches has its disadvantages:

- As with hubs, broadcasts are sent over the entire LAN, even if the data packets are only important for a certain segment of the LAN. A sufficient number of network stations thus leads to a clear reduction of the available bandwidth in the LAN.
- The entire data traffic on the physical LAN is “public”. Even if individual segments use different IP address ranges, any station on the LAN can theoretically tap into data traffic from all of the logical networks on the Ethernet segment. Protecting individual LAN segments with firewalls or routers further increases the requirements of network administration.

One possibility to resolve these problems are virtual LANs (VLANs) as described in IEEE 802.1p/q. With this concept, several virtual LANs are defined on a single physical LAN. They do not obstruct one another and, what's more, they cannot receive or tap into the data traffic of the other VLANs on the physical Ethernet segment.

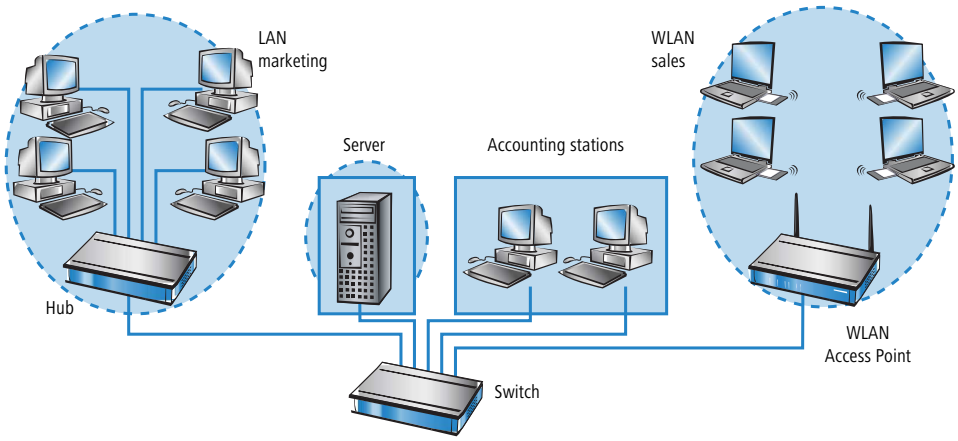
12.2 VLAN and how it works

By defining VLANs on a LAN we aim to achieve the following objectives:

- Data traffic from certain logical units should be concealed from the other network users.
- Broadcast traffic should also be restricted to these logical units, to avoid placing unnecessary load on the entire LAN.
- Data traffic from certain logical units should be handled with a higher priority for certain network users.

An example by way of illustration: In a LAN, a switch is connected to a hub, which connects 4 PCs in the Marketing department to the network. A server and two PCs in the Accounting department are connected directly to the switch.

The final segment is a wireless-network base station that connects four WLAN clients from the Sales department to the network.



The PCs from Marketing and Sales should be able to communicate with one another. The Accounting department also needs access to the server, but their communications should remain concealed from the other PCs.

12.2.1 Frame tagging

By marking data packets in a particular way, the data traffic in a virtual LAN can be concealed from the other network participants and, if required, the traffic can be prioritized. This mechanism relies on the marking of the MAC frames with an additional "tag". The procedure is referred to as “frame tagging”.

Frame tagging must be implemented so as to meet the following requirements:

- Data packets both with and without frame tagging must be able to exist in parallel on a physical LAN.
- Stations and switches on the LAN that do not support the VLAN technology need to ignore packets with frame tagging and treat them just like “normal” data packets.

Tagging is implemented by an additional field in the MAC frame. This field contains two pieces of information that are essential for the virtual LAN:

- **VLAN-ID**: The virtual LAN is distinguished by a unique number. This ID determines which logical (virtual) LAN the data packet belongs to. This 12-bit value allows up to 4094 different VLANs to be specified (the VLAN IDs 0 and 4095 are reserved or not permissible).

  Many devices use the VLAN ID 1 as the default VLAN ID. On an unconfigured device, all ports belong to this default VLAN. This assignment can be changed again during the configuration.

- **Priority**: The priority of a VLAN-tagged packet is set with a 3-bit value. 0 stands for the lowest priority and 7 for the highest. Data packets without a VLAN tag are handled with a priority of 0.

This additional field makes the MAC frames longer than is actually allowed. These oversized packets can only be correctly recognized and processed by VLAN-enabled stations and switches. For network users without VLAN support, frame tagging rather incidentally still results in the desired behavior:

- Switches that do not support VLAN simply forward these packets while ignoring the additional fields in the MAC frame.
- Stations that do not support VLAN are unable to recognize the packets' protocol and drop them silently.

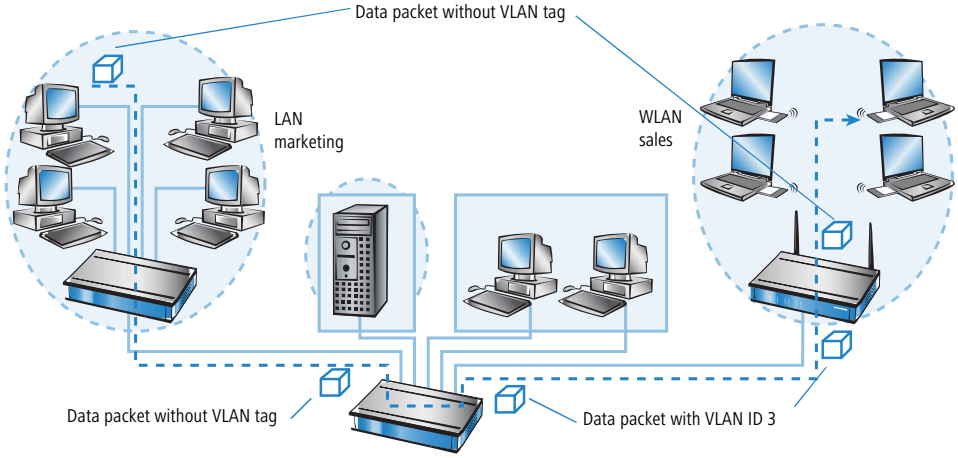
Older switches on the LAN may be unable to forward the oversize frames between the different ports, so the packets are simply dropped.

12.2.2 Implementation in the LAN interfaces

Virtual LANs are intended to group particular stations into logical units. Generally speaking however, the stations themselves are unable to generate or process the necessary VLAN tags.

The data traffic between the network participants always travels via the various interfaces of the distributors in the LAN. These distributors (switches, base stations) thus have to handle the VLAN tags in the data packets according to the particular application, in terms of creating, processing, and if necessary, removing the tags. Because the logical units are connected to the various interfaces of the distributors, the rules governing the generation and processing of VLAN tags are assigned to these individual interfaces.

Let's take up the first example again:



A computer in Marketing sends a data packet to a computer in Sales. The hub in Marketing simply forwards the packet to the switch. The switch receives the packet on port no. 1 and knows that this port belongs to the VLAN with the VLAN-ID 3. It inserts the additional field with the correct VLAN tag into the MAC frame and forwards the packet only on the ports (2 and 5) that also belong to VLAN 3. The base station in Sales receives the packet on the LAN interface. Due to its settings, the base station detects that the WLAN interface also belongs to VLAN 3. It strips the VLAN tag from the MAC frame and transmits the packet on the wireless interface. The WLAN client is able to process the packet, which now has the normal length, like any other data packet without VLAN tagging.

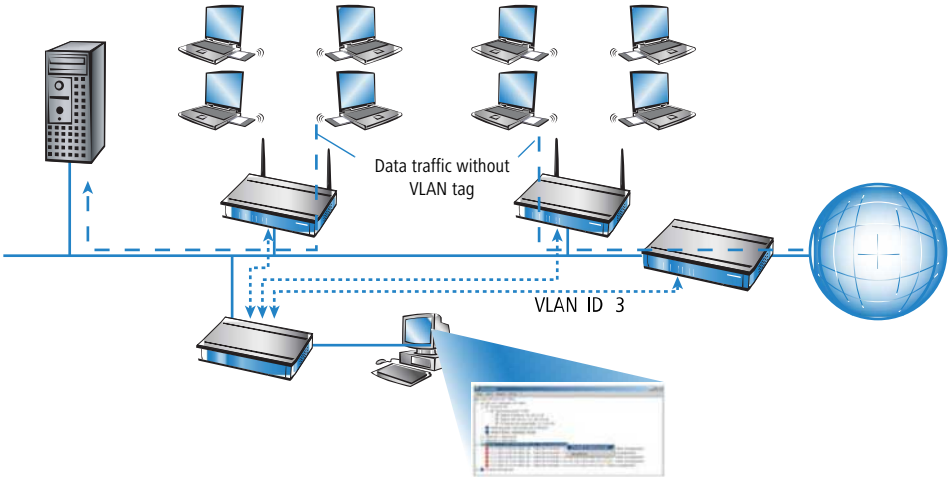
12.2.3 Example applications

The primary application of virtual LANs is the support of different logical networks—each separated into its own secure environment—on a single, shared Ethernet infrastructure.

The following sections present examples of how virtual LANs are used in this context.

12.2.3.1 User and management traffic on a LAN

Several hotspots are located on a University campus. They provide access to the library server and the Internet for students with WLAN notebooks. The hotspots are connected to the University's LAN. This LAN is also used by administrators, who access the base stations to perform various management tasks via SNMP.

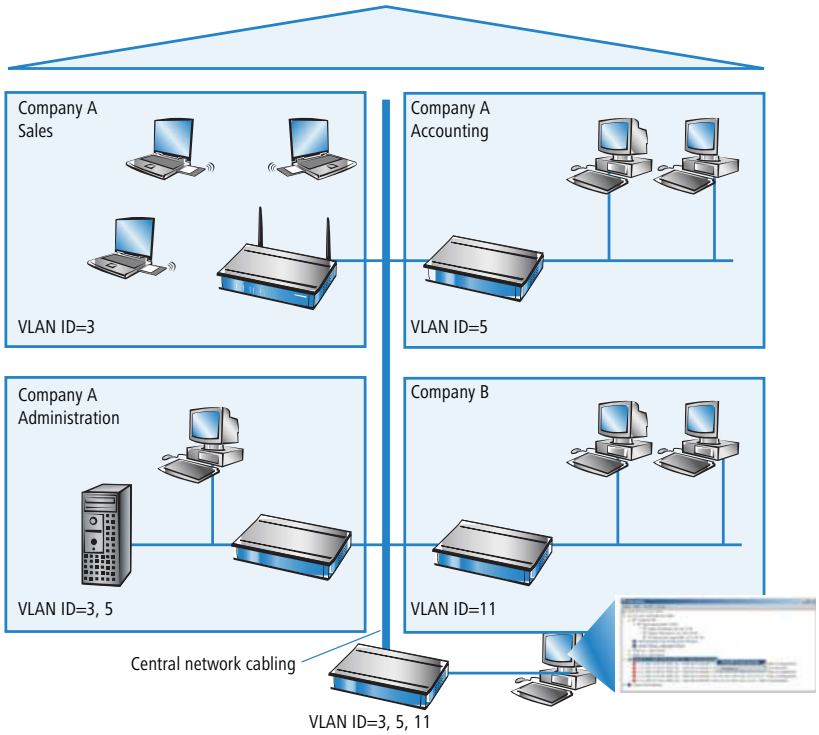


Setting up a virtual LAN between the base stations and the administrators' switch serves to protect the management traffic from the "public" traffic on the LAN.

12.2.3.2 Different organizations on a LAN

Flexibility in the modern working world brings new challenges for administrators in the design and maintenance of network structures. Office buildings are often dynamic venues where the tenants have shifting demands for space, and where even within a company, the teams are frequently reorganized. However, in both of these cases, each unit needs

to have an independent, secured LAN. Achieving this with changes to the hardware is possible either with considerable effort or not at all because, for example, the office building may be equipped with just one central cable infrastructure.



An elegant solution to this task is to use virtual LANs. Even with subsequent changes of departments or companies within the building, the network structure is easily adjusted.

All network users in this example use the central Ethernet, which is, like the connected devices, supervised by a service provider. Company A has three departments on two floors. The Sales department can communicate with the Administration department via VLAN ID 3, the Accounting department with the Administration via VLAN ID 5. The networks of the Accounting department and Sales do not see each other. Company B is also shielded by VLAN ID 11 against all other networks, only the service provider can access all devices for maintenance purposes.

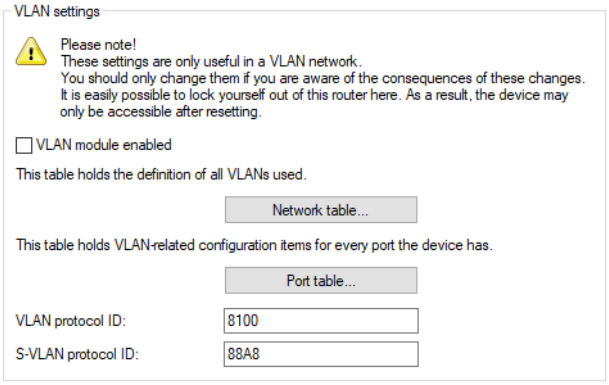
12.3 Configuration of VLANs

There are two important tasks when configuring the VLAN capabilities of the devices:

- Defining virtual LANs and giving each one a name, a VLAN ID, and allocating the interfaces
- For each interface, define how data packets with or without VLAN tags are to be handled

12.3.1 General settings

This dialog contains the general settings for the VLAN.



LANconfig: **Interfaces** > **VLAN**

Command line: **Setup** > **VLAN**

12.3.1.1 To activate the VLAN module

You should only activate the VLAN module if you are familiar with the effects this can have.

Faulty VLAN settings may cause access to the device's configuration to be blocked.

To ensure that your initial VLAN configuration works properly, you not only have to switch on the VLAN module, you also have to adjust the VLAN ID of the management IP network (typically "Intranet"). This is usually the VLAN ID 1, which is the default setting for the port VLAN ID in the VLAN module. These steps must be performed together, either using LANconfig or using the WEBconfig action under **Extras** > **Activate VLAN module**. Clicking on **Execute** enables the VLAN module and simultaneously sets the VLAN ID for all IPv4 and IPv6 networks with the VLAN ID 0 to VLAN ID 1.

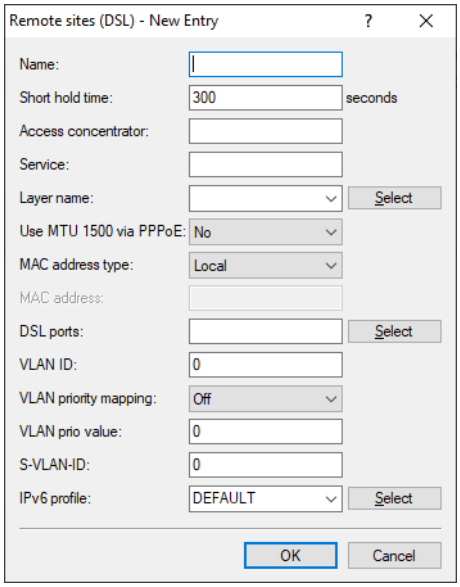
12.3.1.2 VLAN tagging mode

When transmitting VLAN tagged networks via provider networks that use VLAN themselves, providers sometimes use special VLAN tagging IDs. In order for VLAN transmission to allow for this, the Ethernet2 type of the VLAN tag can be set as a 16-bit hexadecimal value as tag value. The default is 8100 (802.1p/q VLAN tagging) other typical values for VLAN tagging could be 9100 or 9901.

12.3.1.3 Q-in-Q VLAN

The router supports VLAN double tagging ("stacked VLAN") or Q-in-Q VLAN according to IEEE 802.1ad on WAN connections. With Q-in-Q VLAN, service providers support layer-2 Ethernet connections between customer sites and so

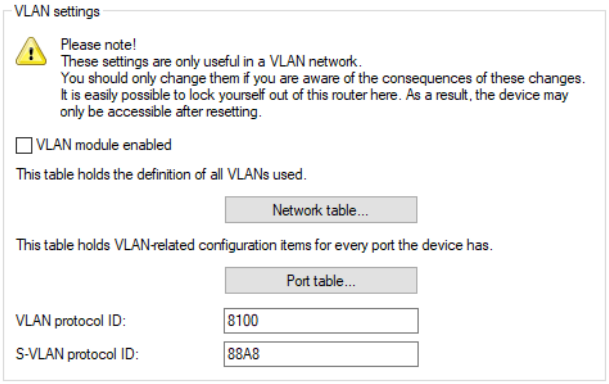
that the customer's own VLAN can be transmitted unmodified. The inner VLAN (C-VLAN) is used by the customer, the outer VLAN (S-VLAN) by the service provider.



LANconfig: **Communication** > **Remote sites** > **Remote sites (DSL)**

S-VLAN ID

Here you configure the S-VLAN for VLAN double tagging (Q-in-Q VLAN connections according to IEEE 802.1ad). The VLAN is also referred to as the outer VLAN. The S-VLAN protocol ID that is used can be configured under **Interfaces** > **VLAN**.



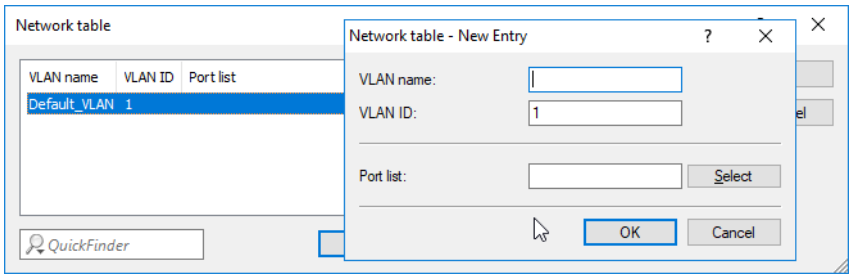
LANconfig: **Interfaces** > **VLAN**

S-VLAN protocol ID

Defines the VLAN tagging ID for Q-in-Q VLAN tagging. The Ethernet2 type of the VLAN tag is a “tag value” configured as a 16-bit hexadecimal value. The default according to IEEE 802.1ad is “88a8”, and another common value for VLAN tagging would be “8100”, for example.

12.3.2 The network table

The network table defines the virtual LANs that the device belongs to.



LANconfig: **Interfaces** > **VLAN** > **VLAN table**

Command line: **Setup** > **VLAN** > **Networks**

VLAN name

The name of the VLAN only serves as a description for the configuration. This name is not used anywhere else.

VLAN ID

This number uniquely identifies the VLAN.

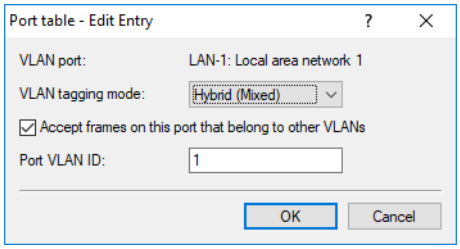
Port table

This table is used to enter the interfaces for this device that belong to the VLAN.

For a device with a LAN interface and a WLAN port, ports that to be entered could include "LAN-1" and "WLAN-1". Port ranges are defined by entering a tilde between the individual ports: "P2P-1~P2P-4".

12.3.3 The port table

The port table is used to configure each of the device's ports that are used in the VLAN. The table has an entry for each of the device's ports with the following values.



LANconfig: **Interfaces** > **VLAN** > **Port table**

Command line: **Setup** > **VLAN** > **Port-Table**

Port

The name of the port; this cannot be edited

Tagging mode

Controls the processing and assignment of VLAN tags at this port.

Access (never)

Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.

Trunk (always)

Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they are dropped.

Hybrid (mixed)

Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.

Allow all VLANs (allows packets from other VLANs to enter this port)

This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.

Port VLAN-ID

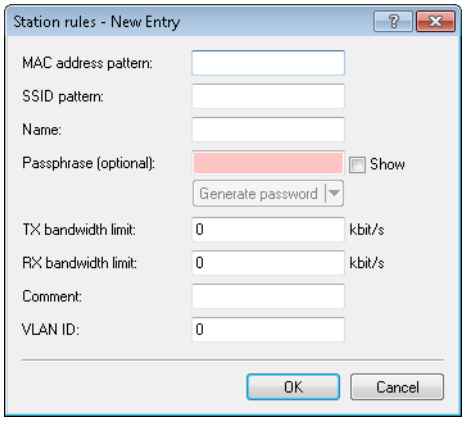
This port ID has two functions:

- Untagged packets received at this port in **Hybrid (mixed)** mode are assigned to this VLAN, as are all ingress packets received in **Access (never) mode**.
- In the **Hybrid (mixed)** mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port receive **no** VLAN tag; all others are given a VLAN tag.

12.4 Configurable VLAN IDs

12.4.1 Different VLAN IDs per WLAN client

VLANs are usually connected to a LAN interface on the device. Therefore, all packets that pass through this interface receive the same VLAN ID when the VLAN module is enabled. However, in some cases, administrators will want to assign different WLAN users to different VLANs.



LANconfig: **Wireless LAN** > **Stations/LEPS** > **Station rules**

Command line: **Setup** > **WLAN** > **Access-List**

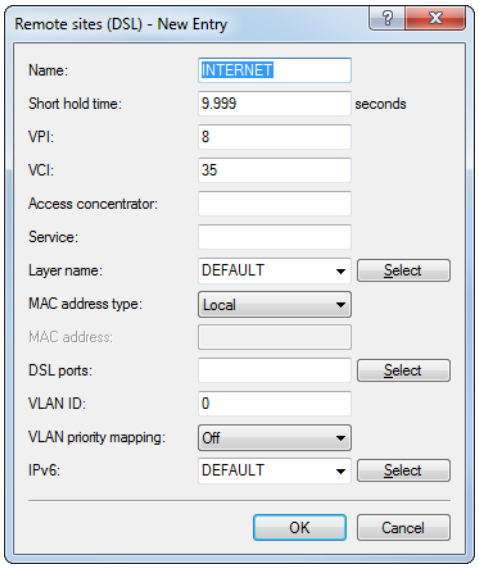
The client-specific VLAN ID accepts values from 0 to 4094. The default value of 0 stands for an unspecified VLAN ID. In such a case, the client will be assigned to the VLAN port of the logical WLAN.

The following requirements must be met in order to ensure successful client-specific VLAN assignment:

- VLAN operation must be enabled.
- The VLAN IDs that are to be assigned to the individual clients must be included in the VLAN network table.
- The LAN interfaces and all WLAN interfaces that are used by the clients must be assigned to the corresponding VLAN.

12.4.2 VLAN IDs for DSL interfaces

Some DSL networks use VLAN tags in the same way as they are used in local networks to differentiate between logical networks on shared transmission media. The router can process these VLAN tags correctly if a VLAN ID is defined for each DSL remote site.



LANconfig: **Communication** > **Remote sites** > **Remote sites (DSL)**

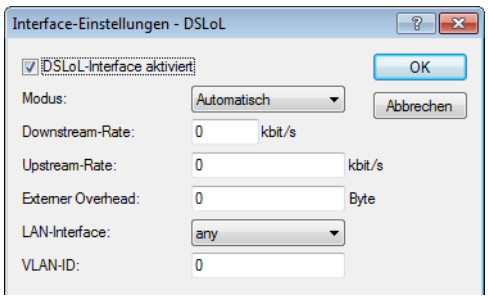
Command line: **Setup** > **WAN** > **DSL-Broadband-Peers**

VLAN ID

ID used to explicitly identify the VLAN over the DSL connection.

12.4.3 Special VLAN IDs for DSLoL interfaces

In order to better separate the data traffic on a DLSoL interface from other traffic, the **VLAN ID** for the DSLoL interface can be set up under **Setup** > **Interfaces** > **DSLoL** or in LANconfig under **Interfaces** > **WAN** > **Interface settings**.



12.5 VLAN tags on layer 2/3 in the Ethernet

12.5.1 Introduction

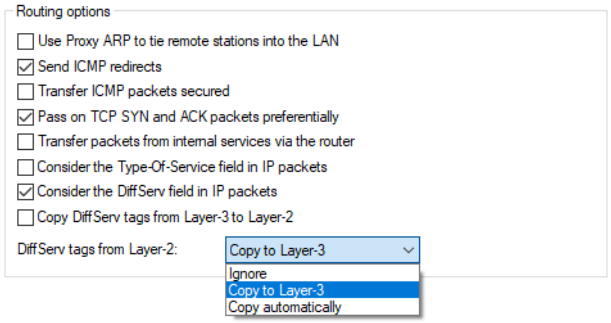
VLAN tags enable a simple form of QoS control even when using switches that cannot evaluate IP headers. The IEEE 802.1p standard defines a priority tag in the VLAN header with a length of 3 bits, which correspond to the first 3 bits of the DSCP fields (Differentiated Services Code Point – DiffServ) and/or the precedence in the ToS field (Type of Service). The processing of VLAN tagged packets requires that packets in the receive direction are regarded differently to packets in the send direction.

- Upon receipt of a tagged Ethernet packet, it may be processed in one of three ways:
  - The VLAN tag is ignored.
  - The VLAN tag is always copied to the DiffServ or TOS field.
  - The VLAN tag is copied to the DiffServ or TOS field if this is not marked already, i.e. the precedence is '000'.
- When a packet is transmitted over Ethernet, the VLAN tag can be set depending on the precedence. This should only happen if the recipient of the tag can understand it, i.e. tagged packets can be received. Tags are thus only set for packets which are sent to addresses from which the LCOS already received tagged packets.

When a tagged packet is received, the tag is saved to the associated entry in the connection list. If a packet is to be sent with a precedence setting, then the VLAN ID recorded earlier is entered into the packet together with the precedence to form a VLAN tag. Where a connection causes other connections to be opened, e.g. with FTP, then the tag is inherited to the new entries.

12.5.2 Configuring VLAN tagging on layer 2 / 3

Configuring VLAN tagging on layer 2 / 3 involves the definition of the general routing settings and the behavior upon receipt and transmission of tagged packets.



LANconfig: **IP router** > **General**

Command line: **Setup** > **IP-Router** > **Routing-Method**

Interpret the type-of-service field

The TOS / DiffServ field is regarded as a TOS field; the bits 'low delay' and 'high reliability' are evaluated.

Consider the DiffServ field in IP packets

The TOS / DiffServ field is regarded as a DiffServ field. After evaluating the precedence, packets with the code points AFxx are saved and packets with the code points EF receive preferential treatment. All other packets are transmitted as normal.

DiffServ tags from Layer 2

The setting for Layer2-Layer3 tagging regulates the behavior when a data packet is received.

Ignore

VLAN tags are ignored.

Copy to layer 3

Priority bits in the VLAN tag are always copied to the precedence of the DSCP.

Copy automatically

Priority bits in the VLAN tag are only copied to the DSCP precedence if this is '000'.

Copy DiffServ tags from layer 3 to layer 2

The setting for Layer3-Layer2 tagging regulates the behavior when a data packet is transmitted. With this option enabled, VLAN tags with priority bits originating from the DSCP precedence are generated if the recipient has sent at least one tagged packet.

13 Wireless LAN – WLAN

13.1 Introduction

The following sections are a general description of the LCOS operating system functions relating to wireless networks. The functions provided by your specific device are outlined in the manual supplied with it.

This chapter gives you a brief introduction to wireless networking technology. It also provides an overview of the many different applications, fraction and capabilities of LANCOM WLAN devices.

A wireless LAN connects individual end-user devices (PCs and mobile computers) to form a local network (also called – **L**ocal **A**rea **N**etwork). In contrast to a traditional LAN, communication takes place over a wireless connection and not over network cables. In this case we refer to a radio LAN as a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

A wireless LAN provides the same functionality as a cable-based network: Access to files, servers, printers etc. as well as the integration of individual work stations into a corporate mail system or access to the Internet.

There are obvious advantages to wireless LANs: Notebooks and PCs can be installed where they are needed—problems with missing connections or structural changes are a thing of the past with wireless networks. Apart from that, wireless LANs can also be used for connections over longer distances. Expensive leased lines and the associated construction measures can be saved.

LANCOM Systems differentiates between two different types of WLAN device, each with its own field of application and consequently offering specialized functions and configuration options.

- Access points or APs are generally used to connect one or more WLANs to a cabled LAN. As such, they merely function as a "bridge" to transfer data to and from the clients. Routing into the Internet or to other remote stations is handled by other network components. APs generally have just one or more Ethernet interfaces.
- In addition to one or more Ethernet interfaces, LANCOM wireless routers are equipped with WAN interfaces for VDSL, ADSL and/or DSL. In a single device, they combine WLAN functions with the task of routing data into the Internet or to other remote stations.

The following sections mostly refer to "access points" as a synonym for both types of device, unless we explicitly differentiate between a LANCOM wireless router and a LANCOM access point.

The devices operate either as standalone APs with their own configuration (WLAN modules in "access point mode") or as components in a WLAN infrastructure, which is controlled from a central WLAN controller ("managed mode").

13.2 Application scenarios

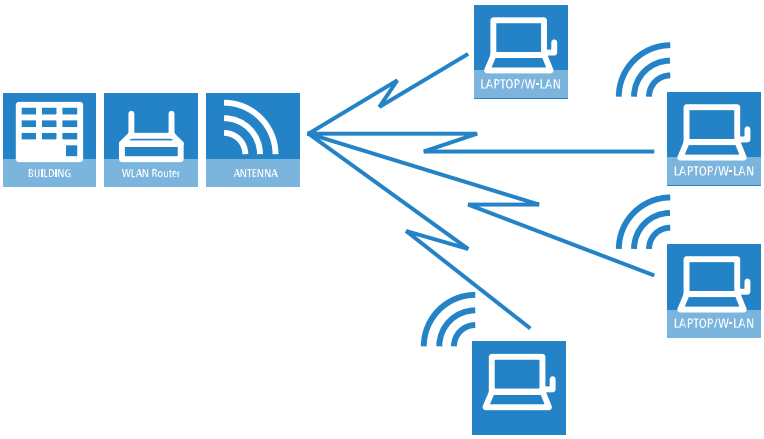
Wireless LAN systems can act as an extension to or even as a replacement for cabled networks. In some cases wireless LANs even provide completely new application possibilities, which can mean a major advance in the way work is organized, or significant cost savings.

- Extensive wireless LANs, possibly connected to a LAN, with one or more APs (infrastructure mode)
- Hotspot or guest access
- Connecting two LANs over a wireless link (point-to-point mode)
- Relay function for connecting networks via multiple APs
- Connecting devices with an Ethernet interface via an AP (client mode)

- Central management by a WLC (managed mode)
- WDS (Wireless Distribution System)
- Data transfer to mobile objects in industrial environments.
- Transmission of VPN-encrypted connections with VPN pass through
- Simple, direct connection between terminal devices with an AP (ad-hoc mode)

13.2.1 Infrastructure mode

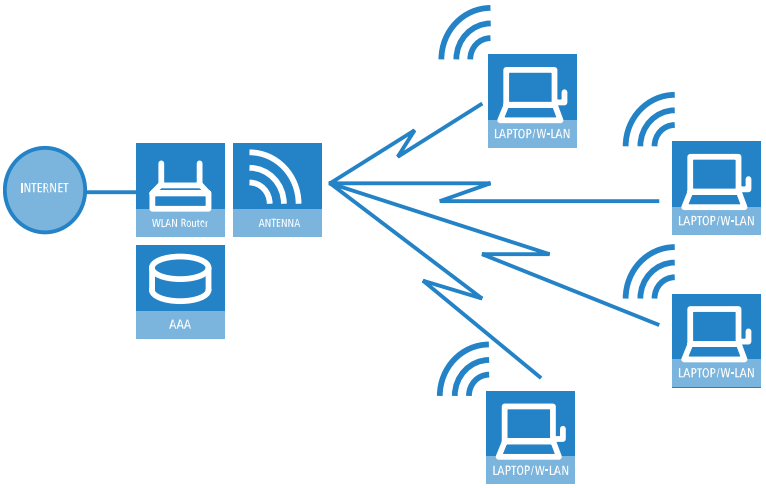
In infrastructure mode, WLAN clients connect to a central AP. The AP provides one or more wireless LAN networks. It regulates the client's rights to access the radio cell, communications between the clients, and access to further networks. In larger scale WLAN scenarios (e.g. in companies with offices extending between several buildings or floors) multiple APs can provide WLAN clients with access to a common, shared network. The clients can roam between the different APs, if necessary. A common term used here is “campus coverage” because this solution is used by a large number of colleges and universities to provide students and staff with network access.



13.2.2 Hotspot or guest access

A hotspot is a special variant of the infrastructure mode described above. Whereas the normal infrastructure mode provides the members of a closed user group with access to a network that includes all the necessary services, a hotspot provides network access (generally restricted to Internet only) to wireless LAN clients at a fee. In addition to the differences in AP configuration, setting up a hotspot requires authentication, authorization and accounting (AAA) functions such as those provided by the Public Spot options. Hotspots are generally set up at public locations where people have a short-term need to access the Internet, such as at airports, cafés or hotels.

A hotspot provides network access to a WLAN client for a limited time period and without having to configure the AP. This method is often used by companies, for example to provide guests with temporary Internet access.

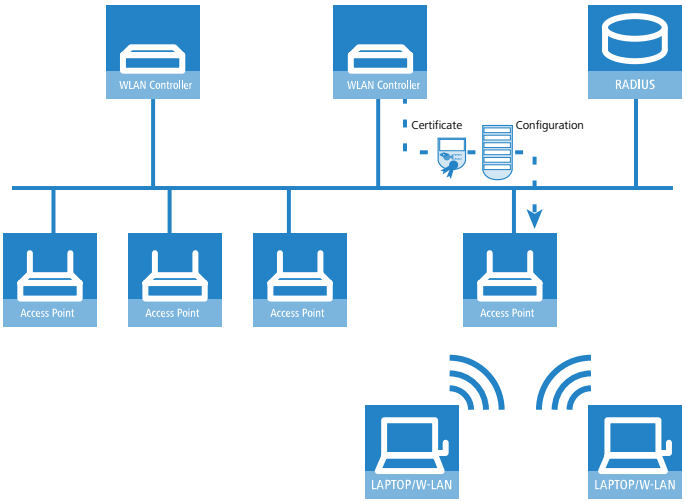


13.2.3 Managed mode

The widespread use of wireless devices provides great convenience and flexibility in network access for businesses, universities and other organizations. With centralized WLAN management, the APs in managed mode are not configured themselves but at a central location, the WLAN controller (WLC).

The WLC authenticates the APs and transmits a certificate and the correct configuration to any approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the APs simultaneously.

Split management can be used to separate the WLAN configuration from the rest of the router configuration. This allows router settings and VPN settings to be adjusted locally, for example in a branch office or home office installation, and the WLAN configuration is regulated by a LANCOM WLAN controller at the main office.

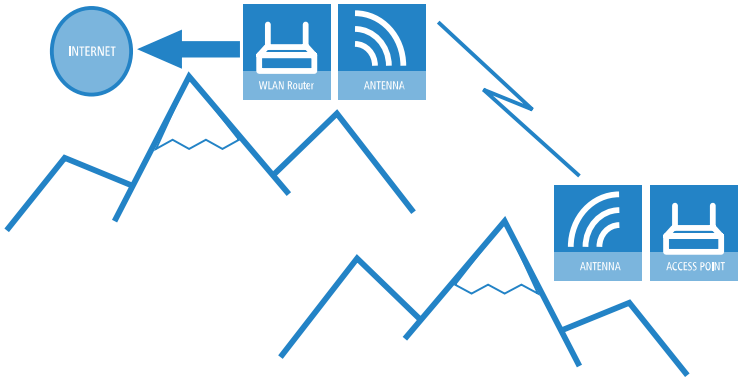


13.2.4 WLAN bridge (point-to-point)

Whereas the scenarios discussed so far have involved connecting multiple WLAN clients to one AP (point-to-multipoint), outdoor wireless LAN systems are particularly advantageous for providing a link between two APs (point to point). By setting up a wireless link between two APs, a distant production building on extensive company premises can be very easily integrated into the company network, for example.



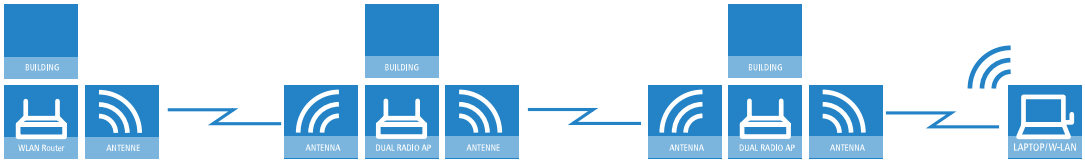
A point-to-point connection can also be used in difficult terrain (such as mountainous areas or islands) to provide Internet access in areas where cabling would be too expensive. With a direct line of sight between the two APs, distances of several kilometers can be bridged by this type of wireless link.



13.2.5 WLAN bridge in relay mode

In some cases, the distance between the two locations to be connected exceeds the range of a single wireless link. This may be the case when the distance between the APs exceeds the radio range, or when obstacles block the line of site between the two APs.

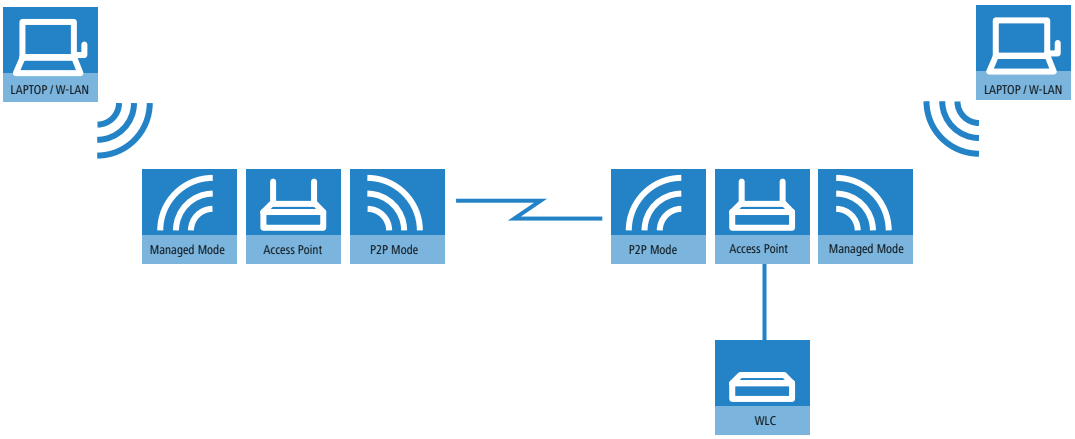
In these cases, the two end points can be connected by stringing together multiple APs, each of which has two WLAN modules. Because the intermediate APs often operate solely as relay stations, the operating mode of these APs is referred to as “relay mode”.



Even though the radio module of any LANCOM AP can operate several P2P links and support wireless LAN clients all at the same time, for performance reasons we recommended that relay stations be equipped with LANCOM APs with two wireless modules.

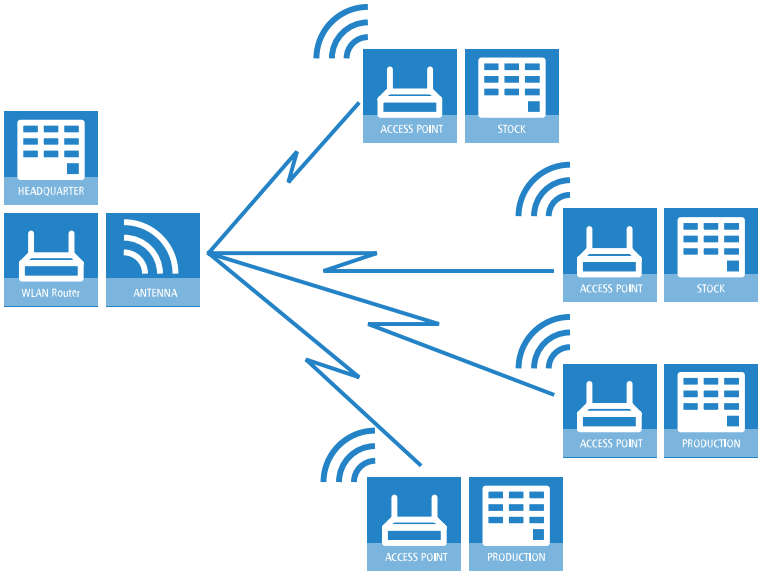
13.2.6 WLAN bridge to the AP – managed and unmanaged mixed

APs managed from a central WLC are generally connected to the network via cabled Ethernet. Where this is not possible, managed APs can be integrated into the LAN via a WLAN bridge, assuming that the APs are equipped with two WLAN modules. In this scenario, one WLAN module operates as a managed AP which obtains its configuration from the central WLC. The other WLAN module is permanently configured as a WLAN bridge.



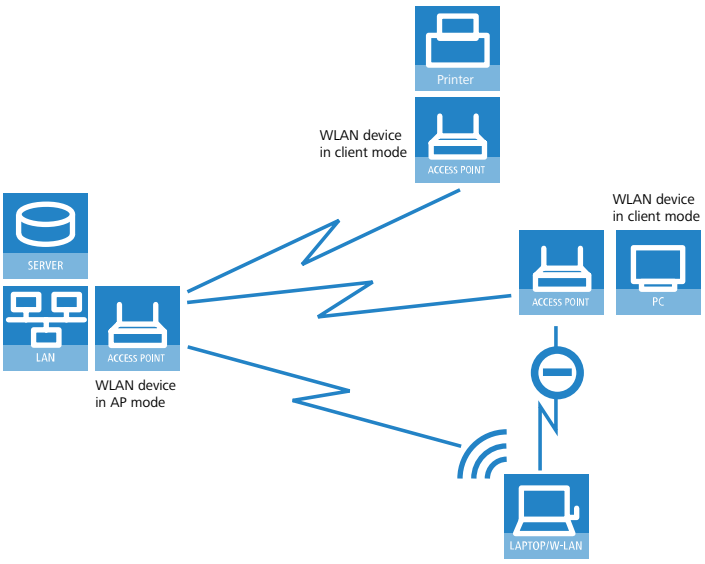
13.2.7 Wireless distribution system (point-to-multipoint)

A special type of wireless link is the connection of several distributed APs to a central point – the point-to-multipoint wireless LAN (P2MP) is also referred to as a Wireless Distribution System (WDS). This mode of operation allows for example several buildings on a company's premises to be connected to the central administrative building. The central AP or wireless router is configured as “master” and the remote WDS stations as “slaves”.



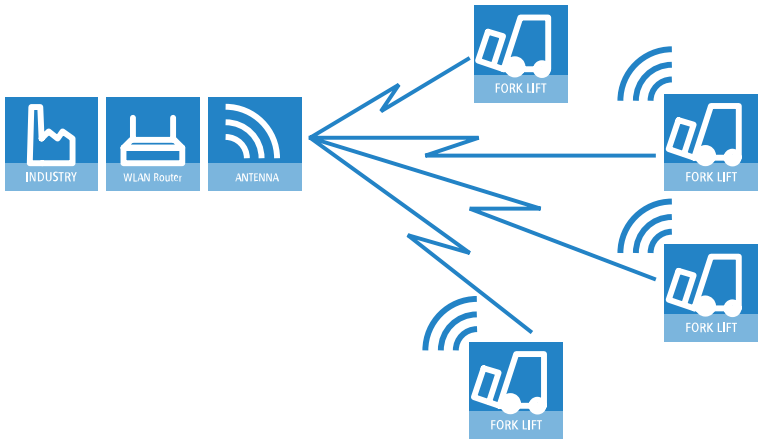
13.2.8 Client mode

In order for individual devices equipped with an Ethernet interface to be connected to a wireless LAN, APs can be switched to client mode, in which they act as conventional wireless LAN adapters and not as APs. The use of client mode therefore allows devices fitted with only an Ethernet interface, such as PCs and printers, to be integrated into a wireless LAN.



13.2.9 Client mode with mobile objects in industry

Completely new applications allow wireless LAN systems in industrial environments to transmit data to mobile objects. In logistics, for example, this means that fork-lift trucks can stay continuously connected to the company network via the wireless LAN. In combination with mobile barcode scanners, inventory movements within a warehouse can be monitored in real time and passed on to an ERP system, which then provides all employees with up-to-the-minute information on current inventories at all times.



13.3 WLAN standards

LANCOM WLAN devices operate with the IEEE 802.11 standard. This is a collection of standards that build on the earlier IEEE standards for LANs. The best known of these is IEEE 802.3 for Ethernet. Among the various IEEE 802.11 standards, some specify wireless transmissions in different frequency bands and at different speeds.

By complying with these IEEE standards, LANCOM WLAN products operate with devices from other manufacturers reliably and without problems.

The WLAN module in the APs only operates in one frequency band at a time, i.e. either at 2.4 GHz or 5 GHz. It is impossible for a single WLAN module to operate at different frequencies simultaneously. However, APs with two WLAN modules (dual radio) can operate each module at a different frequency (depending on the hardware). As the standards are backwards compatible, different standards can be operated simultaneously on a single WLAN module, although this will result in lower data rates.

13.4 WLAN security

13.4.1 Basics

Even though one constantly hears the blanket term “Security” when talking about computer networks, it is still important for the coming exposition to differentiate a little more closely between the requirements it actually entails.

13.4.1.1 Authentication

The first point in security is access security:

- Here, a protective mechanism is involved which allows access to the network only to authorized users.
- On the other hand, however, it must also be ensured that the client is connected to the precise desired AP, and not to some other AP with the same name which has been smuggled in by some nefarious third party. Such an authentication can be provided, for example, using certificates or passwords.

13.4.1.2 Authenticity

Authenticity: Proof of the authorship of the data and the originality of the data content; the process of establishing this proof is known as authentication.

13.4.1.3 Integrity

Once access is provided, one would like to ensure that data packets reach the receiver without any falsification, that is, that no-one can change the packets or insert other data into the communication path. The manipulation of data packets themselves cannot be prevented, but changed packets can indeed be identified using suitable checksum processes, and then dropped.

13.4.1.4 Confidentiality

Quite separate from access security is confidentiality, that is, unauthorized third parties must not be able to read the data traffic. To this end, the data are encrypted. This sort of encryption process is exemplified by AES or RC4. Along with encryption, of course, there must also be a corresponding decryption on the receiving end, generally with the same key (a so-called symmetric encryption process). The problem naturally then arises, how the sender can give the key to the receiver for the first time—a simple transmission could very easily be read by a third party, who could then easily decrypt the data traffic.

In the simplest case, this problem is left to the user, that is, one simply assumes that the user can make the key known at both ends of the connection. In this case, we refer to pre-shared keys, or PSK.

More sophisticated processes come into play when the use of PSK is impractical, for instance in an HTTP connection established with SSL—in this case, the user can't retrieve a key from a remote web server quite so easily. In this case, so-called asymmetric encryption methods such as RSA can be used, that is, to **de**crypt the data, a different key is used than the one used to **en**crypt it, meaning that key pairs are used. Such methods are, however, much slower than symmetric encryption methods, which leads to a two-phase solution:

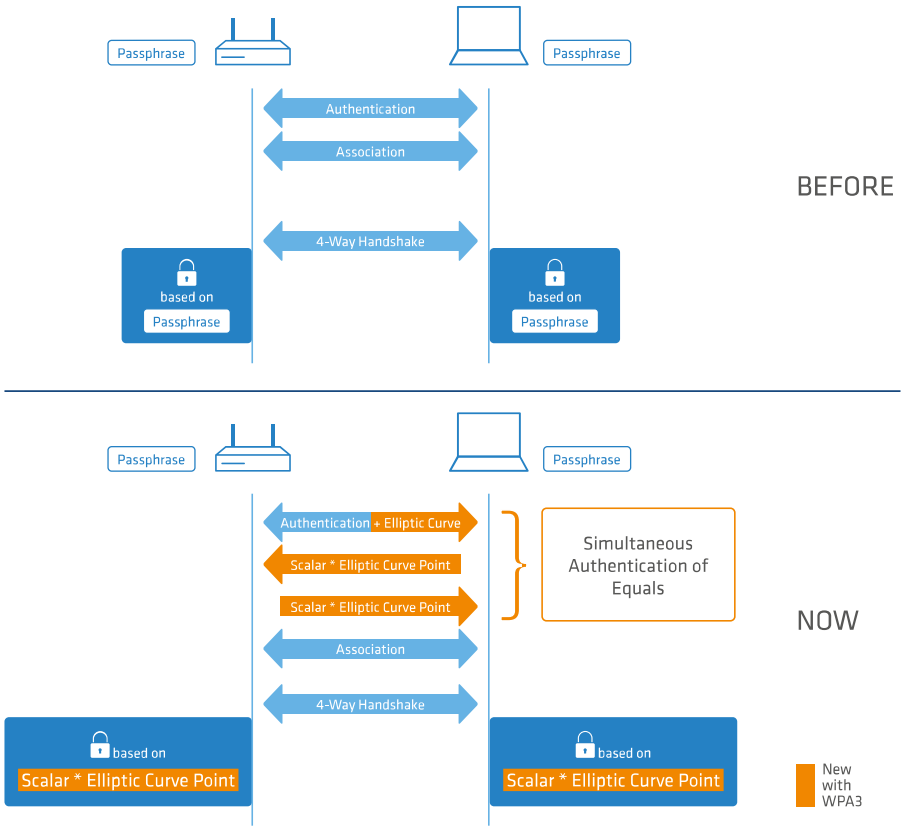
- The sender possesses an asymmetric key pair. It transmits the public part of the key pair, i.e. the key for **en**cryption, to the receiver as a certificate, for example. Since this part of the key pair cannot be used for **de**cryption, there are no misgivings with regard to security.

› The receiver selects any symmetrical key. This symmetrical key that is used both for **en**cryption and for **de**cryption, must now be securely transmitted to the sender. It is encrypted with the sender's public key and returned to the sender. The only way that the symmetrical key can be decrypted again is with the sender's private key. Potential eavesdroppers observing the key exchange cannot decrypt this information, and consequently the transmission of the symmetrical key is secure.

13.4.2 WPA3 (Wi-Fi Protected Access 3)

Compared to the predecessor standard WPA2 introduced by the Wi-Fi Alliance in 2004, the WPA3 standard introduced in 2018 offers improved security by combining various security methods. Like WPA2, WPA3 also exists in the versions WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) authentication method, which only requires a password for authentication but which prevents brute-force and dictionary attacks. Furthermore, for the first time this method offers forward secrecy, i.e. captured WPA3-secured traffic cannot be decrypted subsequently after the attacker gains knowledge of the pre-shared key.



Also available with WPA3 is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Both variants now require the use of protected management frames (PMF) according to IEEE 802.11w. PMF prevents attackers from computing the WLAN password from captured material gained by using fake management frames to force a disassociation and then eavesdropping the re-authentication.

13.4.2.1 WPA3-Personal

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

With **WPA3** selected, only WLAN clients that support WPA3-Personal will be able to login. This configuration enforces authentication with the Simultaneous Authentication of Equals (SAE). Similarly, this SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

13.4.2.2 WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Rather, it set out policies to ensure greater consistency in the application of these protocols and to assure the desired level of security.

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

By selecting **WPA3**, only WLAN clients that support WPA3-Enterprise will be able to log in. This SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

Suite B cryptography

Also available is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

The switch **WPA 802.1X security level** under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings** is used to enable the optional Suite B encryption. With “Suite B 192 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

With “Suite B 128 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-128 is also enforced.

Because the session key types AES-GCMP-128 and AES-GCMP-256 are not supported by all WLAN modules, the use of Suite B cryptography may be limited or impossible, depending on the device type.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

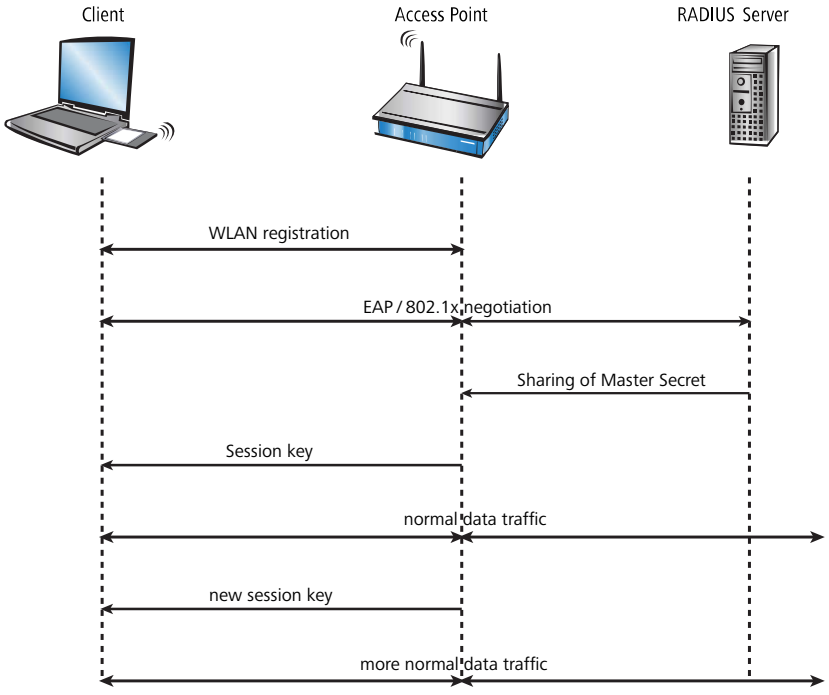
13.4.3 IEEE 802.11i / WPA2

In mid-2004 the IEEE adopted the standard 802.11i, also known as WiFi Protected Access 2 (WPA2). WPA2 enables the authentication and authorization of users by IEEE802.1X and it supports AES encryption, which is a far more secure method than WEP or WPA. The following sections outline some relevant technical aspects.

13.4.3.1 EAP and IEEE 802.1X

A clear increase in WLAN security can be achieved by using keys that are dynamically negotiated instead of keys with fixed values. The established process for this purpose is the Extensible Authentication Protocol (EAP). As the name suggests, the original purpose of EAP is authentication, that is, the regulated access to a WLAN—the possibility of installing a valid key for the next session is more or less a byproduct. The figure below illustrates the basic procedure of a session secured by EAP.

In principle, EAP / 802.1X can be used in combination with WEP. However, this method is generally employed with WLANs using WPA2.



In the first phase, the client registers with the AP as usual, and enters the state in which it can now send and receive over the AP in the formerly used WEP—but not with EAP, because in this state the client still doesn't have a key to secure its data traffic from eavesdropping. Instead, the client is in an 'intermediate state' from the point of view of the AP, in which only particular packets from the client are forwarded, and these are only directed to an authentication server. These packets are the EAP/802.1X mentioned previously. The AP packs these packets in RADIUS queries and sends them on to the authentication server. The AP converts the replies from the RADIUS server back into EAP packets, and returns them to the client.

The AP is thus a sort of middle man between client and server: It doesn't have to check the contents of these packets, it just has to check that no other data traffic to or from the client can occur. Over this "tunnel" through the AP, the client and server authenticate one another, that is, the server checks the client's access privilege to the network, and the client checks that it is talking to the right network. This helps to detect "rogue" access points set up by hackers.

A whole series of authentication processes exist which can be used in this tunnel. A common method is for instance TLS, in which server and client exchange certificates; another is TTLS, in which only the server supplies a certificate—the client is authenticated using only a user name and password.

After the authentication phase, a secure tunnel even without encryption has been set up, in which the AP is connected in the next step. For this, the RADIUS server sends the so-called 'Master Secret', a session key calculated during the negotiation, to the AP. The LAN behind the AP is considered secure in this scenario, so that this transmission can be performed in cleartext.

With this session key, the AP now takes over the tunnel and can use it to provide the actual key to the client. Depending on the capabilities of the access point hardware, this can be a true session key, i.e. a key which will only be used for data packets between the AP and precisely this client. Older WEP uses a hardware group key, which the AP will use for communication with multiple clients.

The particular advantage of this procedure is that the AP can regularly change the key over the EAP tunnel, that is, it can perform a so-called rekeying. In this way, keys can be replaced by new ones long before they run the risk of being cracked due to IV collisions. A common 'use time' for such keys might be 5 minutes.

Status counters for IEEE 802.1X login attempts

A table showing the number of accepted and rejected connect requests for each logical interface is located in the LCOS menu tree under **Status** > **IEEE802.1x** > **Ports**.

The overview also indicates the number of times the authorization limit was reached for each interface.

Ports

Port	Num-Accept	Num-Reject	Num-ReauthMax-reached
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

13.4.3.2 WPA with passphrase

The handshake described in the EAP/802.1X section runs strictly under WPA, i.e. the user will never have to define any keys. For environments where no RADIUS server is available to provide master secrets (for instance in smaller companies), WPA provides the PSK method. In this case the user enters an 8 – 63 character passphrase on the access point and on all other stations: This passphrase is used together with the SSID to calculate the master secret with a hash method. The master secret is therefore constant in such a PSK network, although different session keys still result.

In a PSK network both access security and confidentiality depend on the passphrase not being divulged to unauthorized people. As long as this is the case, WPA-PSK provides significantly improved security against break-ins and eavesdropping

over any WEP variant. For larger installations in which such a passphrase would have to be made known to too large a user community for it to be kept secret, EAP/802.11X is used in combination with the key handshake described here.

Access points and wireless routers with their standard factory settings cannot be commissioned by means of the WLAN interface. The WLAN modules are switched off. The access points search the LAN for a WLC which will supply a configuration profile.

Status counters for WPA-PSK login attempts

An overview of the number of failed WPA-PSK login attempts is located in the LCOS menu tree under **Status** > **WLAN** > **Encryption**.

There is also an overview of successful login attempts, as well as the number of authorizations rejected due to an incorrect passphrase.

Encryption

Interface	Encryption	Method	WPA-Version	WPA1-Session-Keytypes	WPA2-Session-Keytypes	PMK-Caching	Pre-Authentication	OKC	Prot.-Mgmt-Frames	WPA2-Key-Management	WPA-PSK-Num-Success	WPA-PSK-Num-Failures	WPA-PSK-Num-Wrong-Passphrase
WLAN-1	Yes	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-2	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-3	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-4	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-5	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-6	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0

Select an interface in the table (e.g. WLAN-1) to display the information for the selected interface.

Encryption

Interface	WLAN-1
Encryption	Yes
Method	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Session-Keytypes	TKIP/AES
WPA2-Session-Keytypes	TKIP/AES
PMK-Caching	Yes
Pre-Authentication	Yes
OKC	No
Prot.-Mgmt-Frames	No
WPA2-Key-Management	Standard
WPA-PSK-Num-Success	0
WPA-PSK-Num-Failures	0
WPA-PSK-Num-Wrong-Passphrase	0

13.4.3.3 TKIP

The Temporal Key Integrity Protocol (TKIP) was a temporary solution for use until the introduction of a stronger encryption method, but it at least dealt with the problems of the then popular WEP. Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

If an SSID uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

13.4.3.4 AES

The most obvious extension is the introduction of a new encryption process, namely AES-CCM. As the name already suggests this encryption scheme is based on AES, the successor to DES, unlike WEP and TKIP, which are both based on RC4. Not all older WLAN clients support TKIP, so 802.11i continues to specify TKIP, although with the opposite prerequisites: Any 802.11i-compliant hardware must support AES, while TKIP is optional. In WPA, this was exactly the other way around, with the use of AES being optional. With WPA3, the only permitted security methods are those

considered to be secure at the time of adoption. Methods such as TKIP, with known security vulnerabilities, may no longer be used.

The suffix CCM denotes the way in which AES is used in WLAN packets. The process is actually quite complicated, for which reason CCM is only sensibly implemented in hardware—software-based implementations are possible, but would result in significant speed penalties due to the processors commonly used in access points.

In contrast to TKIP, AES only requires a 128-bit key for the encryption and protection against packet falsification. Furthermore, CCM is fully symmetric, i.e. the same key is used in both communications directions—a standards compliant TKIP implementation, on the other hand, requires the use of different Michael keys in the send and receive directions, meaning that CCM is significantly easier in use than TKIP.

Like TKIP, CCM uses a 48-bit Initial Vector in each packet—an IV repetition is impossible in practice. As in TKIP, the receiver notes the last IV used and drops packets with an IV which is equal to or less than the comparison value.

13.4.3.5 Pre-authentication and PMK caching

802.11i helps with the use of WLAN for speech connections (VoIP) in enterprise networks. Especially in connection with WLAN-based wireless telephony, quick roaming (switching from one AP to another without lengthy interruptions) is of special significance. In telephone conversations, interruptions of 100 milliseconds are irritating, but the full authentication process over 802.1X, including the subsequent key negotiation with the AP, can take significantly longer.

For this reason, the so-called PMK caching was introduced as a first measure. The PMK serves as the basis for key negotiation in an 802.1X authentication between client and access point. In VoIP environments it is possible that a user moves back and forth among a relatively small number of APs. Thus it may happen that a client switches back to an AP in which it was already registered earlier. In this case it makes no sense to repeat the entire 802.1X authentication. For this reason, the AP provides the PMK with a code called the PMKID, which it transmits to the client. Upon a new registration, the client uses the PMKID to ask whether this PMK is still stored. If yes, the 802.1X phase can be skipped and the connection is quickly restored. This optimization is unnecessary if the PMK in a WLAN is calculated from a passphrase as this applies everywhere and is known.

Another measure allows for some acceleration even in the case of first-time authentication, but it requires a little care on the part of the client: The client must detect a degrading connection to the AP during operation and select a new access point while it is still in communication with the old AP. In this case it has the opportunity to perform the 802.1X negotiation with the new AP over the old one, which again reduces the "dead time" required for the 802.1X negotiation.

13.4.4 TKIP and WPA

As clarified in the last section, the WEP algorithm is flawed and insecure in principle; the measures taken so far were largely either 'quick fixes' with limited improvement, or so complicated that they were basically impractical for home use or smaller installations.

After the problems with WEP became public knowledge, the IEEE began with the development of the standard IEEE 802.11i. As an interim solution, the Wi-Fi Alliance defined the Wi-Fi Protected Access (WPA) 'standard'. WPA uses the following changes:

- TKIP and Michael as replacement for WEP
- A standardized handshake procedure between client and AP for determination/transmission of the session key.
- A simplified procedure for deriving the Master Secret mentioned in the last section, which can be performed without a RADIUS server.
- Negotiation of encryption procedure between AP and client.

Encryption makes use of components familiar from WEP but benefits from decisive improvements with the "Michael hash" from improved encryption and the TKIP method for calculation of the RC4 key. Furthermore, the internally incremented IV transmitted in cleartext in the packet is 48 bits long instead of 24--thus the problem with the repeating IV value is practically excluded.

As a further detail, TKIP also mixes the MAC address of the sender into the calculation of the key. This ensures that the use of identical IVs by different senders cannot lead to identical RC4 keys and thus again to attack possibilities.

The Michael hash does not, however, represent a particularly tough cryptographic hurdle: If the attacker can break the TKIP key or get encrypted packets past the CRC check via modifications similar to those for WEP, then not many barriers remain. For this reason, WPA defines countermeasures if a WLAN module detects more than two Michael errors per minute: Both the client and the AP break data transfer off for one minute, afterwards renegotiating the TKIP and Michael keys.

Over time, ways are found to compromise the encryption protocols. The Wi-Fi Alliance has counteracted this with the WPA2 and later the WPA3 certification standards, which implement more modern encryption methods while prohibiting the use of methods that are known to be insecure.

13.4.4.1 Negotiating the encryption method

Since the original WEP definition specified a fixed key length of 40 bits, the only option when a client associated at an AP was whether encryption should be used or not. Key lengths exceeding 40 bits require the key length to be announced. WPA provides a mechanism with which client and AP can agree on the encryption and authentication procedures to be used. The following information is made available:

- A list of encryption methods which the AP provides for the pairwise key—here, WEP is explicitly disallowed.
- A list of authentication methods a client may use to show itself to the WLAN as authorized for access—available methods include EAP/802.1X or PSK.

As mentioned, the original WPA standard specifies only TKIP/Michael as an improved encryption method. With the further development of the 802.11i standard, the AES/CCM method described below was added. In a WPA network it is now possible for some clients to communicate with the AP using TKIP, while other clients use AES.

13.4.5 WEP

WEP is an abbreviation for Wired Equivalent Privacy. The primary goal of WEP is the confidentiality of data. In contrast to signals which are transmitted over cables, radio waves spread out in all directions—even into the street in front of the house and other places where they really aren't desired. The problem of undesired interception is particularly obvious in wireless data transmission, even though it can also arise in larger installations with wired networks—however, access to cables is far more easily restricted than is the case with radio waves.

WEP offers far lower security than IEEE802.1X/WPA2. For reasons of compatibility to older WLAN clients, LANCOM APs continue to support this method of encryption. However, LANCOM expressly recommends the use of a better form of WLAN security (e.g. IEEE 802.1X/WPA2 or WPA3).

13.4.6 LANCOM Enhanced Passphrase Security (LEPS)

The encryption method WPA2 protects data traffic in the WLAN from “interception”. The required passphrase is easily handled as a central key; a RADIUS server such as that for 802.1X installations is not required.

Nevertheless, the tap-proof WPA2 method still has some weaknesses:

- One passphrase applies **globally** for **all** WLAN clients
- The passphrase may fall into unauthorized hands if treated carelessly
- A “leaked” passphrase then offers any attacker free access to the wireless network

This means in practice that: Should the passphrase “go missing” or if an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point needs to be changed in the interests of security—in every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients. In the case mentioned above, the situation of an employee leaving the company requires merely his “personal” passphrase to be deleted; all others remain valid and confidential.

With LEPS, LANCOM Systems GmbH Systems has developed two efficient methods that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoid the potential security loopholes that come with global passphrases.

LEPS-U (LANCOM Enhanced Passphrase Security User) assigns an individual password for the SSID to each individual client or to entire groups. LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) additionally authenticates the clients by their MAC address, which is ideal for secure enterprise networks.

13.4.6.1 LANCOM Enhanced Passphrase Security User (LEPS-U)

LANCOM Enhanced Passphrase Security Users (LEPS-U) allows a set of passphrases to be configured and assigned to individual users or groups. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

This is useful for onboarding devices into the network. For example, a network operator "onboarding" multiple WLAN devices into different areas of the network does not want to configure each specific device; instead this should done by the users of the devices themselves. In this case, users are given a preshared key for the company WLAN for use with their own devices. The preshared key is used to map each user to a VLAN, thus automatically assigning them to a specific network. The configuration of LEPS-U takes place on the infrastructure side only, which assures full compatibility to third-party products.

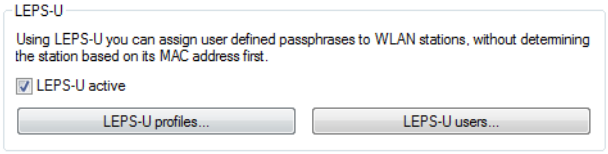
The security issue presented by global passphrases is fundamentally remedied by LEPS-U. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should "get lost" or an employee with knowledge of their passphrase leaves the company, then only the passphrase of that user needs to be changed or deleted. All other passphrases remain valid and confidential.

For technical reasons, LEPS-U is only compatible with WPA version WPA2.

For technical reasons, LEPS-U is not compatible with Fast Roaming.

Configuration

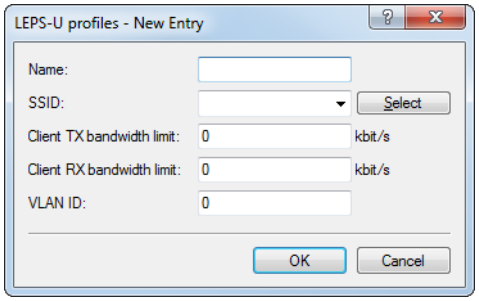
The **LEPS-U profiles** and **LEPS-U users** are configured in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS-U**. The switch **LEPS-U active** enables the LEPS-U feature.



When configured in LEPS-U, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. This is done with LEPS-U profiles, which avoids having to repeat all of the settings for every new user. You then create the LEPS-U users with their individual passphrases and link them to one of the LEPS-U profiles created previously.

LEPS-U profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users.



Name

Enter a unique name for the LEPS-U profile here.

SSID

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

Client RX bandwidth limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

VLAN-ID

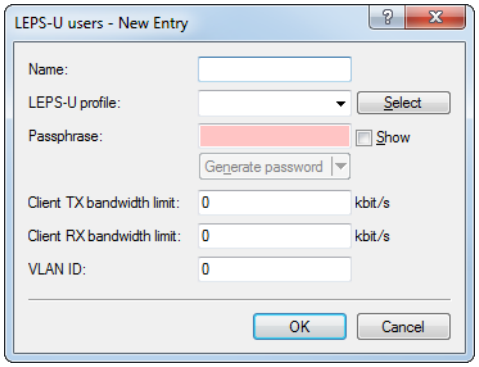
Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

LEPS-U users

Create individual LEPS-U users here. Each LEPS-U user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.

There are platform-specific restrictions on the number of LEPS-U users created at the same time.

Device	Users
L-15x, L-3xx, OAP-32x, OAP-8xx, IAP-32x, IAP-82x, LN-630acn	› up to 300 users per SSID › Access Point total: 2,000 users
L-45x, L(N)-8xx, L-13xx, LN-17xx	› per SSID up to 1,000 users › Access Point total: 6,000 users



Name

Enter a unique name for the LEPS-U user here.

LEPS-U profiles

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

Passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Client RX bandwidth limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

13.4.6.2 LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

LEPS-MAC uses an additional column in the ACL (access-control list) to assign an **individual** passphrase consisting of any 8 to 63 ASCII characters to each MAC address. Authentication at the access point is only possible with the correct combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS-MAC thus shuts out a potential attack on the ACL. If WPA2 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN as the combination of MAC address and passphrase requires both to be known before an encryption can be negotiated.

LEPS-MAC can be used both locally in the device and centrally managed by a RADIUS server. LEPS-MAC works with all WLAN client adapters available on the market without any modification. Full compatibility to third-party products is assured as LEPS-MAC only involves configuration in the access point.

Compared to LEPS-U, the administrative overhead is slightly higher because the MAC address has to be entered for each device.

Configuration

The configuration of LEPS-MAC involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. This is done either with an entry in the list under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules** (see *Stations* on page 1146) or in the RADIUS server. One entry is generated per MAC address—from the point of view of the RADIUS server, the MAC address is therefore a user. It is also necessary to activate the MAC filter under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**, i.e. data will be transmitted for the WLAN clients entered here.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

If you are storing client-specific passphrases in the user table of a RADIUS server, a LAN-based device can serve as the central RADIUS server and take advantage of LEPS-MAC.

13.4.7 Background WLAN scanning

To detect other access points within range, LANCOM Wireless Routers actively scan all of the available channels (just as a WLAN client would do to find an available access point). If another access point is active, the relevant information is stored to the scan table. Since this recording occurs in the background in addition to the access points' "normal" radio activity, it is called a "background scan".

Background scanning is mainly used for the following tasks:

- Rogue AP detection
- Fast roaming for WLAN clients

13.4.7.1 Rogue AP detection

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues. An example of rogue APs are access points that a company's employees connect to the network without the knowledge or permission of the system administrators, thereby consciously or unconsciously making the network vulnerable to potential attackers via unsecured WLAN access. Not quite as dangerous, but disruptive all the same are access points that belong to third-party networks yet are within the range of the local WLAN. If such devices also use the same SSID and channel as the local AP (default settings), then local clients could attempt to log on to external networks.

Unidentified access points within the range of the local network frequently pose a possible threat and security gap. At the very least, they are a disturbance. Therefore, background scanning identifies rogue APs and helps to decide whether further measures in securing the local network need to be introduced.

13.4.7.2 Fast roaming in client mode

However, the background scanning method can be used for objectives other than rogue AP detection. A LANCOM Access Point in client mode that logs itself on to another access point can also use the roaming procedure in a mobile installation. This is the case, for example, when a LANCOM Access Point used in an industrial application scenario is mounted to a forklift that navigates its way through multiple warehouses with separate access points. Under normal circumstances, the WLAN client would only log on to another access point when the connection to the access point it had been using until that moment was lost. With the background scanning function, the LANCOM Access Point using the client mode can collect information about other available access points in advance. In this case the client is not switched to another access point once the existing connection has been lost completely, but rather when another access point within its range has a stronger signal.

13.4.7.3 Evaluating the background scan

The information on the access points found can be viewed in the LANCOM Access Point statistics. The WLANmonitor presents the scan results quite conveniently and also offers additional functions such as access point grouping or automatic notification via e-mail whenever a new WLAN device appears.

13.4.8 Starting an environment scan at a configurable time

Your WLAN's environment can be regularly searched for rogue APs.

You can configure the times of the automatic environment scan for rogue APs.

Environment scans should be performed at times that minimize interference to normal operations.

This feature allows you to perform the scan of the configured frequency band each day at a predefined time.

In this case, scan refers to:

- Active scanning using probe requests.
- Passive scanning for beacons.



It is not always possible to use active scanning, for example where a 5-GHz channel is not DFS-free. No transmissions are permitted in this case.

The configuration is performed from the command console, shown here with default values as an example:

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Environment-Scan
> ls -a

[1.3.6.1.4.1.2356.11][2.23.20.27]
Ifc      Operating  Hour    Minute  Channel-List
[1]      [2]         [3]    [4]     [5]
=========-------------------------------------------------------------------
WLAN-1    No          3      0
WLAN-2    No          3      0
```

"Hour" and "Minute" are used to set the time at which the daily environment scan is performed. These fields also permit the use of the CRON syntax. The channel list can be used to limit the channels to be scanned (as a comma-separated list). If this list is left empty, all of the channels of the frequency band operating on the module are scanned.

During the scan, the WLAN module spends about three seconds on each channel. The next channel is then scanned. Once all of the configured channels have been scanned, the module returns to normal operating mode.

During the scan the module is not capable of regular WLAN operations, in contrast, for example, to the background scan. However, only one of the two modules can perform an environment scan at any one time, and the other module operates normally.

In addition to the time-controlled activation of the environment scan, it can also be activated permanently. For this purpose, the WLAN module can be switched to the operating mode "Scanner" (see operation mode 7):

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> l

Ifc       Operating     Operation-Mode  Link-LED-Function     Broken-Link-Detection
=============================================================================
WLAN-1    Yes           Scanner         Normal                No
WLAN-2    Yes           managed-AP      Normal                No

root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> set ?

Possible input for columns in table 'Operational':
[  1] Ifc                  : WLAN-1 (1), WLAN-2 (2)
[  2] Operating            : Yes (0), No (1)
[  3] Operation-Mode       : Access-Point (1), managed-AP (4), Station (0),
                             Probe (5), Scanner (7)
[  4] Link-LED-Function    : Normal (0), Client-Mode-Strength (1), P2P-1-Strength (8))
[  5] Broken-Link-Detection : No (0), LAN-1 (1), LAN-2 (2)
```

This performs the environment scan as described above: After scanning the configured channels, the scan does not terminate but it starts again from the beginning.

This operating mode allows the use of an AP as a full-time "scanner" AP.

The result of the environment scan can be found in the table **Status** > **WLAN** > **Environment-Scan-Results**.

See *Environment scan* on page 1041 for the configuration in LANconfig.

13.4.9 Replay-attack recognition

Every packet encrypted with AES or TKIP contains a unique sequence number so that the receiver can recognize and and drop replays. Where QoS is active, the recipient has to run a replay counter for each different priority level.

If not, an attacker could replay a sniffed packet on a different priority level. This situation is actually the basis for a number of methods of attacking TKIP.

As of LCOS version 7.70, recipients can conduct replay checks for each priority level, and there is also an additional 'global' check that keeps track of the sequence numbers recently used by the remote station. Senders are prohibited from repeating sequence numbers on different priority levels, meaning that to a certain extent replay attacks on another priority level can be recognized.

Some WLAN clients, such as those used in mobile phones, operate with a faulty AES implementation, whereby the sender uses a separate sequence counter for each priority level. It is normal for these devices to repeat sequence numbers.

In order to allow these devices to operate in the WLAN, it is possible to omit the global check of the crypto sequence.

Command line: **Setup** > **WLAN**

Omit-Global-Crypto-Sequence-Check

This is where you set the value for the crypto sequence check.

Possible values:

› Auto, Yes, No

Default:

› Auto

Special values:

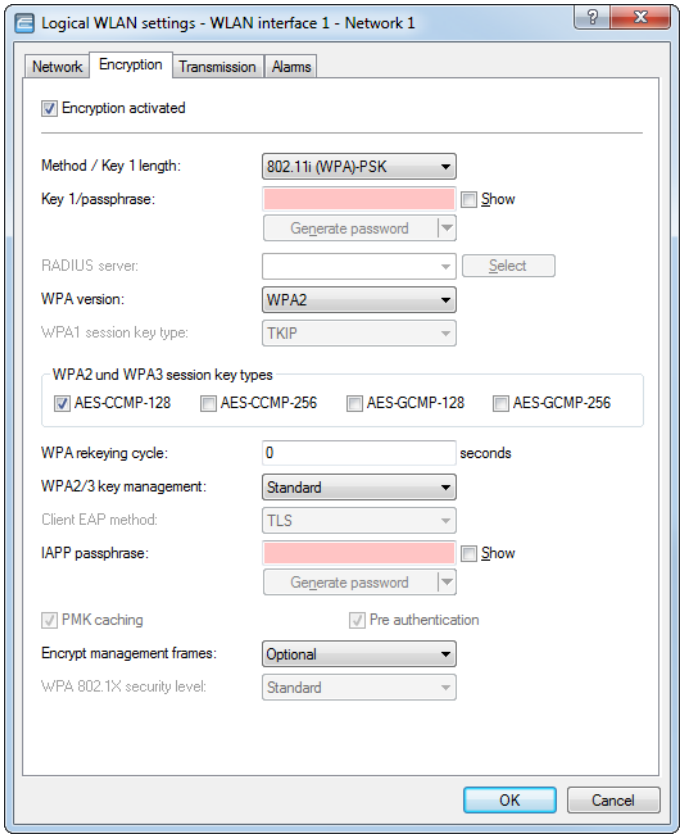
› Auto: LCOS contains a list of relevant devices. In the 'Auto' setting, the global sequence check is disabled. For other devices not included in this list, the global sequence check has to be disabled manually.

13.4.10 WLAN protected management frames (PMF)

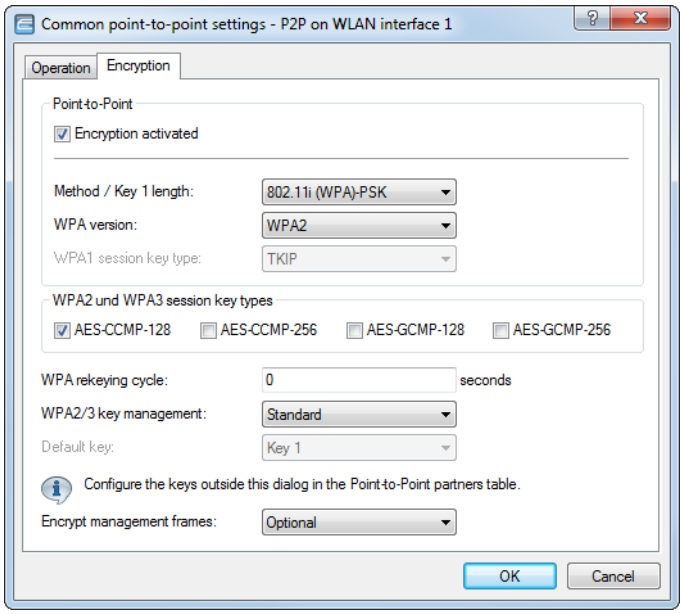
By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an AP. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications if they don't have the corresponding key.

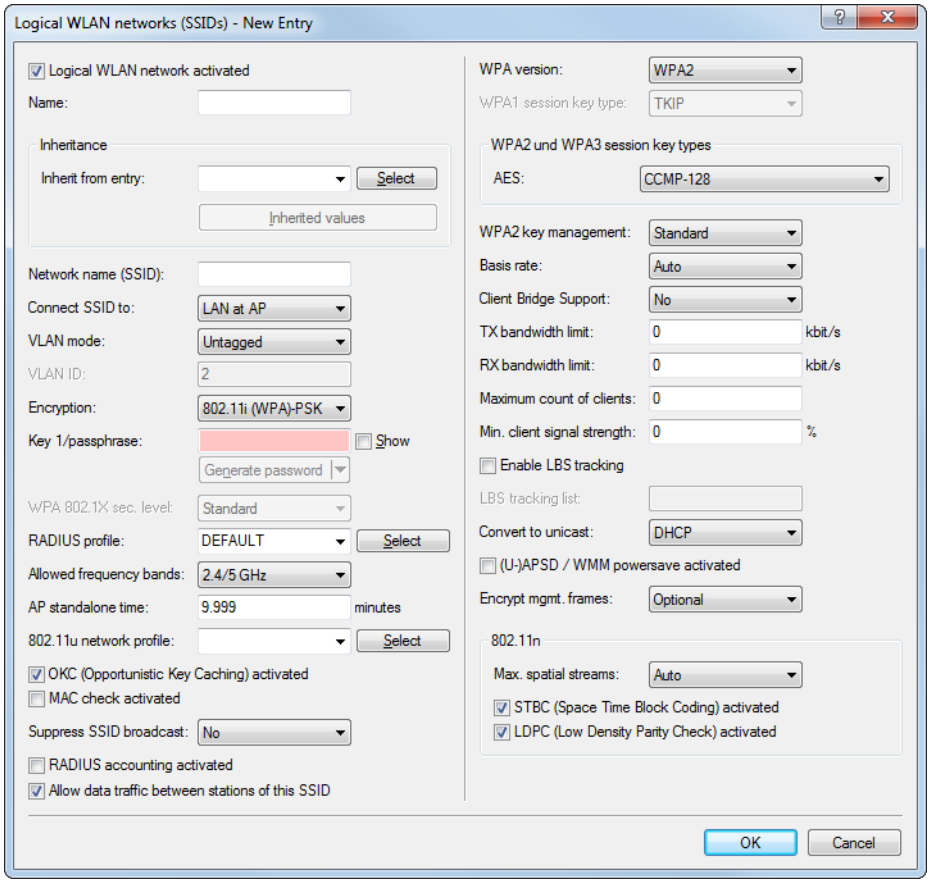
To enable protected management frames for a logical WLAN interface, in LANconfig you navigate to **Wireless LAN** > **General** > **Logical WLAN settings**, open the configuration of the appropriate WLAN interface, switch to the **Encryption** tab, and click the appropriate option in the selection list **Encrypt management frames**.



To encrypt management frames between the base stations of a P2P WLAN bridge, in LANconfig you navigate to **Wireless LAN** > **General** > **Common point-to-point settings**, open the P2P configuration of the appropriate WLAN interface, switch to the **Encryption** tab, and click the appropriate option in the selection list **Encrypt management frames**.



To manage the encryption of management frames for a WLAN controller, in LANconfig you navigate to **WLAN Controller** > **Profiles**, click on **Logical WLAN networks (SSIDs)** and click the appropriate option in the selection list **Encrypt mgmt. frames**.



The following options are available in each of these configurations:

No

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

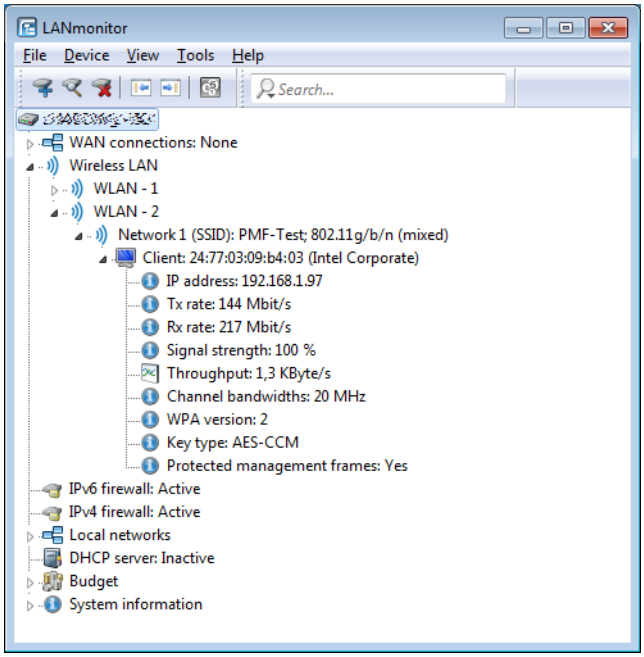
Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

LANmonitor displays information about WLAN management frame encryption below each client.



13.5 LANCOM Active Radio Control (ARC)

The intelligent WLAN optimization concept xml:lang="en"behind **LANCOM Active Radio Control (ARC)** helps you to sustainably optimize your radio field and proactively avoid sources of interference on the WLAN. Active Radio Control consists of numerous complementary functions in the LANCOM operating system LCOS, which combine to significantly improve the performance of your WLAN. All of the features in Active Radio Control are included for free in the LANCOM operating system LCOS and they are easy to operate with the appropriate management tools.

RF optimization

Automatic selection of optimum WLAN channels: WLAN clients benefit from improved throughput thanks to reduced channel overlap. In controller-based WLAN installations, the optimal channels are selected automatically for managed access points.

For more information about RF optimization, see the relevant section *RF optimization* on page 1194.

Band steering

Make optimal use of your WLAN's bandwidth: Automatically controlled by the access point, clients steered to the 5-GHz frequency band can effectively double the WLAN performance because only here are sufficient channels available for channel bundling.

For more information about band steering, see the relevant section *WLAN band steering* on page 977.

Adaptive noise immunity

Better WLAN throughput thanks to immunity to interfering signals: WLAN clients benefit from significantly improved data throughput thanks to interference-free signal coverage. Enabling the adaptive noice immunity allows an access point to block out interfering signals and to focus exclusively on WLAN clients with sufficient signal strength.

For more information about adaptive noise immunity, see the relevant section *Adaptive noise immunity for reducing interference on the WLAN* on page 982.

Spectral scan

Check your WLAN radio spectrum for sources of interference: With LANCOM Spectral Scan, you have a professional tool for efficient WLAN troubleshooting. A scan of the entire radio spectrum identifies sources of interference from outside the WLAN and allows a graphical representation.

For more information about spectral scanning, see the relevant section *Spectral scan* on page 983.

13.5.1 Adaptive RF Optimization

Improved WLAN throughput due to dynamic selection of the best WLAN channel by the access point in case of interference.

Choosing a WLAN channel specifies which part of the frequency band is used by an access point for its logical WLANs. To ensure the flawless operation of a WLAN within range of another access point, each of the access points should be using a separate channel—otherwise the WLANs have to share the medium. For this purpose, LANCOM access points use the feature Adaptive RF Optimization: The access point permanently scans the radio field for interfering signals. If a threshold is exceeded on the current WLAN channel (by means of the “wireless quality indicators”), the access point

automatically switches to a qualitatively better channel. This intelligent feature enables the access point to dynamically adapt to an ever-changing radio field in order to maximize the WLAN's stability.

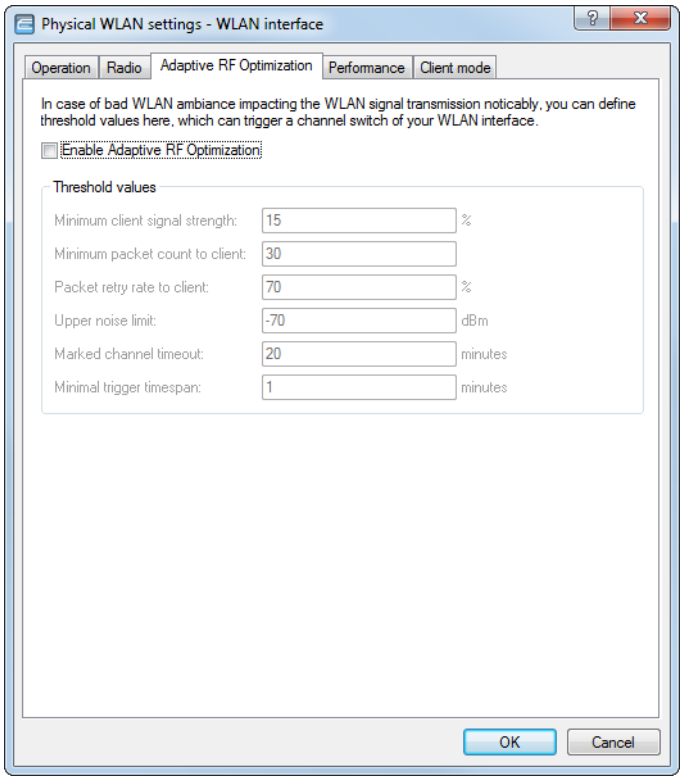


In LANconfig you have the option to manually configure the different thresholds that are used as the basis for an automatic channel change.

13.5.1.1 Setting up Adaptive RF Optimization with LANconfig

In order to use LANconfig to configure the function Adaptive RF Optimization, it is necessary for the devices that you want to configure to offer the feature "Wireless Quality Indicators". Further information about WQI is available in the reference manual.

To configure Adaptive RF Optimization, open LANconfig and go to **Wireless LAN** > **General**. In the "Interfaces" section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure and go to the tab **Adaptive RF Optimization**.



Enable Adaptive RF Optimization

To enable monitoring of the WLAN radio field via Adaptive RF Optimization, check the box **Enable Adaptive RF Optimization**.

You then configure the thresholds that trigger automatic channel changes.

Minimum client signal strength

Setting for the minimum client signal strength. Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change. The value is set in % with a default of 15).

Minimum packet count to client

Setting for the minimum number of packets sent to a client (TX). Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change (default value: 30).

Packet retry rate to client

Setting for the upper limit of packets that are resent to a client. If a client receives a proportion of resent packets that exceeds this percentage value, the device will consider this client the next time the need for a channel change is evaluated. The value is set in % with a default of 70).

Upper noise limit

Setting for the upper limit of acceptable noise on the channel. The value is set in dBm with a default of -70).

Marked channel timeout

If a channel is considered unusable, it will be marked/blocked for the length of time specified here. This value also blocks the channel change trigger in case all channels have been blocked. The value is set in minutes (default value: 20).

Minimal trigger timespan

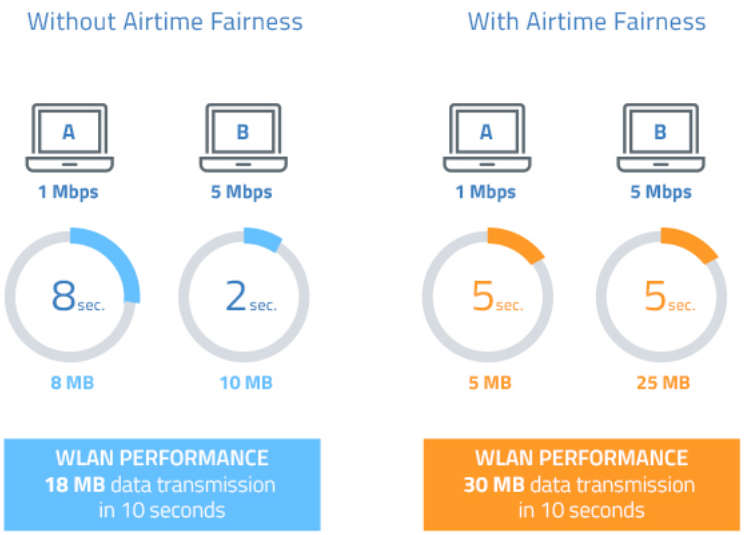
Here you specify for how long a limit is exceeded continuously before an action is triggered. The timer is reset if no limits are exceeded for a period of 20 seconds. If a limit is exceeded for the entire time span, the current channel is blocked/marked. The value is set in minutes (default value: 1).

For this setting we recommend small single-digit values.

13.5.2 Airtime Fairness

By fairly sharing the WLAN transmission time between all of the active clients, the available bandwidth is used to maximum effect and WLAN performance is improved.

Especially in WLAN scenarios with a high client-density, the devices have to compete for the available bandwidth. Here, the AP offers transmission slots to each of the clients in turn—without any consideration for the necessary transmission times. Legacy clients end up slowing down faster clients, even though the faster ones could complete their data transmission more quickly. The feature "Airtime Fairness" ensures that the available bandwidth is used efficiently. To this end, the WLAN transmission time ("airtimes") is fairly distributed between the active clients. The consequence: Thanks to all clients being provided with the same airtime, faster clients can achieve more data throughput in the same amount of time.

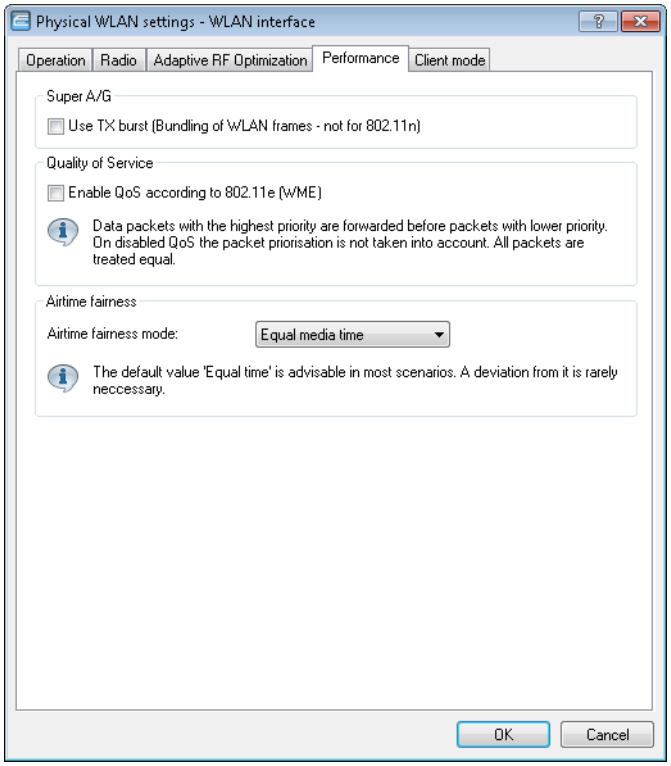


"Airtime" refers to the WLAN transmission time. Airtime Fairness provides WLAN transmission time to all of the active clients according to the mode configured for the Airtime Fairness. This, for example, stops older clients from slowing down more modern clients.

For devices with WLAN modules supporting the IEEE 802.11ac standard, the **Airtime Fairness** feature is automatically enabled in the WLAN module.

13.5.2.1 Setting up Airtime Fairness with LANconfig

Go to **Wireless LAN** > **General**. In the **Interfaces** section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure, and go to the tab **Performance**.



In the section **Airtime fairness mode** you select the Airtime Fairness operating mode:

Round robin scheduling

Each client receives a time slot for transmission, one after the other.

Equal media time

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because they can transmit a greater amount of data to the access point in a given amount of time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

802.11n preferred

This setting prefers clients using IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

Equal media volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down the other clients.

This setting is only recommended where it is necessary for all clients to receive the same throughput.

13.5.3 WLAN band steering

The IEEE 802.11 standard contains virtually no criteria by which a WLAN client should select the AP for a connection. While there are, for example, general guidelines for the preference given to an AP with a higher RSSI value (i.e. the received signal strength), WLAN clients do not, in practice, adhere strictly to these definitions or the general guidelines. If both 2.4 GHz and 5 GHz are used to broadcast an SSID, there is normally no way of influencing the client as regards the preferred frequency band.

WLAN "client steering" is based on the principle that many clients find the APs available to them by means of an active scan. Active scanning here means that a client sends probe requests containing the network ID to which the client is to connect. APs with this ID then send a test response, enabling the client to create a list of available APs. The vast majority of WLAN clients only connect to APs from which they have received a probe response, and this can be used to steer their selection process.

There are several, sometimes highly advanced, criteria for steering. One of these criteria relates to the wireless frequency ranges used for client communication. Modern dual-band WLAN clients are expected to prefer the 5 GHz frequency band over the (now) overcrowded 2.4 GHz band. Band Steering is the term given to purposefully assigning a WLAN client to a particular frequency band or range.

The list of detected or "seen" clients contains all clients from which the AP has received a test request packet. In combination with the radio frequency on which the WLAN client sends the probe request, this list is one of the bases used by the AP to decide whether or not to respond to the request.

Other criteria depend on the reported client IDs and the configuration of the devices. It may be the case, for example, that fewer SSIDs are reported on the preferred frequency band than are on the one with the lower preference. Similarly, too low a transmit strength when SSIDs are reported can result in the client not receiving any probe responses at all on the preferred frequency band. For the latter scenario, it is important to ensure that the AP does not suppress probe responses on the less favored frequency band. The minimum signal strength responsible here can be set in the following ways :

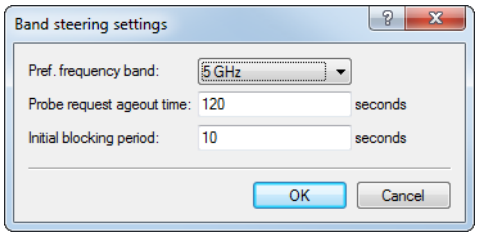
- LANconfig: **Wireless LAN** > **General** > **Logical WLAN settings** > **Network** > **Minimum client signal strength**
- Command line: **Setup** > **Interfaces** > **WLAN** > **Network** > **Minimum client strength**

In LANconfig, band steering is activated for the access point under **Wireless LAN** > **Client management** > **Client management** > **Management mode** by selecting **AP-based band steering** and is administered under **Wireless LAN** > **Client management** > **Expert settings** > **Band-steering settings**.

WLAN band steering is a component of *LANCOM Active Radio Control (ARC)*

13.5.3.1 Configuring band steering

This dialog enables you to configure the settings for band steering in LANconfig.



The following features are available under **Wireless LAN** > **Client management** > **Expert settings** > **Band-steering settings**:

Preferred frequency band

Specifies the frequency band to which the device steers WLAN clients. Possible values are:

- **2.4 GHz**: The device steers clients to the 2.4-GHz frequency band.

› **5 GHz**: The device steers clients to the 5-GHz frequency band.

Probe request age-out time

The time for which the access point steers the WLAN client to the preferred frequency band. The default value is 120 seconds.

Initial block time

If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a WLAN client to a preferred 5-GHz band. Instead, the 2.4-GHz radio module would answer the client request and forward it to the 2.4-GHz band.

By setting an initial block time, the radio module that is configured to 2.4-GHz only responds to client requests after the specified delay. The default value is 10 seconds.

The delayed response to the 2.4 GHz probes causes WLAN clients, which would otherwise expect to find an access point in the 2.4 GHz band, to scan again in the 5 GHz band.

Registration of a purely 2.4-GHz WLAN client also occurs after this delay time. If no 5-GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

13.5.4 Client Management

With Client Management, Wi-Fi clients are steered to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular band steering and client steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

Compared to the previous client steering feature supported by WLCs, Client Management operates independently and without a WLC. The access points communicate with one another using the protocol IAPP.

For the access points to communicate with one another, they need to be able to exchange IAPP messages. IAPP messages are transmitted by multicast. If necessary, the infrastructure—and switches in particular—requires exemptions to be created for IGMP snooping or other filtering mechanisms. IAPP uses the multicast group 224.0.1.76.

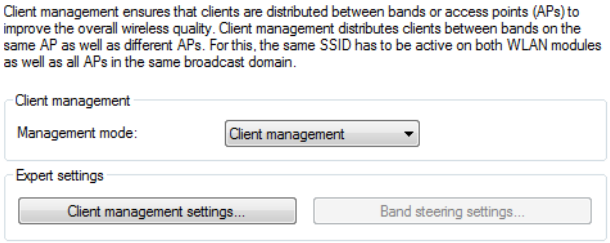
LANCOM switches in the default setting are already set up correctly for Client Management.

In this way Client Management ensures that clients are evenly distributed across the frequency bands and access points to optimize overall WLAN performance. A requirement for this is that the WLAN modules and access points in a broadcast domain all transmit on the same SSID.

13.5.4.1 Configuration of Client Management

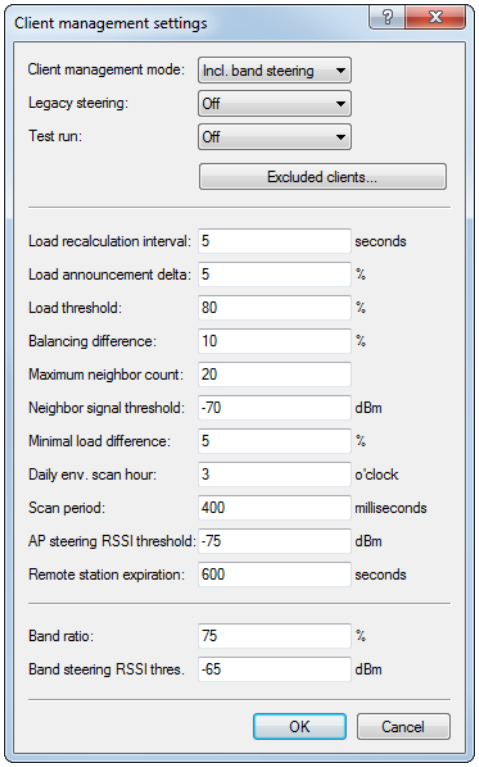
Client Management is switched on and off under **Wireless LAN** > **Client Management** > **Client Management** > **Management mode**. For new installations, this is turned on by default and usually does not require any special settings.

As an alternative for access points with multiple WLAN modules, **AP-based band steering** can also be activated. See also *WLAN band steering* on page 977.



Expert settings

The settings for Client Management are configured under **Wireless LAN** > **Client Management** > **Expert settings** > **Client Management**. The default settings are ideal for operating Client Management in offices and school environments.



Client Management mode

Access points with multiple WLAN modules can operate Client Management with and without band steering.

Default setting:with band steering

Legacy steering

Configures whether clients that do not fully support 802.11v are also directed to other access points by Client Management. Even with legacy steering activated, Client Management first steers the 802.11v-capable clients to other access points; only then does it steer the clients that do not support 802.11v. Legacy steering forcibly disconnects these clients from the WLAN. The AP prevents the client from re-associating with it for a certain period, so that the client itself selects another access point. Compared to clients steered with 802.11v, this can lead to a poorer user experience, although this depends mainly on the behavior of the legacy clients.

Default setting: Off

Test run

Operates the Client Management in test mode: Environment scans are performed and steering decisions are made by the system and recorded to the syslog, but no actual client steering takes place. Use the test run to test the behavior of Client Management without actually making changes to your network.

Default setting: Off

Excluded clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering.

Use the table to configure the MAC addresses of the clients that are to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

Load recalculation interval

Configures the interval at which the load on the AP is calculated and decisions are made to steer the clients. Increase the value to reduce the load on the network. Decrease the value to steer clients faster. Values < 2 seconds are not recommended as this negatively impacts network performance. Values > 10 seconds are not recommended as client steering does not happen in time. We recommend that you use the default value.

Default value: 5 seconds

Load announcement delta

Configures the percentage change in current load at which an access point communicates the load to other access points outside of the regular announcement interval. Increase the value in installations with many mobile clients. Decrease the value in installations with fewer moving clients. The default setting has been chosen for office and school environments. Note that this value should be lower than the value configured for the balancing difference to avoid miscalculations.

Default value: 5 %

Load threshold

Configures the load threshold at which the access point starts steering regardless of the load threshold of the neighbor access points. Increase the value in low-quality/high-density scenarios such as stadiums. Decrease the value in high-quality/high-throughput scenarios such as offices/schools.

Default value: 80 %

Balancing difference

Configures the load difference between access points at which clients are steered to the access point with the lesser load. High values lead to less balanced installations, low values lead to more steering of the clients. Increase the value if excessive client steering is happening. Decrease the value to achieve maximum balancing across the installation. The default setting has been chosen for office and school environments.

Default value: 10 %

Maximum neighbor count

Configures the number of neighbor access points that Client Management on this access point takes into consideration. In high-density scenarios, a lower number can be advantageous as clients are predominantly steered to nearby access points and less management communication is required between the access points. Values < 4 are not recommended, as there are not enough available access points for useful steering decisions. Values > 72 are not supported due to limitations of the 802.11 protocol.

Default value: 20 APs

Neighbor signal threshold

Configures the signal strength that an AP must display in order to be classified as a neighbor access point. Increase the value for high-density scenarios (for example: -60, -50). Decrease the value for scenarios where widespread coverage is required (e.g. -80, -90).

Default value: -70 dBm

Minimum load difference

Configures the minimum load difference between neighboring access points for steering to be performed between these access points. Steering is only performed when the configured load threshold is exceeded. To avoid miscalculation, the minimum load difference should not exceed the value for balancing difference. Increase the value for less steering in the installation. Decrease the value for more steering in the installation.

Default value: 5 %

Daily env. scan hour

Configures the time (00-23) at which the daily environment scan is performed as required by Client Management. The exact time of the scan is spread over a 30-minute window to minimize conflicts between concurrent environment scans. The environment scan takes about 15 seconds. No WLAN data is exchanged while the WLAN module is scanning.

Default value: 03:00 hours

Scan period

Configures the length of the environment scan used to identify neighbor access points. The scan period should be 2 to 2.5 times the configured beacon interval; the default value is suitable for the default beacon interval. This value can be configured from 200 ms to 1000 ms.

Default value: 400 ms

AP steering RSSI threshold

The signal strength that a client must have on a remote access point in order to be steered to it.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

Default value: -75 dBm

Remote station expiration

Time for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

Default value: 600 seconds

Band ratio

Configures the intended distribution of clients between the radio bands. The configured ratio specifies what proportion of clients should be steered to the 5-GHz band.

Default value: 75 %

Band steering RSSI threshold

Configures the signal strength (RSSI) that a client "displays" on the other radio band in order to be steered there. The default setting is suitable for office environments.

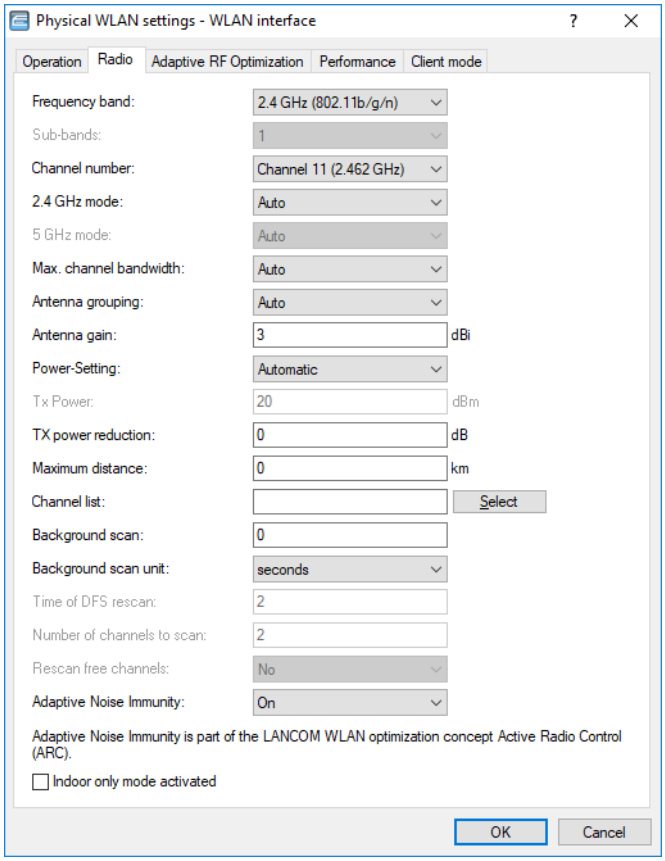
Default value: -65 dBm

13.5.5 Adaptive noise immunity for reducing interference on the WLAN

A wireless LAN can be subjected to interference from various sources. Devices such as microwave ovens or cordless phones interfere with data transmission, and even the network devices themselves can emit interference and hinder communications. Each type of interference has its own characteristics. Adaptive noise immunity (ANI) enables the access point to use different error conditions to determine the best way to compensate for the interference. By automatically increasing noise immunity, the size of the radio cell can be reduced to mitigate the impact of interference on the data transfer.

The current values and any previous actions are to be found on the command line under **Status** > **WLAN** > **Noise-Immunity**.

You can enable adaptive noise immunity in LANconfig under **Wireless LAN** > **General** > **Interfaces** > **Physical WLAN settings** > **Radio**.



To enable the adaptive noise immunity function, go to the Radio tab and set the value in the selection field **Adaptive noise immunity** to "On".

Adaptive noise immunity is a component of *LANCOM Active Radio Control (ARC)*

13.5.6 Spectral scan

In addition to connecting computers to the Internet, professional users are increasingly using wireless local area networks (WLAN) for business-critical applications. Examples include accessing of patient files, online monitoring of production facilities, and the transmission of video and audio data (ideally without any time lags). The reliability and performance of WLAN systems are thus increasingly important.

The rising significance and usage of WLAN for data transmission is resulting in more and more scenarios where the equipment and systems of various users are crowding the WLAN frequency ranges. These may include, for example, microwave ovens, cordless telephones, Bluetooth devices and video transmitters, with their signals occurring on a continual or intermittent basis. The simultaneous usage of a frequency band or frequency range gives rise to interference that can disrupt or negatively impact the reliability and performance of a WLAN. This type of interference can result in data packets or connections being lost. If the interference is too strong, the complete failure of the WLAN may result.

It is therefore becoming increasingly important to use targeted analysis to check the frequency ranges. These checks should identify the interference or other interference factors, and introduce countermeasures as required. It can also be used to ensure that the WLAN is working properly and operating interference free.

Targeted analysis can also clarify or identify the following:

- Proper, fault-free operation of the WLAN
- Existence of interference or noise
- Display or identify the bands with interference
- Strength of the interference signal
- Regularity or frequency of the interference signal
- Type, and possibly source, of the interference signal

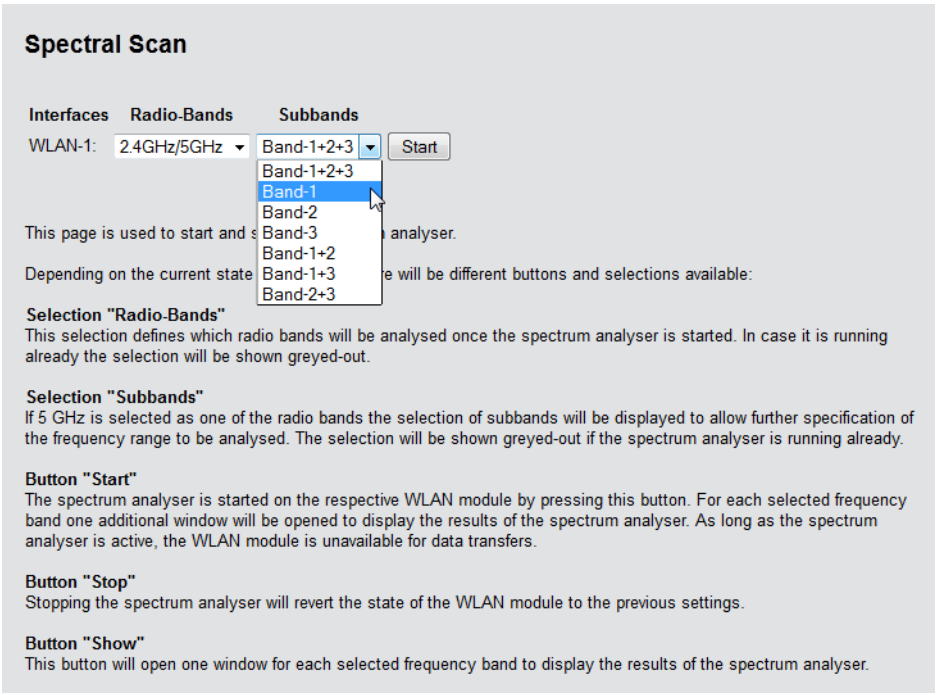
The WLAN-related frequency ranges are subject to spectral analysis. Results are displayed graphically, i.e. in the form of real-time diagrams or real-time overviews of frequencies and interference. However, graphical analyses of a spectral range are open to some freedom of interpretation. Therefore, the following scenario should be fairly commonplace: You ascertain that the frequency currently being used is being subjected to interference that is continual and of constant signal strength. However, you cannot unequivocally ascertain or even "read-out" which room or building the signal is coming from, nor the type of equipment which is transmitting the interfering signal.

Spectral Scan is a component of the *LANCOM Active Radio Control (ARC)*

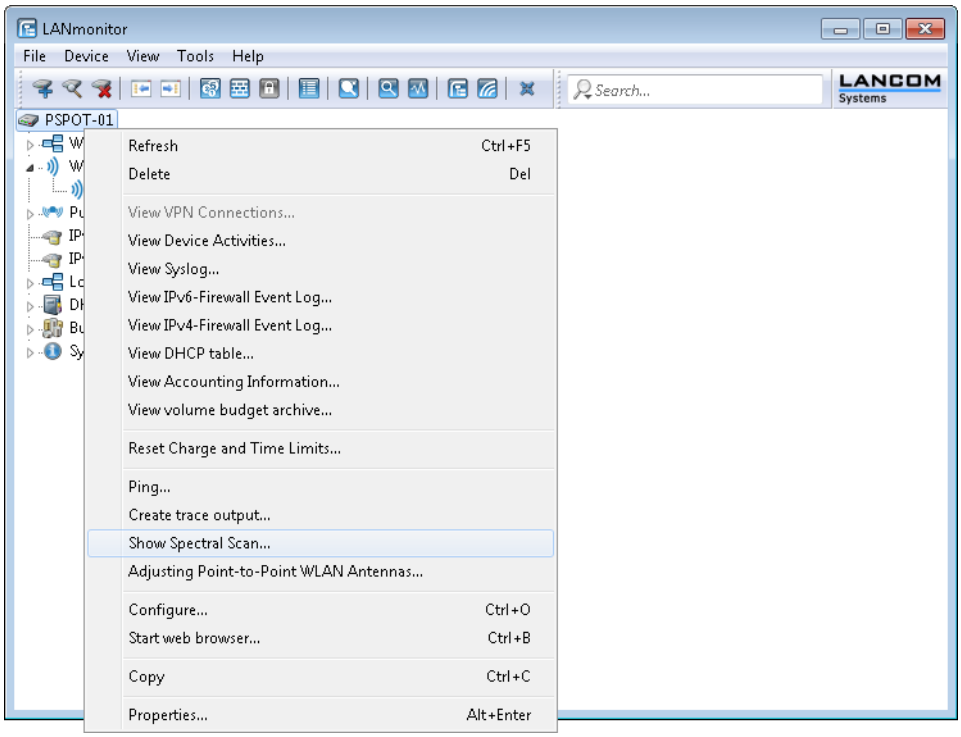
13.5.6.1 Functions of the software module

The "Spectral Scan" software module enables you to run a spectral analysis directly on the access point. There is no need to purchase any additional software or hardware as the integrated features can be used to analyze the frequency ranges and bands in question. This gives you a graphical overview of the frequency response characteristics within your WLAN at all times, so that you can detect interference and safeguard against it.

Clicking on the menu option**Extras** > **Spectral scan** in WEBconfig opens the window shown below:



The Spectral Scan can also be started from LANmonitor. To do this, right-click the relevant device in the list and select **Display spectral scan** in the context dialog.



When the WLAN module is disabled (**Setup** > **Interfaces** > **WLAN** > **Operational**), a message is displayed and the spectral scan cannot be started. Configure the access point for "Base station" operation or ensure that a WLC configures the AP.

The following entries, buttons and selection menus are available here:

- **Interfaces**: Shows the selected WLAN module for analysis.
- **Radio bands**: Use this selection menu to set which frequency band(s) you wish to analyze. The relevant field is grayed out once the spectral scan has started on this module.
- **Subbands**: This selection menu is only enabled if '5GHz' or '2.4 GHz/5 GHz' is selected in **Radio bands**. You are then able to specify which sub-bands of the 5GHz band are included in the analysis.
- **Start**: Clicking this button starts the "spectral scan" on the relevant WLAN module. A separate window opens for each of the selected frequency bands.
- **Stop**: This buttons ends the analysis. The WLAN module then returns to the previous mode and is available again with its usual functionality.

  This button is only shown once the module has been started.

- **Show**: Once the spectral scan has started, click this button to open a window for each selected frequency band. Click the button repeatedly to open multiple windows.

During the analysis, the WLAN module being analyzed does not send any data or transmit any SSID.

Please refer to Section *Spectral scan analysis window* for further information on the diagrams displayed.

13.5.6.2 Spectral scan analysis window

The spectral scan is displayed in a browser application. For this to work properly, your browser must support the latest version of WebSockets and the HTML5 `<canvas>` element. The browser integrated in LANmonitor meets all of these requirements.

In the separate analysis window of the spectral scan, there are different ways to show the frequencies and frequency ranges along with any potential interference. The following buttons are available at the top of the window:

- **Current**: Shows or hides the curve of the values being measured.
- **Maximum**: Shows or hides the maximum values of the ongoing spectrum scan in relation to the currently set history range.
- **Average**: Shows or hides the average values of the ongoing spectral scan in relation to the currently set history range.
- **History**: Shows or hides the values last measured.
- **Number of history values**: Determines the number of the most recent results to be displayed. You are able to show at least the last 5 and at most the last 50 measuring points for every frequency.
- **Last channel**: Shows or hides the channel last used.
- **Frequency**: Switches the display on the X-axis between WLAN channel and frequency.

The window contains two graphical views showing the readings in a different manner. The top diagram shows the signal strength in dBm on the Y-axis, and either the WLAN channel or the relevant frequency on the X-axis. The lower diagram contains the analysis progression over time in the form of a waterfall diagram, with the Y-axis showing the time and the X-axis again showing the WLAN channel or the relevant frequency. These view formats depict both continuous and occasional interference on the frequencies, so helping you to take appropriate action to improve the connection (e.g. by changing the channel or identifying and eliminating the interference source). For example, certain interference sources such as microwave devices, DECT telephones (working in the 2.4 GHz frequency range) and audio-video transmitters exhibit very typical transmit patterns that occur prominently in both diagrams.

On the lower border of the window there is a slider labeled **Time slider**. This enables you to extend or limit the time period analyzed for the waterfall diagram. Alternatively, you can use the input box to the right of the slider to select how many readings you would like to display in the waterfall diagram. The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached.

Below are some examples of analysis results, which graphically represent other settings in different ways:

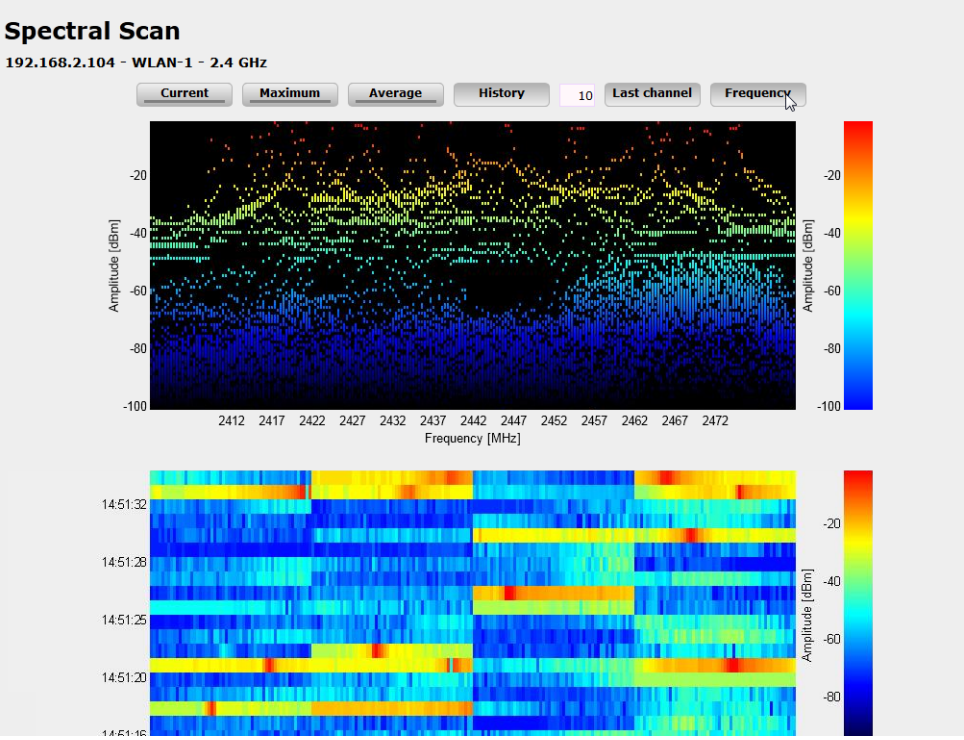


Figure 16: Spectral scan, frequency display of the last 10 history values

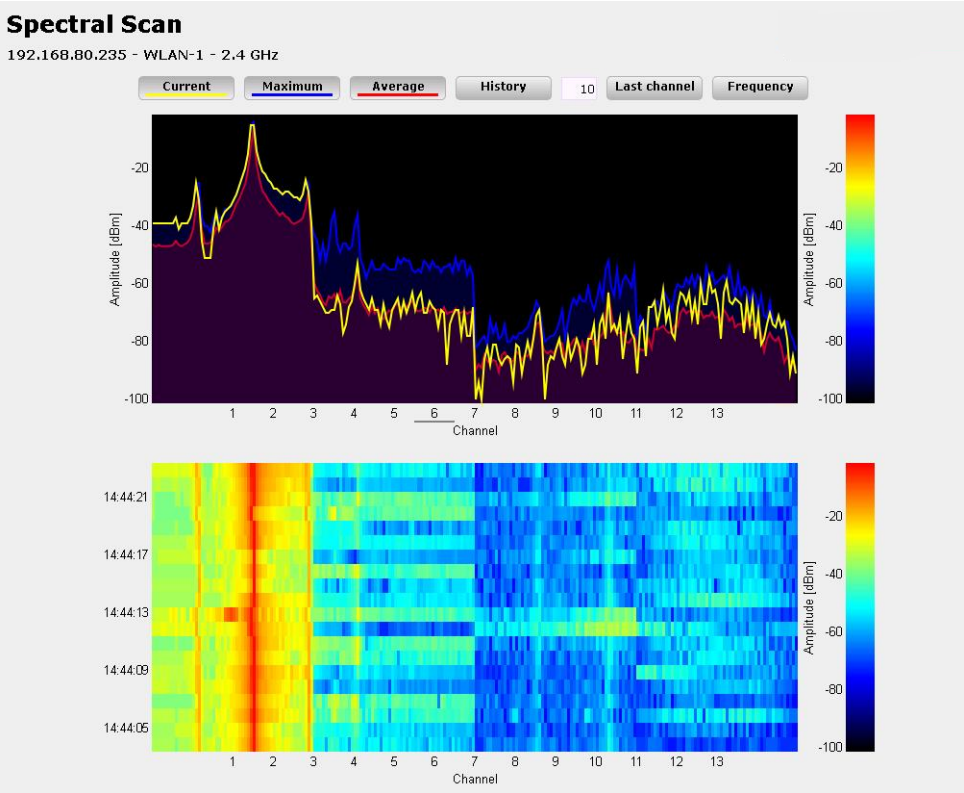


Figure 17: Spectral scan, channel display of Current, Maximum and Average, interference from radio camera

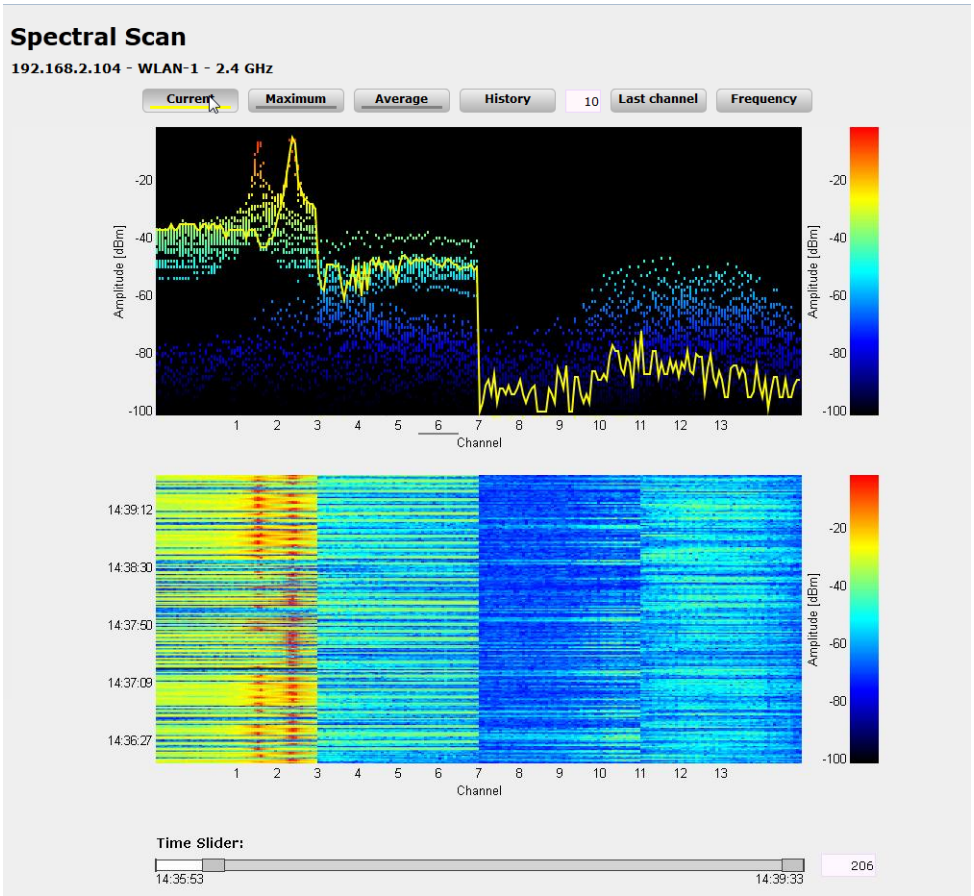


Figure 18: Spectral scan, channel display of Current, last 10 history values and "Time Slider", interference from baby phone

13.6 Dynamic frequency selection (DFS)

For the DFS method (Dynamic Frequency Selection) required for 5 GHz WLANs, an unused frequency is automatically selected, for example, to avoid interference from radar systems. Occasionally, however, signals from weather radar stations cannot be identified reliably.

For this reason the European Commission is extending the requirements of the standards ETSI EN 301 893 V1.3.1 and ETSI EN 301 893 V1.4.1 to additionally avoid the use of three channels (120, 124 and 128) in subband 2 of the 5 GHz band, and not to allow use of these bands for automatic channel selection until a process to auto-detect weather radar station signals is made available. The versions EN 301 893 V1.3 and EN 301 893 V1.4 are referred to as "DFS-2".

In the middle of 2010 the new version ETSI EN 301 893 V1.5.1 came into force, which was accompanied by changes in the usage of WLAN frequencies in the ranges 5.25 to 5.35 GHz and 5.47 to 5.725 GHz. The new Version 1.5.1 regulates the DFS (Dynamic Frequency Selection) method for the protection of radar stations from WLAN systems working in this frequency range. By using DFS to detect certain patterns in the radio signals received, it is now possible to detect active radar stations, and WLAN systems can automatically switch their operating channel. To differentiate from previous regulations, the new standard EN 301 893-V1.5 for the updated DFS is referred to as "DFS-3".

A pulse pattern can generally be described in terms of its pulse rate, pulse width and the number of pulses. Former DFS technology was only able to detect fixed radar patterns as defined by the various combinations of pulse rates and pulse widths which were stored in the WLAN device. According to DFS-3, the device is now able to recognize changing pulse rates and pulse widths as radar patterns. Furthermore, two or three different pulse rates may be used within a radar signal.

The version ETSI EN 301 893 V1.5.1 (DFS-3) expired on January 01, 2013. The new version ETSI EN 301 893 v1.6.1 (known as "DFS-4"), which applied thereafter, also detects shorter radar pulses.

The version ETSI EN 301 893 V1.5.1 (DFS-4) expired on December 31, 2014. The new version ETSI EN 301 893 V1.7.1 applies (known as "DFS-5"), which applied thereafter, brought some changes to signal strengths. Since then there have been several other revisions to this standard.

The detection of weather radar stations (channels 120, 124 and 128 in the 5.6 to 5.65 MHz frequency range) is subject to special conditions. The DFS implementation in LCOS does not support the more stringent detection conditions. Therefore, these three channels will be omitted from newer versions of LCOS.

Operating principles

After switching on or booting, the device randomly selects one of the available channels (e.g. based on the country settings). It checks whether radar signals exist on this channel, and whether it is already in use by another WLAN. This scan is repeated until it finds a radar-free channel with as few other networks as possible. The selected channel is then monitored for radar signals for a further 60 seconds. For this reason, data traffic may be interrupted for a period of 60 seconds while the frequencies are scanned for a free channel.

To avoid these pauses in data transmission every time the channel is changed, devices carry out the scan **before** a channel is chosen. Information about scanned channels is stored to an internal database.

- Was a radar signal detected on the channel?
- How many other networks were found on the channel?

This database helps the AP to select from the list of radar-free channels with the lowest number of other networks (the operating channel). After the channel has been selected, data transmission can continue immediately without any waiting.

- The "blacklist" in the database stores the channels to be blocked due to the detection of radar signals. This entries are removed from the list every 30 minutes in order to keep the information up to date.
- The "whitelist" in the database stores the channels where no radar was detected. These entries remain valid for 24 hours, although if radar signals be detected in the meantime, an entry is made to the blacklist.

By default, the AP permanently uses the channel that was selected as the operating channel during the first scan. Connections can now be operated for any length of time on the channel selected by the DFS algorithm until either a radar signal is detected or the radio cell is restarted (e.g. by changing the device configuration, firmware upload, or restart).

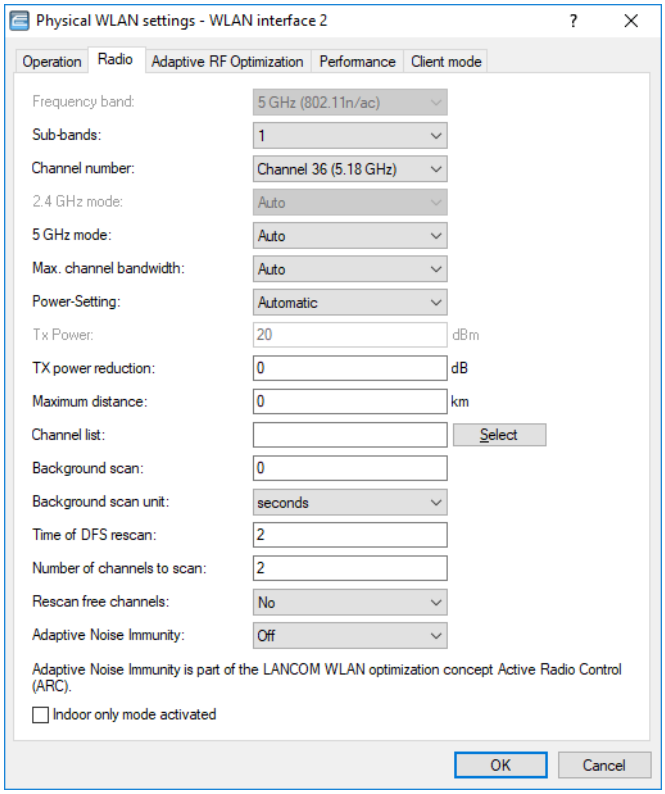
A new 60-second scan is necessary under the following conditions:

- The device is switched on or cold-started. In this case the database is empty, so the device cannot select the preferred channels from the whitelist. A scan has to be performed.
- Within the first 24 hours of scanning, it becomes necessary to switch channels because a radar signal is detected within range of the AP. In this case, the AP can refer to alternatives in the whitelist. It then informs associated WLAN clients and/or P2P partners of the new operating channel and switches to this channel. This process takes place within about a second, so the switch can be considered to be uninterrupted.
- The device is in operation for 24 hours already, so a new channel scan is required. Entries in the whitelist are "out of date" and thus discarded. The AP has no alternative channel that it can switch to directly. In this case the database requires new information from a scan and WLAN operation is interrupted for one minute.

In principle the operator of the WLAN is responsible for maintaining the ETSI standards. For this reason LANCOM recommends that you perform an update to a firmware version with DFS support.

13.6.1 DFS configuration

In LANconfig you access the DFS settings under **Wireless LAN** > **General**, then click **Physical WLAN settings** and select the **Radio** tab.



Time of DFS rescan

This entry determines at what time (0 - 24h) the device deletes the DFS database and performs a DFS rescan. If this item is left empty, the device only performs a DFS rescan when no further free channel is available. This is the case when the number of channels determined during the initial DFS scan falls below the minimum number of free channels.

The cron command options can be used to define the time: The entry '1,6,13' starts the rescan at 01:00h, 06:00h and 13:00h. The entry ' 0-23/4 ' starts a rescan every four hours between 00:00h and 23:00h.

Number of channels to scan

This entry determines the minimum number of free channels that a DFS scan has to achieve. The default value of '2' means that the device performs a DFS scan for as long as it takes to detect 2 free channels. If the device has to switch channels, for example if it detects an active radar pattern, the second channel is immediately available for the change.

A value of '0' disables the restriction. The physical WLAN interface performs a DFS scan on all available channels.

Rescan free channels

With this item you select whether, following the completion of a DFS rescan, the physical WLAN interface deletes occupied channels or saves them for subsequent DFS rescans.

- **Yes:** The physical WLAN interface deletes occupied channels after completing a DFS rescan so that they are available again for a new DFS rescan.
- **No**: The device saves occupied channels after completing a DFS rescan and so that the device immediately skips them during a new DFS rescan.

You can select a preference for certain channels. LCOS is trying first, whether a channel set in **Channel number** can be used, then it tries the channel set in the **Channel list** through the channels listed. If all these channels are not available due to radar detection, then the possible channels for the selected country will be tried.

After the DFS locking time has elapsed, an attempt is made to switch back to the set channel. If this channel is still not available, a channel configured in the channel list is used. The DFS blocking time becomes effective as soon as a channel is blocked due to radar detection and it is usually 30 minutes.

This preference helps to be able to use fixed channel schemes in 5 GHz, because this allows the full channel scheme to be restored faster after DFS events.

If no dedicated channel is configured for the WLAN module (channel list empty and radio channel "0" or "Automatic"), then after a channel change triggered by radar detection, the new channel is retained and not changed to the last channel used.

13.7 APSD – Automatic Power Save Delivery

13.7.1 Introduction

Automatic Power Save Delivery (APSD) is an extension to the IEEE 802.11e standard. APSD is available in two versions:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

These two methods differ in the way that they use the transmission channels, among others. LANCOM APs and wireless routers support U-APSD, which forms the basis for the Wi-Fi-certified WMM Power Save (WMMPS).

U-APSD allows WLAN devices to save considerable amounts of energy. This function has come into demand due to the increasing use of WLAN-capable telephones (Voice over WLAN – VoWLAN).

Activating U-APSD for a wireless LAN enables WLAN devices making calls to switch into "doze mode" while they wait for the next data packet. Transmission of VoIP data takes place in a fixed time pattern—WLAN devices synchronize their phases of activity with this cycle, so that they are ready in good time to receive the next packet. This significantly reduces power consumption and the batteries provide a considerably longer call time.

The precise behavior of the power-saving mode is negotiated between the AP and WLAN client under consideration of the actual application at hand. This makes APSD much more flexible than former power saving methods, referred to in this context as "legacy power save".

13.7.2 Configuration

Command line: **Setup** > **Interfaces** > **WLAN** > **Network**

APSD

Activates APSD power saving for this logical WLAN network.

Possible values:

- On, off

Default:

- Off

Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

13.7.3 Statistics

Command line: **Status** > **WLAN** > **Networks**

APSD

Indicates whether APSD is activated or deactivated for the respective WLAN (SSID). APSD is only indicated as active if it is activated in the settings for the logical WLAN and also if the general QoS module is activated.

Command line: **Status** > **WLAN**

Station table

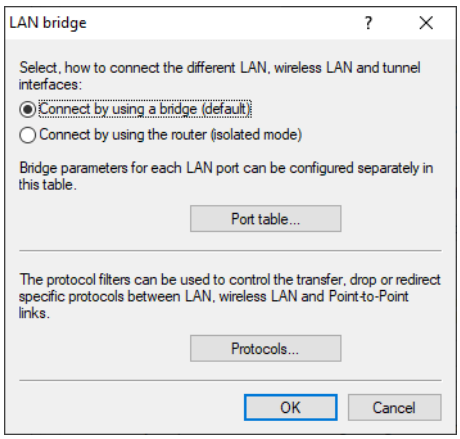
Displays the access categories for which associated WLAN clients are using APSD:

- Voice (highest priority)
- Video
- Best effort (including data traffic from "legacy power-save" clients)
- Background (lowest priority).

13.8 WLAN routing (isolated mode)

The standard setting allows data traffic to be "bridged" between LAN and WLAN, i.e. layer-2 transparent transmission. Data traffic between the cabled network and the wireless LAN is **not** directed via the IP router. Consequently, the firewall and Quality of Service functions integrated into the firewall are not available for traffic between LAN and WLAN. In order to be able to use these functions, the WLAN interfaces are set to "isolated mode" and the data traffic is intentionally routed via the IP router.

To ensure that the IP router can correctly transmit the data between the LAN and WLAN, the two areas must have different IP address ranges. Further information is available in the Advanced Routing and Forwarding (ARF) section.



LANconfig: **Interfaces** > **LAN** > **LAN bridge**

Command line: **Setup** > **LAN-Bridge** > **Isolated-Mode**

13.9 IEEE 802.11e user priority converted into VLAN tags

IEEE 802.11e is an extension to the WLAN standards that incorporates quality-of-service (QoS) functions. An access point operating this standard can assign a user priority to each wireless client associated with it. By prioritizing wireless data packets, the access point can provide preferred handling for voice over IP clients, for example. On the LAN side, access points are commonly connected with a switch, and different LAN segments are often separated by VLANs. The wired LAN uses other mechanisms for the prioritization of data packets.

The following example application illustrates this:

- A wireless client (e.g. VoIP phone) is connected to an access point, QoS is enabled on the WLAN, the data between the phone and access point is not VLAN tagged.
- On the Ethernet side, the access point is connected to a VLAN-capable switch, and the data between AP and switch is VLAN tagged.

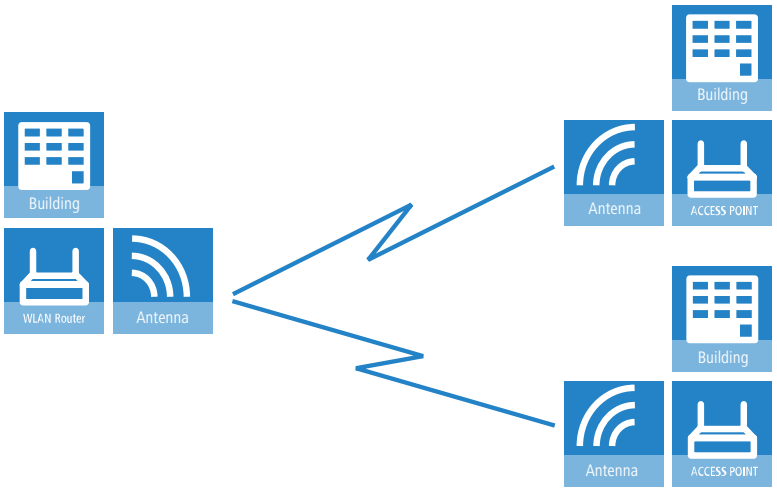
The access point is the interface between wired LAN and wireless LAN, and it converts the different prioritization information accordingly:

- When an access point receives data for transfer to a WLAN client, it determines the priority of each data packet either from the VLAN tag or the ToS/DSCP field in the IP header. The access point sends the packets to the client with this priority.
- However, data packets transferred from the WLAN client to the access point do not have a VLAN tag. What's more, in this direction the access point does not inspect the IP header. Instead, the access point takes the user priority of the WLAN packet and translates this into the appropriate VLAN tag to be attached to outgoing data packets on their way to the switch.

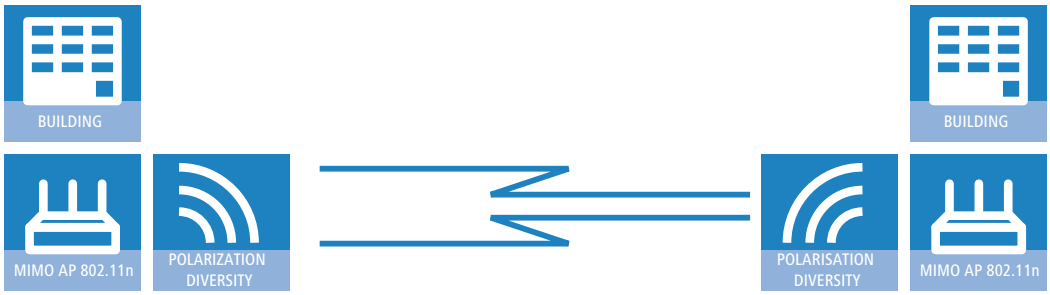
13.10 Establishing WLAN bridges

13.10.1 Configuring WLAN bridges

LANCOM APs can serve not only as central stations in a wireless network, they can also operate in point-to-point mode to form links over longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart—without direct cabling or expensive leased lines.



When using APs and appropriately polarized antennas in accordance with IEEE 802.11n two wireless links can be established simultaneously between the end points of a point-to-point connection. This allows higher data throughput to be achieved or greater distances to be covered than when using other standards.

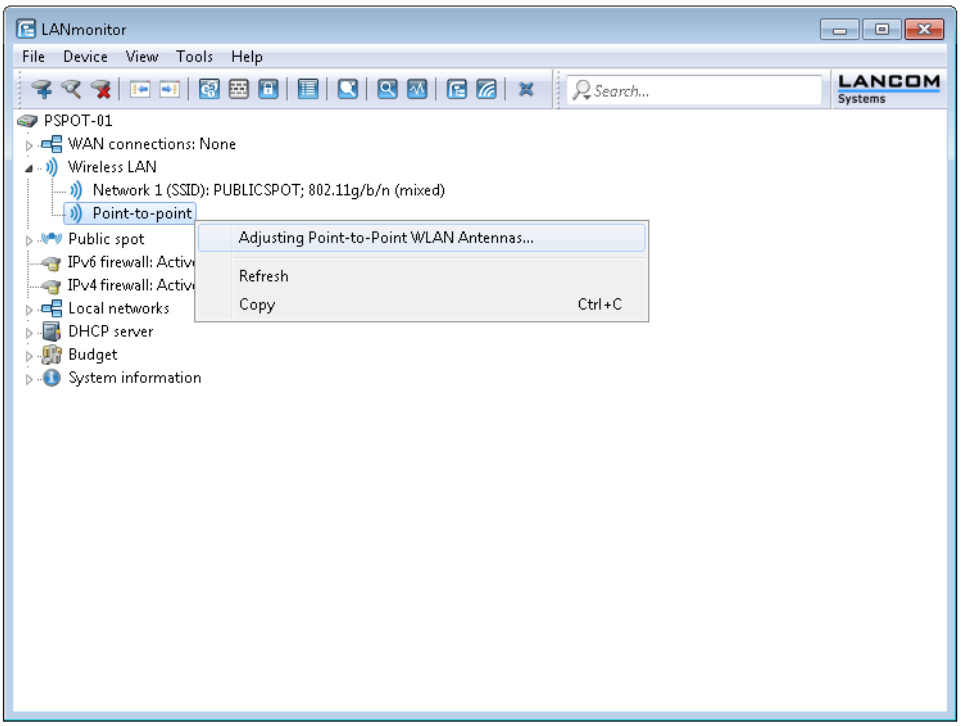


This section introduces the basic principles involved in designing WLAN bridges and provides tips on aligning the antennas.

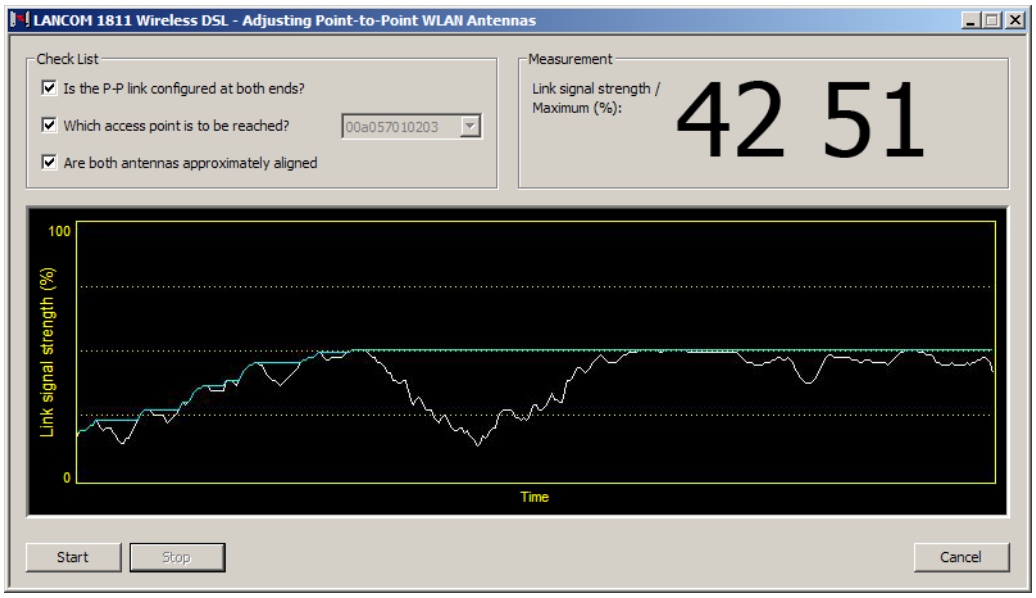
13.10.2 Setting up WLAN bridges with LANmonitor

To find the best possible alignment for point-to-point connection antennas, the current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor. LANmonitor provides not only an optical display of link strength, but an acoustic signal as well.

In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option **Adjusting Point-to-Point WLAN Antennas**.



Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The trend of the signal strength over time and the maximum value are also displayed in a diagram.



Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

An acoustic signal can be activated to help align the antennas precisely. With this option, the PC can emit a tone which varies according to signal strength. Maximum signal strength over the link is signaled by a constant tone. If the signal strength drops below the maximum, tones are emitted at intervals indicating the difference from the former maximum. The shorter the interval, the closer the current link signal strength is to the maximum.

13.10.3 Geometric dimensioning of outdoor wireless network links

The following basic questions must be answered when designing wireless links:

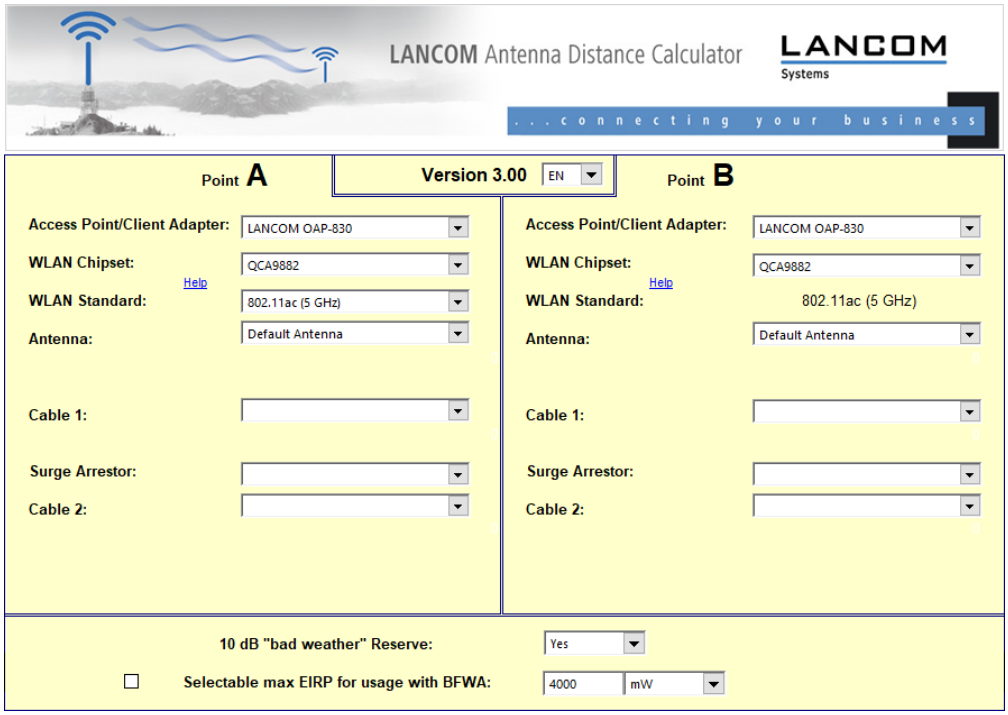
- Which antennas are necessary for the desired application?
- How do the antennas have to be positioned to ensure problem-free connections?
- What performance characteristics do the antennas need to ensure sufficient data throughput within the legal limits?

13.10.3.1 Antenna selection with the LANCOM Antenna Distance Calculator

The *LANCOM Antenna Distance Calculator* is a program that you can use for calculating the output power at the AP and to make a first estimate of the achievable ranges and data rates.

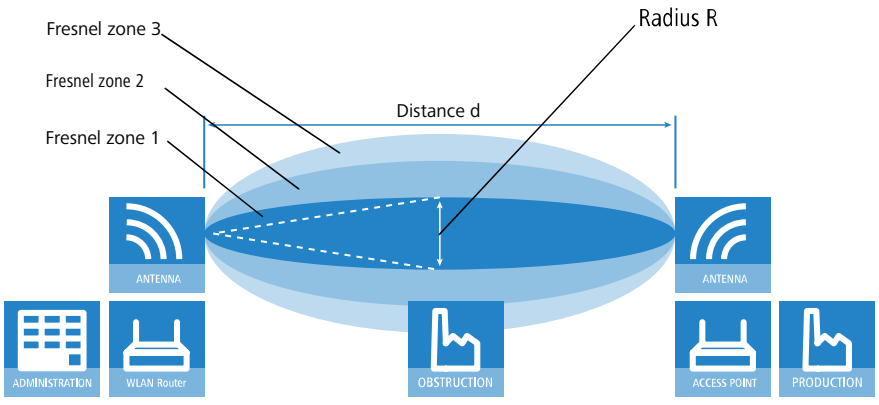
After selecting your components (APs, antennas, lightning protection and cable) the calculator works out the data rates, ranges, and the antenna gain settings that have to be entered into the AP.

Please note that when using 5 GHz antennas additional technologies such as dynamic frequency selection (DFS) may be stipulated depending on the country of use. The operator of the wireless LAN system is responsible for ensuring that local regulations are met.



13.10.3.2 Positioning the antennas

Antennas do not broadcast their signals linearly, but within an angle that depends on the model in question. The spherical expansion of the signal waves produces amplification or interference of the effective power output at certain distances along the connection between the transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.



The Fresnel zone 1 must remain free from obstruction in order to ensure that the maximum level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object not only screens off a portion of the Fresnel zone, but the resulting reflections also lead to a significant reduction in signal reception.

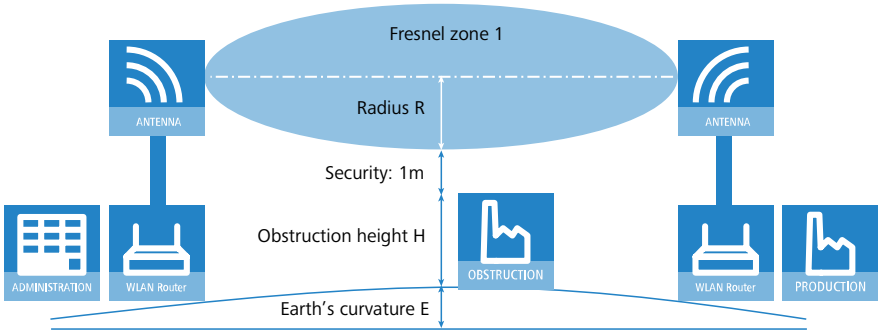
The radius (R) of Fresnel zone 1 is calculated with the following formula assuming that the signal wavelength ( ) and the distance between transmitter and receiver (d) are known.

R = 0,5 * √ (* d)

The wavelength in the 2.4 GHz band is approx. 0.125 m, in the 5 GHz band approx. 0.05 m.

Example: With a separating distance of 4 km between the two antennae, the radius of Fresnel zone 1 in the 2.4-GHz band is **11 m**, in the 5-GHz band **7 m**.

To ensure that the Fresnel zone 1 remains unobstructed, the height of the antennas must exceed that of the highest obstruction by this radius. The full height of the antenna pole (M) should be as depicted:



M = R + 1m + H + E (earth's curvature)

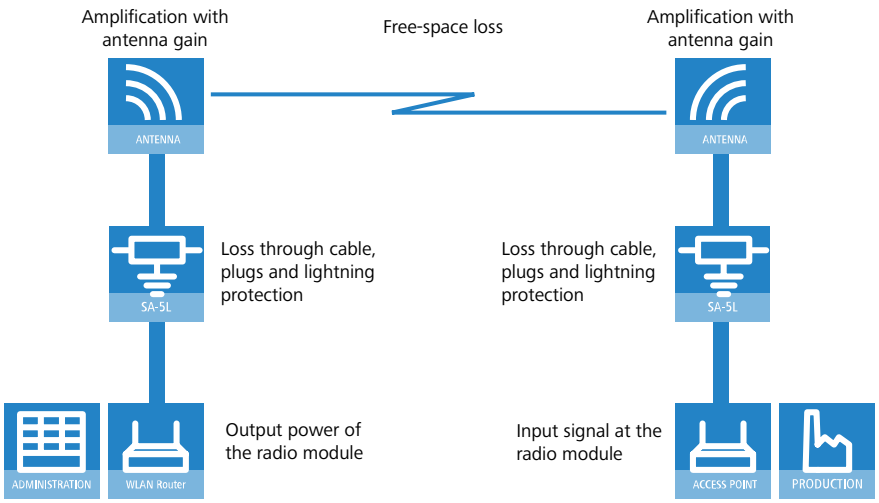
The allowance for the curvature of the earth (E) can be calculated at a distance (d) as E = d² * 0.0147 – i.e. at a distance of 8 km this is almost 1 m.

Example: With a distance of 8 km between the antennae, the result in the 2.4-GHz band is a pole height above the level of the highest obstruction of approx. **13 m**, in the 5-GHz band **9 m**.

13.10.3.3 Antenna power

The power of the antennas must be high enough to ensure acceptable data transfer rates. On the other hand, the country-specific legal regulations regarding maximum transmission power should not be exceeded.

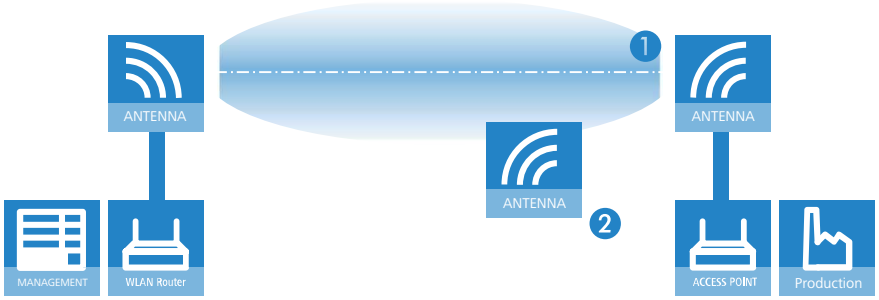
The calculation of effective power considers everything from the radio module in the transmitting AP to the radio module in the receiving AP. In between there are attenuating elements such as the cable, plug connections or simply the air transmitting the signals and amplifying elements such as the external antennas.



13.10.4 Antenna alignment for P2P operations

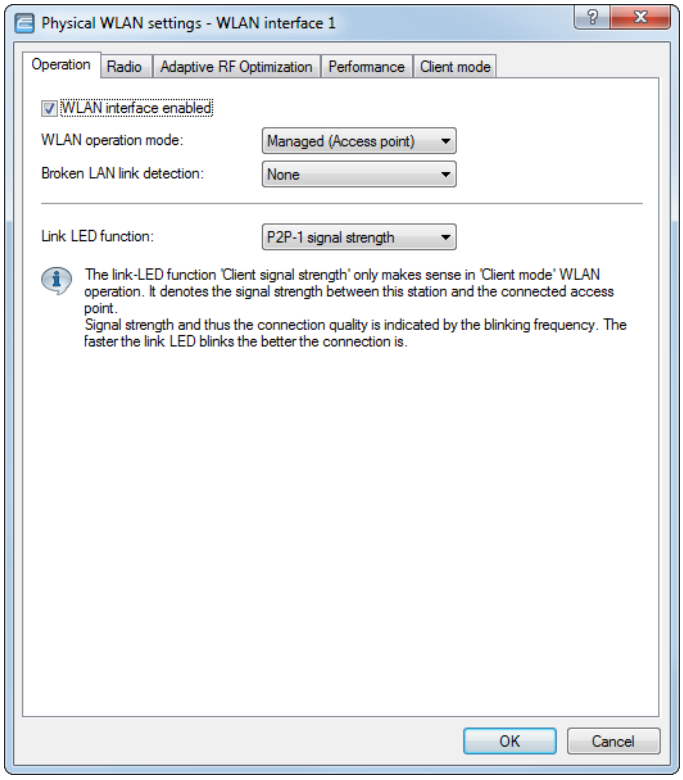
Protecting components from the consequences of lightning strikes and other electrostatic influences is a vital aspect in the design and installation of WLAN systems for outdoor use. Please refer to the appropriate notes on “Lightning and surge protection” as otherwise LANCOM cannot provide any guarantee for damage to components. Information on the installation of WLAN systems for outdoor deployment is available in the ‘LANCOM Outdoor Wireless Guide'.

The precise alignment of the antennas is of critical importance for establishing P2P connections. The more central the receiving antenna is located in the “ideal line” of the transmitting antenna, the better is the actual power and the effective bandwidth **1**. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result **2**.

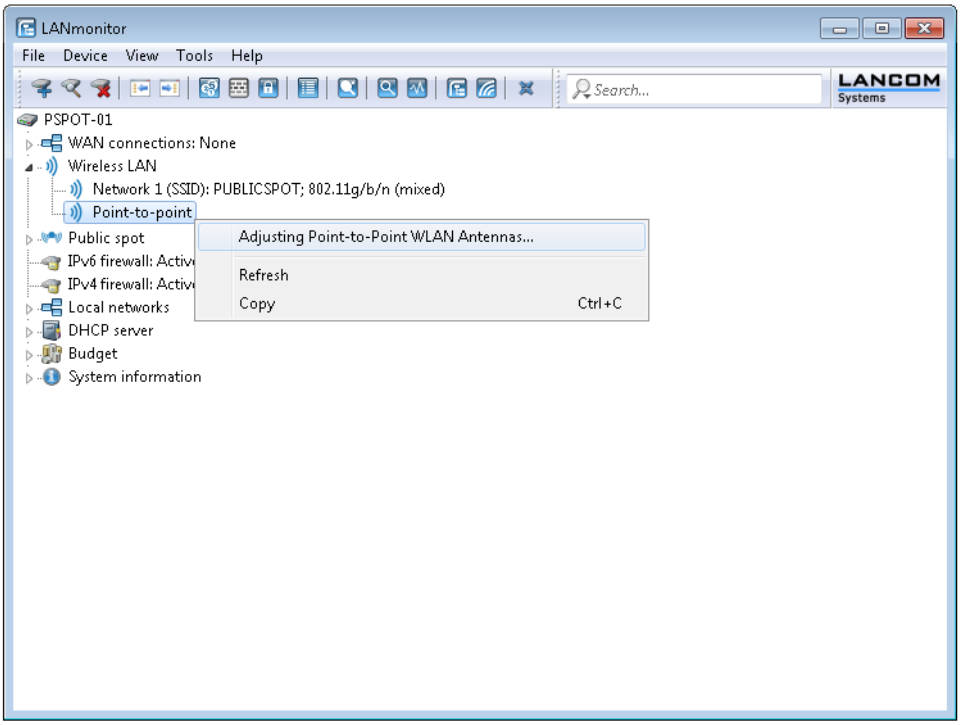


The current signal quality over a P2P connection can be displayed on the device's LEDs or in LANmonitor in order to help find the best possible alignment for the antennas.

The display of signal quality with the LEDs must be activated for the physical wireless LAN interface (LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Operation**). The faster the LED blinks the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double the frequency indicates that the signal strength is twice as high).



In LANmonitor the connection quality display is opened with the context menu. Right-clicking with the mouse on **Point-to-point** activates the option **Adjusting Point-to-Point WLAN Antennas**.

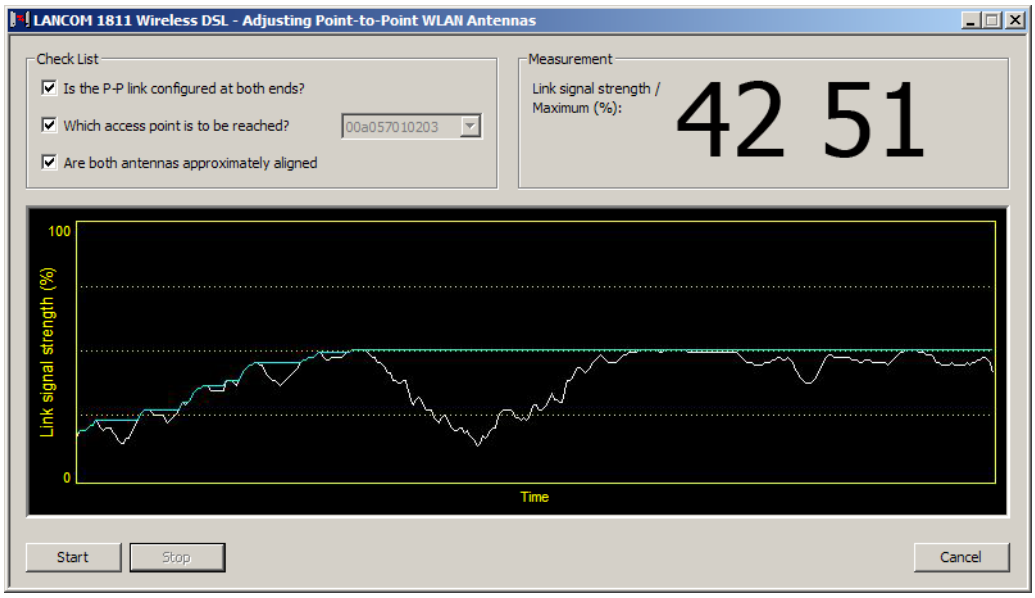


The **Point-to-point** entry is only visible in LANmonitor if the monitored device has at least one base station defined as a remote station for a P2P link (LANconfig: **Wireless LAN** > **General** > **Common point-to-point settings** > **Operation**).

In the dialog for setting up point-to-point links, LANmonitor prompts for the information required to establish the P2P connection:

- Is the P2P connection configured at both ends (remote base station defined with MAC address or station name)?
- Is the point-to-point mode of operation activated?
- Which AP should be monitored? All of the base stations defined as P2P remote sites in the device concerned can be selected here.
- Are both antennas approximately aligned? The basic P2P connection has to be working before fine-tuning can be performed with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. The trend of the signal strength over time and the maximum value are also displayed in a diagram.



Initially only one of the two antennas should be adjusted until a maximum value is achieved. This first antenna is then fixed and the second antenna is then adjusted to attain the best signal quality.

13.10.5 Surveys for wireless bridges

After planning and installation, the wireless bridge can be analyzed to determine the actual data throughput.

Further information about the available tools and taking measurements can be found in the *LANCOM Outdoor Wireless Guide*, available as a download from *www.lancom-systems.com*.

13.10.6 Activating point-to-point operation mode

The operation mode used by an AP to exchange data with other APs is set in LANconfig under **Wireless LAN** > **General** > **Common point-to-point settings** > **Operation** with the **Point-to-point operation mode** option:

Off

The AP communicates with mobile clients only.

On

The AP communicates with other base stations and with mobile clients.

Exclusive

The AP communicates with other base stations only.

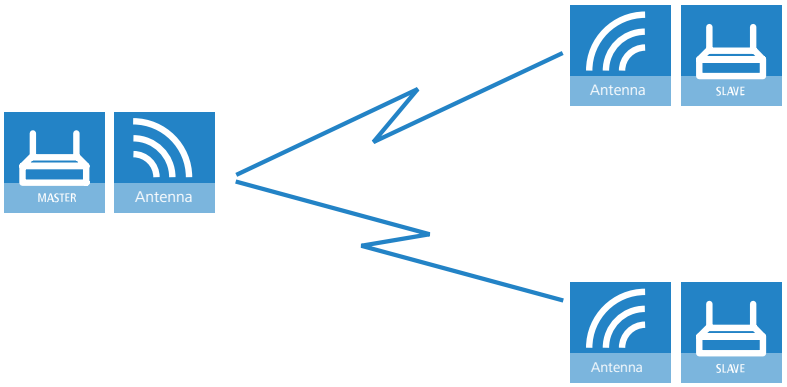
In the 5-GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple APs, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate **Channel selection scheme**.

Master

This AP makes the decisions when selecting a free WLAN channel.

Slave

All other APs will search for a channel until they have found a transmitting Master.



Thus it is recommended for the 5 GHz band that one central AP should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

It is imperative that the channel selection scheme is configured correctly if the WLAN bridges are to be encrypted with 802.11i/WPA (a master as authentication server and a slave as client).

Automatic channel selection for P2P links in the 5-GHz band is only enabled if the selected country profile supports DFS.

13.10.7 Configuration of P2P connections

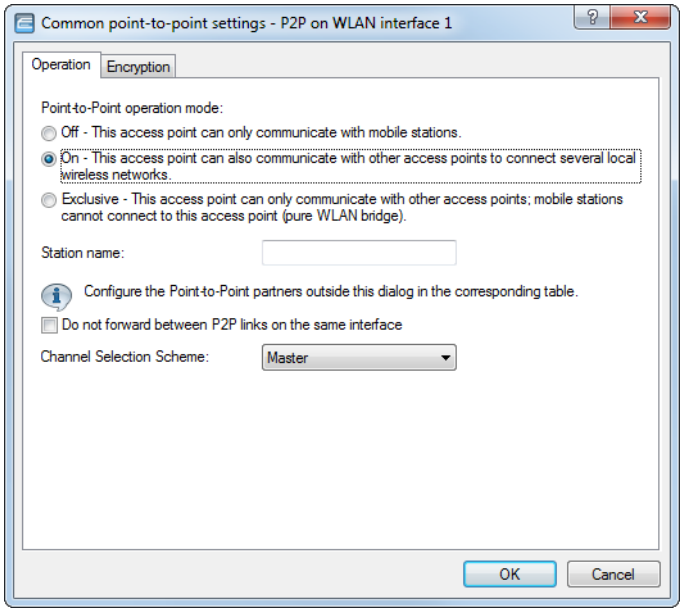
In the configuration of point-to-point (P2P) connections, enter the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names of the remote sites. The configuration can be done in LANconfig either by using the Setup wizard **Configure WLAN** or manually using the configuration dialog.

The following steps show you how you create an encrypted or unencrypted P2P basic configuration.

Along with a P2P connection, each of the APs automatically operates an SSID ***** P2P INFO *****. This SSID works purely as an administrative network for establishing the connection and for the availability check ("Alive") of a point-to-point partner. It is not possible for the WLAN clients to connect to this network.

1. Open the configuration dialog for the device that is to operate as the P2P master or P2P slave, and navigate to the page **Wireless LAN** > **General** > **Physical WLAN settings**.

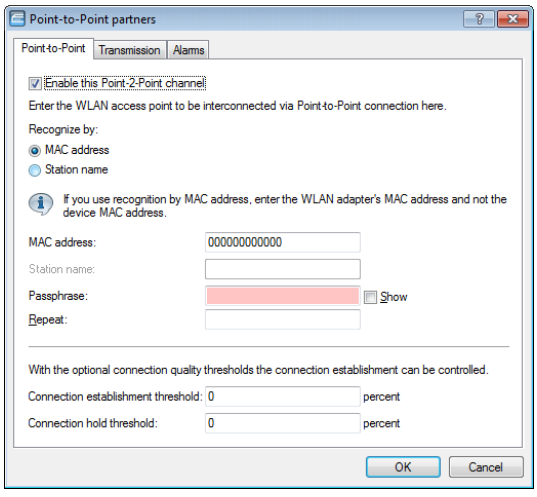
2. Select the WLAN interface which you want to use explicitly for the P2P connection and move to the tab **Point-to-Point**.



3. Enable the desired **Point-to-point operation mode**, such as **On**.
4. Set the **Channel selection scheme** to **Master** or **Slave**.
5. Optional: If the remote site should identify the physical interface by an alias and not the MAC address, then enter a corresponding descriptor into the field **Station name**, for example `P2P_MASTER` or `P2P_SLAVE`.
6. Optional: Adjust the settings on the tab **P2P encryption** for the IEEE 802.11i encryption of the P2P connection, if necessary.

   IEEE 802.11i can attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security MAC (LEPS-MAC).

   The setting options are practically identical with those of the physical WLAN interfaces, see *Encryption settings* on page 1028. By default, P2P encryption is enabled and filled-out with meaningful values.
7. Close the dialog with **OK** and under **Point-to-Point partners** on the same page of the configuration dialog select a logical P2P connection, such as **P2P-1-1**.



8. Enable the selected P2P channel on the **Point-to-Point** tab and specify whether the device identifies the remote station using a **MAC address** or a **Station name**. Here you then enter either the MAC address of the physical WLAN interface which the remote station uses for the P2P connection, or its station name accordingly.
   You will find the WLAN MAC address on a sticker located under each of the antenna connectors on the housing of the device. Only use the string that is marked as the "WLAN-MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.

   Alternatively, you will also find the MAC address in the status menu under **WLAN** > **Interfaces** > **MAC-Address**.

9. In **Passphrase**, enter a shared secret of at least 8 characters (recommended: 32 characters), which is used to additionally encrypt the P2P connection. The P2P encryption must be enabled for this (see above).
   When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the AP transfers this information to register with the remote site.
10. Optional: Move to the **Transmission** tab to enter the limits and settings for packet transmission.

    The setting options are practically identical with those of the logical WLAN networks (see *Alarm settings* on page 1037). By default, all parameters are adjusted for optimization and automatic operation.

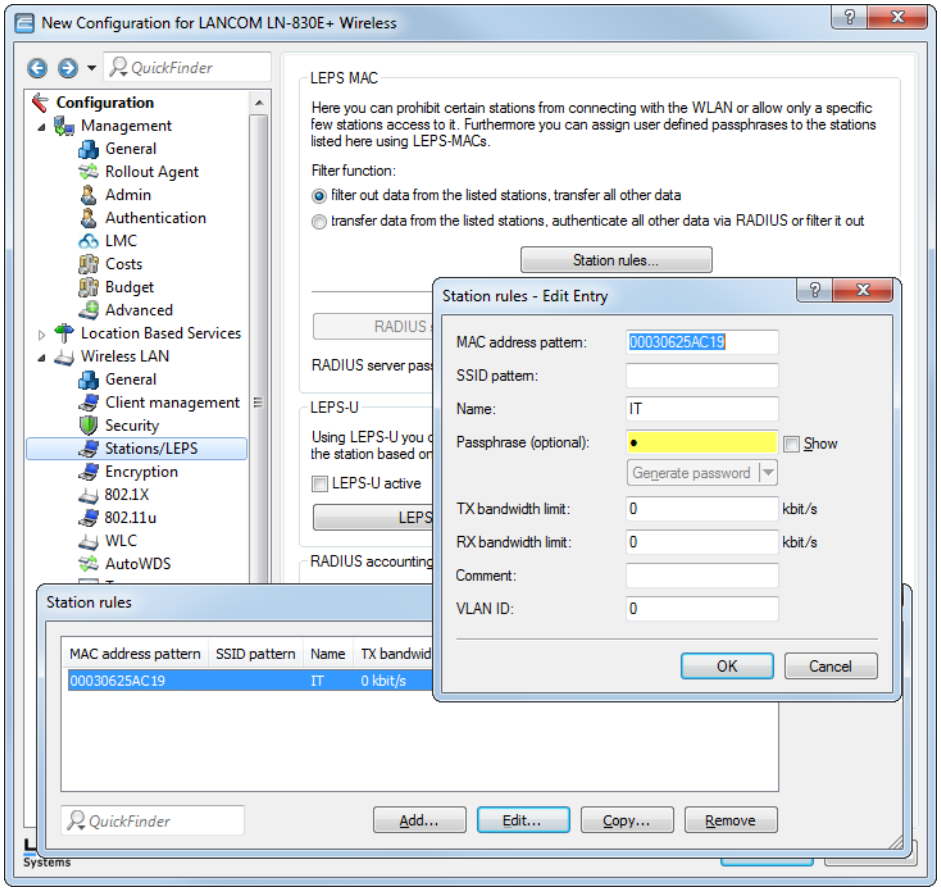
11. Close the dialog with **OK** and save the configuration to your device.
12. You continue by performing the corresponding configuration steps for the remote station (slave or master).

13.10.8 LEPS-MAC for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security MAC (LEPS-MAC) which involves the matching of MAC address and passphrase.

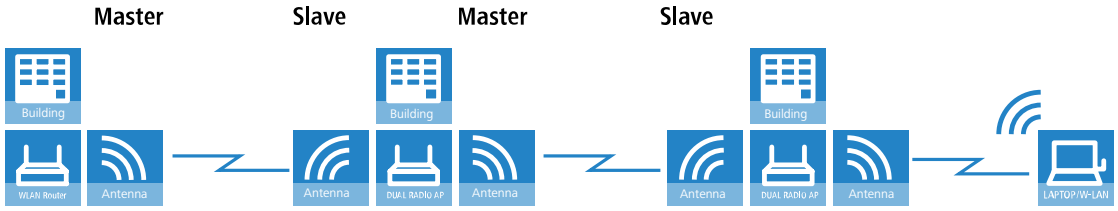
LEPS-MAC can be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an AP in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS-MAC remain secure.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration section 'Wireless LAN' on the 'Stations' tab under the button **Stations**.



13.10.9 Access points in relay mode

APs equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.



Employing relay stations with two WLAN modules each also cuts down on the problems from “hidden stations”.

13.11 Adaptive transmission power

Dynamic transmission power adaptation is an essential feature for WLAN environments with professional backup scenarios. If an AP fails, the remaining access points automatically increase their transmission power to ensure full WLAN coverage at all times.

To do this, specify how many APs operate within a broadcast domain. So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs becomes equal to the expected number of devices. The other APs return their transmission power to the default value.

For more about the configuration, see *Backup transmission power reduction (Adaptive Transmission Power)* on page 1044.

13.12 Opportunistic key caching (OKC)

Authentication of wireless clients using EAP and 802.11X has become standard in corporate networks, and these methods are becoming even more widespread with the integration of the Hotspot 2.0 specification for public Internet access. The disadvantage of 802.11X authentication is the significantly longer time between login and connection, because up to twelve data packets have to be exchanged between the WLAN client and the access point. For most applications, which are all about data exchange, this may not be particularly important. However, for time-critical applications such as Voice over IP, it is important that the authentication at neighboring WLAN radio cells does not affect communication.

To counteract this, authentication strategies such as PMK caching and pre-authentication have become established, although pre-authentication does not fix all of the problems. On the one hand, there is no guarantee that the WLAN client can recognize whether the access point can perform pre-authentication. On the other hand, pre-authentication causes considerable load on the RADIUS server, which needs to handle the authentication of all clients and all access points in the WLAN.

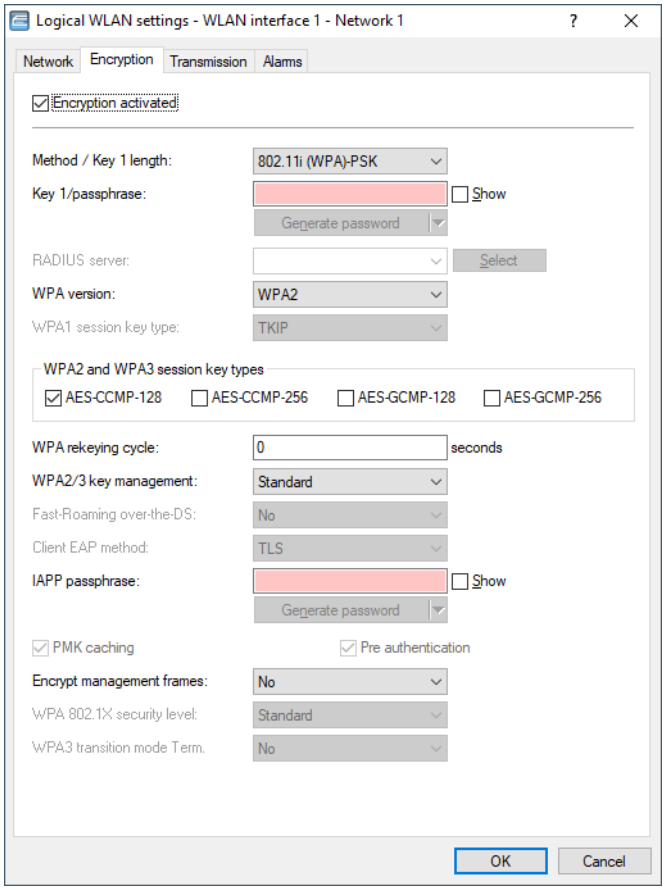
Opportunistic key caching delegates the key management to a WLAN controller, or to a central switch, which manages all of the access points in the network. If a client logs on to an access point, the WLAN controller behind it works as an authenticator to manage the keys and send the PMK to the access point, which is ultimately received by the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID. It then send this to the new access point in the hope that OKC is enabled there (therefore "opportunistic"). If the access point cannot handle the PMKID, then it negotiates an 802.11X authentication with the client in the usual manner.

A LANCOM access point can even perform OKC if the WLAN controller is temporarily unavailable. In this case, it stores the PMK and sends this to the WLAN controller when it becomes available again. Ultimately it sends the PMK to all of the access points in the network, which allows clients to use OKC to login after a change of radio cell.

13.12.1 Encrypted OKC via IAPP

By setting an IAPP passphrase (PMK-IAPP secret) on an AP, it is possible to transfer the encrypted PMK (pairwise master key) to the other APs and store it there.

To enter the IAPP passphrase in LANconfig, navigate to **Wireless LAN** > **General** > **Logical WLAN settings** > **Encryption**.



13.13 Fast roaming

By operating authentication according to the IEEE 802.1X standard and key management according to the IEEE 802.11i standard, modern WLAN installations offer a high degree of security and confidentiality for the transmitted data. However, these standards require transmission of additional data packets during the connection negotiation as well as additional computing power on the client and server.

The original IEEE 802.11 only required up to six data packets to establish a data connection between a WLAN client and an AP. The standard extension IEEE 802.11i improved on weak points of WEP encryption; however, depending on the authentication method, it substantially increased the length of the login process.

This extra time for the WLAN client to login to the AP is not a problem for non-time-critical applications. However, for smooth, loss-free roaming of a WLAN client from one AP to the next (as required, for example, for Voice-over-IP applications or in industrial, real-time environments), a delay of more than 50 ms is not acceptable.

Methods such as pair-wise master key caching (PMK caching), pre-authentication, opportunistic key caching (OKC) and the use of central WLCs for key management improve the time for the key negotiation between the WLAN client and AP during login. Despite this, the comparatively long time required for key negotiation between the WLAN client and the AP has still not been reduced to a viable extent.

Along with the improved encryption protocols, IEEE 802.11e makes it possible to reserve additional bandwidth with the AP. This allows the WLAN client to prevent interruptions, for example for VoIP connections at times of high network

loads at the AP. For roaming from one AP to the next, the WLAN client must again reserve this additional bandwidth on the new AP. However, the additional management frames required for this considerably increase the login time.

The IEEE 802.11r standard provides a simplified authentication process for mobile WLAN clients to roam trouble-free from one AP to the next. The goal is to once again reduce the number of data packets for the login on the AP to the four to six packets known from 802.11.

Similar to opportunistic key caching (OKC), a centralized key management (preferably by a WLC) supplies the APs connected to it with the credentials of the WLAN clients. In contrast to OKC, the WLAN client performing fast roaming can detect whether the AP supports IEEE 802.11r

APs managed by the WLC transmit the mobility domain information element (MDIE) to inform the WLAN clients about which "mobility group" the AP belongs to, among other things. Based on this information, the WLAN client detects whether it belongs to the same domain and can therefore authenticate without delay. This mobility domain is announced to a WLAN client the first time it authenticates at an AP.

The domain identifier and other special keys generated during the initial authentication and transmitted to all managed APs now reduce the stages of negotiation to the desired four to six steps when authenticating at a new AP.

To avoid futile and thus time-wasting login attempts with expired PMKs, IEEE 802.11r provides additional information about the validity periods of keys. In this manner, the client negotiates a new PMK while connected to the current AP. This is also valid on the AP that the WLAN client wants to connect to next.

Additionally, IEEE 802.11r uses "resource requests" to reserve additional bandwidth on the new AP, so that there is no need to cause added delay by transferring unnecessary data packets during the IEEE 802.11e authentication.



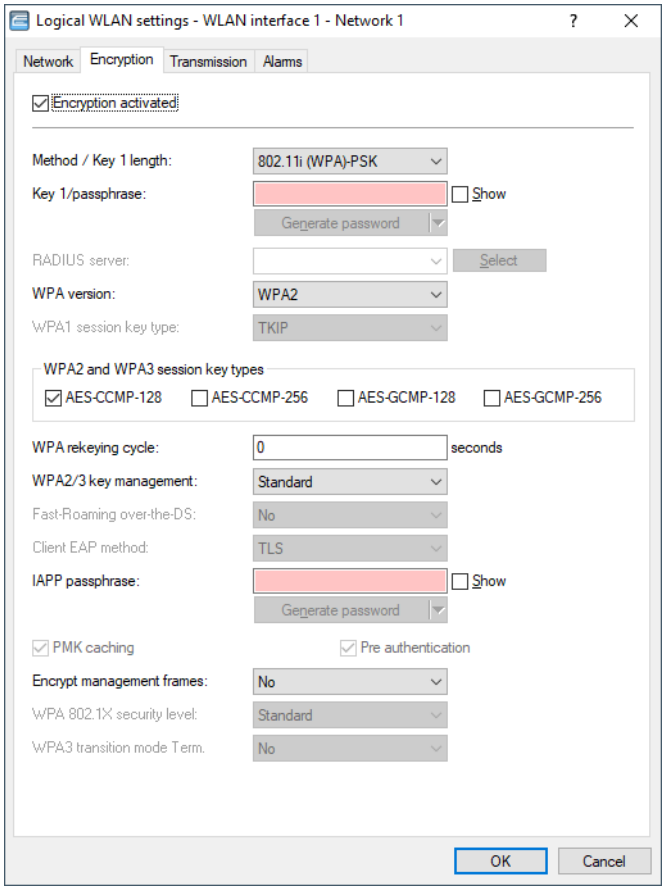
Older WLAN clients may have trouble establishing a connection to an SSID with enabled 802.11r. Therefore, it is advisable to use two SSIDs here: One SSID for older clients without 802.11r support and another SSID with enabled 802.11r for clients that support 802.11r.

Fast roaming is setup in LANconfig under **Wireless LAN** > **General** > **Logical WLAN settings** > **Encryption** > **WPA2/3 key management**.

13.13.1 Fast roaming with IAPP

In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). APs that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between themselves and ensure uninterrupted connections.

To enter the IAPP passphrase in LANconfig, navigate to **Wireless LAN** > **General** > **Logical WLAN settings** > **Encryption**.



Please note the use of IEEE 802.11r requires **WPA2/3 key management** in the encryption settings to be set to "Fast roaming".

13.14 Bandwidth limitations in the WLAN

The bandwidths that are available can be limited so that they can be better distributed among several participants in the WLAN. This bandwidth limit is available, for example, for wireless ISPs who want to provide their customers with a specified bandwidth.

Unlike bandwidth management using QoS (Quality of Service), this procedure does not allow a minimum bandwidth, but an exactly defined maximum bandwidth instead. Even if more bandwidth were actually available due to low traffic from other network stations, only the bandwidth specified here is provided to the user.

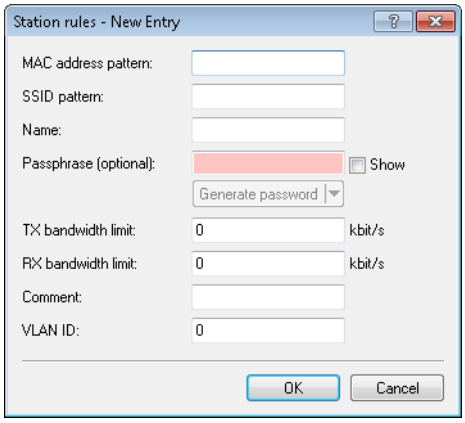
These settings are the difference between operating a device as an AP or in client mode.

13.14.1 Operating as an access point

In the AP operating mode, the maximum permitted bandwidths can be specified in Tx and Rx direction for the WLAN clients that register with the AP. The values of the maximum Tx and Rx bandwidths are entered in kbps in the MAC access list. A value of '0' indicates that there is no intention to restrict the bandwidth in this transmission direction. The bandwidth that is actually provided is determined from the value that is entered here and the value that is transmitted by the client.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for “Send data” and Tx stands for “Receive data”.

The maximum bandwidths for the connected clients are entered in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules**.



Comment

Comment on this entry.

VLAN-ID

VLAN ID for the WLAN client.

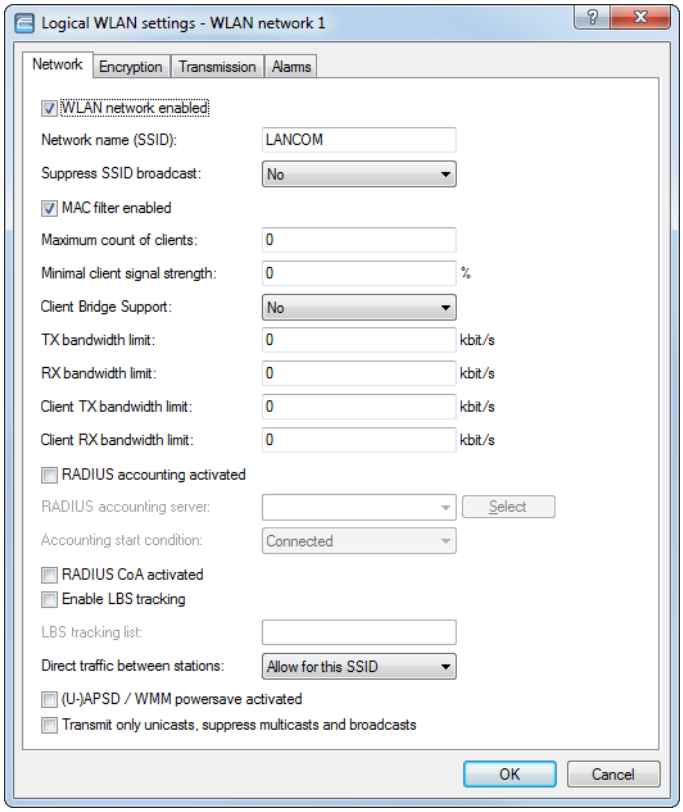
- Possible values: 0 to 4094
- Special values: 0: Switches the use of VLAN off.

13.14.2 Operating as a Client

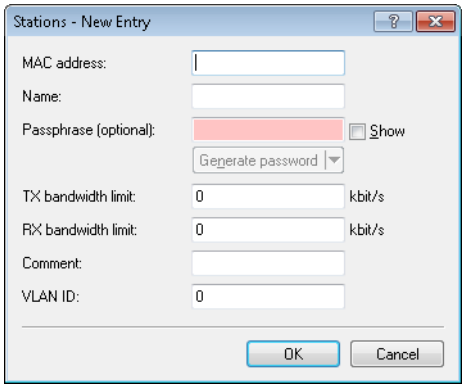
If the device is operated as a WLAN client, the device can transmit its maximum bandwidth when it registers with the AP. The AP then provides the actual maximum bandwidths with proprietary limits for this client where necessary.

The significance of the Rx and Tx values depends on the device's operating mode. In this case, as a client, Tx stands for “Send data” and Rx stands for “Receive data”.

The maximum bandwidths for a device in client mode are entered in LANconfig under **Wireless LAN** > **General** by clicking on **Logical WLAN settings**, selecting the corresponding logical WLAN interface and the **Network** tab.



On the WLC, bandwidth restrictions are set for each individual station under **WLAN controller** > **Stations/LEPS** > **LEPS-MAC** and by clicking on **Station rules**.



13.14.3 Bandwidth restriction of the LAN interfaces

For a device with an integrated WLAN module, you can specify a bandwidth limit for individual LAN ports. The table of LAN interfaces contains the parameters necessary to configure bandwidth restrictions.

13.15 Automatic adjustment of multicast and broadcast transmission rates

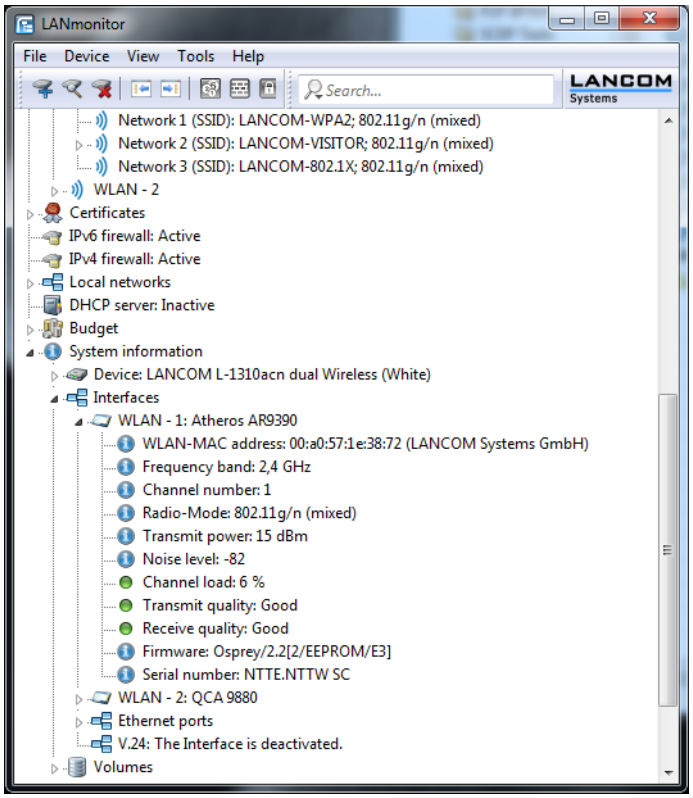
Whereas with unicast broadcasts the access point and client can negotiate the optimum transfer rate between them, multicast and broadcast transmissions communicate in just one direction: From the access point to the client. The clients cannot report back the access point with their actual maximum transmission speeds.

The access point has two options for setting the transmission rate for multicast and broadcast transmissions:

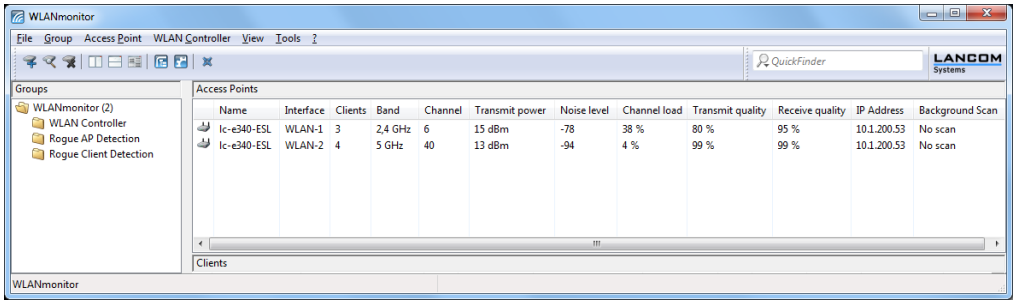
- **Fixed bit rate**: The transfer rate is set so that the slowest client in the WLAN can receive error-free transmissions even under unfavorable conditions. This can lead to the situation that the LANCOM transmits at a lower rate sends than environmental conditions and the clients would actually allow. As a result, the access point slows down the communications in the WLAN unnecessarily.
- **Automatic bit rate**: By setting the transmission rate to auto, the access point collects information about the transmission rates of the various WLAN clients. Clients automatically notify the access point of this rate with each unicast communication. The access point takes the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

13.16 LANCOM "Wireless Quality Indicators" (WQI)

LANmonitor optionally displays the signal quality of the individual interfaces with the **Wireless Quality Indicators**. This representation of reception and transmission quality (RX and TX) helps you to make a quick assessment of signal quality. To display this information in LANmonitor, open the section **System information** for the device. The indicators are displayed under **Interfaces**.



The WLANmonitor also displays the **Wireless quality indicators**. To do this click on the main folder for the group.



13.17 Configuring the WLAN parameters

The settings for the cellular networks are made at various points in the configuration:

- Some parameters concern the physical WLAN interfaces. Some LANCOM models have just one WLAN interface (single radio), and others have a second WLAN module integrated (dual radio). The settings for the physical WLAN interface apply to all of the logical wireless networks supported by this module. These parameters include, for example, the transmission power of the antenna and the operating mode of the WLAN module (AP or client).
- Other parameters are related solely to the logical wireless network that is supported by a physical interface. These include, for example, the SSID or the activation of encryption, such as 802.11i with AES.
- A third group of parameters affect the wireless network operation, but are not significant only to WLANs. These include, for example, the protocol filter in the LAN bridge.

13.17.1 General WLAN settings



LANconfig: **Wireless LAN** > **General**

Command line: **Setup** > **WLAN**

Country

Regulations for the operation of WLAN modules differ from country to country. The use of some radio channels is prohibited in certain countries. To operate the APs while observing the regulations in the relevant country, the Country setting is used to set up all of physical WLAN interfaces for the country where they are operated.

ARP handling

Mobile stations in the wireless network that are on standby do not answer the ARP requests from other network stations reliably. If 'ARP handling' is activated, the AP takes over this task and answers the ARP requests on behalf of stations that are on standby.

E-mail address for WLAN events

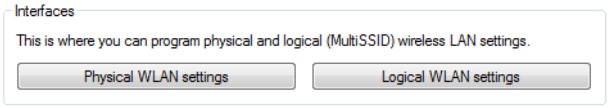
Information about events in the WLAN is sent to this e-mail address, if this is activated with the following switch.

Send e-mails

Activates the sending of notification mails to the e-mail address just specified.

13.17.2 The physical WLAN interfaces

In addition to the general WLAN parameters, a variety of settings apply specifically to each WLAN module in the AP.

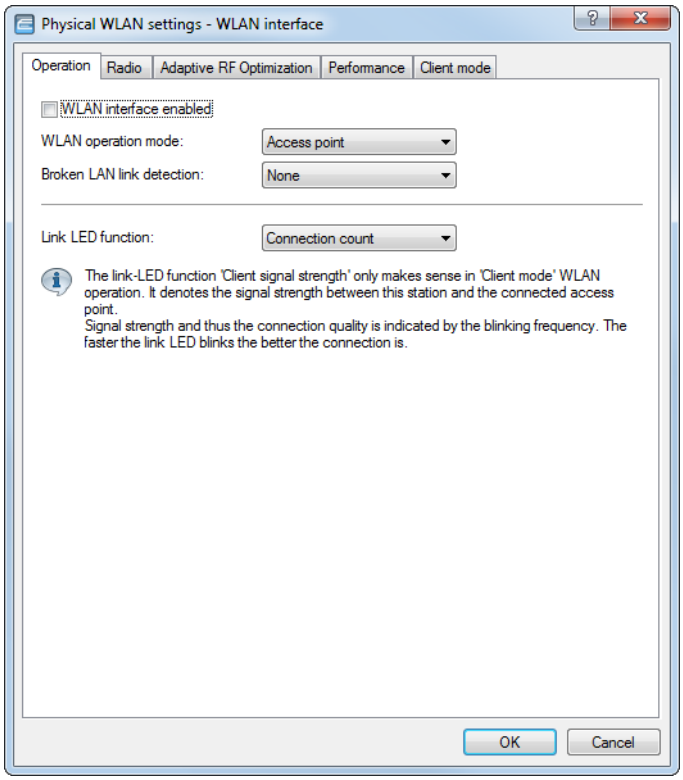


LANconfig: **Wireless LAN** > **General** > **Interfaces** > **Physical WLAN settings.**

If the AP has more than one radio module, you first select the relevant module in order to access its configuration pages.

13.17.2.1 Operation

This section contains the settings used for operation.



LANconfig: **Wireless LAN** > **General** > **Physical wireless LAN settings** > **Operation**

Command line: **Setup** > **Interfaces** > **WLAN** > **Operational**

WLAN interface enabled

If the WLAN interface is not required, it can be completely deactivated.

WLAN operation mode

LANCOM APs provide different operating modes:

Access point

An access point acts as a link between WLAN clients and the cabled LAN.

Client

In client mode, the device attempts to connect to another AP and to authenticate with a wireless network. In this case the device uses a radio link to connect a wired device to a base station.

Managed

As a managed AP, the device searches for a central WLC from which it can retrieve a configuration.

Probe

In the **Probe** operating mode the device collects WLAN information only, for example for an integrated spectrum analyzer.

Broken LAN-link detection

When an AP is not connected to the cabled LAN, it is normally unable to fulfill its primary task, namely the authorization of WLAN clients for access to the LAN. The broken-link detection function allows a device's WLAN to be disabled if the connection to the LAN should fail. Clients associated with that AP are then able to login to a different one (even one with a weaker signal).

This function allows the WLAN modules in a device to be disabled if the assigned LAN interface has no connection to the LAN.

Possible values:

None

Broken-link detection is disabled.

LAN-1 to LAN-n

Depends on the LAN interfaces available in the device. All of the WLAN modules in the device will be deactivated if the LAN interface set here should lose its connection to the cabled LAN.



The interface names LAN-1 to LAN-n represent the logical LAN interfaces. To make use of this function, the physical Ethernet ports on the device must be set with the corresponding values LAN-1 to LAN-n.



Broken-link detection can also be used for WLAN devices operating in WLAN client mode. With broken-link detection activated, the WLAN modules of a WLAN client are only activated when a connection exists between the relevant LAN interfaces and the cabled LAN.

Link LED function

When setting up point-to-point connections or operating the device as a WLAN client, the best possible positioning of the antennas is facilitated if the signal strength can be recognized at different positions. The WLAN link LED can be used for displaying the signal quality during the set-up phase. In the corresponding operating mode, the WLAN link LED blinks faster with better reception quality.

Possible values:

Connection count

In this operation mode, the LED uses "inverse flashing" in order to display the number of WLAN clients that are logged on to this AP as clients. There is a short pause after the number of flashes for each client. Select this operation mode when you are operating the device in access point mode.

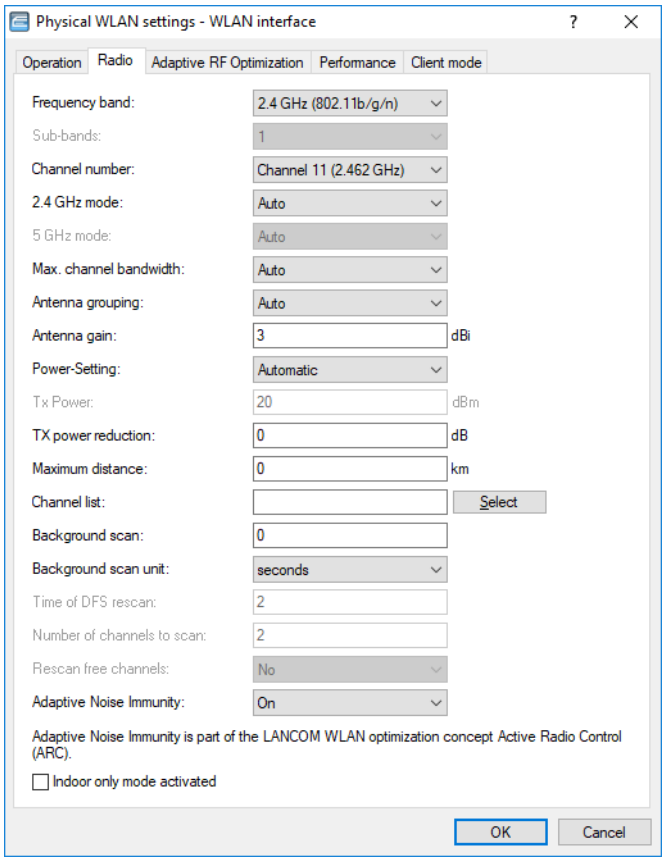
Client signal strength

In this operation mode, this LED displays the signal strength of the AP with which the device has registered itself as a client. The faster the LED blinks, the better the signal. Select this operation mode only if you are operating the AP in client mode.

P2P-1 to P2P-x signal strength

In this operation mode, the LED displays the signal strength of respective P2P partner with which the AP forms a P2P path. The faster the LED blinks, the better the signal.

13.17.2.2 Radio settings



LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Radio**

Frequency band, subbands

Selecting the frequency band determines whether the wireless LAN module operates in the 2.4-GHz or 5-GHz band, which in turn determines the available radio channels.

Furthermore in the 5-GHz band, a subband can be selected which is linked to certain radio channels and maximum transmission powers.

In some countries, the use of the DFS method for automatic channel selection is a legal requirement. Selecting the subband also defines the radio channels that can be used for the automatic channel selection.

Channel number

Specify the channel for data transmission in the WLAN here.

In the 2.4-GHz band, two separate wireless networks must be at least three channels apart to avoid interference.

2.4-GHz mode / 5-GHz mode

Here you specify the wireless standard(s) that the physical WLAN interface provides to the WLAN clients.

In the 2.4-GHz and the 5-GHz frequency bands, there are several different wireless standards that an AP can use for transmission. In the 2.5-GHz frequency band, these were to date the standards IEEE 802.11b, IEEE 802.11g and IEEE 802.11n; in the 5-GHz frequency band, the standards are IEEE 802.11a, IEEE 802.11n and IEEE 802.11ac. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

For example, if there are only 802.11n-enabled devices in your WLAN, we recommend you select the greenfield mode: By doing this you prevent login of slower clients which would otherwise act as a brake on the network.

By selecting a compatibility mode, you are able to achieve the best possible data rates without excluding slower WLAN clients (e.g., for 2.4 GHz "802.11b/g/n (mixed)"; for 5 GHz "802.11a/n (mixed)"). In compatibility mode, a physical WLAN interface works according to the fastest standard, but reverts to a slower standard if a slower WLAN client logs on to the network. When using 802.11b, you can select whether the physical WLAN interface should exclusively support 11-Mbps mode or also the older 2-Mbps mode ("(2-Mbps compatible)").

For APs operating according to the 802.11g standard you can optionally increase the data transfer speeds up to 108Mbps. In what is referred to as Turbo mode, an AP simultaneously uses two neighboring free channels for the radio transmission. With an AP in the 108Mbps Turbo mode, the only WLAN clients that can establish a connection to this AP are those also operating with the 108Mbps Turbo mode.

Turbo mode is associated with the 802.11g standard, although it was never officially adopted by the IEEE. The technology represents the proprietary extensions of various chipset manufacturers who also market this technology under the name "802.11g+" or "802.11g++". Turbo mode is therefore exclusively available on APs with pure 802.11g hardware.

If you leave the selection of the 2.5/5-GHz mode up to the device with the "Automatic" setting, the selection of the best mode depends on the frequency band in use and the capabilities of the device hardware:

- In the 2.4-GHz mode, the automatic setting results in either **802.11 b/g/n (mixed)** or **802.11 b/g (mixed)**.
- In the 5-GHz mode, the automatic setting results in either **802.11a/n/c (mixed)**, **802.11 a/n (mixed)**, or **54Mbps mode**.

In principle, according to 802.11n APs in the 2.4-GHz frequency band are backwards compatible to the IEEE 802.11b and IEEE 802.11g standards. Only the 802.11n-specific functions are not available for 802.11n hardware operated in 802.11b or 802.11g mode. However, this backwards compatibility is not available in the 5-GHz frequency band: The affected 802.11n devices must explicitly support 802.11a.

Max. channel bandwidth

Specify how and to what extent the AP specifies the channel bandwidth for the physical WLAN interface(s). Possible values:

Automatic

The AP automatically adjusts the channel bandwidth to the optimum. The AP allows the use of the maximum available bandwidth, assuming that the current operating conditions allow this. Otherwise, the AP limits channel bandwidth to 20MHz.

20 MHz

The AP uses channels bundled at 20 MHz.

40 MHz

The AP uses channels bundled at 40 MHz.

80 MHz

The AP uses channels bundled at 80 MHz.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Antenna grouping

Available for 802.11n only.

LANCOM APs with 802.11n support can use up to three antennas to transmit and receive data. Using several antennas with 802.11n can have different purposes:

- Improved data throughput: Using "spatial multiplexing" allows parallel data streams to be implemented to transmit double the amount of data.
- Improving wireless coverage: "Cyclic shift diversity (CSD)" can be used to transmit a radio signal in different phases. This reduces the risk of the signal being erased at certain points in the radio cell.

Depending on the application the use of the antennas can be set:

- When using the device in AP mode to connect wireless LAN clients it is generally recommended to use all three antennas in parallel in order to achieve good network coverage.
- To work with 2 parallel data streams; for example for point-to-point links with an appropriate dual slant antenna, the antenna ports 1 + 2 **or** 1 + 3 are used. The unused antenna port is deactivated.
- For applications with only one antenna (for example an outdoor application with just one antenna) the antenna is connected to port 1 and ports 2 and 3 are deactivated.
- The "Auto" setting means that all available antennas are used.

Please note the following when connecting antennas: Antenna connector 1 must always be used. Depending on the mounting and cabling, the second antenna may be connected either to connector 2 or connector 3. The configuration of the device software must agree with the actual antenna connections.

Antenna gain

Where the transmission power of an antennae exceeds the levels permitted in the country of operation, the power must be attenuated accordingly. Here you enter the gain of the antenna minus the actual cable loss. For an AirLancer Extender O-18a antenna with a gain of 18 dBi and a 4 m cable with a loss of 1 dB/m, the 'Antenna gain' would be entered as 18 - 4 = 14. This value for true antenna gain is dynamically used to

calculate and emit the maximum permissible power with regards to other parameters such as country, data rate and frequency band.

Power setting

The **Automatic** mode uses the maximum permitted transmission power that can be realized by the access point hardware. In addition, the current WLAN transmission power can be reduced by a fixed value configured in the field **TX power reduction**. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5-GHz subbands. For example, higher transmission powers are permitted in the 5-GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. In the **Manual** mode, the actual maximum **transmission power** can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

Under no circumstances will the access point exceed the legal limits for transmission power. These are always respected automatically, regardless of the settings made here.

TX power

The desired transmission power in dBm.

TX power reduction

Static reduction of the transmission power by the value entered here. Other parameters are not taken into account.

The transmission power reduction simply reduces the emitted power. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, the highest possible data transfer rates.

Maximum distance

The run-time over large distances between transmitter and receiver give rise to increasing delays for the data packets. If a certain limit is exceeded, the responses to transmitted packets no longer arrive within a given time limit. The entry for maximum distance increases the wait time for the responses. This distance is converted into a delay as required by the data packets for wireless communications.

Channel List

Access points automatically carry out channel selection for the frequency band available in the country of operation, assuming that no entry is made here.

Enter the channels to be available for automatic selection. If just one channel is defined here, then only this channel will be used and no automatic selection takes place. For this reason you should ensure that the channels entered here are legal for use in the defined country of operation. Channels which are invalid for the frequency band are ignored.

If radar detection is enabled, the channels entered here are preferred. If radar pulses are detected on these channels, the device will attempt to switch to further channels that are not listed here. Only when radar detection is switched off by activating the indoor-only mode is the selection of the channels performed exclusively.

The channels for automatic selection are specified as a comma-separated list.

For example, the entry "1, 7-9, 13" means that the automatic channel search is limited to the channels 1, 7 to 9, and 13.

Background scan / Background scan unit

If a value is entered here, the wireless router or AP searches currently unused frequencies in the active band to find available APs. This value is the time interval between search cycles.

- The background scan function is usually deployed for rogue AP detection for the device in AP mode. This scan interval should correspond to the time span within which rogue APs should be detected, e.g. 1 hour.
- Conversely, for the device in client mode, the background scan function is generally used for improved mobile WLAN client roaming. In order to achieve fast roaming, the scan time is limited here, for example, to 260 seconds.
- When the background scan time is '0' the background scanning function is deactivated.

The time interval allows the entered value to be defined in milliseconds, seconds, minutes, hours or days.

To avoid adverse effects on data transfer rates, the interval between channel scans in AP mode is at least 20 seconds. Lesser values will be corrected to this minimum value automatically. For example, with 13 channels to scan in the 2.4-GHz band, one scan of the full spectrum takes at least 13 x 20s = 260 seconds.

Background scanning can be limited to a lower number of channels when indoor mode is activated. This allows roaming for the mobile wireless router or AP in client mode to be improved even further.

DFS configuration

Configure the DFS settings here.

For information on Dynamic Frequency Selection, see *Dynamic Frequency Selection (DFS)*.

Adaptive noise immunity

Adaptive Noise Immunity can be activated or deactivated here.

For information on Adaptive Noise Immunity, see *Adaptive Noise Immunity*.

Indoor-only mode activated

By selecting the frequency band (2.4 or 5 GHz) you determine which channels can be used to transmit data, among other things. From these available channels, automatic channel selection causes an AP to select a vacant channel in order, for example, to avoid interference with other radio signals.

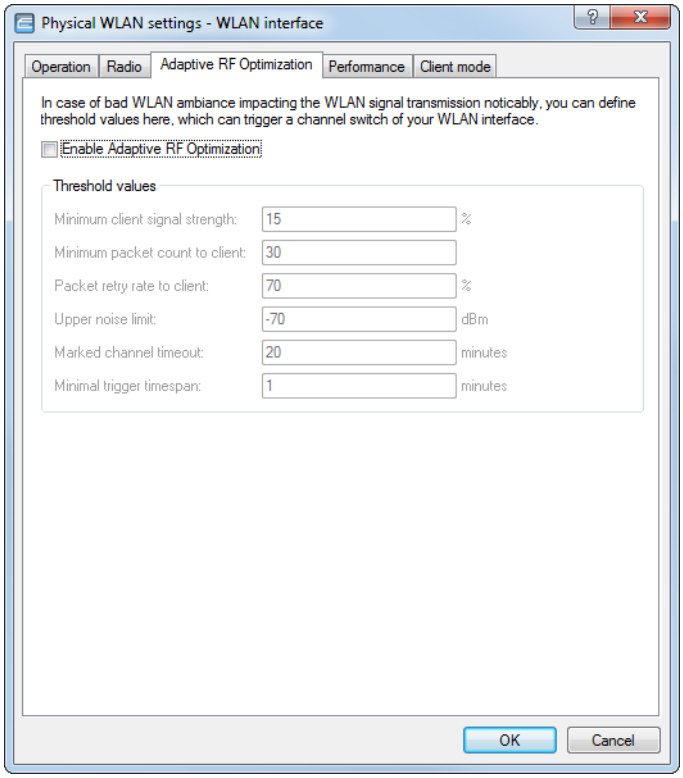
In some countries, there are special regulations on the frequency bands and channels which may be used for WLAN for indoor and outdoor operation. For example, in France, not all available channels in the 2.4-GHz band may be used in outdoor operation. In some countries the DFS procedure is required for outdoor operation in the 5-GHz band in order to avoid interference from radar systems.

The option 'indoor-only' sets up an AP for operation exclusively within closed buildings. This restriction on the other hand allows the channels to be managed more flexibly under automatic channel selection.

The indoor-only function only functions correctly if the country in which the AP is being operated has been set.

Activating the indoor-only function is only permitted when the AP and all connected clients are located within a closed space.

13.17.2.3 Adaptive RF Optimization



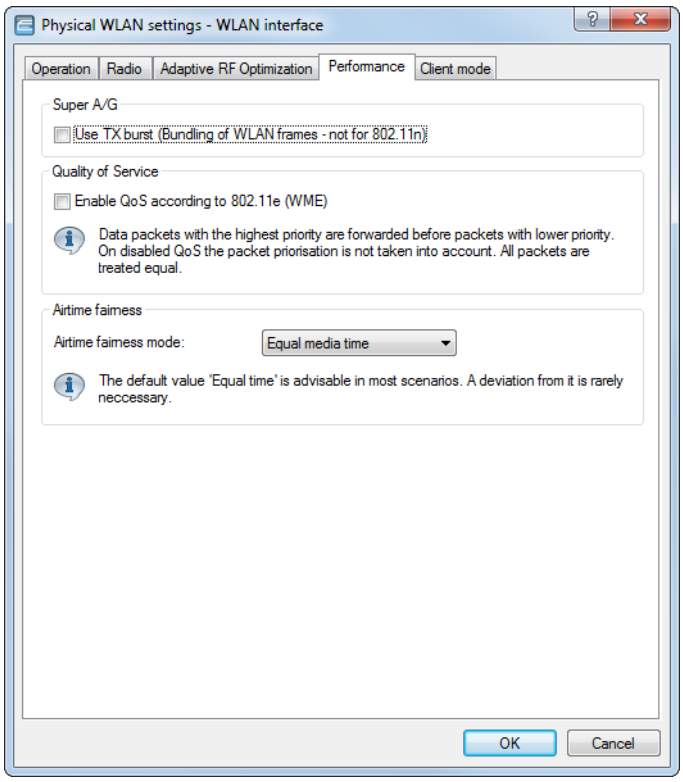
LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Adaptive RF optimization**

Configure the settings for the adaptive RF optimization here. For further information, please see *Adaptive RF Optimization* on page 972:

13.17.2.4 Performance

LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Performance**

Command line: **Setup** > **Interfaces** > **WLAN** > **Performance**



Use TX burst

Enables/prevents packet bursting for increasing throughput. Bursting leads to less fairness on the medium.

Enable QoS according to 802.11e (WME)

With the extension to the 802.11 standard, 802.11e, Quality of Service can be provided for transfers via WLAN. Among others, 802.11e supports the prioritization of certain data-packet types. This extension is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN). The WiFi alliance certifies products that support Quality of Service according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) which make up separate queues to be used for prioritization. The 802.11e standard sets priorities by referring to the VLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

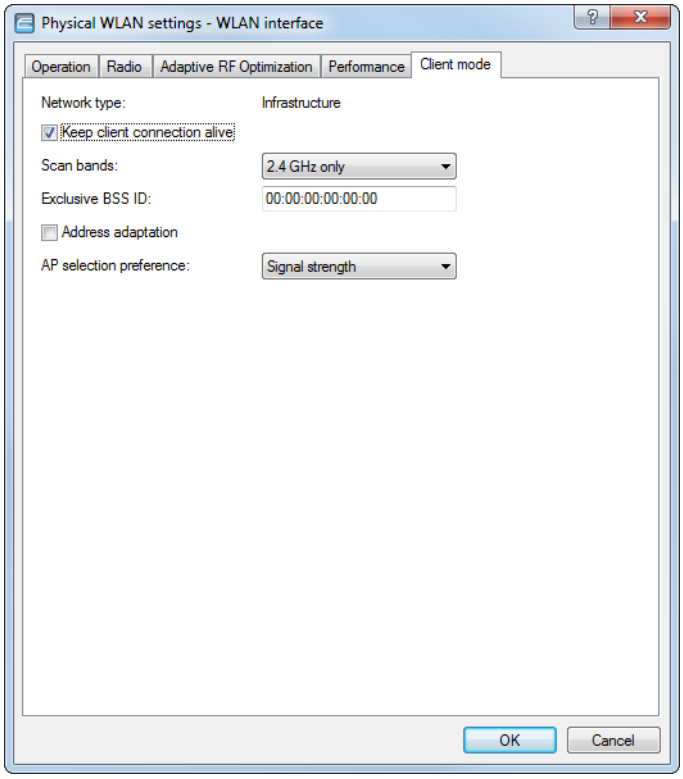
Priorities can only be set if the WLAN client and the AP both support 802.11e or WMM, and also if the applications are able to mark the data packets with the corresponding priorities.

Airtime Fairness

Configure the settings of airtime fairness here. For further information, please see *Airtime Fairness* on page 975:

13.17.2.5 Client mode

If the device is operating as a client, the tab 'Client mode' can be used for further settings that affect the behavior as a client.



LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Client mode**

Command line: **Setup** > **Interfaces** > **WLAN** > **Client-Modes**

Keep client connection alive

This option ensures that the client station keeps the connection to the access point alive even if the connected devices are not exchanging any data packets. If this option is disabled, the client station is automatically logged off the wireless network if no packets are transferred over the WLAN connection within a specified time.

Scan bands

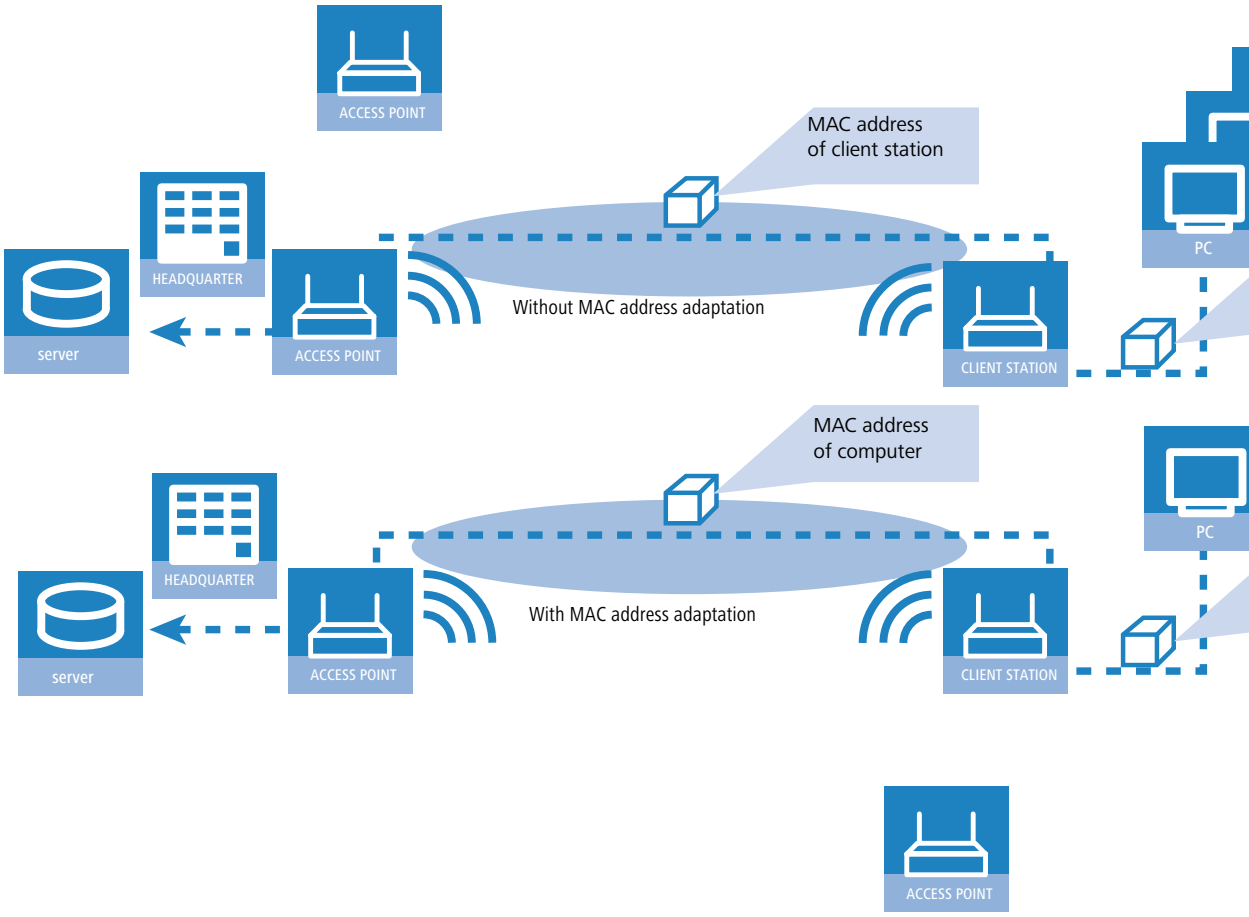
This defines whether the client station scans just the 2.4 GHz, just the 5 GHz, or all of the available bands for access points.

Exclusive BSS ID

If the client station is to log onto one particular AP only, the MAC address of the WLAN module in this AP can be entered here.

Address adaptation

In client mode, the client station normally replaces the MAC addresses in data packets from the devices connected to it with its own MAC address. The AP at the other end of the connection only ever "sees" the MAC address of the client station, not the MAC address of the computer(s) connected to it.



In some installations it may be desirable for the MAC address of a computer to be transmitted to the AP and not the MAC address of the client station. The option **Address adaptation** prevents the MAC address from being replaced by the client station. Data packets are transferred with their original MAC addresses—in the WLAN, the AP takes the client's MAC address.

Address adaptation only works when just **one** computer is connected to the client station.

AP selection preference

If several APs are available that match different profiles, the following criteria can be used to select the AP.

Profile

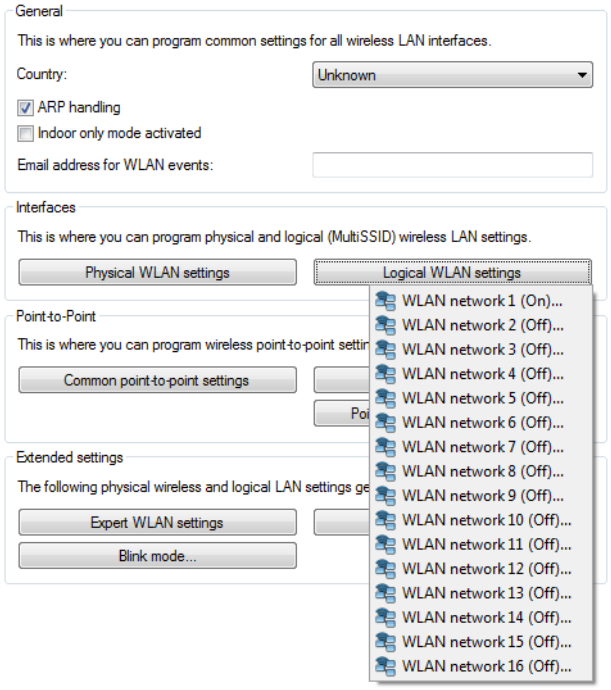
The profile with the smallest index is chosen, even if a stronger AP is available that matches a profile of a higher index.

Signal strength

The signal strength is the most important selection criterion.

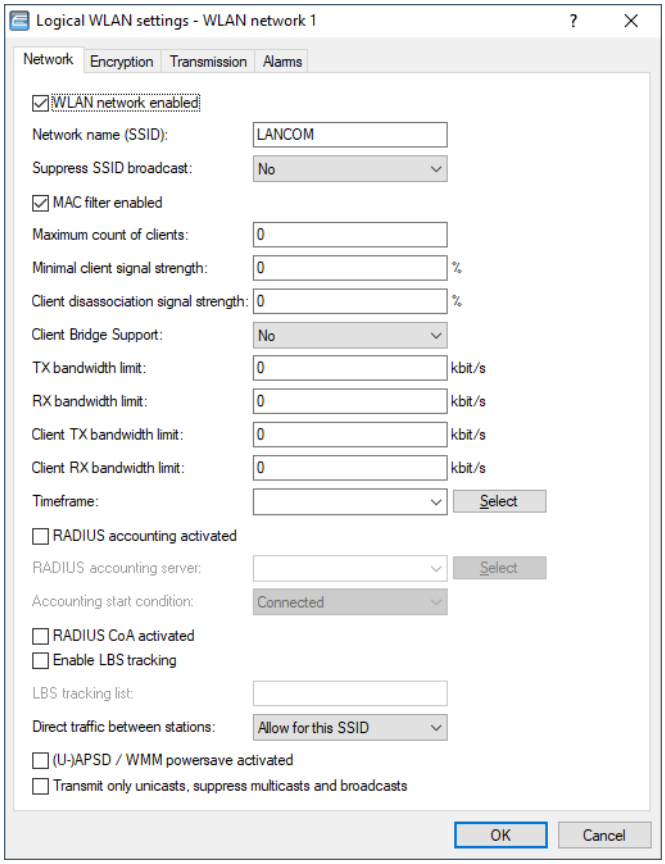
13.17.3 The logical WLAN interfaces

Every physical WLAN interface can support up to 16 different logical cellular networks (Multi-SSID). Parameters can be defined specifically for each of these networks, without the need of additional access points.



13.17.3.1 Network settings

The following settings are made in LANconfig in **Wireless LAN** > **General** > **Logical WLAN settings** > **Network**.



WLAN network enabled

This switch enables or disables the corresponding logical WLAN.

Network name (SSID)

Specify a unique SSID (the network name) for each of the required logical wireless LANs. Only clients configured with the same SSID can associate with this wireless network.

Suppress SSID broadcast

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the **Tightened** option. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the "Tightened" mode enabled, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

No

The AP publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the AP responds with the SSID of the radio cell (public WLAN).

Yes

The AP does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the AP similarly responds with an empty SSID.

Tightened

The AP does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the AP does not respond.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the AP, this transmits the SSID in cleartext so that it is briefly visible to all clients in the WLAN network.

MAC filter enabled

The MAC addresses of the clients that are allowed to associate with an AP are stored in the MAC filter list (**Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

Use of the MAC filter list is required for logical networks in which the clients register via LEPS-MAC with an individual passphrase. The passphrase used by LEPS-MAC is also entered into the MAC filter list. The AP always consults the MAC filter list for registrations with an individual passphrase, even if this option is deactivated here.

Maximum count of clients

Here you set the maximum number of clients that may associate with this AP. Additional clients wanting to associate will be rejected by the AP.

Minimum client signal strength

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the AP stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the AP and cannot associate with it. This ensures that the client has an optimized list of available APs, as those offering only a weak connection at the client's current position are not listed.

Client disassociation signal strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value **Minimum client signal strength** is also set and the **Client disassociation signal strength** is less than this value.

Client bridge support

Enable this option for an AP if you have enabled the client-bridge support for a client station in WLAN client mode.

The client-bridge mode only operates between two LANCOM devices.

TX bandwidth limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID (limit in kbps). A value of `0` disables the limit.

RX bandwidth limit

With this setting, you define the overall bandwidth that is available in the reception direction within this SSID (limit in kbps). A value of `0` disables the limit.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Timeframe

Select one of the time frames defined in *Timeframe* on page 1669. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

RADIUS accounting activated

Enable this option to switch on RADIUS accounting for this SSID.

RADIUS accounting server

If you operate RADIUS for the central administration of accounts and access credentials in your wireless network, then the access point forwards requests for the authorization and accounting to the RADIUS server by default. If you are using a WLAN controller for access point management, then the controller can forward RADIUS requests from all of these access points to the RADIUS server.

In some cases, the operator of access points or WLAN controllers may wish to use a different RADIUS server for each logical wireless network (SSID). This may be the case, for example, when multiple customers share the same technical WLAN infrastructure but use their own authentication systems (e.g. with Wireless as a Service – WaaS).

In these cases, you have the option to choose a separate RADIUS profile for each logical WLAN (i.e. each SSID). The RADIUS profile contains all of the necessary information to use the appropriate RADIUS server, including the optional backup solution.

Here you specify a RADIUS accounting server for the respective SSID. The servers that can be selected here are specified in the table under **Wireless LAN** > **Stations/LEPS** > **RADIUS Accounting** > **RADIUS accounting servers**.

Accounting-Start-Condition

Normally, the WLAN stack sends a RADIUS "accounting start" message as soon as the WLAN client is connected. Often the WLAN client has no IP address at this time, most likely because one has not yet been issued by the DHCP server. Consequently the `Framed-IP-Address` attribute in the RADIUS accounting message may lack meaningful content.

Connected

Accounting starts when the WLAN client takes on the status “Connected”. This is the default setting.

Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6).

Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address.

Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address.

APIPA addresses (`169.254.1.0` – `169.254.254.255` and `fe80:`) are not recognized as valid IP addresses.

RADIUS CoA activated

RADIUS CoA (Change of Authorization) provides the capability to modify current WLAN sessions. A modification is initiated when the CoA client sends a CoA message to the NAS. This message contains the identifying characteristics for the session to be modified, the attributes to be modified, and their new values.

Another option is to disconnect the current session. This is done with a disconnect message (DM) sent to the NAS, whereupon the NAS terminates the connection.

For more information about the configuration of RADIUS CoA see the section *Configuring dynamic authorization with LANconfig* on page 1558.

Enable LBS tracking

This option specifies whether the LBS server is permitted to track the client information.

This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

Direct traffic between stations

Check this option if all stations logged on to this SSID may communicate with one another.

(U)APSD / WMM power save activated

Enable this option to signal stations that the power saving function (U)APSD ([Unscheduled] Automatic Power Save Delivery) is supported.

(U)APSD is established in the 802.11e standard, and helps VoWLAN devices to increase their battery life. The related devices switch to power saving mode after login on a (U)APSD-capable AP. If the AP receives data packets for the related devices thereafter, it temporarily stores the data and waits until the VoWLAN device is available again. It then forwards the data. Afterwards, (U)APSD increases the latency time of the radio module, whereby it ultimately consumes less power. The individual rest periods may be so short that a VoWLAN device can still use the power saving function in the call state itself. However, the relevant devices must also support (U)APSD.

WWM (Wi-Fi Multimedia) Power Save is a power saving function of the Wi-Fi Alliance and is based on U-APSD. Certain LANCOM APs are WMM® Power Save CERTIFIED by the Wi-Fi Alliance.

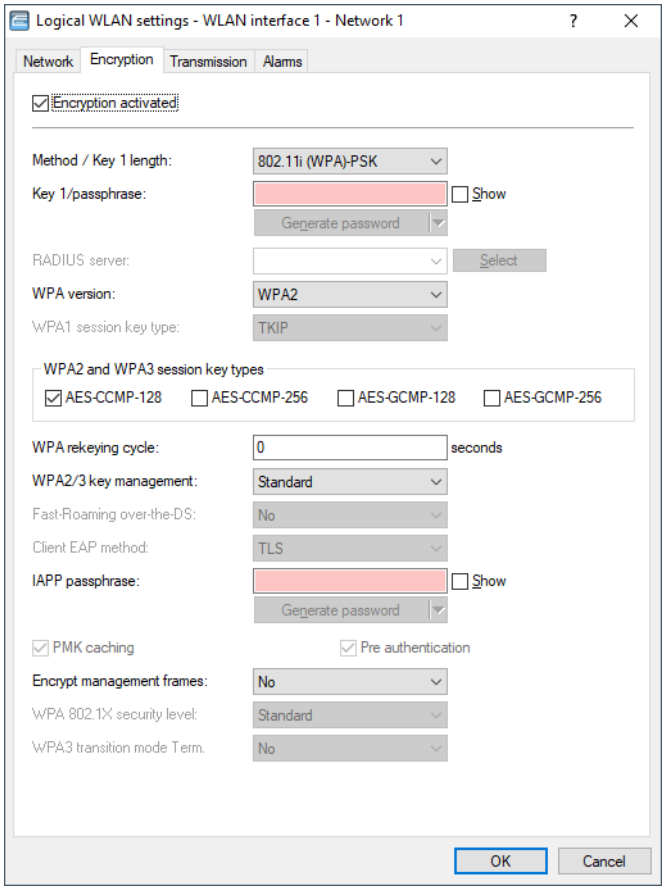
Only transmit unicasts, suppress broadcast and multicasts

Multicast and broadcast transmissions within a WLAN cell cause a load on the bandwidth of the cell, especially since the WLAN clients often do not know how to handle these transmissions. The AP already intercepts a large part of the multicast and broadcast transmissions in the cell with ARP spoofing. With the restriction to unicast transmissions it filters out unnecessary IPv4 broadcasts from the requests, such as Bonjour.

The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

13.17.3.2 Encryption settings

Details for the encryption over the logical interface in LANconfig are set under **Wireless LAN** > **General** > **Logical WLAN settings** > **Encryption**.



Enable encryption

Enable or disable encryption for this WLAN interface.

Method/key 1 length

Set the encryption method to be used here. Possible values are:

802.11i (WPA)-PSK

Encryption according to the 802.11i standard offers the highest security. The 128-bit AES encryption used here offers security equivalent to that of a VPN connection. Select this setting if no RADIUS server is available and authentication is based on a pre-shared key.

802.11i (WPA)-802.1X

Select this option if authentication is performed by a RADIUS server. When using this setting, additionally ensure that the RADIUS server is configured in the 802.1X settings.

WEP 152, WEP 128, WEP 64

Encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively. This setting should only be used if the WLAN client does not support the modern methods.

WEP 152-802.1X, WEP 128-802.1X, WEP 64-802.1X

Encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively, and with additional authentication via 802.1X/EAP. This setting is also only to be recommended when the hardware

used by the WLAN client does not support the 802.11i standard. The 802.1X/EAP authentication offers a higher level of security than WEP encryption alone.

Enhanced Open

Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. Also, the widespread practice of securing a hotspot with WPA2-PSK and publicly posting the shared key provides limited security. Since WPA2-PSK does not provide Perfect Forward Secrecy, an attacker who knows the key can use it to decrypt recordings of data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot. Just set the encryption method. That is all you need to do to encrypt communications for clients that support this method. To use Enhanced Open with the Public Spot, also see *Setting up a secure hotspot with Enhanced Open* on page 1357.

Enhanced Open Transitional

The Enhanced Open Transition mode allows connections to clients that support Enhanced Open and also to those that do not yet support Enhanced Open. With the transition mode in operation, the regular Enhanced Open SSID is operated in parallel to an unencrypted/open SSID with the same name and otherwise identical settings.

A prerequisite for this is that at least one other SSID is available and unused on the selected radio module. Depending on the device, a total of 15 or 16 SSIDs are available per radio module. If no SSID is available, both the Open Transition SSID and the actual Enhanced Open SSID will not be activated.

Key 1/passphrase

In line with the encryption method activated, you can enter a special WEP key for the respective logical WLAN interface or a passphrase when using WPA-PSK:

- The passphrase, or the "password" for the WPA-PSK method, is entered as a string of at least 8 and up to 63 ASCII characters.

  Please be aware that the security of this encryption method depends on the confidential treatment of this passphrase. Passphrases should not be made public to larger circles of users.

- The WEP key 1, that applies only to its respective logical WLAN interface, can be entered in different ways depending on the key length. Rules for entering the keys can be found in the description of the WEP group key.

RADIUS server

If you operate RADIUS for the central administration of accounts and access credentials in your wireless network, then the access point forwards requests for the authorization and accounting to the RADIUS server by default. If you are using a WLAN controller for access point management, then the controller can forward RADIUS requests from all of these access points to the RADIUS server.

In some cases, the operator of access points or WLAN controllers may wish to use a different RADIUS server for each logical wireless network (SSID). This may be the case, for example, when multiple customers share the same technical WLAN infrastructure but use their own authentication systems (e.g. with Wireless as a Service – WaaS).

In these cases, you have the option to choose a separate RADIUS profile for each logical WLAN (i.e. each SSID). The RADIUS profile contains all of the necessary information to use the appropriate RADIUS server, including the optional backup solution.

If you select an authentication method based on the IEEE 802.1X standard under **Method/Key 1 length**, you specify the profile of a RADIUS server here.

WPA-Version

WPA version for encryption offered by the access point to the WLAN clients.

WPA1

WPA2 only

WPA2

WPA2 only

WPA1/2

WPA1 and WPA2 in one SSID (radio cell)

WPA2/3

WPA2 and WPA3 in one SSID (radio cell)

WPA3

WPA3 only

WPA1/2/3

WPA1, WPA2 and WPA3 in one SSID (radio cell)

WPA1 session key type

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key for WPA1 can be selected here:

AES

The AES method will be used.

TKIP

The TKIP method will be used.

AES/TKIP

The AES method will be used. If the client hardware does not support the AES method, TKIP will be used.

WPA2 and WPA3 session key types

Here you select the methods that should be offered for generating the WPA2 or WPA3 session or group keys. The following Advanced Encryption Standard (AES) methods can be offered: AES-CCMP-128, AES-CCMP-256, AES-GCMP-128, AES-GCMP-256.

WPA rekeying cycle

Here you configure the time in seconds after which the access point performs rekeying when operating a version of WPA. By default, the value is set to “0”, so there is no renegotiation of the key.

WPA2/3 key management

Here you specify the standard to be used for WPA2/3 key management. Possible values are:

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming as per 802.11r

SHA256

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

Combinations of these three settings

Activates a corresponding combination.

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the AP are compatible. Unsuitable clients may refuse a connection if an option other than **Standard** is enabled.

Fast-Roaming over-the-DS

With Fast Roaming over-the-DS (Distribution System) you can activate an option of the IEEE 801.11r standard, which takes advantage of the LAN connection between the access points. The roaming request is sent to the access point that the client is connected to. The AP forwards the request to the new access point and the swap is performed. This means significantly faster roaming speeds than possible with the usual "over-the-air fast transition", which is a big benefit to real-time applications such as VoIP.

Client EAP method

In WLAN client operating mode, APs can authenticate themselves to another AP using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.

Note that the selected client EAP method must match the settings of the access point that the AP is attempting to log onto.

In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode. The client EAP method setting has no function on logical WLAN networks other than WLAN 1.

IAPP passphrase

This passphrase is used to implement encrypted opportunistic key caching. See *Opportunistic key caching (OKC)* on page 1004.

PMK caching

When establishing a connection from a WLAN client to an AP operating with 802.1X-authentication, the two stations negotiate a shared key, known as the Pairwise Master Key (PMK), for the subsequent encryption. In applications with mobile WLAN clients (laptops in large offices, moving objects with WLAN connections in the industrial sector, smartphones), the WLAN clients often switch between the APs they use to access the WLAN network. And although WLAN clients roam back and forth between different APs, in most cases these tend to be the same ones.

APs typically save a negotiated PMK for a certain period of time. WLAN devices in WLAN client mode also store PMKs. As soon as a WLAN client starts a login procedure for which a connection already existed, the WLAN client can directly transfer the existing PMK to the AP. In this way, the two remote stations skip the PMK negotiation phase while establishing the connection, and the WLAN client and AP establish the connection much faster.

Pre-authentication

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the AP previously. The WLAN client uses pre-authentication to reduce the time to logon to the AP at the first logon attempt.

Usually, a WLAN client carries out a background scan of the environment to find existing APs that it could connect to. APs that support WPA2/802.1X can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1X authentication as follows:

- The WLAN client logs on to the new AP via the infrastructure network, which interconnects the APs. This can be an Ethernet connection or a WDS link (wireless distribution system), or a combination of both connection types.
- A pre-authentication is distinguished from a normal 802.1X authentication by the differing Ethernet protocol (EtherType). This allows the current AP and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new AP and the WLAN client.

  The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.
- When the client wants to connect to the new AP, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the PMK caching.

On the client side, the number of concurrent pre-authentications is limited to four. This minimizes the network load on the central RADIUS server in network environments with large numbers of APs.

Encrypt management frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don't have the corresponding key.

As of WPA3, management frames must be encrypted. For WPA2, this is optional.

WPA 802.1X security level

WPA-3 additionally features support for the Commercial National Security Algorithm (CNSA) Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

The switch **WPA 802.1X security level** under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings** is used to enable the optional Suite B encryption. With "Suite B 192 bits" support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

With "Suite B 128 bits" support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-128 is also enforced.

Because the session key types AES-GCMP-128 and AES-GCMP-256 are not supported by all WLAN modules, the use of Suite B cryptography may be limited or impossible, depending on the device type.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

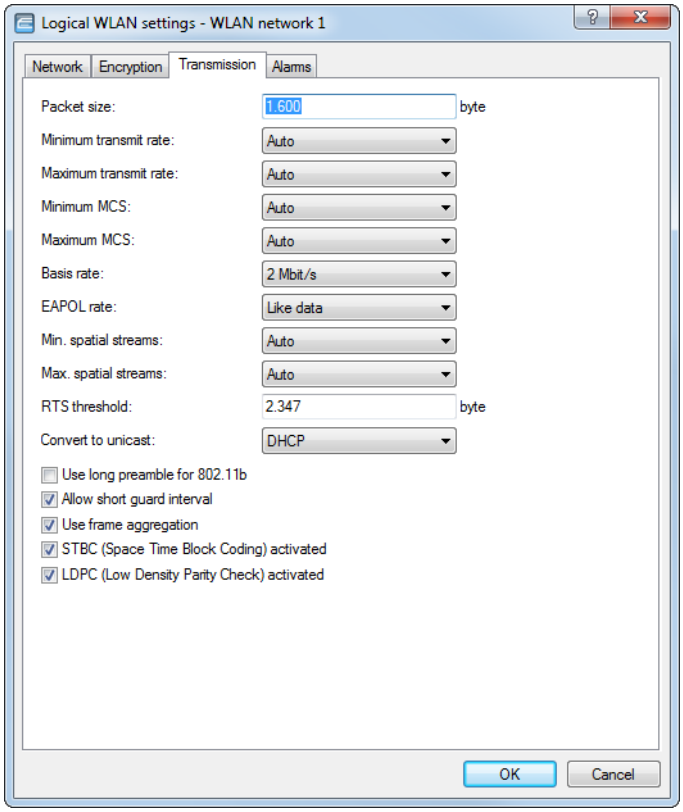
This option is only displayed if the device supports it.

WPA3 Transition Mode Term.

This setting uses an additional info element to explicitly signal WLAN clients that the WPA3-PSK (SAE) encryption method is supported in the mixed WPA2/3 mode. If the client supports the "Transition Mode Termination" feature, it will always use WPA3-PSK (SAE) to authenticate with this SSID. This prevents a downgrade to WPA2-PSK, which is otherwise also allowed in mixed WPA2/3 mode.

13.17.3.3 Transmission settings

Details for the data transmission over the logical interface in LANconfig are set under **Wireless LAN** > **General** > **Logical WLAN settings** > **Transmission**.



Packet size

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

Minimum and maximum transmit rate

Normally the AP negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients. The AP adjusts the transmission speeds to the reception conditions. As an alternative, you can set fixed values for the minimum and maximum transmission speeds if you wish to prevent the dynamic speed adjustment.

Modulation coding scheme, MCS (802.11n only)

A specific MCS number denotes a unique combination from the modulation of the individual carriers (BPSK, QPSK, 16QAM, 64QAM), coding rate (i.e. proportion of error correction bits in the raw data) and number of spatial streams. 802.11n uses this term instead of the term “data rate” used in older wireless LAN standards because data rate is no longer an unambiguous description.

MCS index	Data streams	Modulation	Coding rate	Data throughput (GI=0.4 s, 40 MHz)
0	1	BPSK	1/2	15
1	1	QPSK	1/2	30
2	1	QPSK	3/4	45
3	1	16QAM	1/2	60
4	1	16QAM	3/4	90
5	1	64QAM	1/2	120
6	1	64QAM	3/4	135
7	1	64QAM	5/6	150
8	2	BPSK	1/2	30
9	2	QPSK	1/2	60
10	2	QPSK	3/4	90
11	2	16QAM	1/2	120
12	2	16QAM	3/4	180
13	2	64QAM	1/2	240
14	2	64QAM	3/4	270
15	2	64QAM	5/6	300

The MCS selection therefore indicates the type and minimum or maximum number of modulation parameters that should be used for one or two spatial data streams. Within these limits, the appropriate MCS is selected when the connection is established depending on the current conditions and may be adapted during the connection if required. This also defines the maximum attainable data throughput, indicated in the last column of the table (here for the short guard interval GI = 0.4 s using the 40MHz channel).

Basis rate

The defined basis rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster". By setting the transmission rate to auto, the AP collects information about the transmission rates of the various WLAN clients. Clients automatically notify the AP of this rate with each unicast communication. The AP takes

the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

EAPOL rate (EAP over LAN)

WLAN clients use EAPOL to log on to APs via WPA and 802.1X. They encapsulating EAP packets in Ethernet frames to allow EAP communications on layer-2 connections.

Under certain circumstances it may be desirable to select a lower data rate for the transfer of EAPOL packets than that available for the payload data. In the case of mobile WLAN clients, high data rates can cause EAPOL packet losses, which in turn leads to considerable delays in client association. This procedure can be stabilized by selecting specific data rates for EAPOL.

With the default selection "Like data", EAPOL packets are handled like normal data packets. This means that the standard transmission rate for data packets is applied, or the usual rate adaptation for data packets is used.

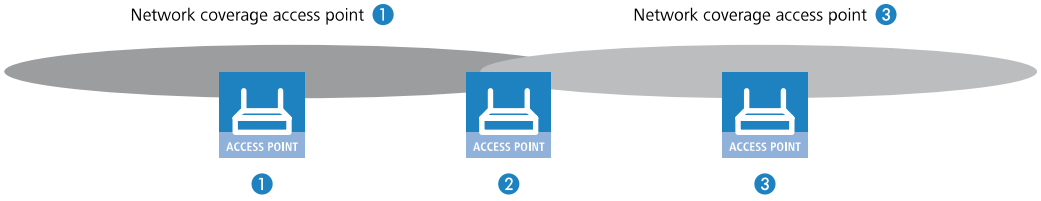
Number of spatial streams (802.11n only)

The spatial multiplexing function allows several separate data streams to be transmitted over separate antennas in order to increase data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

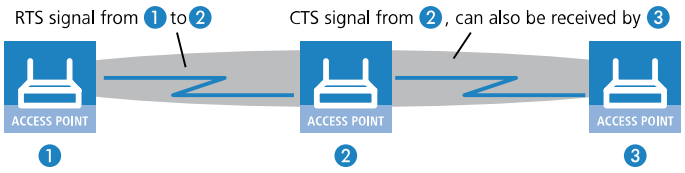
With the 'Auto' setting all spatial streams that are supported by the wireless LAN module in question are used.

RTS threshold

The RTS threshold prevents the occurrence of the “hidden station” phenomenon.



Here, the three APs **1**, **2**, and **3** are positioned such that no direct wireless connection between the two outer devices is possible. If **1** sends a packet to **2**, **3** is not aware of this as it is outside of **1**'s coverage area. **3** may also try, during the transmission from **1**, to send a packet to **2** as well, because **3** has no knowledge of the medium (in this case the wireless connection) being blocked. A collision results and neither of the transmissions from **1** nor **3** to **2** will be successful. The RTS/CTS protocol is used to prevent collisions.



To this end, **1** precedes the actual transmission by sending an RTS packet to **2**, that **2** answers with a CTS. The CTS sent by **2** is now within “listening distance” of **3**, so that **3** can wait with its packet for **2**. The RTS and CTS signals each contain information about the time required for the transmission that follows.

A collision between the very short RTS packets is improbable, although the use of RTS/CTS leads to an increase in overhead. The use of this procedure is only worthwhile where long data packets are being used and the risk of collision is higher. The RTS threshold is used to define the minimum packet length for the use of RTS/CTS. The best value can be found using trial and error tests on location.

The RTS/CTS threshold value also has to be set in the WLAN client, as far as the driver and/or operating system allow this.

Convert to unicast

You have the following options for converting data streams to unicast:

None

No data streams are converted to unicast.

DHCP

Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

Multicast

After activation of the feature, multicast data streams intended for transmission over WLAN interfaces are converted on the MAC layer or WLAN layer into individual unicast data streams for each client. Although the packets are identical for each client, the fact that they are now part of a unicast means that they can be transmitted at the highest possible data rate supported by the respective client. Even though the packets are now duplicated, in most scenarios the much faster transmission means that significantly less airtime is consumed, which benefits the other transmissions.

In order for the feature to work, you need to enable and configure IGMP snooping on the device. IGMP snooping is used to determine which client wants to receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

DHCP and multicast

Converts DHCP and multicast data streams to unicast.

Use long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the AP. “Long preamble” should only be set when the clients require this setting to be fixed.

Allow short guard interval (802.11n only)

This option is used to reduce the transmission pause between two signals from 0.8 s (default) to 0.4 s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

Use frame aggregation (802.11n only)

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This method serves to reduce the packet overhead, and the data throughput increases.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

STBC (space time block coding) activated (802.11n only)

STBC is an IEEE 802.11n coding procedure. The function 'STBC' (Space Time Block coding) additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas. This results in better reception conditions in a MIMO system.

LDPC (low density parity check) activated (802.11n only)

LDPC is an error correction method. IEEE 802.11n uses convolution coding (CC) as the standard method for error correction, and the more effective LDPC method of error correction is available an an option.

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Hard retries (in WEBconfig only)

This value defines the number of times that the hardware should attempt to send packets before a Tx error message is issued. Smaller values mean that a packet which cannot be sent blocks the sender for less time.

Soft retries (in WEBconfig only)

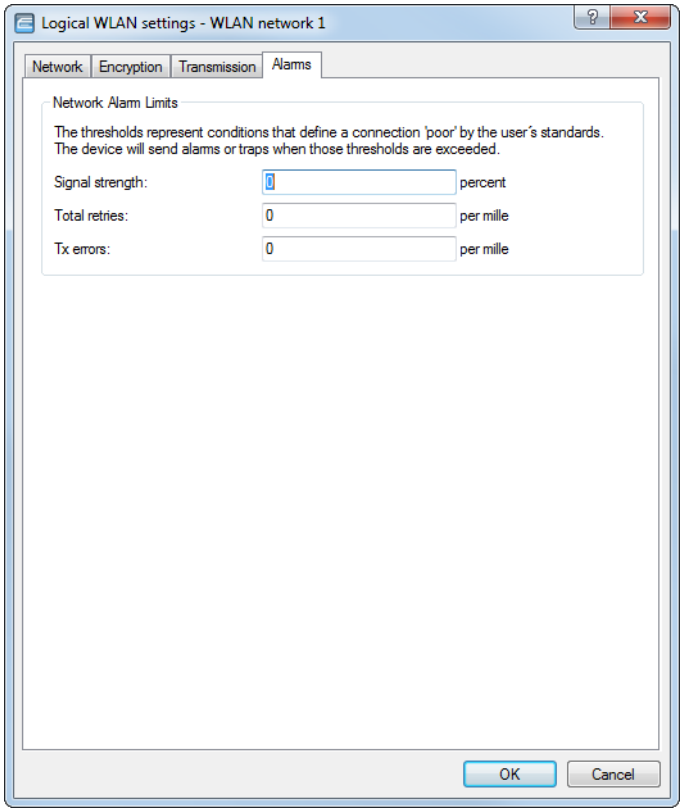
If the hardware was unable to send a packet, the number of soft retries defines how often the system should attempt retransmission.

The total number of attempts is thus (soft retries + 1) * hard retries.

The advantage of using soft retries at the expense of hard retries is that the rate-adaption algorithm immediately begins the next series of hard retries with a lower data rate.

13.17.3.4 Alarm settings

Details for the alarms sent over the logical interface in LANconfig are set under **Wireless LAN** > **General** > **Logical WLAN settings** > **Alarms**.



Typical situations that cause problems in the wireless LAN environment include a decrease in signal strength below a certain threshold, the percentage of lost packets exceeding a certain threshold, or packets frequently having to be resent—all of which can greatly reduce the available bandwidth.

In order to recognize and react to these situations, LANCOM WLAN devices now issue alerts to provide information on the over- or undershooting of threshold values.

A connection is not absolutely rated as poor. The assessment always depends on the parameters that are specified. It should be noted that threshold limits that are too high or too low can lead to incorrect evaluation, and that a very large number of false alerts could be the result. A certain amount of packet loss and fluctuating signal strengths are to be expected even for stable wireless connections.

Here you can set the limit values for the individual SSIDs. Threshold values can also be set for point-to-point links (WLAN bridges) operated by an AP. These limits are used to evaluate a client's connection to the SSID and the connection to a P2P remote.

Signal strength

The parameter specifies the minimum of the required signal strength in percent. The alarm is triggered when the signal strength falls below the configured value. An alarm limit must be between 1 and 100. The value 0 switches the alarm off.

In the case of client and P2P links, separate values are evaluated for beacon and data signal strength. If available, the beacon signal is preferred for comparison because the values are up-to-date, even though there is currently no traffic on the connection.

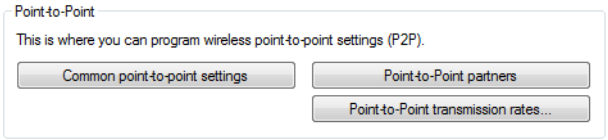
Total retries

This parameter specifies the maximum limit of the retry rate per mille. The alarm is triggered when the ratio of total retries and Tx packets reaches the configured value. An alarm limit must be between 1 and 1000. The value 0 switches the alarm off.

Tx-Errors

This parameter specifies the maximum limit of the transmit error rate per mille. The alarm is triggered when the ratio of Tx errors and Tx packets reaches the configured value. An alarm limit must be between 1 and 1000. The value 0 switches the alarm off.

13.17.4 Point-to-point

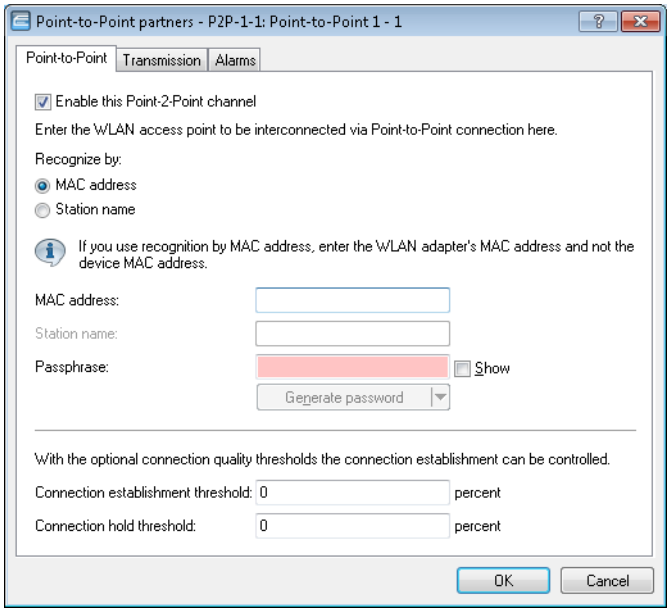


LANconfig: **Wireless LAN** > **General** > **Point-to-point**

Here you configure the settings required by an AP for a point-to-point WLAN bridge. For further information, please see *Establishing WLAN bridges* on page 992:

13.17.5 Point-to-point partners

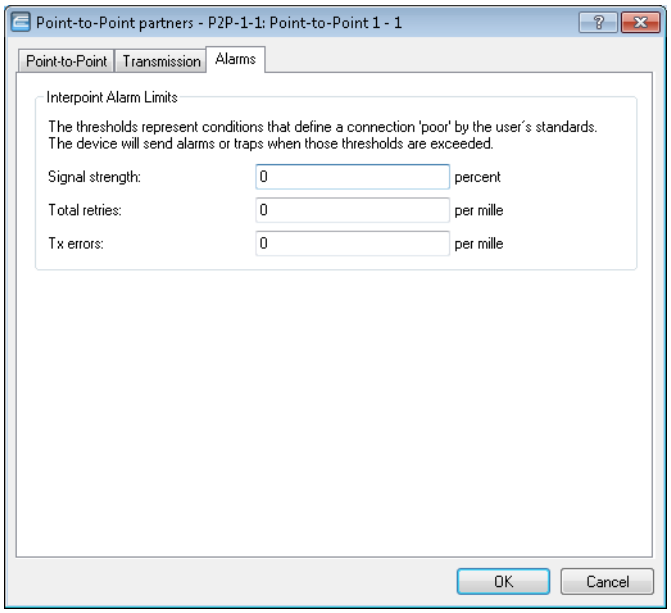
Up to 16 point-to-point connections can be activated for each WLAN module. In LANconfig you find these settings under **Wireless LAN** > **General** > **Point-to-point** > **Point-to-point partners**



Proceed as follows to set up a point-to-point link:

1. Select the option **Enable this point-2-point channel**.
2. Select whether the P2P peer is to be identified by its **MAC address** or its **Station name**.
3. The corresponding text box is activated. Enter the MAC address or station name.

If you work with detection by MAC address, enter the MAC address of the WLAN module here and not that of the device itself.



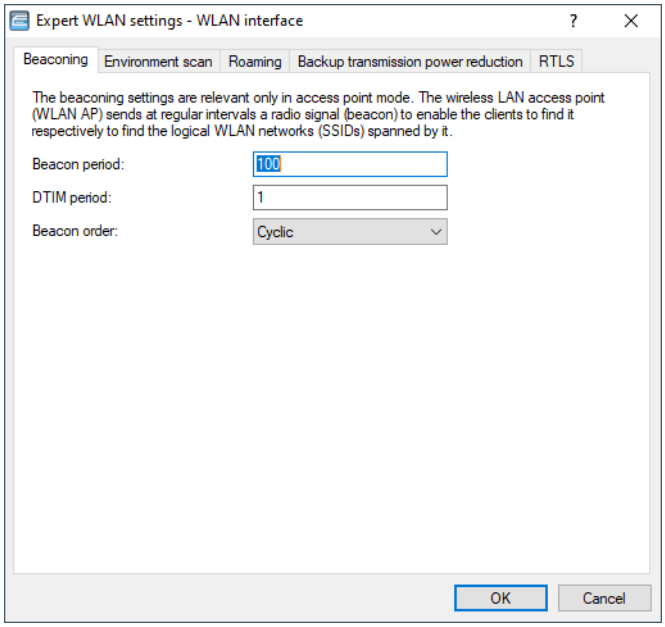
On the **Alarm** tab,you can set threshold values for **signal strength**, **total repetitions** and **Tx errors** for the point-to-point connection. If the value exceeds or falls below this value, the access point sets off alarms or traps.

Conclude your entries by clicking on **OK**.

13.17.6 Expert WLAN settings

13.17.6.1 The beaconing table

Settings in the beaconing table influence the transmission of beacons by the access point in AP mode. In part this can influence the roaming behavior of clients, and in part this serves to optimize the MultiSSID mode for older WLAN clients.



LANconfig: **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **Beaconing**

Command line: **Setup** > **Interfaces** > **WLAN** > **Beaconing**

Beacon period

This value defines the time interval in K s between beacon transmission (1 K s corresponds to 1024 microseconds and is a measurement unit of the 802.11 standard. 1 K s is also known as a Timer Unit (TU)). Smaller values result in a shorter beacon timeout period for the client and enable quicker roaming in case of failure of an AP, but they also increase the WLAN overhead.

DTIM period

This value defines the number of beacons which are collected before multicasts are broadcast. Higher values enable longer client sleep intervals, but worsen the latency times.

Beacon order

Beacon order refers to the order in which beacons are sent to the various WLAN networks. For example, if three logical WLAN networks are active and the beacon period is 100 K s, then the beacons will be sent to the three WLANs every 100 K s. Depending on the beacon order, the beacons are transmitted at times as follows.

Cyclic

In this mode the AP transmits the first beacon transmission at 0 K s to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (100 K s) WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (200 K s) the order is WLAN-3, WLAN-1, WLAN-2. After this the sequence starts again.

Staggered

In this mode, the beacons are not sent together at a particular time, rather they are divided across the available beacon periods. Beginning at 0 K s, WLAN-1 only is sent; after 33.3 K s WLAN-2, after 66.6 K s WLAN-3. At the start of a new beacon period, transmission starts again with WLAN-1.

Simple burst

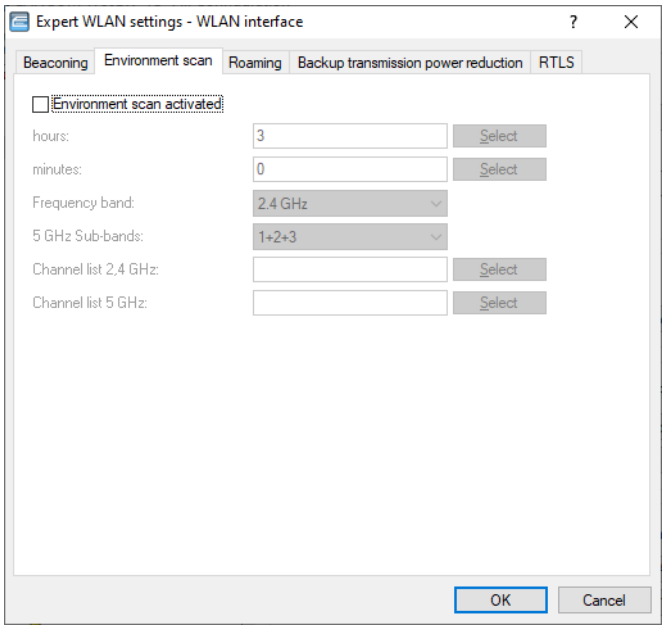
In this mode the AP always transmits the beacons for the WLAN networks in the same order. The first beacon transmission (0 K s) is WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

Some older WLANs are unable to process the quick succession of beacons which occur with simple burst. Consequently these clients often recognize the first beacons only and can only associate with this network.

Staggered transmission of beacons produces better results but increases load on the AP's processor. The preset cyclic transmission proves to be a good compromise as all networks are transmitted first in turn.

13.17.6.2 Environment scan

Your WLAN's environment can be regularly searched for rogue APs. See also *Starting an environment scan at a configurable time* on page 967. These settings in LANconfig are located under **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **Environment scan**.



Environment scan activated

Activates / deactivates the environment scan.

The following parameters are grayed out if the environment scan is disabled.

Hours

Contains the hour value of the time for the environment scan.

Minutes

Contains the minute value of the time for the environment scan.

Frequency band

Contains the frequency bands for the environment scan.

Possible values:

2.4 GHz

The 2.4-GHz frequency band is scanned.

5 GHz

The 5-GHz frequency band is scanned.

2.4/5 GHz

Scans the 2.4-GHz and 5-GHz frequency bands.

5-GHz subbands

Contains the subbands of the 5-GHz frequency band.

Channel list 2.4 GHz

Specifies the 2.4-GHz channels for the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 2.4-GHz frequency band.

Possible values (multiple selection allowed):

1 to 13

In steps of 1.

Channel list 5 GHz

Specifies the 5-GHz channels for the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 5-GHz frequency band.

Possible values (multiple selection allowed):

36 to 64

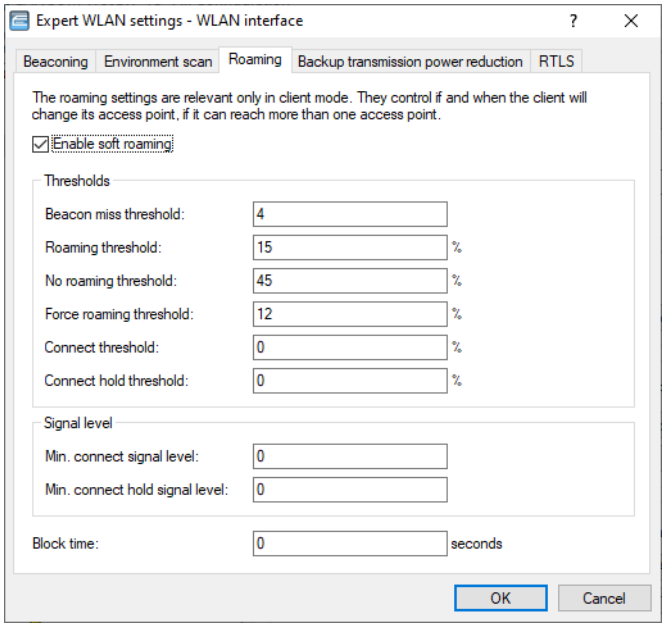
In steps of 4.

100 to 140

In steps of 4.

13.17.6.3 The roaming table

The roaming table contains various threshold values which control the behavior of the WLAN device when it is roaming in the 'Client' operating mode.



LANconfig: **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **Roaming**

Command line: **Setup** > **Interfaces** > **WLAN** > **Roaming**

Enable soft roaming

With this option enabled, a client uses scan information to roam to a stronger AP (soft roaming). Roaming due to connection loss (hard roaming) is unaffected by this. The roaming threshold values only take effect when soft roaming is activated.

Beacon miss threshold

The beacon loss threshold defines how many AP beacons can be missed before a registered client starts searching again.

Higher values will delay the recognition of an interrupted connection, so a longer time period will pass before the connection is re-established.

The lower the value set here, the sooner a potential interruption to the connection will be recognized; the client can start searching for an alternative AP sooner.

Values which are too small may cause the client to detect lost connections more often than necessary.

Roaming threshold

This value is the percentage difference in signal strength between access points above which the client will switch to the stronger AP.

Other contexts require the value of signal strengths in dB. The following conversion applies:

64dB – 100%

32dB – 50%

0dB – 0%

No roaming threshold

This threshold refers to the field strength in percent. Field strengths exceeding the value set here are considered to be so good that no switching to another AP takes place.

Force roaming threshold

This threshold refers to the field strength in percent. Field strengths below the value set here are considered to be so poor that a switch to another AP is required.

Connect threshold

This value defines field strength in percent defining the minimum that an AP has to show for a client to attempt to associate with it.

Connect hold threshold:

This threshold defines field strength in percent. A connection to an AP with field strength below this value is considered as lost.

Min. connect signal level

Similar to the connect threshold, but specified as absolute signal strength.

Min. connect hold signal level

Similar to the connection hold threshold, but specified as absolute signal strength.

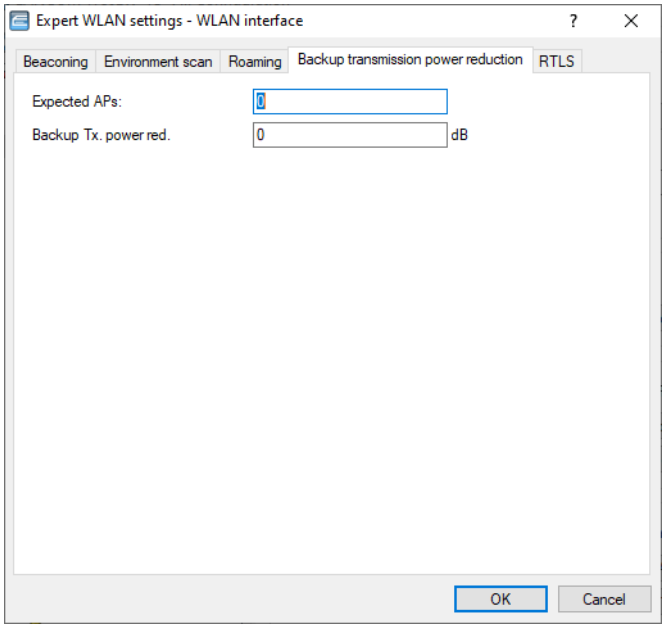
Block time

If your device is operating as a WLAN client in an environment with multiple WLAN access points all with the same SSID, you can define a time period during which the WLAN client will avoid associating with a particular AP after receiving an "association-reject" from it.

Possible values are 0 to 4294967295 seconds.

The default value is 0 seconds. Client authentication is not blocked.

13.17.6.4 Backup transmission power reduction (Adaptive Transmission Power)



LANconfig: **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **Backup transmission power reduction**

Configure the settings of backup transmission power reduction here. For further information, please see *Adaptive transmission power* on page 1004:

Expected APs

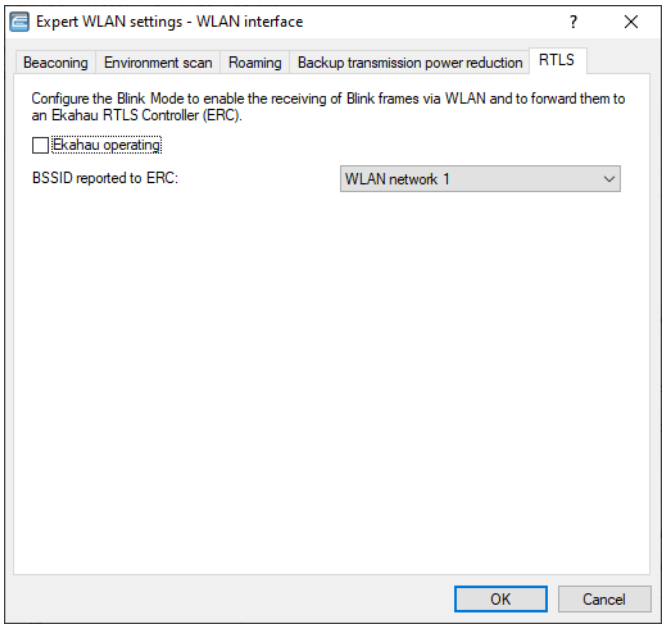
Specify how many APs operate within a broadcast domain.

Backup TX power red.

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

The default transmission power reduction is configured under **Wireless LAN** > **General** by clicking the button **Physical WLAN settings** (selecting the WLAN interface, if necessary) and accessing the **Radio** tab.

13.17.6.5 RTLS



LANconfig: **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **RTLS**

Configure the settings for the AiRISTA Flow blink mode here. For further information, please see *AiRISTA Flow Blink Mode* on page 1048:

Ekahau operating

Enable or disable the blink mode for this interface here.

BSSID reported to ERC

Here you select the logical WLAN interface that the device reports to the ERC.

The ERC "maps" this BSSID to a particular location. For example, if this location were a server room, the ERC knows that Wi- Fi tag "A" is located in the server room as long as the "blink" arrives from the BSSID belonging to the corresponding APs.

13.17.7 Configurable data rates per WLAN module

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates "announced" by the AP to the client for its communication with the AP (RX).

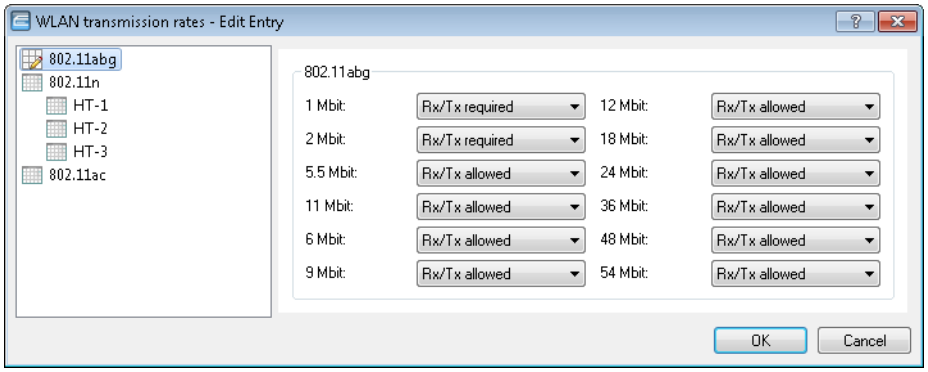
This rate adaptation specifies a minimum and a maximum data rate, and it also allows you to disable certain data rates between these limits.

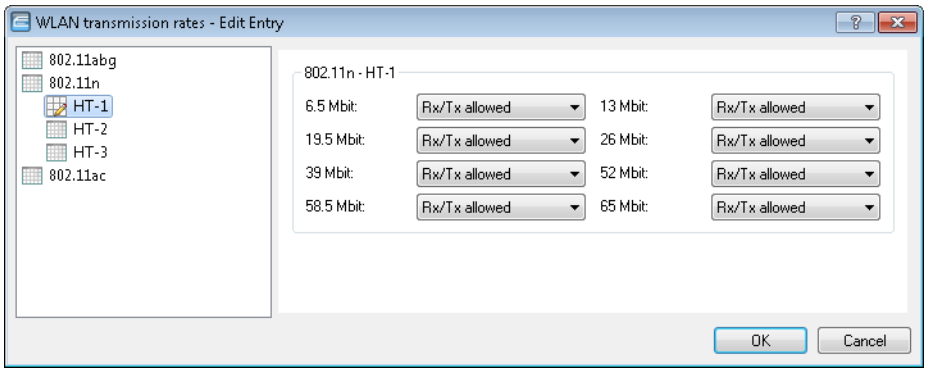
The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

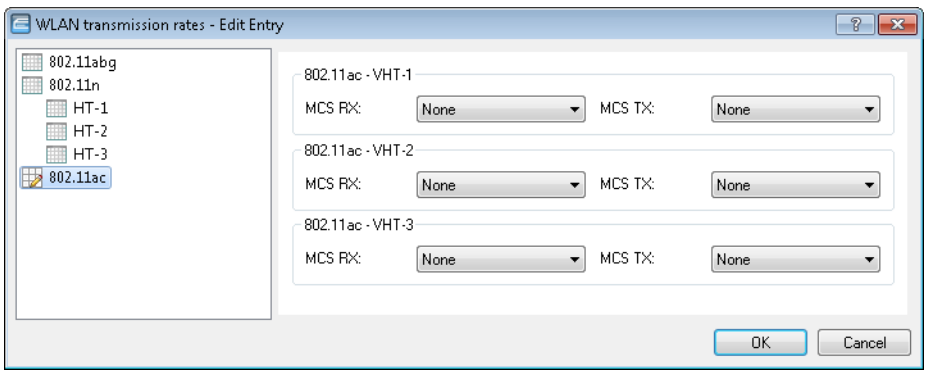
13.17.7.1 Configuring the data rates with LANconfig

To configure the data rates with LANconfig, switch to the view **Wireless LAN** > **General**, and in the section **Extended settings** open the dialog **WLAN transmission rates**. LANconfig lists the settings for all of the available interfaces. To change the setting for an interface, select its entry and click on **Edit**.

On the left you select the standard that you want to configure.







The configuration can be modified for each of the standards separately

- 802.11abg
- 802.11n
  - HT-1
  - HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Depending on the standard, the following settings are available for each transmission rate and each SSID or P2P link:

Rx/Tx required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx allowed

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx allowed

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Deactivated

The AP does not announce this rate and does not use it to communicate with the client.

MCS-9/8/7

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

None

With 802.11ac modules, the respective stream option is disabled for the corresponding data direction.

13.17.8 RTLS (real-time location system)

RTLS enables a device to be localized in real time. This device is a specialized WLAN transmitter that sends out specially coded WLAN packets. The access points in the vicinity receive these packets and forward them with additional data to the real-time localization system. By enabling the precise determination of the location of the WLAN transmitter, the whereabouts of objects or people carrying the WLAN transmitter can be implied.

13.17.8.1 Stanley AeroScout RTLS

The AeroScout RTLS system facilitates various tasks such as asset management, environmental monitoring and staff workflows by means of special sensors connected via WLAN and "tags". This feature enables the AeroScout tags (i.e. specifically coded WLAN packets) to be forwarded to the AeroScout Location Engine via a LANCOM WLAN infrastructure.

The following operating modes are supported:

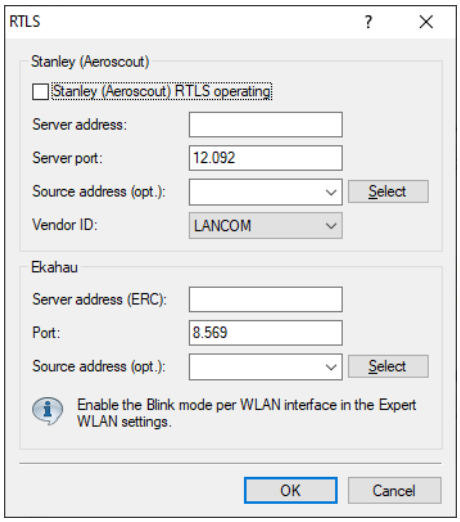
- Forwarding of AeroScout tag messages

  The WDS mode is supported. Make sure that the tags in the AeroScout system are configured for WDS mode. The IBSS mode is not supported.

- Wi-Fi client reports

Configuring Stanley AeroScout RTLS

To configure access to the Stanley AeroScout RTLS server with LANconfig, open the view **Wireless LAN** > **General** > **Extended settings** > **RTLS** and configure the section **Stanley (AeroScout)**.



Stanley (AeroScout) RTLS operating

Enable this option to activate the forwarding to the AeroScout Location Engine.

This feature is always activated for all WLAN modules of an access point.

Server address

Configure the IP address of the AeroScout Location Engine here.

Server port

Configure the server port of the AeroScout Location Engine if the default value is not being used.

Source address (optional)

Optionally, configure the source network for the connection to the AeroScout Location Engine. This is only necessary if multiple ARF networks are configured.

Vendor ID

Here you configure the vendor ID that the access point reports to the AeroScout Location Engine. If your version of the AeroScout Location Engine does not yet support the dedicated LANCOM vendor ID, you can switch to the vendor ID “Motorola”.

13.17.8.2 AiRISTA Flow Blink Mode

Ekahau and their "Real Time Location System" (RTLS) allow you to determine the location of objects and persons within a wireless LAN. This works with special Wi-Fi transmitters known as "Wi-Fi tags" that are located on the device or person's body and which send specially coded Wi-Fi packets. APs located nearby receive these packets, enrich them with additional information (e.g. RSSI), encapsulate them in the "TaZmen Sniffer Protocol" (TZSP) and forward this information to the

"Ekahau RTLS Controller" (ERC) installed on the network. The ERC analyzes this data to determine the position of the Wi-Fi tag.

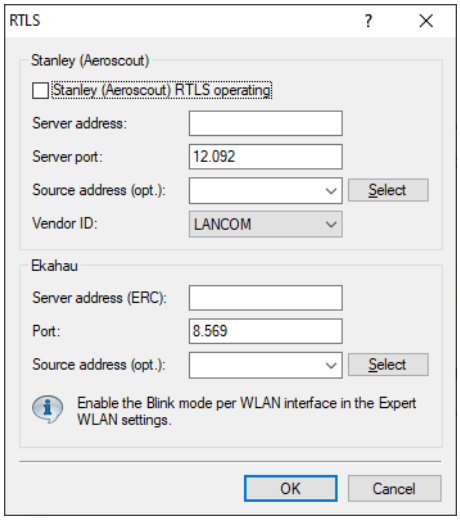
The Wi-Fi tags support three modes for sending the Wi-Fi packets:

- **Associated mode**: In "associated mode" the Wi-Fi tag functions like a Wi-Fi client. It associates with a nearby AP and stays in constant contact with it. While this provides seamless positioning, this mode consumes more power and the battery life of the Wi-Fi tag is reduced. In "associated mode" the Wi-Fi tags use the Ekahau Location Protocol (ELP).
- **Blink mode**: In "blink mode", the Wi-Fi tag transmits short Wi-Fi packets but does not connect to an AP. In "blink mode" the Wi-Fi tags use the "Ekahau Blink Protocol" (EBP).
- **Mixed mode**: In "Mixed mode", the Wi-Fi tags use EBP to send the RSSI and ELP to send status messages to the ERC.

Configuring AiRISTA Flow blink mode (formerly Ekahau blink mode)

The blink mode only works with 802.11n WLAN modules, not with 802.11ac WLAN modules. Correspondingly, it is not possible to activate the 'blink mode' for 802.11ac WLAN modules in LANconfig. The option is permanently disabled for devices of this type.

To configure access to the RTLS Server (ERC) with LANconfig, open the view **Wireless LAN** > **General** > **Extended settings** > **RTLS** and configure the section **Ekahau**.



Server address (ERC)

Enter the address of the ERC. You can enter an IP address or a host name.

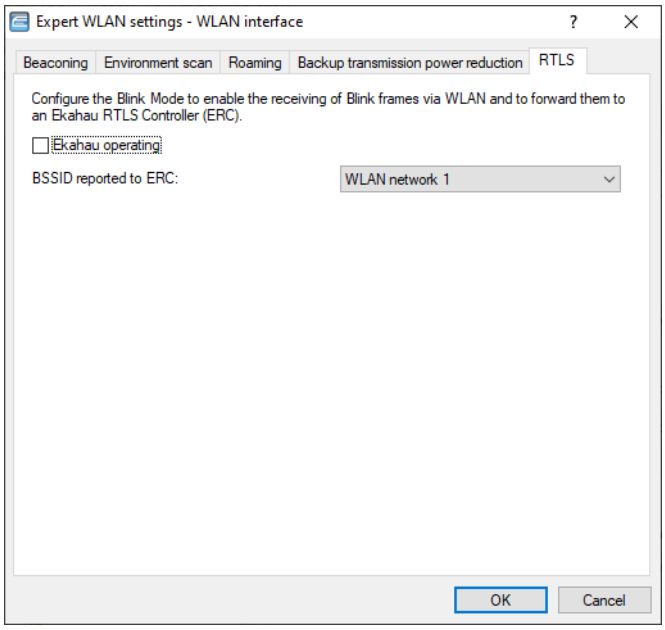
Port

Contains the default UDP port (8569) for communication with the ERC. Change this value only in exceptional cases.

Source address (optional)

Optionally, specify a source address.

To configure the blink mode for each physical WLAN interface, navigate to **Wireless LAN** > **General** > **Extended WLAN settings** and click **Expert WLAN settings**. If applicable, select the desired WLAN interface from the drop-down list and switch to the **RTLS** tab.



Ekahau operating

Enable or disable the Ekahau blink mode for this interface here.

BSSID reported to ERC

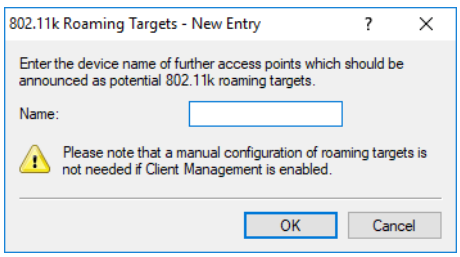
Here you select the logical WLAN interface that the device reports to the ERC.

The ERC "maps" this BSSID to a particular location. For example, if this location were a server room, the ERC knows that Wi- Fi tag "A" is located in the server room as long as the "blink" arrives from the BSSID belonging to the corresponding APs.

13.17.9 IEEE 802.11k Roaming Targets

The IEEE 802.11k standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the client in the "Neighbor Report" as defined for the standard. 802.11k has so far been used as part of the client management, so it does not need to be configured separately. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately.

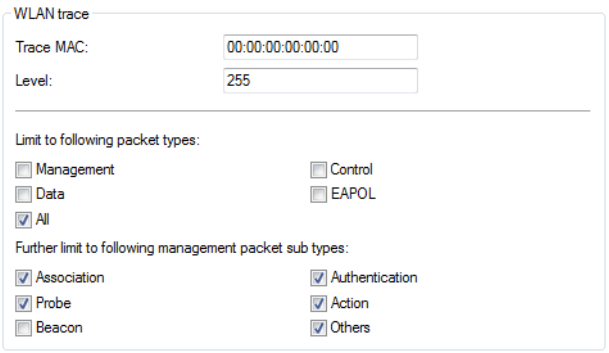
You can find the new table under **Wireless LAN** > **General** > **Extended settings** > **802.11k Roaming Targets**. Enter the potential roaming targets here.



13.17.10 WLAN data trace

A trace can often help with problems. Settings that are specific to WLAN traces can be made here. See also *Trace information* on page 305.

LANconfig: **Wireless LAN** > **Trace**



Trace-MAC

The output of trace messages for the WLAN-Data-Trace can be set for a certain client. The corresponding MAC address is entered here.

Every network card has its own MAC address that is unique in the world. The address is a 12-character hexadecimal number (e.g. 00A057010203). This address can generally be found printed on the network card.

Entering '000000000000' deactivates this function and outputs trace messages for all clients.

Trace level

The output of trace messages for the WLAN data trace can be restricted to contain certain content only. The value entered here restricts the packets in the WLAN-DATA trace to the specified level.

Possible values:

0 to 255

Special values:

0: Reports that a packet has been received/sent

1: Adds the physical parameters for the packets (data rate, signal strength, etc.)

2: Adds the MAC header

3: Adds the Layer-3 header (e.g. IP)

4: Adds the Layer-4 header (TCP, UDP...)

5: Adds the TCP/UDP payload

255: No restrictions on content. The trace includes the entire packets.

Default:

255

Packet types

Similar to Trace MAC and Trace level, the output from WLAN DATA traces can be restricted by the type of packet sent or received, e.g. management (authenticate, association, action, probe-request/response), control (e.g. powersave poll), EAPOL (802.1X negotiation, WPA key handshake).

Possible values:

Management

Control

Data

EAPOL

All

Default:

All

Management packets

With this selection it is possible to set which type of management frames should automatically appear in the WLAN-DATA trace

Possible values:

Association: (Re)Association Request/Response, Disassociate

Authentication: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Other: all other management frame types

Default:

Association

Authentication

Probes

Action

Other

13.17.11 Client Management

With Client Management, Wi-Fi clients are steered to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular band steering and client steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

Compared to the previous client steering feature supported by WLCs, Client Management operates independently and without a WLC. The access points communicate with one another using the protocol IAPP.

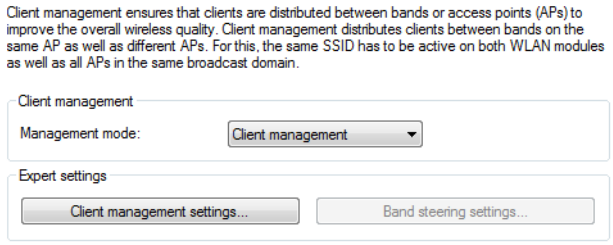
For the access points to communicate with one another, they need to be able to exchange IAPP messages. IAPP messages are transmitted by multicast. If necessary, the infrastructure—and switches in particular—requires exemptions to be created for IGMP snooping or other filtering mechanisms. IAPP uses the multicast group 224.0.1.76.

LANCOM switches in the default setting are already set up correctly for Client Management.

In this way Client Management ensures that clients are evenly distributed across the frequency bands and access points to optimize overall WLAN performance. A requirement for this is that the WLAN modules and access points in a broadcast domain all transmit on the same SSID.

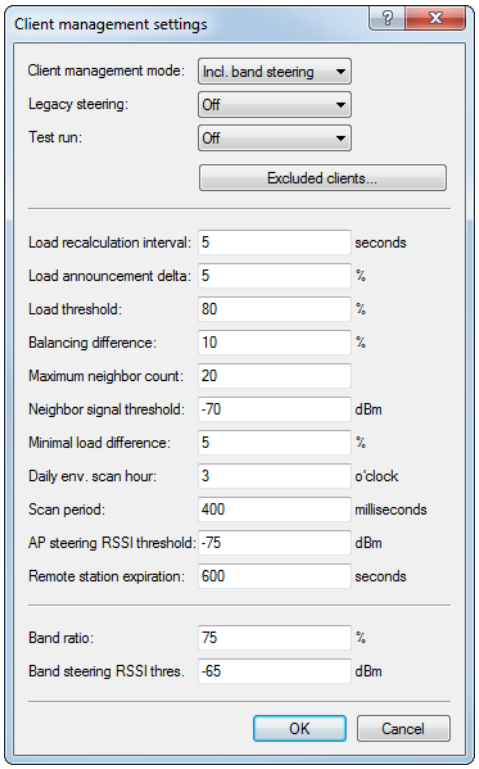
13.17.11.1 Configuration of Client Management

Client Management is switched on and off under **Wireless LAN** > **Client Management** > **Client Management** > **Management mode**. For new installations, this is turned on by default and usually does not require any special settings. As an alternative for access points with multiple WLAN modules, **AP-based band steering** can also be activated. See also *WLAN band steering* on page 977.



Expert settings

The settings for Client Management are configured under **Wireless LAN** > **Client Management** > **Expert settings** > **Client Management**. The default settings are ideal for operating Client Management in offices and school environments.



Client Management mode

Access points with multiple WLAN modules can operate Client Management with and without band steering.

Default setting:with band steering

Legacy steering

Configures whether clients that do not fully support 802.11v are also directed to other access points by Client Management. Even with legacy steering activated, Client Management first steers the 802.11v-capable clients to other access points; only then does it steer the clients that do not support 802.11v. Legacy steering forcibly disconnects these clients from the WLAN. The AP prevents the client from re-associating with it for a certain period, so that the client itself selects another access point. Compared to clients steered with 802.11v, this can lead to a poorer user experience, although this depends mainly on the behavior of the legacy clients.

Default setting: Off

Test run

Operates the Client Management in test mode: Environment scans are performed and steering decisions are made by the system and recorded to the syslog, but no actual client steering takes place. Use the test run to test the behavior of Client Management without actually making changes to your network.

Default setting: Off

Excluded clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering.

Use the table to configure the MAC addresses of the clients that are to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

Load recalculation interval

Configures the interval at which the load on the AP is calculated and decisions are made to steer the clients. Increase the value to reduce the load on the network. Decrease the value to steer clients faster. Values < 2 seconds are not recommended as this negatively impacts network performance. Values > 10 seconds are not recommended as client steering does not happen in time. We recommend that you use the default value.

Default value: 5 seconds

Load announcement delta

Configures the percentage change in current load at which an access point communicates the load to other access points outside of the regular announcement interval. Increase the value in installations with many mobile clients. Decrease the value in installations with fewer moving clients. The default setting has been chosen for office and school environments. Note that this value should be lower than the value configured for the balancing difference to avoid miscalculations.

Default value: 5 %

Load threshold

Configures the load threshold at which the access point starts steering regardless of the load threshold of the neighbor access points. Increase the value in low-quality/high-density scenarios such as stadiums. Decrease the value in high-quality/high-throughput scenarios such as offices/schools.

Default value: 80 %

Balancing difference

Configures the load difference between access points at which clients are steered to the access point with the lesser load. High values lead to less balanced installations, low values lead to more steering of the clients. Increase the value if excessive client steering is happening. Decrease the value to achieve maximum balancing across the installation. The default setting has been chosen for office and school environments.

Default value: 10 %

Maximum neighbor count

Configures the number of neighbor access points that Client Management on this access point takes into consideration. In high-density scenarios, a lower number can be advantageous as clients are predominantly steered to nearby access points and less management communication is required between the access points. Values < 4 are not recommended, as there are not enough available access points for useful steering decisions. Values > 72 are not supported due to limitations of the 802.11 protocol.

Default value: 20 APs

Neighbor signal threshold

Configures the signal strength that an AP must display in order to be classified as a neighbor access point. Increase the value for high-density scenarios (for example: -60, -50). Decrease the value for scenarios where widespread coverage is required (e.g. -80, -90).

Default value: -70 dBm

Minimum load difference

Configures the minimum load difference between neighboring access points for steering to be performed between these access points. Steering is only performed when the configured load threshold is exceeded. To avoid miscalculation, the minimum load difference should not exceed the value for balancing difference. Increase the value for less steering in the installation. Decrease the value for more steering in the installation.

Default value: 5 %

Daily env. scan hour

Configures the time (00-23) at which the daily environment scan is performed as required by Client Management. The exact time of the scan is spread over a 30-minute window to minimize conflicts between concurrent environment scans. The environment scan takes about 15 seconds. No WLAN data is exchanged while the WLAN module is scanning.

Default value: 03:00 hours

Scan period

Configures the length of the environment scan used to identify neighbor access points. The scan period should be 2 to 2.5 times the configured beacon interval; the default value is suitable for the default beacon interval. This value can be configured from 200 ms to 1000 ms.

Default value: 400 ms

AP steering RSSI threshold

The signal strength that a client must have on a remote access point in order to be steered to it.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

Default value: -75 dBm

Remote station expiration

Time for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

Default value: 600 seconds

Band ratio

Configures the intended distribution of clients between the radio bands. The configured ratio specifies what proportion of clients should be steered to the 5-GHz band.

Default value: 75 %

Band steering RSSI threshold

Configures the signal strength (RSSI) that a client "displays" on the other radio band in order to be steered there. The default setting is suitable for office environments.

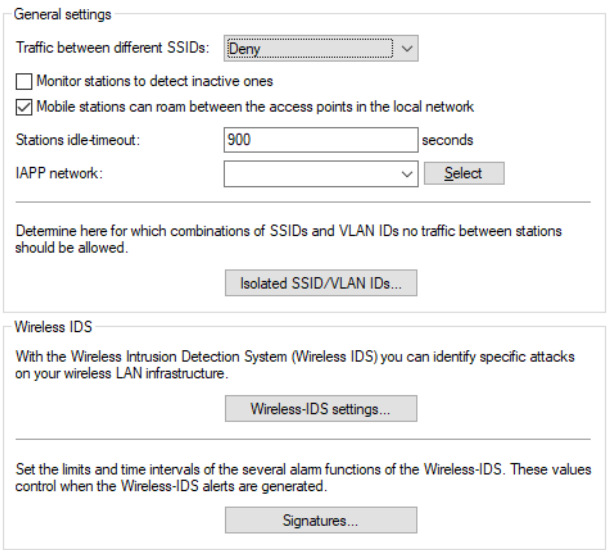
Default value: -65 dBm

13.17.12 WLAN security

In this part of the configuration, you can place limitations on the communications available to the users in the wireless network. This is done by limiting the data transfer between user groups according to individual stations or the protocol being used.

13.17.12.1 General settings

Here you find the general settings for WLAN security.



LANconfig: **Wireless LAN** > **Security**

Traffic between different SSIDs

Depending on the application, it may be required that the WLAN clients connected to an AP can—or expressly cannot—communicate with other clients. Communications between clients in different SSIDs can be allowed

or stopped with this option. For models with multiple WLAN modules, this setting applies globally to all WLANs and all modules.

Communications between clients in a logical WLAN is controlled separately by the logical WLAN settings (Inter-Station-Traffic). If the Inter-SSID-Traffic is activated and the Inter-Station-Traffic deactivated, a client in one logical WLAN can communicate with clients in another logical WLAN. This option can be prevented with the VLAN settings or protocol filter.

Monitor stations to detect stations that are inactive

In particular for public WLAN access points (public spots), the charging of usage fees requires the recognition of stations that are no longer active. Monitoring involves the AP regularly sending packets to logged-in stations. If the stations do not answer these packets, then the charging systems recognizes the station as no longer active.

Mobile stations can switch between base stations in the local network (roaming)

In addition to controlling the communication between clients, you can also define whether neighboring access points can exchange information via the inter-access point protocol IAPP. The IAPP is a protocol for communication between APs. The "handoff AP" receives information that a WLAN client associated with it is switching to another AP, and that the client can be removed from its list.

Stations idle-timeout after ... seconds

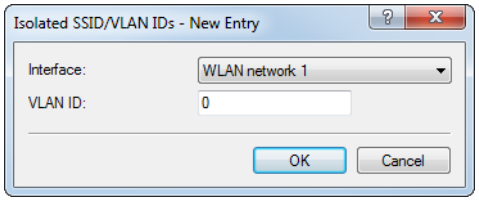
Specify a duration in seconds after which inactive stations are removed from the list of currently connected stations.

IAPP network

Roaming information exchanged via the IAPP protocol may cause high network loads. For this reason we advise that you select an ARF network to be used for the IAPP communications.

13.17.12.2 Isolated SSID/VLAN IDs

This menu allows you to map a "collective VLAN" where WLAN clients are unable to communicate with one another. Communication is only possible between WLAN client and AP (hotspot scenario). Outside of this "collective VLAN", communication between the clients can be permitted. This works perfectly transparently within a common SSID where the clients are assigned to different VLANs.



LANconfig: **Wireless LAN** > **Security** > **Isolated SSID/VLAN IDs**

Here you specify the combinations of SSIDs and VLANs between which the traffic between clients is prohibited. This table functions as a blacklist because, generally speaking, we define just a few VLANs where the communication is forbidden, but several where it is allowed.

This mechanism also works when the clients are associated with different APs (although care should be taken to ensure that the table configurations match). A prerequisite for this is that the APs are able to communicate via IAPP.

Interface

The list of available WLAN networks.

VLAN ID

The identification number of the VLAN.

Allow traffic between stations of this SSID must be permitted globally in order for it to be restricted again with this feature.

13.17.12.3 Wireless Intrusion Detection System (WIDS)

An Intrusion Detection System (IDS) recognizes attacks on a network and reports these attacks to a network management system. Especially in a professional environment, an IDS is essential for the detection and handling of potential attacks or interference.

The Wireless Intrusion Detection System (WIDS) in LCOS devices monitors the different WLANs by using a wide range of specified thresholds. If a potential attack is detected, the system reports it immediately via e-mail, SYSLOG, or SNMP traps.

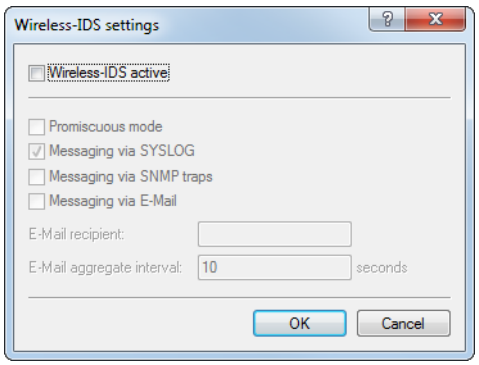
Attacks are detected by monitoring for known or similar patterns.

The WIDS configuration is either done directly on the AP, or by means of a WIDS profile assigned to the AP by a WLC.

Please note that detection based on pattern recognition (heuristics) can lead to false alarms ("false positives").

Configuring WIDS on the AP

To configure the Wireless Intrusion Detection System (WIDS) open LANconfig and go to **Wireless LAN** > **Security** > **Wireless-IDS settings**.



Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

Promiscuous mode

With the ("promiscuous mode") enabled, the AP additionally receives packets that were not directed at it, but to other network participants.

This mode is necessary to be able to detect the attacks listed below. However, the promiscuous mode affects the performance. For this reason, activating the promiscuous mode automatically causes frame aggregation to be switched off.

Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

Messaging via e-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

E-mail recipient

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

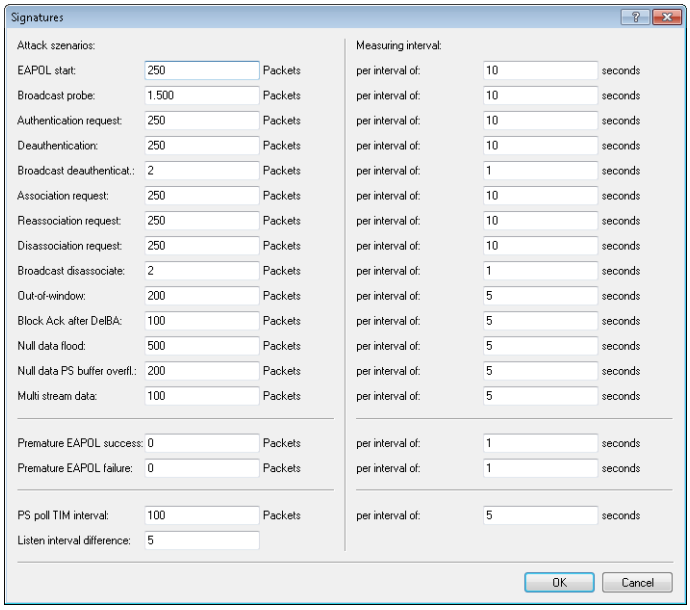
E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

Signatures

To configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions, change to **Wireless LAN** > **Security** > **Signatures**. These settings are used by the WIDS to determine if an attack is taking place.



The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

- EAPOL-Start
- Broadcast probe
- Authentication request
- Deauthentication request (*)
- Broadcast deauthentication
- Association request
- Reassociation request
- Disassociation request (*)
- Broadcast disassociate

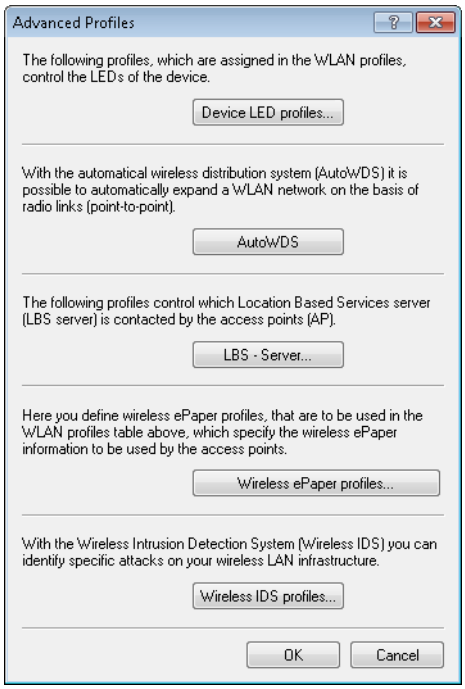
- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (*)
- Premature EAPOL failure (*)
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.

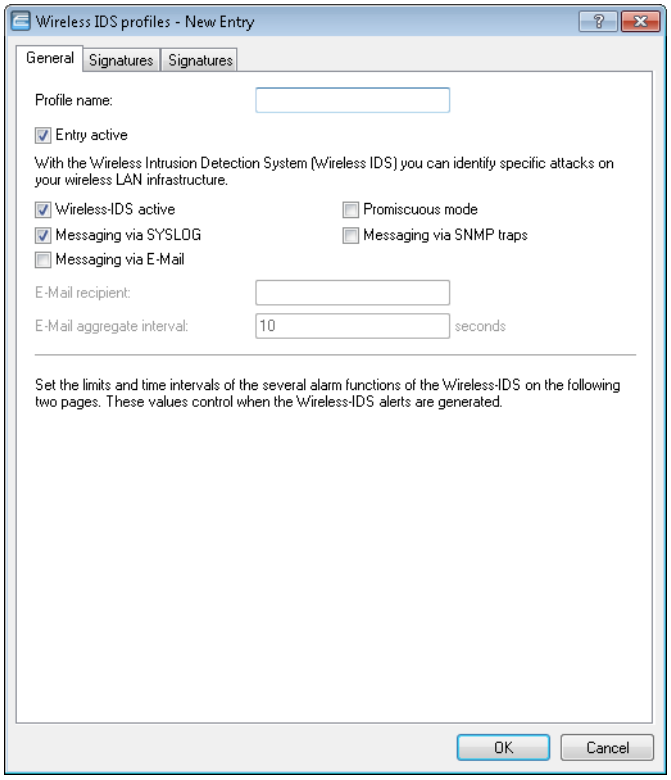
(*) These attacks are only detected if promiscuous mode is active.

Configuring WIDS profiles on the WLC with LANconfig

To configure a profile for the Wireless Intrusion Detection System (WIDS) with LANconfig, go to the view **WLAN controller** > **Profiles** and click on **Advanced profiles**.



Create or edit the WIDS profiles under **Wireless IDS profiles**.



Profile name

Enter an identifier for this profile. You allocate this profile name to a WLAN profile under **WLAN controller** > **Profiles** > **WLAN profiles**.

You need to specify a profile name for the configuration of the WIDS signatures.

Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

Promiscuous mode

With the ("promiscuous mode") enabled, the AP additionally receives packets that were not directed at it, but to other network participants.

This mode is necessary to be able to detect the attacks listed below. However, the promiscuous mode affects the performance. For this reason, activating the promiscuous mode automatically causes frame aggregation to be switched off.

Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

Messaging via e-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

E-mail recipient

The e-mail address of the recipient when messaging via e-mail is activated.

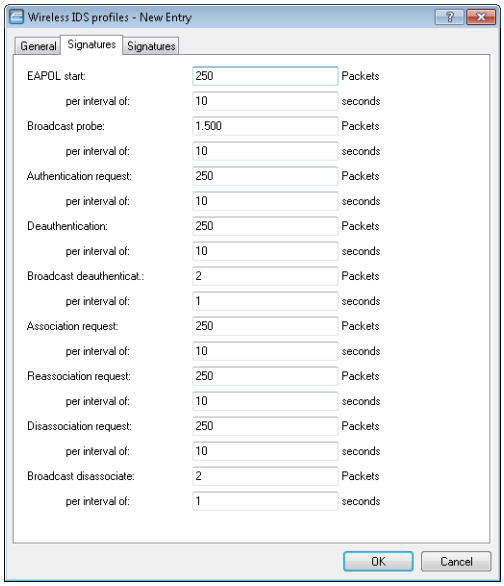
The field must contain a valid e-mail address.

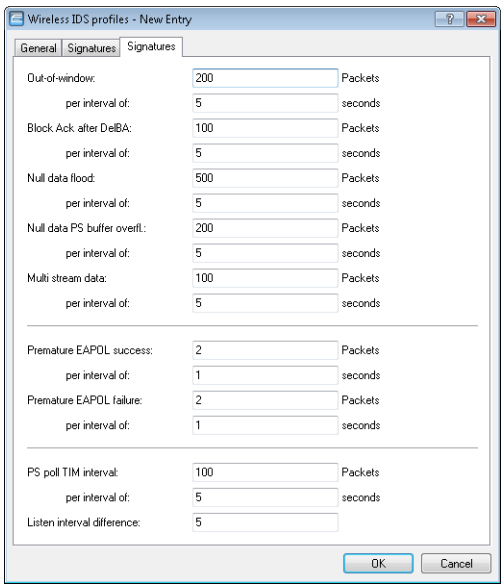
E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

The “Signatures” tabs are used to configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.





The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

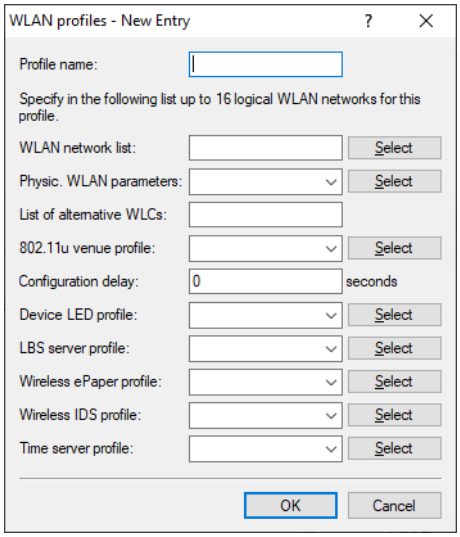
› EAPOL-Start

- Broadcast probe
- Authentication request
- Deauthentication request (*)
- Broadcast deauthentication
- Association request
- Reassociation request
- Disassociation request (*)
- Broadcast disassociate
- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (*)
- Premature EAPOL failure (*)
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.

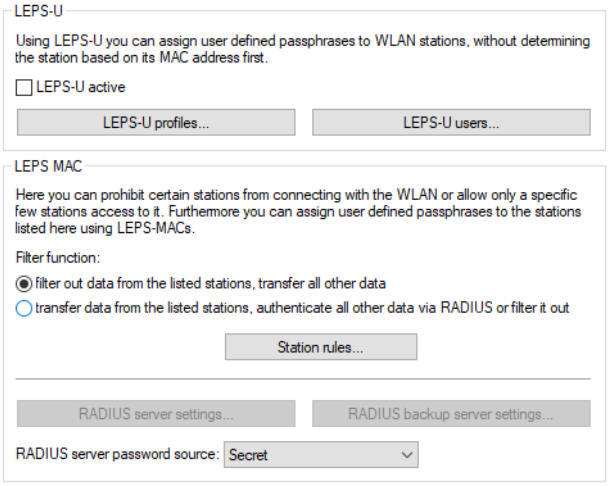
(*) These attacks are only detected if promiscuous mode is active.

Save the WIDS profile and then assign it to a WLAN profile under **WLAN controller** > **Profiles** > **WLAN profiles**.



13.17.13 Selecting approved stations for the WLAN

In LANconfig, the client that can login to the WLAN are configured under **Wireless LAN** > **Stations/LEPS**.



13.17.13.1 LEPS-U

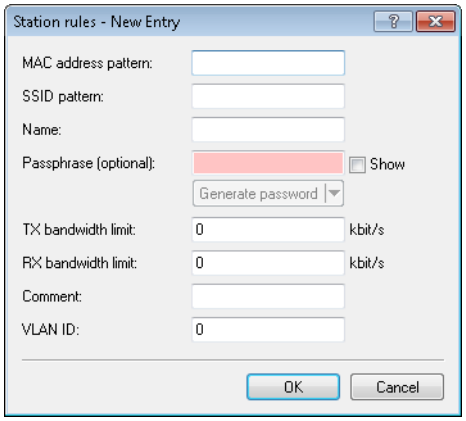
See *LANCOM Enhanced Passphrase Security User (LEPS-U)* on page 964.

13.17.13.2 Access-control list (LEPS-MAC)

With the **A**ccess **C**ontrol **L**is (ACL) you can permit or prevent individual WLAN clients accessing your WLAN. The decision is based on the MAC address that is permanently programmed into WLAN adapters.

If you centrally manage your LANCOM WLAN routers and LANCOM APs with a WLC, you will find the station table under **WLAN controller** > **Stations/LEPS** > **LEPS-MAC** under the button **Station rules**.

Check under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** to see if the setting **Filter out data from the listed stations, transfer all other** is activated. New stations to be included in your wireless network are added with the button **Station rules**.



MAC address pattern

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

It is possible to use wildcards.

SSID pattern

WLAN clients with the corresponding MAC addresses have access that is limited to this SSID.

The use of wildcards makes it possible to allow access to multiple SSIDs.

Name

You can enter any name you wish and a comment for any WLAN client. This enables you to assign MAC addresses more easily to specific stations or users.

Passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

TX bandwidth limit

Transmission-bandwidth restriction for WLAN clients currently authenticating themselves. A LANCOM Access Point in client mode transmits its own setting to the access point during login. This, together with the value set here, forms the bandwidth minimum as the bandwidth limit.

RX bandwidth limit

Reception-bandwidth restriction for WLAN clients currently authenticating themselves. A LANCOM Access Point in client mode transmits its own setting to the access point during login. This, together with the value set here, forms the bandwidth minimum as the bandwidth limit.

The RX bandwidth restriction is only active for WLAN devices in client mode. This value is not used by normal WLAN clients.

Comment

You can enter a comment here.

VLAN-ID

This VLAN ID is assigned to packets that are received from the client with the MAC address entered here. In case of VLAN-ID '0', the station is not assigned a specific VLAN ID. Instead, the VLAN ID of the radio cell (SSID) applies.

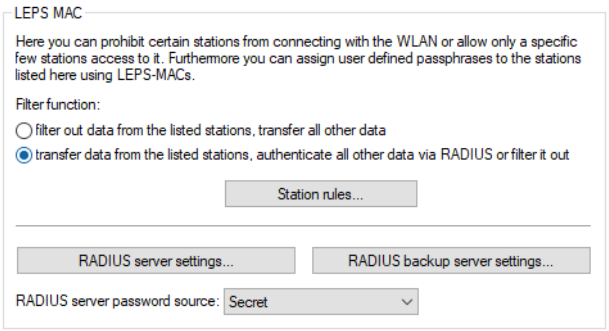
If filter rules contradict, the individual rule has a higher priority: A rule without wildcards in the MAC address or SSID takes precedence over a rule with wildcards. When creating these entries, the user should ensure that filter rules do not contradict. The definitions in the filters can be checked in a Telnet session with the trace command `trace WLAN-ACL`.

The filter criteria in the station list either allow or deny WLAN clients to access your wireless network. The entries **Name**, **Bandwidth limit**, **VLAN ID** and **Passphrase** are meaningless if the device uses valid filter criteria to deny access to the WLAN.

13.17.13.3 WLAN and RADIUS

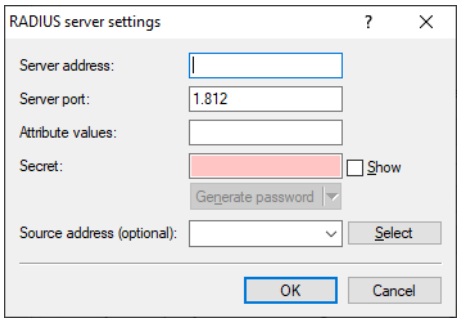
RADIUS is used for user authentication and accounting. For further information on this protocol, refer to the section *RADIUS* on page 1186.

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.



To use the RADIUS functionality for WLAN clients, go to the **LEPS-MAC** section and set the filter function to the option “Transfer data from the listed stations, authenticate all other data via RADIUS or filter it out”.

In LANconfig, the configuration is performed under **Wireless LAN** > **Stations/LEPS**. Here you configure the **RADIUS server settings** and the **RADIUS backup server settings**.



Server address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server used for central user management.

Server port

Specify here the port used for communication to your RADIUS server (default: 1,812).

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the following form:

`<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Secret

Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

Backup server address

Enter the IP address (IPv4, IPv6) or the hostname of the backup RADIUS server used for central user management.

Backup server port

Specify here the port used for communication to your backup RADIUS server (default: 1,812).

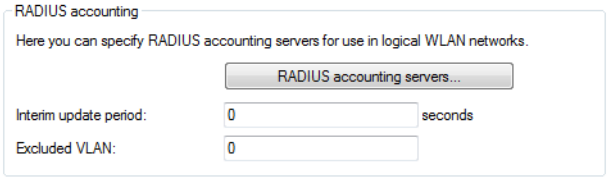
Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

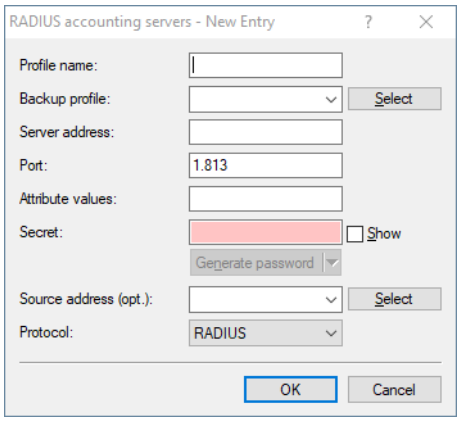
RADIUS server password source

Select whether you want to use a **Secret** or the **MAC address** as the password source for the RADIUS server.

RADIUS accounting



A RADIUS server that is to be used for accounting requires the appropriate configuration. The configuration is carried out with LANconfig under **Wireless LAN** > **Stations/LEPS** > **RADIUS accounting**. Configure the settings for a **RADIUS accounting server** here.



Profile name

Name of the RADIUS server performing the accounting for WLAN clients. The name entered here is used to reference that server from other tables.

Backup profile

Enter the name of the RADIUS backup server used for the accounting of WLAN clients if the actual accounting server is not available. This allows you to specify a "backup chaining" of multiple backup servers.

Server address

Here you enter the IPv4 or IPv6 address or the hostname of the RADIUS server used by the RADIUS client for the accounting of WLAN clients.

- The RADIUS client automatically detects which address type is involved.
- You also need to set the general values for retry and timeout in the RADIUS section.

Port

Port for communication with the RADIUS server during accounting (default: 1,812).

Attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

Attribute values can be set in quotation marks to allow the use of spaces or semicolons in the value definitions. To use a quotation mark as a character, use a leading backslash. To use the backslash itself as a character, use a double backslash.

It is also possible to use a number of placeholders:

- %n – replaced by the configured device name.
- %e – replaced with the serial number of the device as displayed in the device system info.
- %% – replaced by a single % character.
- %{name} – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

For more information about RADIUS attributes, please see *RADIUS attributes* on page 1551.

Secret

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that specified in the accounting server.

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Protocol

Select the protocol. Either **RADIUS** or **RADSEC**. For more information about RADSEC, please see *RADSEC* on page 1560.

Accounting Interim Interval

The accounting function in the device can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate this restart by calling the function `do /Setup/WLAN/RADIUS-Accounting/Restart-Accounting`.

Excluded VLAN

Here you enter the ID of the VLAN that the device is to exclude from RADIUS accounting. The RADIUS server then receives no information about the traffic in that VLAN.

13.17.14 Encryption settings

APs from LANCOM support the most up-to-date methods of encryption and security for data that is transferred via WLAN.

- The IEEE standard 802.11i/WPA stands for the highest degree of security that is currently available for WLAN connections. This standards uses a new encryption procedure (AES-CCM) which, in combination with other methods, achieves levels of security equaled only by VPN connections until now. However, using AES-capable hardware provides much faster transmission than relying on VPN protection.
- WEP is also supported to ensure compatibility with older hardware. WEP (**W**ired **E**quivalent **P**rivacy) is the encryption method originally incorporated in the 802.11 standard for the encryption of data in wireless transmission. This method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. A number of security loopholes in WEP have come to light over time, and so the latest 802.11i/WPA method should be used wherever possible.

To simplify the task of configuration, as of LCOS 10.20 the WLAN encryption settings appear as an additional tab in the dialog for the Logical WLAN settings. When configuring an SSID, it is no longer necessary to switch back and forth between the logical WLAN settings dialog and the WLAN encryption settings dialog.

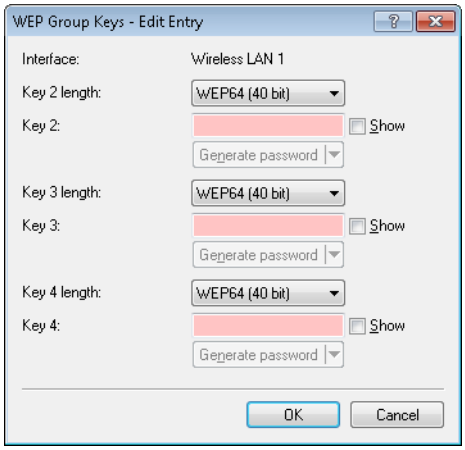
The logical WLAN settings are to be found under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**.

13.17.14.1 WEP group keys

The WEP method uses keys of 40 (WEP64), 104 (WEP128) or 128 bits (WEP152) in length. Each WLAN interface has four WEP keys: A special key for each logical WLAN interface and three common group WEP keys for each physical WLAN interface.

If 802.1X/EAP is in use and the **Enable dynamic re-keying** option is enabled under **Wireless LAN** > **802.1X** > **Interfaces**, the group keys from 802.1X/EAP are used and are consequently no longer available for WEP encryption.

As of LCOS 9.00 the system no longer displays WPA and WEP group keys in cleartext on the CLI, but masked (********). As a result, it is no longer possible to read these keys via SNMP, for example.



LANconfig: **Wireless LAN** > **Encryption** > **WEP group keys**

Command line: **Setup** > **Interfaces** > **WLAN** > **Group-Encryption-Keys**

Rules for entering WEP keys

WEP keys can be entered as ASCII characters or in hexadecimal form. The hexadecimal form begins with the characters '0x'. The keys have a length depending on the WEP method:

Method	ASCII	HEX
WEP 64	5 character example: 'aR45Z'	10 character example: '0x0A5C1B6D8E'
WEP 128	13 characters	26 characters
WEP 152	16 characters	32 characters

The ASCII character set includes the characters '0' to '9', 'a' to 'z', 'A' to 'Z' and the following special characters: ! " # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ‘ { | } ~

The HEX form uses the numbers '0' to '9' and the letters 'A' to 'F' to display each character as a character pair, which is why twice the number of characters is required to display a HEX key.

Select the length and the format (ASCII or HEX) of the key depending on the best option available in the wireless network cards that register with your WLAN. If the encryption in an AP is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.

13.17.14.2 Group keys per VLAN

In a VLAN environment, the central network administration generally assigns a unique VLAN ID to each virtual network. Which VLAN a client belongs to is mostly decided by the physical connection between the client and the network.

The central instance that manages the network (e. g. a VLAN-capable switch) internally assigns its ports to certain VLAN IDs. A data packet arriving at a port is internally passed on only to the ports with the corresponding VLAN IDs. Packets are not sent to the other network nodes that are connected to ports with different (or no) VLAN IDs.

In the case of multiple VLANs that offer various service levels, data communications are channeled through different logical wireless LANs (SSIDs). For example, employees receive access to the corporate network and the Internet via a specific SSID. Guests receive a different SSID that offers access limited to the Internet.

LANCOM access points also maintain VLAN network tables, which control the assignment of wireless LAN clients to individual VLANs. In large network environments, a RADIUS server usually handles the rights management and the assignment of clients to the VLANs. After successful authentication, the RADIUS server returns the data to the corresponding access point. For the duration of the client association, this data is stored in the AP's VLAN network table.

If necessary, the different WLAN clients associated with the same access point obtain different VLAN IDs. This is handled by the dynamic VLAN network tables in the access points. VLAN-internal communication is protected by a session key negotiated when logging onto the access point. This ensures that data communications by clients in different VLANs remain isolated from each other even though the various clients are using the same logical wireless LAN (SSID) to communicate with the access point.

A client associating with an access point in a wireless LAN is also assigned with a group key for the reception of broadcast or multicast messages.

Broadcast and multicast messages do not support VLAN tagging. This is why wireless LAN clients that are located in an isolated VLAN cannot be excluded from receiving these messages. In the ideal case, the wireless clients ignore broadcast and multicast messages from outside the VLAN.

Since these messages are increasingly being used for network configuration, the following problems arise:

- Network protocols such as "UPnP" and "Bonjour" use these messages to announce new services in the network.

  Theoretically, wireless LAN clients could set up access to servers that they have no access to at all.

- The Internet standard IPv6 uses multicast broadcasting to transmit router information to the clients.

  There is a risk that wireless LAN clients from outside the VLAN can use this information to evade access to the VLAN for which they are actually registered.

The widespread use of IPv6 will lead to an increase in this type of client problem.

To avoid these problems, the access point can assign a separate group key to each VLAN, instead of one that applies to all wireless LAN clients. Thus the access point sends its broadcast and multicast transmissions not to all existing wireless clients, but solely to a specific VLAN and the clients registered there. The wireless LAN clients in other VLANs therefore cannot decrypt these broadcasts.

The IEEE 802.11 standard provides for the administration of 4 different keys. One key is always reserved for the secure unicast communication between the access point and a wireless LAN client.

Thus in principle a maximum of 3 separate VLANs can be managed with their own group keys. Each group key is either managed automatically by the access point or manually by the network administrator. When the wireless LAN client logs on to the network, the access point sends it the corresponding VLAN group key to decrypt the broadcast and multicast transmissions for that VLAN.

This results in 2 possible scenarios:

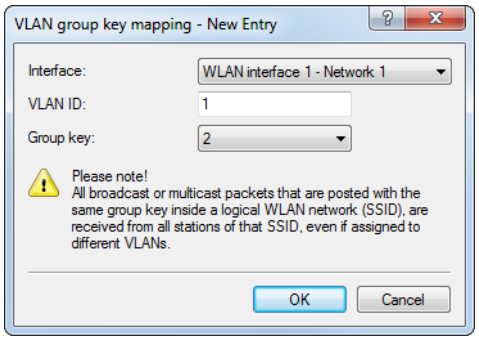
- No more than 3 VLANs are set up in the area of an access point: These VLANs are securely separated from each other by the 3 VLAN group keys.
- More than 3 VLANs exist within range of an access point: In this case, at least two VLANs share a group key. The administrator must find the optimal distribution of the shared group keys between the VLANs.

VLAN group keys are managed in 2 tables:

- The configuration table in which the assignment is carried out manually by the administrator.
- The status table in which the automatic group key assignment by the access point can be viewed.

Managing VLAN group keys

If you want to use different VLAN IDs on a single logical wireless LAN network (SSID), you have the option to assign the appropriate group key for broadcast and multicast transmissions. This setting in LANconfig is found under **Wireless LAN** > **Encrytion** > **VLAN group key mapping**



The automatic assignment of group keys is carried out in the following steps:

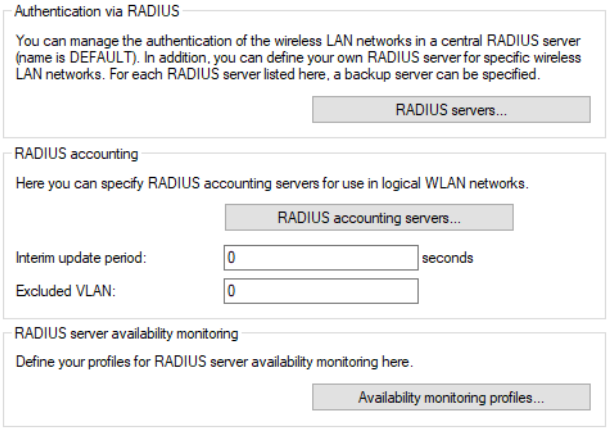
1. When a wireless LAN client logs on, the access point checks whether its VLAN ID is already listed in the status table and assigned to a group key accordingly.
2. If not, the access point consults the configuration table to check whether there is a manual assignment. Should this be the case, then it creates a mapped entry in this table.
3. If there is no manual assignment either, the access point adds a new entry for this client and assigns the group key with the fewest users.

The status table displaying the current automatic VLAN group key assignments for each SSID can be found on the command line at **Status** > **WLAN** > **VLAN-Groupkey-Mapping**

13.17.15 IEEE 802.1X / EAP

The international industry standard IEEE 802.1X and the Extensible Authentication Protocol (EAP) enable access points to carry out reliable and secure access checks. The access information can be managed centrally on a RADIUS server and can be called up by the access point on demand. RADIUS is used for user authentication and accounting. For further information on this protocol, refer to the section *RADIUS* on page 1186.

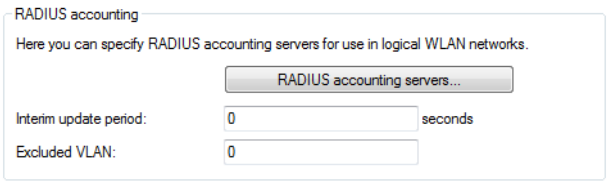
In LANconfig you configure the RADIUS server under **Wireless LAN** > **802.1X**.



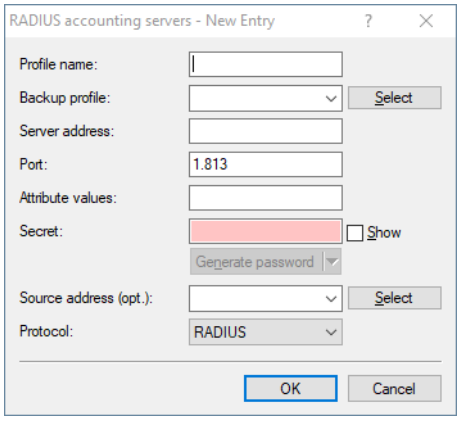
A description of how to configure a RADIUS server for IEEE 802.1X can be found under *Dial-in using 802.1X and RADIUS* on page 1530.

13.17.15.1 RADIUS accounting

RADIUS is used for user authentication and accounting. For further information on this protocol, refer to the section *RADIUS* on page 1186.



A RADIUS server that is to be used for accounting requires the appropriate configuration. The configuration is carried out with LANconfig under **Wireless LAN** > **802.1X** > **RADIUS accounting**. Configure the settings for a **RADIUS accounting server** here.



Profile name

Name of the RADIUS server performing the accounting for WLAN clients. The name entered here is used to reference that server from other tables.

Backup profile

Enter the name of the RADIUS backup server used for the accounting of WLAN clients if the actual accounting server is not available. This allows you to specify a “backup chaining” of multiple backup servers.

Server address

Here you enter the IPv4 or IPv6 address or the hostname of the RADIUS server used by the RADIUS client for the accounting of WLAN clients.

- The RADIUS client automatically detects which address type is involved.
- You also need to set the general values for retry and timeout in the RADIUS section.

Port

Port for communication with the RADIUS server during accounting (default: 1,812).

Attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

Attribute values can be set in quotation marks to allow the use of spaces or semicolons in the value definitions. To use a quotation mark as a character, use a leading backslash. To use the backslash itself as a character, use a double backslash.

It is also possible to use a number of placeholders:

- %n – replaced by the configured device name.
- %e – replaced with the serial number of the device as displayed in the device system info.
- %% – replaced by a single % character.
- %{name} – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

For more information about RADIUS attributes, please see *RADIUS attributes* on page 1551.

Secret

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that specified in the accounting server.

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Protocol

Select the protocol. Either **RADIUS** or **RADSEC**. For more information about RADSEC, please see *RADSEC* on page 1560.

Accounting Interim Interval

The accounting function in the device can be used to check the budgets of associated wireless LAN clients, among other things. Wireless Internet Service Providers (WISPs) use this option as a part of their accounting procedure. Accounting periods generally switch at the end of the month. A suitable action will cause the accounting session to be restarted at this time. Existing WLAN connections remain intact. A cron job can be used to automate this restart by calling the function `do /Setup/WLAN/RADIUS-Accounting/Restart-Accounting`.

Excluded VLAN

Here you enter the ID of the VLAN that the device is to exclude from RADIUS accounting. The RADIUS server then receives no information about the traffic in that VLAN.

Accounting status types "Accounting On" and "Accounting Off"

The RADIUS server and an AP exchange status information, such as the start, end, or update of client sessions at the AP. These data packets are characterized by the behavior of the logged-on clients.

With the status types "Accounting-On" and "Accounting-Off", the AP informs the RADIUS server about its general ability to perform RADIUS accounting:

Accounting-On

When the device switches to an operating state where it can exchange accounting information with a RADIUS server, it sends an "Accounting-On".

Accounting-Off

When the device switches to an operating state where it cannot exchange accounting information with a RADIUS server, it sends an "Accounting-Off".

The following conditions trigger the transmission of an "Accounting-On" or "Accounting-Off":

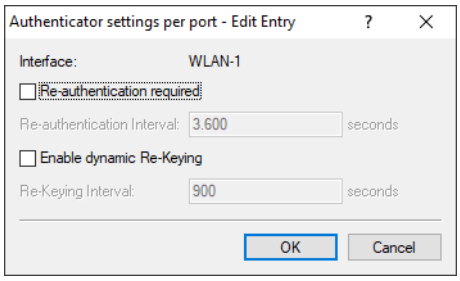
- The device activates or deactivates a physical WLAN interface with the appropriate SSID.

  Deactivation can also be the result of overheating, loss of connection or incorrect link detection.

- The WLAN interface switches into a non-AP mode (i.e. neither managed nor stand-alone-AP) or back.
- In P2P mode, the device switches into "exclusive" mode, which disables all SSIDs.
- The device activates or deactivates an SSID.
- The device activates or deactivates the RADIUS accounting for an SSID.

13.17.15.2 Automatic exchange of WEP keys

IEEE 802.1X also enables the secure transmission and the regular automatic changing of WEP keys. In this way, IEEE 802.1X improves the security of WEP.



LANconfig: **Interfaces** > **802.1X authenticator** > **LAN** > **Authenticator settings per port**

Command prompt: **Setup** > **IEEE802.1X**

Regularly update authentication

Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation.

Re-authentication interval

The interval for regular re-authentication. The default value for re-authentication interval is 3,600 seconds.

Enable dynamic re-keying and key transmission

Here you activate the regular generation and transmission of a dynamic WEP key.

Re-keying interval

Interval for the regular generation of the key.

Specific data rates for EAPOL packets

EAP over LAN (EAPOL) is used to authenticate WLAN clients at APs and makes use of WPA and/or 802.1x. This protocol allows layer-2 connections to support EAP communications by encapsulating EAP packets into Ethernet frames.

Under certain circumstances it may be desirable to select a lower data rate for the transfer of EAPOL packets than that available for the payload data. In the case of mobile WLAN clients, high data rates can cause EAPOL packet losses, which in turn leads to considerable delays in client association. This procedure can be stabilized by selecting specific data rates for EAPOL.

Command line: **Setup** > **Interfaces** > **WLAN** > **Transmission**

› **EAPOL-Rate**

Set the data rate for EAPOL transmission here.

Possible values:

› Like-Data, select from the available speeds

Default:

› Like-Data

Special values:

› Like-Data transmits the EAPOL data at the same rate as payload data.

13.17.16 IEEE 802.11u and Hotspot 2.0

Your device supports WLAN connections according to the IEEE 802.11u standard and the Hotspot 2.0 specification, which is based on it. Using 802.11u you have the option to implement automatic authorization and authentication of your users on a local WLAN network (for example, within your company) or a Public Spot network. The prerequisite for this is that the relevant stations (smartphones, tablet PCs, notebooks, etc.) also support connections for 802.11u and Hotspot 2.0. In detail, the following functions are offered:

› **Automatic network selection**

In a 802.11u-enabled environment, the user does not have to manually detect and select an SSID. Instead, the client independently searches for and selects a suitable Wi-Fi network by automatically requesting and evaluating the operator and network data of all 802.11u- access points that are in range. A previous login to the access point is not required.

Hotspot 2.0 stations also have the ability to retrieve information about the services available in a Wi-Fi network. If specific services that are relevant for a user (e.g., connections via HTTP, VPN or VoIP) are not available for a Wi-Fi network, any networks that do not meet the criteria are excluded from further searches. This ensures that users are always connected to the optimal network.

› **Automatic authentication and authorization**

In 802.11u-enabled environments, the station automatically carries out the user's login if the necessary credentials are available. Authentication can be done, for example, using a SIM card, a username and password, or a digital certificate. Repetitive manual input of the credentials by the user in a login screen is no longer necessary. After successful authentication, the user can immediately use the desired services.

› **Seamless handover**

Connections according to 802.11u and in conjunction with 802.21 facilitate the uninterrupted exchange of data connections between different network types. This enables users to switch their stations seamlessly from a cellular network to a WLAN network as soon as they get within range of a Hotspot 2.0 zone—and vice versa. The same is true for the transfer between two different operators if, for example, the user goes from one homogeneous network to another during a bus trip

› **Automatic roaming**

Connections as per 802.11u facilitate roaming between different operator networks. If a user is in range of a Hotspot 2.0 zone of an operator for which he does not have any credentials, his station still has the option to switch to its home network. Authentication at a third-party Hotspot 2.0 zone is handled by the operator's roaming partner, which then allows the user to access the third-party Wi-Fi network. This is interesting not only in areas where there are only single network operators with access points, it is also especially attractive for people traveling abroad.

Example: For example, a user who is in transit in the city with his 802.11u-enabled smartphone (station) can enable the WLAN feature to browse the Internet. The station then starts trying to find all available Wi-Fi networks in the area. If any of the access points offer 802.11u, the station selects the one network that best fits the required service based

on the operator and network information that was previously obtained, for example, from a hotspot offering Internet access from its own cellular network company. In this case, the subsequent authentication can be performed automatically via the SIM card so that the user does not need to intervene at any time during the process. The encryption method selected for the connection – e.g., WPA2 – is unaffected.

In summary, connections according to 802.11u and with Hotspot 2.0 enabled combine the security features and performance of classic Wi- Fi hotspots with the flexibility and simplicity of data cellular network connections. At the same time, they relieve the cellular networks by redistributing data traffic (and possibly also telephony) to the network connections and frequency bands offered by access points.

Passpoint® Release 2

As of LCOS 10.40 the extended Hotspot 2.0 feature in your WLAN device can be configured as per Passpoint® Release 2 as specified by the Wi-Fi Alliance. The RADIUS server in the LCOS has been equipped with the necessary features since 10.32 version RU4.

Passpoint® Release 2 simplifies the onboarding of devices into a network using the WPA2-Enterprise (802.1X) encryption method. A dedicated onboarding SSID allows a user with a device that supports Passpoint® Release 2 to install a profile and automatically switch to the encrypted network using the stored credentials. This helps to implement hotspots that provide encrypted wireless communication. An onboarding SSID can be used to give guests temporary access credentials.

Similarly, a mobile service provider can relieve the load on their cellular network by introducing Wi-Fi offloading and allowing mobile devices with a SIM card to automatically log into their WLAN network. Customers' devices find the WLAN network from the mobile service provider and automatically login to the operator's WLAN network using the user data stored on the SIM card.

Passpoint® Release 2 adds the following features to Hotspot 2.0:

- Online Sign-Up (OSU) – with Passpoint® Release 2, companies and network operators can use "Online Sign-Up" servers (OSU servers) to deliver profiles to their users. Using an open OSU SSID, users can identify various OSU servers by their icons and thus select the one that suits them best. The OSU server can optionally ask the user for credentials before providing a profile that best suits the user's device. In addition to the open OSU-SSID, an encrypted SSID can be used to exchange user data by means of "anonymous EAP-TLS". This requires the use of a RADIUS server that supports "anonymous EAP-TLS".

  An OSU server is not included with LCOS. However, solutions are available from LANCOM partners.

- OSU icons – icons corresponding to the supported OSU servers can be uploaded to the LCOS as files using the WEBconfig feature **File management**. We recommend PNG as the file format.
- Notification – the network can notify the user about an imminent logout from the RADIUS server. This may be the case if the user credentials have expired or if the specified connection duration has been reached.
- QoS Map – the "QoS Map Set" function enables an access point to instruct its clients to use a specific QoS map. This defines the values for the contention window (media access via EDCA) of the various access categories (voice, video, best effort and background data packets) and the corresponding DSCP parameters. At the same time, the access points also use the values stored in the QoS map.

  Currently available are the two QoS maps required by the Wi-Fi-Alliance and the default QoS map of the LCOS.

13.17.16.1 Hotspot operators and service providers

The Hotspot 2.0 specification of the Wi-Fi Alliance differentiates between hotspot operators and hotspot service providers: A **hotspot operator** only operates one Wi-Fi network, while a **hotspot service provider** (SP) provides the connection for the user to the Internet or a cellular network. Of course, it is possible for an operator to also be an SP. However, in all other cases, a hotspot operator requires the corresponding roaming agreements with an SP or a group of multiple SPs (called a roaming consortium). Only when an operator has made these agreements are the various roaming partners' customers able to authenticate with the hotspot operator. Each service provider operates its own AAA infrastructure. A hotspot communicates this list of possible roaming partners and the name of the hotspot operator using ANQP (see functional description).

13.17.16.2 Functional description

The 802.11u standard is the base standard of IEEE. This standard essentially expands access points or hotspots with the ability to broadcast so-called "ANQP data packets "(Advanced Message Queuing Protocol) in its broadcast signals. ANQP is a query/response protocol that a device can use to request a range of information about the hotspot. This includes both meta-data, such as information about the owner and the venue, as well as information on the underlying network, such as information on operator domains, roaming partners, authentication methods, forwarding addresses, etc. All 802.11u-enabled devices in range have the ability to request these data packets without a prior login to the access point in order to select a network based on the network information.

The Wi-Fi Alliance has added further ANQP elements to the standard, and markets this specification as **Hotspot 2.0**. This Hotspot 2.0 function merely adds additional elements to the standard, which the device can use as criteria for selecting its network. These criteria include, for example, information about the services and WAN metrics available at the hotspot. The associated certification program is called Passpoint®, which is available in different versions. Certain LANCOM access points are Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 and/or 2).

The ANQP data packets are the central information element of the 802.11u standard. However, to signal the support for 802.11u and to transmit data packets, further elements are required for the operation of 802.11u:

- The signaling of 802.11u support in the beacons and probes of a hotspot are done by the element known as the **Interworking element**. In this element, the initial basic network information—such as the network classification, Internet availability (Internet bit) and the OI of the roaming consortium and/or of the operator—are already included. At the same time, it is used by 802.11u-enabled devices as an initial screening criterion when detecting a network.
- ANQP data packets are transferred within the so-called GAS containers. GAS stands for Generic Advertisement Service, and is the name of generic containers that allow a device to request additional internal and external information for the network selection from the hotspot, in addition to the information in the beacons. The GAS containers are transmitted on layer 2 by what are referred to as public action frames.

Login by an 802.11u-enabled client at a Hotspot 2.0

The following functional description schematically illustrates the selection and login process of an 802.11u-enabled device at a Hotspot 2.0.

Login via username/password or digital certificate

1. The hotspots reply with an ANQP response, which contains, among other things, the name of the hotspot operator and a list of NAI realms, which list all available roaming partners (service provider, abbreviated SP).
2. The device loads the locally stored credentials from the WLAN profiles or installed certificates that were set up by the user, and compares the local realms with the NAI realm lists obtained in (2).
   a. If the device successfully finds one, it knows that it can be authenticated successfully on the relevant Wi-Fi network.
   b. If the device successfully finds more than one, the selection of a Wi-Fi network is made based on the user's preference list. This list defines the preferred order of operators in conjunction with the potential roaming partners. In this case, the device compares the operator names listed under (2) with the list, and selects the operator with the highest priority.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate SP. The access point then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for authentication. The authentication is performed using the authentication method determined by the SP. The authentication via username/password uses EAP-TTLS, and authentication via digital certificate uses EAP-TLS.

Login via (U)SIM

1. In contrast to the login via username/password or digital certificate, a device with a (U)SIM does not request the list of NAI realms in its ANQP requests, but rather the 3GPP Cellular Network Information. The ANQP responses contain the cellular network information list of all cellular network providers for which the access point offers authentication.

2. The device loads the parameters for the cellular network from its local (U)SIM card, and compares it with the data retrieved from the cellular network information lists. The list comparison and selection of a preferred provider network is performed analogous to the login via username/password or digital certificate.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate cellular network company. The hotspot then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for the authentication. The presence of a (U)SIM card changes the possible authentication method for the device to EAP-SIM or EAP-AKA.
4. The AAA system verifies the credentials for authentication via the interface MAP (Mobile Application Part) at the HLR server (Home Location Register) of the cellular network company.

If authentication is successful, the device gets access to the WLAN network either via hotspot (credentials for the operator's network are available) or automatic roaming (credentials for the operator's network are not available).

If there are multiple authentication options available for the device (e.g., SIM card and username/password), it has the option of using the preferred EAP authentication method and, therefore, the preferred credentials based on the NAI realm or cellular network information list.

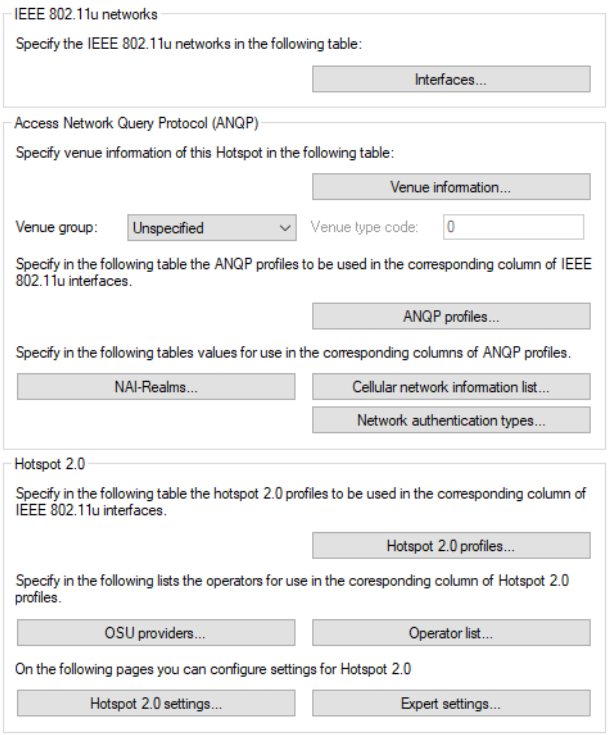
13.17.16.3 Recommended general settings

The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- WPA2-Enterprise Security (802.1X) enabled
- Authentication using EAP with the corresponding variant:
  - EAP-SIM/EAP-AKA for authentication with SIM / USIM card
  - EAP-TLS for authentication with a digital certificate
  - EAP-TTLS for authentication with a username and password
- Enabled and properly configured ARP proxy
- Disabled multicasts and broadcast in cellular networks
- Non-approved data traffic between the cellular network devices (Layer 2 traffic inspection and filtering). The corresponding settings can be found in LANconfig under **Wireless LAN** > **Security** > **Traffic between different SSIDs**.
- Enabled and implemented firewall on the access router, which provides Internet access

13.17.16.4 Configuration menu for IEEE 802.11u / Hotspot 2.0

The configuration menu for IEEE 802.11u and Hotspot 2.0 is located under **Wireless LAN** > **IEEE 802.11u**.



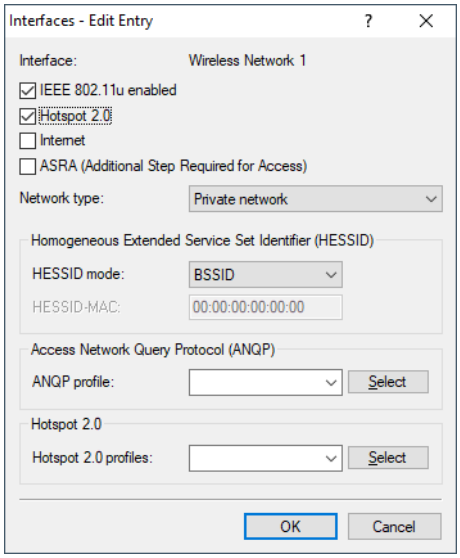
The device offers the ability to individually enable or disable and configure the support the IEEE 802.11u standard as well as the Hotspot 2.0 functionality for each logical WLAN interface using the button **Interfaces**.

Some parameters need to be configured in what are known as “Profiles”. Using profiles, you can group different rows in lists, which you only have to reference from the other windows. Essentially, these are profiles for ANQP data packets and Hotspot 2.0. The relationships between the profile lists is as follows:

```
| -- Interfaces
  |--ANQP profiles
    |--NAI realms
    |--Cellular network information list
    |--Network authentication types
  |--Hotspot 2.0 profiles
    |--Operator list
    |-- OSU providers
```

Activating interfaces

The table **Interfaces** is the highest administrative level for IEEE 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.



Interface

Name of the logical WLAN interface that you are currently editing.

IEEE 802.11u enabled

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Hotspot 2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.

Internet

Select whether the Internet bit is set. The Internet-bit explicitly informs all stations that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

Using this function you only communicate the availability of an Internet connection. You configure the corresponding regulations on the firewall, irrespective of this option.

ASRA – Additional steps for access required

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface. Based on the setting made here, the user has the option to limit network detection of their devices to specific network types. Possible values are:

Private network

Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.

Private with guest access

Similar to **Private network**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

Chargeable public network

Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.

Free public network

Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.

Personal device network

In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.

Emergency services only network

Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

Test or experimental

Describes networks that are set up for testing purposes or are still in the setup stage.

Wildcard

Placeholder for previously undefined network types.

HESSID mode

Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as “HOTSPOT”. Possible values for the HESSID mode include:

BSSID

Select this item to set the BSSID of the device as the HESSID for your homogeneous ESS.

User

Select this item to manually assign a HESSID.

None

Select this item in order to not assign any homogeneous ESS and to isolate it from the device network.

HESSID-MAC

If you selected the setting `user` for the **HESSID mode**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., "008041AEFD7E" for the MAC address 00:80:41:ae:fd:7e.

If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

ANQP profile

Select an ANQP profile from the list. You create ANQP profiles in the configuration menu using the button of the same name.

Hotspot 2.0 profiles

Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

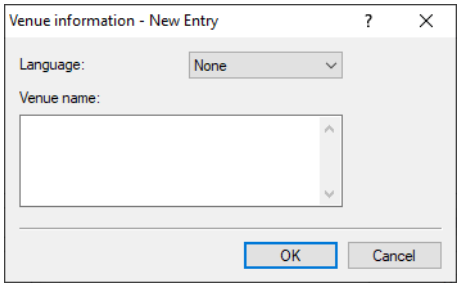
Configuring ANQP data packets

Venue information and group

Information about the access point's location is managed using the table **Venue information** and the subsequent dialogs **Venue group** and **Venue type code**.

In the event of a manual search, additional details on the **Venue information** help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

You can place your device in a predefined category using the **Venue group** and **Venue type code** – as opposed to the user-defined location information.



Language

You have the ability to specify custom information for the location of the access point for each language. The location name that matches your user's language will then be displayed. If a language is not available for a user, its station chooses one based, for example, on the default language.

Location name

Enter a short description of the location of your device for the selected language, for example:

```
Ice Café Valencia
123 Street
City, State 12345
```

The **Venue group** describes the environment where you operate the access point. You define them globally for all languages. The possible values, which are set by the "venue group code", are specified in the 802.11u standard.

Using the **Venue type code**, you have the option to specify the details for the venue group. These values are also specified by the standard. The possible type codes can be found in the following table.

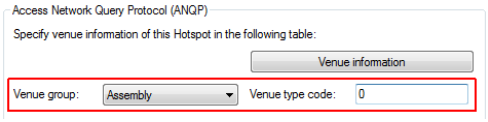


Table 29: Overview of possible values for venue groups and types

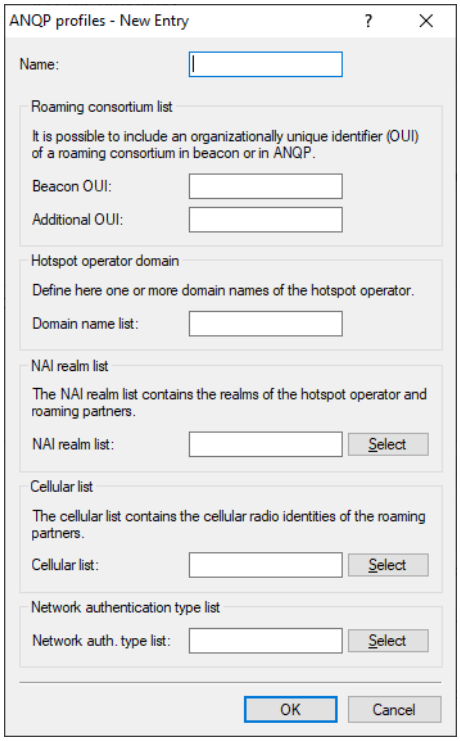
Venue group	Venue type code
Unspecified	
Assembly	› 0 = unspecified assembly › 1 = stage › 2 = stadium › 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) › 4 = amphitheater › 5 = amusement park › 6 = place of worship › 7 = convention center › 8 = library › 9 = museum › 10 = restaurant › 11 = theater › 12 = bar › 13 = café › 14 = zoo, aquarium › 15 = emergency control center
Business	› 0 = unspecified business › 1 = doctor's office › 2 = bank › 3 = fire station › 4 = police station › 6 = post office › 7 = office › 8 = research facility › 9 = law firm
Educational:	› 0 = unspecified education › 1 = primary school › 2 = secondary school › 3 = college
Factory and industry	› 0 = unspecified factory and industry › 1 = factory
Institutional	› 0 = unspecified institution › 1 = hospital › 2 = long-term care facility (e.g., nursing home, hospice) › 3 = rehabilitation clinic › 4 = organizational association › 5 = prison
Commerce	› 0 = unspecified commerce › 1 = retail store

Venue group	Venue type code
	› 2 = food store › 3 = Automobile workshop › 4 = shopping center › 5 = gas station
Halls of residence	› 0 = unspecified residence hall › 1 = private residence › 2 = hotel or motel › 3 = student housing › 4 = guesthouse
Warehouse	› 0 = unspecified warehouse
Utility and miscellaneous	› 0 = unspecified service and miscellaneous
Vehicular	› 0 = unspecified vehicle › 1 = passenger or transport vehicles › 2 = aircraft › 3 = bus › 4 = ferry › 5 = ship or boat › 6 = train › 7 = motorcycle
Outdoor	› 0 = unspecified outdoor › 1 = municipal WLAN network › 2 = city park › 3 = rest area › 4 = traffic control › 5 = bus stop › 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. **ANQP profiles** offer you the ability to group certain ANQP elements and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These elements

include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.



Name

Assign a name for the ANQP 2.0 profile here. This name will appear later in the interfaces table in the selection for ANQP profiles.

Beacon OUI

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

Additional OUI

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

Domain name list

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is

sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

NAI realm list

Select an NAI realm profile from the list. You specify profiles for NAI realms in the configuration menu by clicking the button **NAI realms**.

Cellular list

Select the cellular network identity from the list. You set the identities for cellular networks – similar to profiles – in the configuration menu using the button **Cellular network information list**.

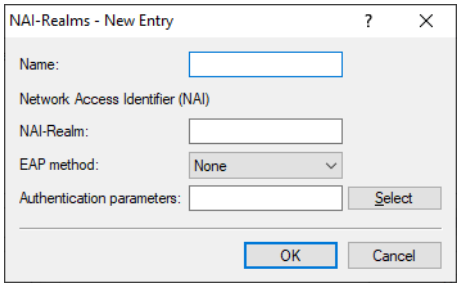
Network authentication type list

Select an authentication profile from the list. You specify profiles for network authentication in the configuration menu by clicking the button **Network authentication types**.

Additionally, the CLI provides the option to show the type of available IP addresses, which they can obtain from the network after successful authentication. You can access the relevant parameters **IPv4-Addr-Type** and **IPv6-Addr-Type** via the path **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.



Name

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. This name will appear later in the ANQP profile in the selection for **NAI realm list**.

NAI realm

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in *RFC 2486* and, in the simplest case, is `<username>@<realm>`. For `user746@providerX.org`, the corresponding realm is `providerX.org`.

EAP-Method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication method Possible values are:

EAP-TLS

Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate that the user has to install.

EAP-SIM

Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.

EAP-TTLS

Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.

EAP-AKA

Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

None

Select this setting when the relevant NAI realm does not require authentication.

Authentication parameters

Click the authentication parameters that match the EAP method, e.g. for EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

or for EAP-TLS `Credentials.Certificate`.

Possible values are:

Table 30: Overview of possible authentication parameters

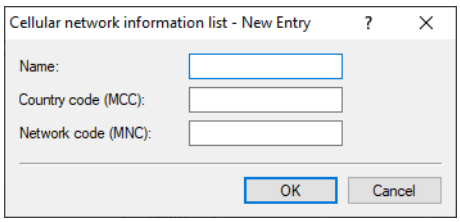
Parameter	Sub-Parameter	Comment
NonEAPAuth		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in *RFC 1994*
	MSCHAP	Implementation of Microsoft CHAP V1, specified in *RFC 2433*
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in *RFC 2759*
Credentials		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password

* The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Parameter	Sub-Parameter	Comment
TunnelEAPCredentials.*	None	No credentials required
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

Cellular network information list

Using this table you manage the identity lists for cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.



Name

Assign a name for the cellular network identity, such as an abbreviation of the network operator in combination with the cellular network standard used. This name will appear later in the ANQP profile in the selection for **Cellular list**.

Country code (MCC)

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.

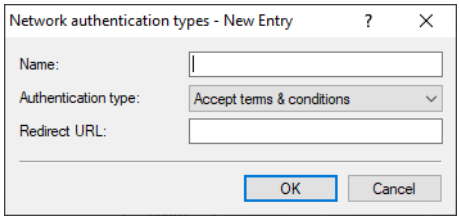
Network code (MNC)

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Network authentication types

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

Please remember to set the ASRA bit in the **Interfaces** table if you set up an additional authentication step.



Name

Assign a name for the table entry, for example `Accept Terms & Conditions`. This name will appear later in the ANQP profile in the selection for **Network auth. type list**.

Authentication type

Choose the context from the list, which applies before forwarding. Possible values are:

Accept terms & conditions

An additional authentication step is set up that requires the user to accept the terms of use.

Online enrollment

An additional authentication step is set up that requires the user to enroll online first.

HTTP redirection

An additional authentication step is set up to which the user is forwarded via HTTP.

DNS redirection

An additional authentication step is set up to which the user is forwarded via DNS.

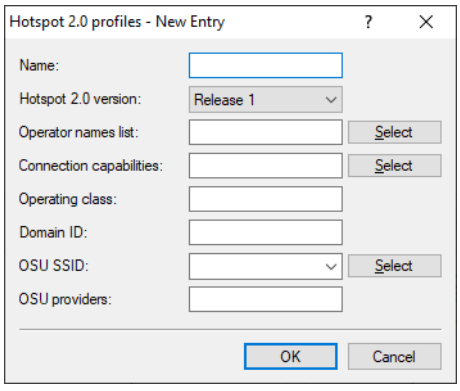
Redirect URL

Enter the address to which the device forwards stations for additional authentication.

Configuring Hotspot 2.0

Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offer you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.



Name

Assign a name for the Hotspot 2.0 profile here. This name will appear later in the interfaces table in the selection for the Hotspot 2.0 profile.

Hotspot 2.0 version

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Operator names list

Select the profile of a hotspot operator from the list. You specify profiles for hotspot operators in the configuration menu by clicking the **Operator list**.

Connection capabilities

Select the connection capabilities for each service. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown". Possible status values for each of these services are "closed" (`-C`), "open" (`-O`) or "unknown" (`-U`):

- `ICMP`: Specify whether to allow the exchange of information and error messages via ICMP.
- `TCP-FTP`: Specify whether to allow file transfers via FTP.
- `TCP-SSH`: Specify whether to allow encrypted connections via SSH.
- `TCP-HTTP`: Specify whether to allow Internet connections via HTTP/HTTPS.
- `TCP-TLS`: Specify whether to allow encrypted connections via TLS.
- `TCP-PPTP`: Specify whether to allow the tunneling of VPN connections via PPTP.
- `TCP-VOIP`: Specify whether to allow Internet telephony via VoIP (TCP).
- `UDP-IPSEC-500`: Specify whether to allow IPsec via UDP and port 500.
- `UDP-VOIP`: Specify whether to allow Internet telephony via VoIP (UDP).
- `UDP-IPSEC-4500`: Specify whether to allow IPsec via UDP and port 4500.
- `ESP`: Specify whether to allow ESP (Encapsulating Security Payload) for IPsec.

If you do not know if a service is available and its ports are open or closed on your network, or you consciously do not want to make any entry for the status, select a `-U` setting.

Using this dialog, you do not define permissions! The stations only use the entries to determine whether to join a network via your device. You configure specific access permissions for your network with other device functions, such as the firewall/QoS.

Operating class

Enter the code for the global operating class of the access point. Using the operating class, you inform a station about the frequency bands and channels that your access point is available on. Example:

- `81`: Operation at 2.4 GHz with channels 1-13
- `116`: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11- 2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at *standards.ieee.org*.

Domain ID

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16- value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

OSU SSID

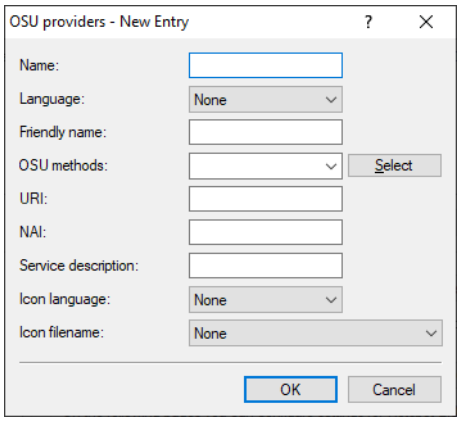
Name of the SSID that provides access to the OSU server.

OSU providers

List of OSU provider names in *OSU providers* on page 1092 that are supported in the profile.

OSU providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.



Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Language

Set the language supported by this OSU provider.

Friendly name

Give this OSU provider a descriptive name.

OSU methods

Set the OSU methods used by this OSU provider. Options are “OMA-DM” or “SOAP-XML-SPP”.

Available methods with the online sign-up server with Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Enter a URI where a client can reach the OSU server.

NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Service description

Enter a descriptive text for this service here.

Icon language

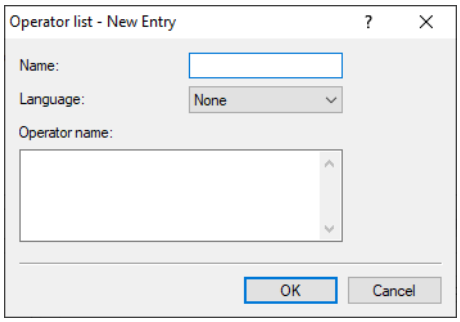
This item sets the language for the selected icon.

Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the ***File management*** feature. We recommend PNG as the file format.

Operator list

Using this table you manage the cleartext name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.



Name

Assign a name for the entry, such as an index number or combination of operator name and language.

Language

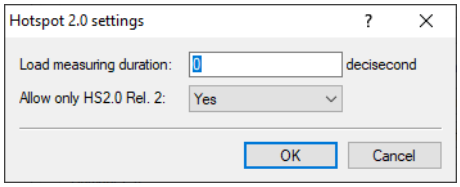
Select a language for the hotspot operator from the list.

Operator name

Enter the cleartext name of the hotspot operator.

Hotspot 2.0 settings

This table is used to configure particular settings for Hotspot 2.0.



Load measuring duration

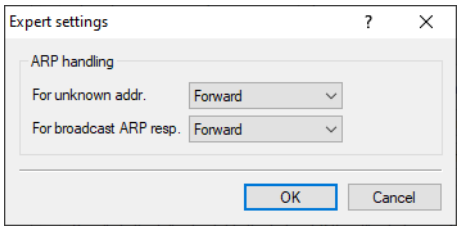
Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

Allow only Hotspot 2.0 Release 2

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

Expert settings

This table is used to configure the expert settings for Hotspot 2.0. The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. An alternative solution would be to suppressing broadcast/multicasts via **Transmit only unicasts, suppress multicasts and broadcasts** in the logical WLAN network settings.



For unknown addresses

In case of an unknown address, the packet is either forwarded or discarded.

For broadcast ARP responses

In case of a broadcast, the packet is either forwarded or discarded.

13.17.17 Static WLAN controller

The widespread use of wireless APs and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations.

Yet in spite of the numerous advantages WLAN infrastructures offer, there are still a number of unsettled issues:

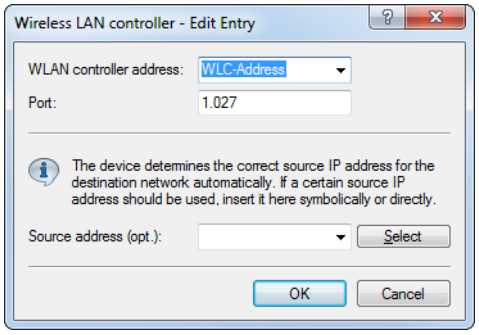
- All APs must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the APs, especially for larger WLAN infrastructures with the appropriate security mechanisms, requires advanced qualifications and experience on the part of those responsible, and it ties up considerable resources in the IT departments.
- The manual customization of the configurations in the APs when changes are made to the WLAN infrastructure can be time-consuming, with the result that different configurations can be present in the WLAN at the same time.
- Combined utilization of the shared communications medium (air) requires effective coordination of the APs to avoid frequency interference and optimize network performance.
- In public places, APs are a potential security risk because the devices themselves, including the security-related data in them such as passwords, etc., are susceptible to theft. In addition, rogue APs may be able to connect to the LAN unnoticed, bypassing the security policies that are in place.

Centralized WLAN management is the solution to these problems. The configuration of the AP is then no longer carried out in the devices themselves but by a central authority instead, the WLAN controller (WLC). The WLC authenticates the APs and transmits the correct configuration to the approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the APs simultaneously. Optionally the configuration provided by the WLC is not stored in the AP's flash memory but in RAM, so security-related data cannot fall into the hands of unauthorized persons in the event that devices are stolen. Only in “standalone operation” is the configuration optionally saved for a defined period to flash memory (in an area that cannot be read out with LANconfig or other tools).

Here you enter the WLC that this managed AP should preferably contact. In order for the AP to receive its configuration from a WLC, navigate to **Wireless LAN** > **General** > **Physical WLAN settings** > **Operation** and set the **WLAN operation mode** to **Managed**.

This setting is not required if the AP and WLC are located in the same IP network.

LANconfig: **Wireless LAN** > **WLC** > **WLAN controller**



WLAN controller address

The name or IP address of the WLAN controller is specified here.

The name of the LANCOM WLAN controller is preset to 'WLC-Address', so in most cases you do not have to change anything here. If DNS address resolution is not possible, enter the IP address of the WLAN controller here.

Port

The port used to communicate with the WLC. Default: 1027

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

13.17.18 Advanced WLAN parameters

- **ProbeRsp-Retries**

  Command line: **Setup** > **Interfaces** > **WLAN** > **Transmission**

  This is the number of hard retries for probe responses, i.e. messages sent from an AP in answer to a probe request from a client.

  Possible values:

  - 0 to 15

  Default:

  - 3

  Default:

  - Values larger than 15 are taken as 15.

- **Block time**

  Command line: **Setup** > **Interfaces** > **WLAN** > **Roaming**

  If your device is operating as a WLAN client in an environment with multiple WLAN access points all with the same SSID, you can define a time period during which the WLAN client will avoid associating with a particular AP after receiving an "association-reject" from it.

Possible values:

› 0 to 4294967295 seconds

Default:

› 0

13.17.18.1 Noise offsets

The radio modules in the WLAN devices can specify the signal and noise levels as absolute values (in dBm). However, the receivers are not calibrated ex-factory. To specify optimal values for noise and signal levels, the noise offsets table can be used to set correction values (in dB) for each frequency band (2.4 / 5 GHz), channel, and WLAN interface. These values are added to the noise and signal values as supplied by the radio modules.

Command prompt: **Setup** > **WLAN** > **Noise-Offsets**

› **Band**

Frequency band for which the noise-offset value is specified.

Possible values:

› 2.4 or 5 GHz

Default:

› 2.4 GHz

› **Channel**

Channel for which the noise-offset value is specified.

Possible values:

› Valid channel descriptors for the selected frequency band; max. 5 characters

Default:

› Blank

› **Interface**

Physical WLAN interface for which the noise-offset value is specified.

Possible values:

› Selection from the list of available WLAN interfaces.

Default:

› WLAN -1

› **Value**

Noise-offset value in dB. This is added to the values output by the radio module.

Possible values:

› Maximum 4 digits.

Default:

› Blank

The operator of the WLAN can determine the values for noise offset with the appropriate measuring equipment. The values can vary depending on production-related variances, aging and environmental factors. Should it be necessary to define exact values for signal level, then the values have to be determined for each device individually, and they should be checked on a regular basis. LANCOM supplies standard values for some

models only. Due to the variances mentioned earlier, LANCOM assumes no liability for the accuracy of these values.

13.17.18.2 UUID info element for LANCOM WLAN access points

All current LANCOM access points have multi-SSID capability. This means that they can simultaneously present different 'virtual' access points to their WLAN clients.

For devices with two radio modules (dual radio), the BSSIDs relate to the logical networks on the corresponding radio module. However, the MAC addresses of the two radio modules are completely independent of one another. Consequently, logical networks with different BSSIDs cannot be unequivocally related to a single device.

However, for the planning and monitoring of networks, it is often desirable to be able to relate logical networks to their respective devices (or radio modules).

LANCOM access points support an Aironet-compatible information element that contains the name of the device as assigned to it by the administrator. The transmission of this information is optional and many operators disable it for security reasons because they want to publish as little information as possible about the access point on the network.

Thus, this information either does not appear for network monitoring at all or, depending on the setting, the information may not identify the device as a LANCOM access point.

Besides this, LANCOM access points possess a UUID (universally unique identifier), which is calculated from the device type and serial number and can identify the device uniquely on the network. By using encryption when generating the UUID, the device type or serial number can only be inferred with considerable effort (brute-force attack for all types of devices and serial numbers).

Transmission of the UUID can be switched on or off independent of the radio module and logical network.

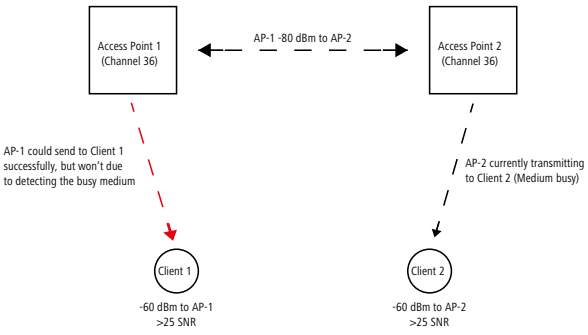
13.17.18.3 Rate adaptation algorithm

Unlike an Ethernet connection, a wireless connection uses variable bit rates. Higher bit rates provide a better throughput, but they require a high signal quality at the receiver end. This is essential for error-free decoding. WLAN devices adapt their bit rate the first time a connection is made or if there is a change to the properties of the medium. This ensures that the device uses the best available bit rate.

Unlike the standard algorithm, the well-known Minstrel algorithm checks not only the neighboring bit rates, but all available bit rates. This is a quicker way of determining the optimal bit rate.

13.17.18.4 Reduction of sensitivity for received packets

In high-density scenarios such as stadiums, exhibition halls or auditoriums, it is inevitable that access points that use the same channel will use the medium to a high capacity. This can result in a situation where the access points withhold their transmissions to the clients because the channel is recognized more often as busy.



An access point can be set artificially "deaf" by reducing the reception sensitivity from LCOS 10.30 RU1 onwards. This means that transmissions further away from the access point are "overheard" and the channel is detected more often

as “free”. In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer “heard”. This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

You set the reduction via the console in value **Setup** > **Interfaces** > **WLAN** > **Radio-Settings** > **Rx-Packet-Sens.-Reduction**. The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

For WLAN controllers, this setting can also be made via the console in the profile of an access point. Under **Setup** > **WLAN-Management** > **AP-configuration** > **Accesspoints** adjust the values **Module-1-Rx-Packet-Sens.-Reduction** resp. **Module-2-Rx-Packet-Sens.-Reduction** accordingly.

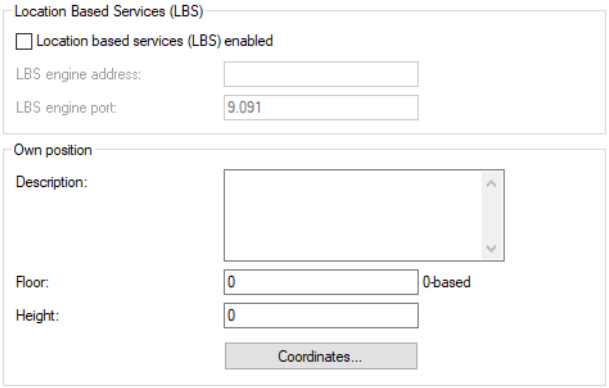
This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

13.17.19 Location-based services (LBS)

LANCOM access points are able to work as LBS clients with an LBS server. In this case, they report any connected clients to the LBS server, which can then offer location-based services to those clients. An HTTP API is supported as of LCOS 10.42, along with a Thrift interface that has been available for some time already.

Using the HTTP interface, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

LANconfig: **Miscellaneous Services** > **Services** > **Location Based Services (LBS)**



Location based services (LBS) enabled

Enables or disables the location-based services.

Server type

Here you configure whether to use the HTTP interface or the Thrift interface.

13.17.19.1 HTTP interface

Using the HTTP API, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

HTTP server URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. When using HTTPS, certificate verification may be disabled, based on a server certificate, or performed a both ends by server and client authentication. For this purpose, a PKCS#12 container with CA and client certificate can be uploaded to the device that contains the CA certificate or the CA and client certificates. This can be performed using LANconfig or WEBconfig. If no PKCS#12 container is uploaded, no certificate verification is carried out when HTTPS is used.

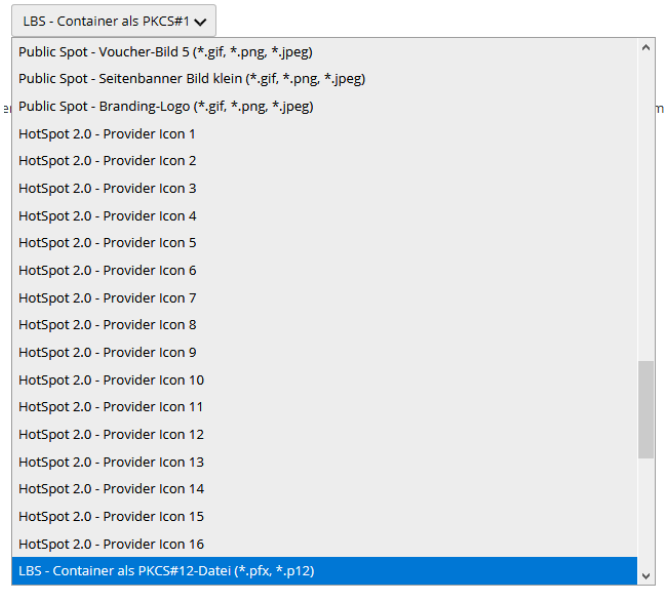


Figure 19: Screenshot WEBconfig

HTTP server secret

The HTTP server secret is transmitted in the JSON messages from the access point to the end point and can be used to additionally authenticate the messages.

HTTP data sources

Here you configure whether to transmit WLAN, BLE, or both types of LBS data.

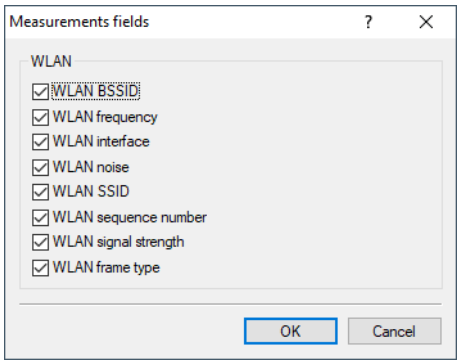
The setting **BLE** is only supported on devices featuring BLE.

Source address

Use this item to configure which loopback address should be used for communication with the HTTP endpoint. This may be necessary if multiple IP networks are configured on the device.

Measurements fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.



Data format of the messages sent to the endpoint

› For **WLAN**:

```
{
  "version": "1.0",
  "secret": "secret",
  "type": "WLAN",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "clientMac": "334455667788",
      "seenTime": 1579792598996,
      "frameSeqNum": 1074,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -56,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    },
    {
      "clientMac": "554433aabbcc",
      "seenTime": 1579792601334,
      "frameSeqNum": 2742,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -45,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    }
  ]
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the access point configuration.

type

The type of data sent. Can be either WLAN or BLE.

deviceMac

The LAN MAC address of the access point.

measurements

This contains at least one measured value. This could also be a number of measurements.

clientMac

The MAC address of the WLAN client.

seenTime

The time stamp (in Unix time) when the WLAN frame from the client was received by the access point.

frameSeqNum

The sequence number of the received WLAN frame.

ssid

The SSID contained in the WLAN frame, if available.

module

Describes the access-point WLAN interface that the WLAN frame was received from. Typically 0 for the first WLAN interface or 2 for the second WLAN interface.

bssid

The BSSID contained in the WLAN frame.

rssi

The signal strength in dBm of the received WLAN frame.

frequency

The frequency in MHz of the WLAN channel that the WLAN frame was received on.

noise

The noise level in dBm on the channel that the WLAN frame was received on.

frameType

The frame type of the received WLAN frame. The following types are available: `PROBE`, `AUTHENTICATION`, `ASSOCIATION`, `DEAUTHENTICATION` or `DEASSOCIATION`.

› For **BLE**:

```
{
  "version": "1.0",
  "secret": "secret",
  "type": "BLE",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "deviceAddress": "001122334455",
      "seenTime": 1579792601269,
      "addressType": "Random",
      "rssi": -77
    },
    {
      "deviceAddress": "ffeeddccbbaa",
      "seenTime": 1579792601273,
      "addressType": "Random",
      "rssi": -61
      "name": "test",
      "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
      "scanResponseData": "050974657374"
    }
  ]
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the AP configuration.

type

The type of data sent. Can be either WLAN or BLE.

deviceMac

The LAN MAC address of the AP.

measurements

This contains at least one measured value. This could also be a number of measurements.

deviceAddress

The address of the BLE device or client.

seenTime

The time stamp (in Unix time) when the BLE frame from the client was received by the AP.

addressType

The type of BLE address. The following address types are available: `Public` or `Random`.

rssi

The signal strength in dBm of the received BLE frame.

name

The name submitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

advertisingData

The complete advertisement transmitted by the BLE device.

scanResponseData

The complete scan response transmitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

13.17.19.2 Thrift API

LBS server address

Enter the address of the LBS server.

LBS server port

Enter the port used by the LBS server.

Description

Enter a description of the device.

Floor

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Height

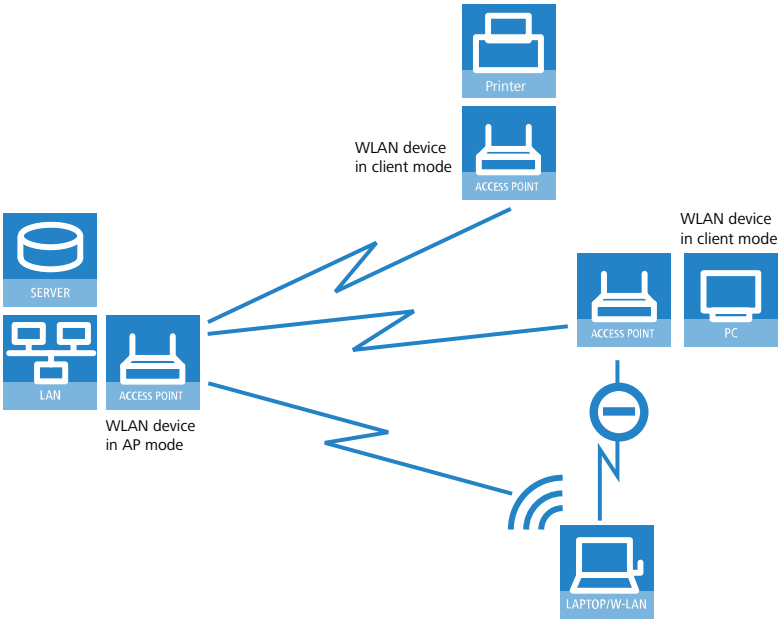
Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Coordinates

Coordinates of the location of the device. These are specified as geographic coordinates for **latitude** and **longitude**.

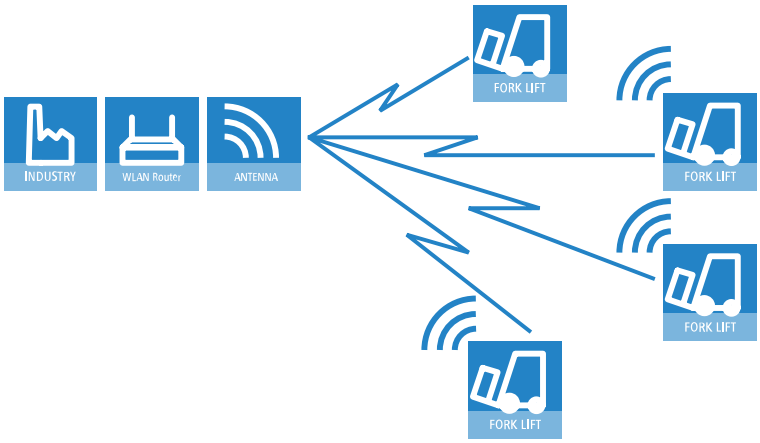
13.18 Configuring the client mode

To connect individual devices with an Ethernet interface into a wireless LAN, LANCOM devices with a WLAN module can be switched to "client mode", whereupon they act as conventional wireless LAN adapters and not as access points (AP). The use of client mode therefore allows devices fitted with only an Ethernet interface, such as PCs and printers, to be integrated into a wireless LAN.



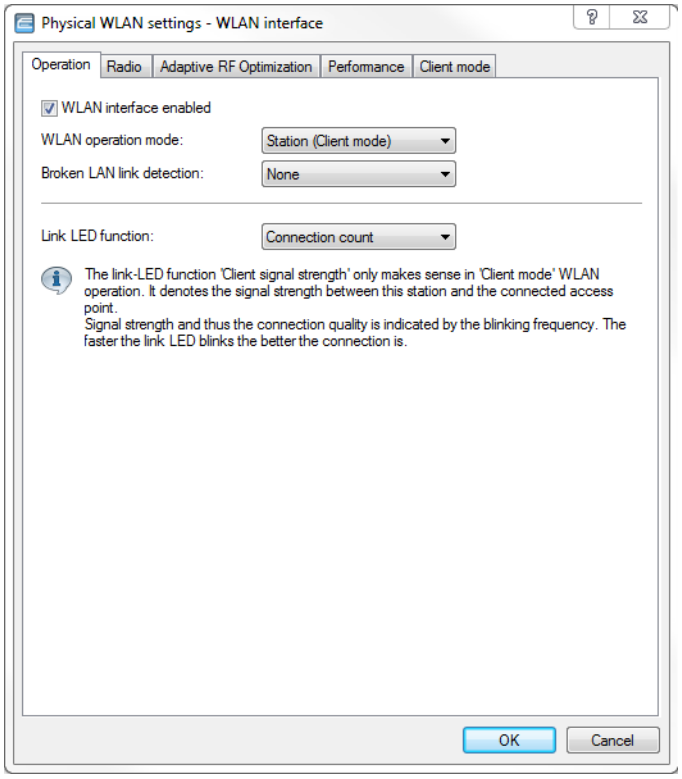
Multiple WLAN clients can register with a WLAN device in AP mode, which is not the case for a WLAN device in client mode.

In industrial applications mobile WLAN clients can also be deployed, such as on a forklift truck, which then has permanent contact to the controller over the wireless connection.



13.18.1 Enabling client mode with LANconfig

To switch your device to client mode using LANconfig, navigate to the view **Wireless LAN** > **General** > **Physical WLAN settings** and, on the **Operation** tab, set the WLAN operation mode to **Client**. Confirm your selection by clicking the **OK** button.



13.18.2 Client settings

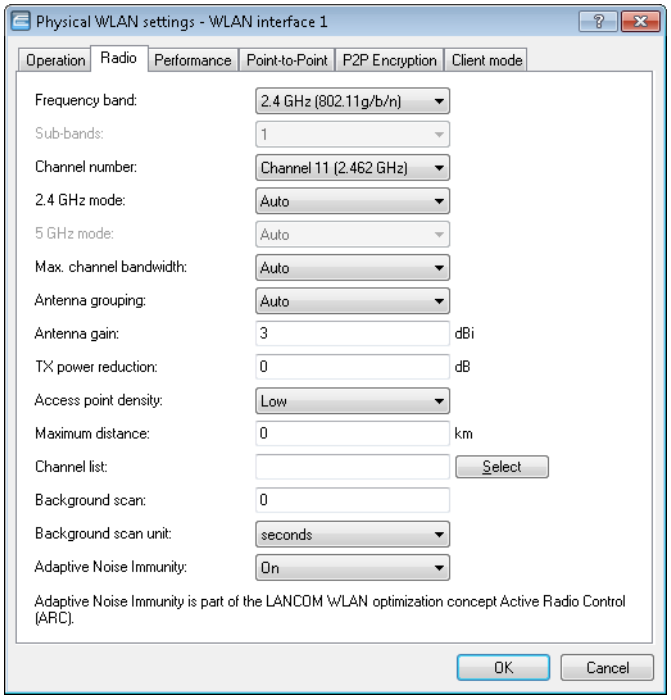
For LANCOM APs and LANCOM wireless routers in client mode, further settings relating to client behavior can be configured from the 'Client mode' tab under the settings for the physical interfaces (**Wireless LAN** > **General** > **Physical WLAN settings**). See *Client mode* on page 1021.

The configuration of the client settings can also be carried out with the WLAN Wizards in LANconfig.

13.18.3 Radio settings

For the WLAN client to connect to an AP, it needs to use suitable frequency bands/channels.

1. To edit the radio settings in LANconfig, go to the 'Radio' tab under the physical WLAN settings for the desired WLAN interface.



2. Set the frequency band, the channels and the 2.4 GHz/5 GHz mode to match the settings of the AP.

Selection of the frequency band and channels is not necessary on some models, such as those devices which support only one frequency band.

13.18.3.1 Greenfield mode for access points with IEEE 802.11n

For access points that comply with the IEEE 802.11n standard, the physical WLAN settings provide the option to allow or restrict data transmission according to the IEEE 802.11n standard.

Along with the selection of the individual a/b/g/n standards and a selection of mixed operating modes, the access points provide the option of using the Greenfield mode. Once activated in the physical WLAN settings for a WLAN interface, the Greenfield mode only allows WLAN clients that support the IEEE 802.11n standard to associate with the corresponding logical WLANs (SSIDs). Other WLAN clients that only work with the standards IEEE 802.11a/b/g cannot associate with these WLANs.

The IEEE 802.11n standard only allows connections that are either encrypted with WPA2/AES or unencrypted. WEP- and TKIP-based encryptions are not allowed in IEEE 802 11n. Please be aware of the following restrictions depending on the actual physical and logical WLAN settings:

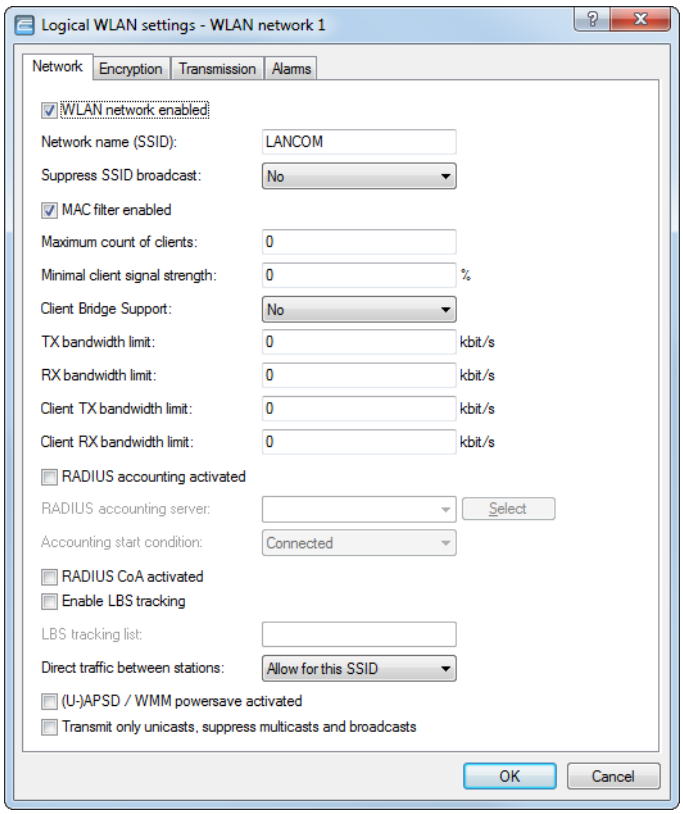
- If, in the Physical settings, you activate support of a mixed-mode which includes the IEEE 802.11n standard and individual WLAN clients on a logical network only support WEP encryption, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with WEP.

- If, in the Encryption settings for a logical WLAN network, you enable not only AES session keys but also TKIP session keys, then the access point will use only the AES session key for this WLAN, because TKIP is not supported by IEEE 802.11n.
- If, in the Encryption settings for a logical WLAN network, you enable only TKIP session keys, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with TKIP.

13.18.4 Setting the SSID of the available network

The SSID of the network to which the client stations are to connect must be entered into the WLAN clients.

1. To enter the SSIDs in LANconfig, navigate to **Wireless LAN** > **General**. After clicking on **Logical WLAN settings**, select the **first** WLAN interface.

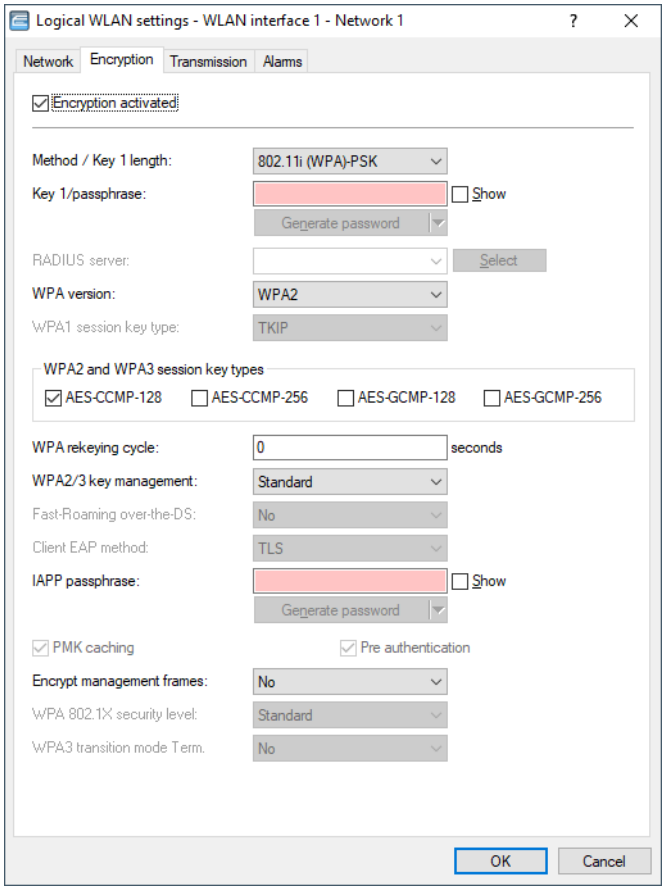


2. On the **Network** tab, enable the WLAN network and enter the SSID of the network the client station should log onto.

13.18.5 Encryption settings

For access to a WLAN, the appropriate encryption methods and key must be set in the client station.

1. To enter the key, in LANconfig navigate to **Wireless LAN** > **General** > **Logical WLAN settings** > **Encryption**.



2. Enable encryption and match the encryption method to the settings for the AP.
3. In WLAN client operating mode, LANCOM APs and LANCOM wireless routers can use EAP/802.1X to authenticate themselves at another AP. For this, select the desired client EAP method here. Note that the selected client EAP method must match the settings of the AP that the device is attempting to log onto.

Depending on the EAP method, the appropriate certificates must be stored in the device:

- For TTLS and PEAP this means the EAP/TLS root certificate only; the key is entered as a combination username:password.
- TLS additionally requires the EAP/TLS device certificate together with the private key.

When working with WPA or 802.1X, settings may need to be made in the RADIUS server.

13.18.6 PMK caching in the WLAN client mode

When establishing a connection from a WLAN client to an access point operating with 802.1x-authentication, the two stations negotiate a shared key, known as the Pairwise Master Key (PMK), for the subsequent encryption. In applications with mobile WLAN clients (laptops in large offices, moving objects with WLAN connections in the industrial sector), the WLAN clients often change the access points via which they are logged in to the WLAN network. And although WLAN clients roam back and forth between different access points, in most cases these tend to be the same ones.

Access points typically save a negotiated PMK for a certain period of time. WLAN devices in WLAN client mode also store PMKs. As soon as a WLAN client starts a login procedure for which a connection already existed, the WLAN client can directly transfer the existing PMK to the access point. In this way, the two remote stations skip the PMK negotiation phase while establishing the connection, and the WLAN client and access point establish the connection much faster.

13.18.7 Pre-authentication in WLAN-client mode

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the access point previously. The WLAN client uses pre-authentication to reduce the time to logon to the access point at the first logon attempt.

Usually, a WLAN client carries out a background scan of the environment to find existing access points that it could connect to. Access points that support WPA2/802.1x can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1x authentication as follows:

- The WLAN client logs on to the new access point via the infrastructure network, which interconnects the access points. This can be an Ethernet connection or a WDS link (wireless distribution system), or a combination of both connection types.
- A pre-authentication is distinguished from a normal 802.1x authentication by the differing Ethernet protocol (EtherType). This allows the current access point and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new access point and the WLAN client.

  The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.

- When the client wants to connect to the new access point, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the *PMK caching*.

On the client side, the number of concurrent pre-authentications is limited to four. This minimizes the network load on the central RADIUS server in network environments with large numbers of access points.

13.18.8 Multiple WLAN profiles in client mode

13.18.8.1 Introduction

In order for individual devices equipped with an Ethernet interface to be connected to a wireless LAN, APs can be switched to client mode, in which they act as conventional wireless LAN clients and not as APs.

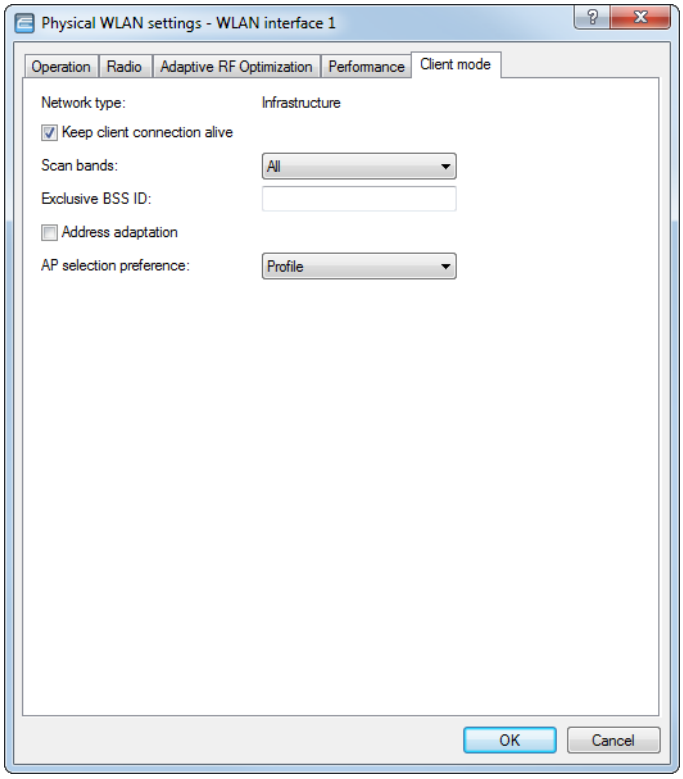
WLAN clients such as notebooks are generally able to save and manage various profiles which allow different APs to be selected depending on the environment (e.g. for a company WLAN or for another WLAN at home). These profiles store various information such as the WLAN SSID and the associated key. The WLAN client automatically selects the profile fitting to the strongest available or preferred WLAN.

LANCOM APs can store up to 16 different WLAN profiles for use in client mode. The profile in client mode activates the networking and transmission parameters, and also the encryption settings for the logical WLAN.

Please observe that a WLAN module in client mode only connects to one AP at a time, even if multiple WLAN profiles have been defined.

13.18.8.2 Configuration

Not only can networking, transmission and encryption parameters be defined separately for each WLAN module, but also which criteria are to be used to select the client profile.



LANconfig: **Wireless LAN** > **General** > **Physical WLAN settings** > **Client mode**

Command line: **Setup** > **Interfaces** > **WLAN** > **Client-Modes** > **WLAN-1**

AP selection preference

Here you select how this interface is to be used.

Possible values:

Signal strength

Selects the profile for the WLAN offering the strongest signal. This setting causes the WLAN module in client mode to automatically switch to a different WLAN as soon as it offers a stronger signal.

Profile

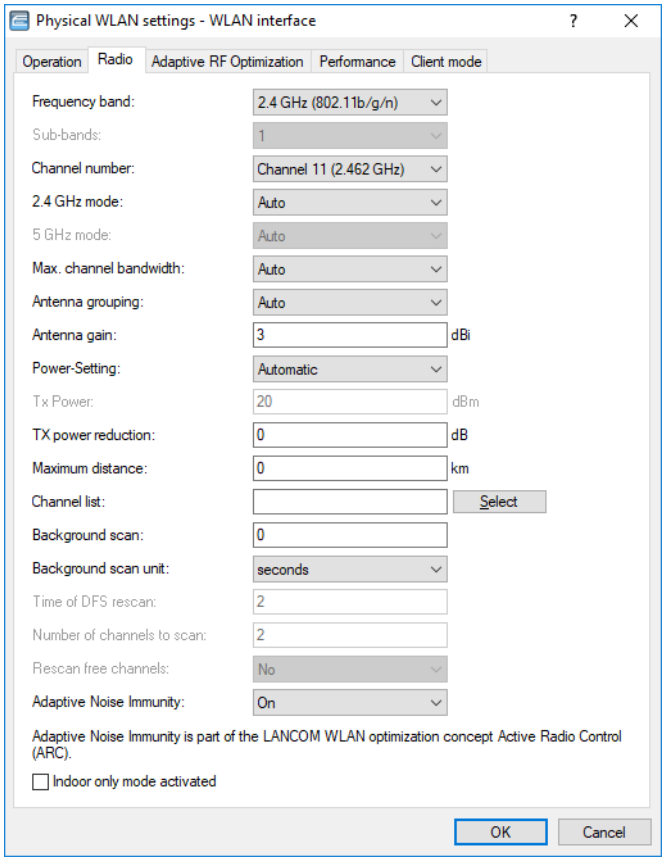
Selects the profile for available WLANs in the order that they have been defined (WLAN index, e.g. WLAN-1, WLAN-2, etc.), even if another WLAN offers a stronger signal. In this setting, the WLAN module in client mode automatically switches to a different WLAN as soon as a WLAN with a lower WLAN index is detected (irrespective of signal strengths).

13.18.9 Roaming

Roaming is defined as the transfer of a WLAN client to another AP once the connection to the access point used so far can no longer be kept alive. To allow roaming, at least one additional AP must be within range of the client, it must provide a network with an identical SSID and matching radio and encryption settings.

Under normal circumstances the WLAN client would only log onto another AP if the connection to the AP used until to that point was lost completely (hard roaming). Soft roaming on the other hand enables the client to use scan information to roam to the strongest AP. With the background scanning function, the device in client mode can gather information on other available APs prior to the connection being lost. In this case the client is not switched to another AP once the existing connection has been lost completely, but rather when another AP within its range has a stronger signal.

1. To enable soft roaming, navigate to **Wireless LAN** > **General** > **Extended settings** > **Expert WLAN settings** > **Roaming** and enable soft roaming for the selected interface. If necessary, enter settings for the other parameters such as the threshold values and signal levels.
2. To configure background scanning in LANconfig, go to the 'Radio' tab under the physical WLAN settings for the relevant WLAN interface.



3. Enter the background scan interval as the time in which the device regularly searches the currently unused frequencies of the active band for available APs. To achieve fast roaming the scan time is set, for example, to 260 seconds (2.4 GHz) or 720 seconds (5 GHz).

13.18.9.1 ARF network for IAPP

APs use the IAPP protocol to communicate and pass information about the handovers of associated WLAN clients which are roaming. APs regularly send out multicast announcements to inform the devices about the BSSIDs and IP addresses of the other APs. A roaming WLAN client informs a new AP about its former AP. The AP uses the information supplied by the IAPP protocol to inform the former AP to remove the WLAN client from its list of associated clients.

Where an AP supports multiple ARF networks, the IAPP announcements are transmitted on all ARF networks. To limit these multicasts to one particular ARF network, it is possible to define an IAPP IP network.

Command line: **Setup** > **WLAN**

› **IAPP-IP-Network**

Here you select the ARF network which is to be used as the IAPP-IP network.

Possible values:

- Selection from the list of ARF networks defined in the device; max. 16 alphanumerical characters

Default:

- Blank

Special values:

- Blank: If no IAPP-IP network is defined, IAPP announcements are transmitted on all of the defined ARF networks.

14 WLAN management

14.1 Initial situation

The widespread use of wireless access points (APs) and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations.

Yet in spite of the numerous advantages WLAN infrastructures offer, there are still a number of unsettled issues:

- All APs must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the APs, especially for larger WLAN infrastructures with the appropriate security mechanisms, requires advanced qualifications and experience on the part of those responsible, and it ties up considerable resources in the IT departments.
- The manual customization of the configurations in the APs when changes are made to the WLAN infrastructure can be time-consuming, with the result that different configurations can be present in the WLAN at the same time.
- Combined utilization of the shared communications medium (air) requires effective coordination of the APs to avoid frequency interference and optimize network performance.
- In public places, APs are a potential security risk because the devices themselves, including the security-related data in them such as passwords, etc., are susceptible to theft. In addition, rogue APs may be able to connect to the LAN unnoticed, bypassing the security policies that are in place.

14.2 Technical concepts

Centralized WLAN management is the solution to these problems. The configuration of the AP is then no longer carried out in the devices themselves but by a central authority instead, the WLAN controller (WLC). The WLC authenticates the APs and transmits the correct configuration to the approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the APs simultaneously. Optionally the configuration provided by the WLC is not stored in the AP's flash memory but in RAM, so security-related data cannot fall into the hands of unauthorized persons in the event that devices are stolen. Only in "standalone" operation is the configuration optionally saved for a defined period to flash memory (in an area that cannot be read out with LANconfig or other tools).

14.2.1 WLC features in the LANCOM vRouter

As of LCOS 10.30 the LANCOM vRouter additionally supports the functions of a WLAN controller. You decide which role your LANCOM vRouter should play: VPN gateway or WLAN controller. The LANCOM vRouter now supports the role of a virtual WLC (vWLC), which means it is capable of managing access points. This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the vRouter license category. All vRouter licenses issued after the release of LCOS 10.30 include a vWLC option.

Product	VPN licenses	AP licenses
vRouter 50	10	10
vRouter 250	50	50
vRouter 500	100	100
vRouter 1000	200	200

Product	VPN licenses	AP licenses
vRouter unlimited	1000	1000

LANCOM Systems GmbH recommends running a vRouter instance either primarily as a VPN gateway/router or as a WLAN controller. The recommended usage may also be split: For example, at the license level “vRouter 1000” (200 VPN licenses and 200 AP licenses):

- 100 concurrent VPN connections and 100 managed APs or
- 150 concurrent VPN connections and 50 managed APs.

14.2.2 The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless Access Points) introduced by the IETF (Internet Engineering Task Force) is a standard for the centralized management of large WLAN infrastructures.

CAPWAP uses two channels for data transfer:

- Control channel, encrypted with Datagram Transport Layer Security (DTLS). This channel is used to exchange administration information between the WLC and the AP.

  DTLS is an encryption protocol is based on TLS but, in contrast to TLS itself, it can be used for transfers over connectionless, unsecured transport protocols such as UDP. DTLS therefore combines the advantages of the high security provided by TLS with the fast transfer via UDP. This also makes DTLS suitable for the transfer of VoIP packets (unlike TLS) because, even after the loss of a packet, the subsequent packets can be authenticated again.
- The payload data from the WLAN is transferred through this data channel from the AP via the WLC into the LAN—encapsulated in the CAPWAP protocol.

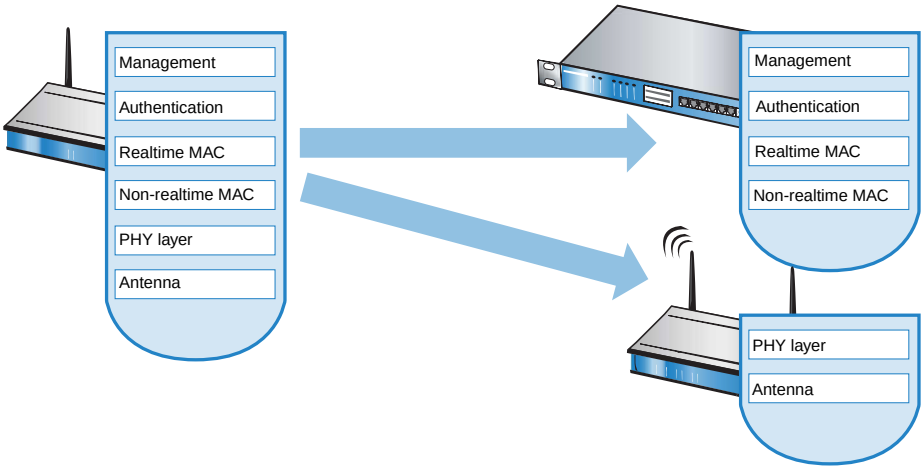
14.2.3 Smart controller technology

In a decentralized WLAN structure with stand-alone APs (operating as so-called "rich access points") all functions for data transfer take place in the PHY layer, the control functions in the MAC layer, and the management functions are integrated in the APs. Centralized WLAN management divides these tasks among two different devices:

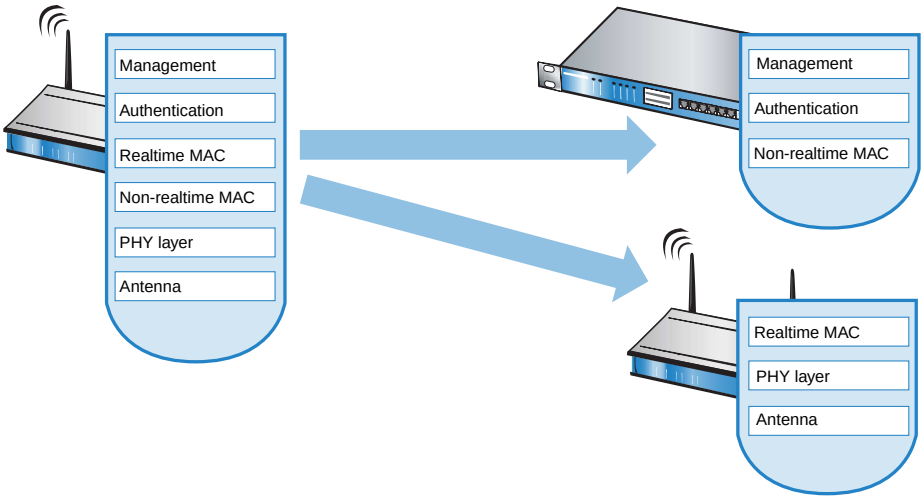
- The central WLC assumes the administration tasks.
- The decentralized APs handle the data transfer at the PHY layer and the MAC features.
- A RADIUS or EAP server can be added as a third component RADIUS or for authentication of WLAN clients (which can also be the case in stand-alone WLANs).

CAPWAP describes three different scenarios for the relocation of WLAN functions to the central WLC.

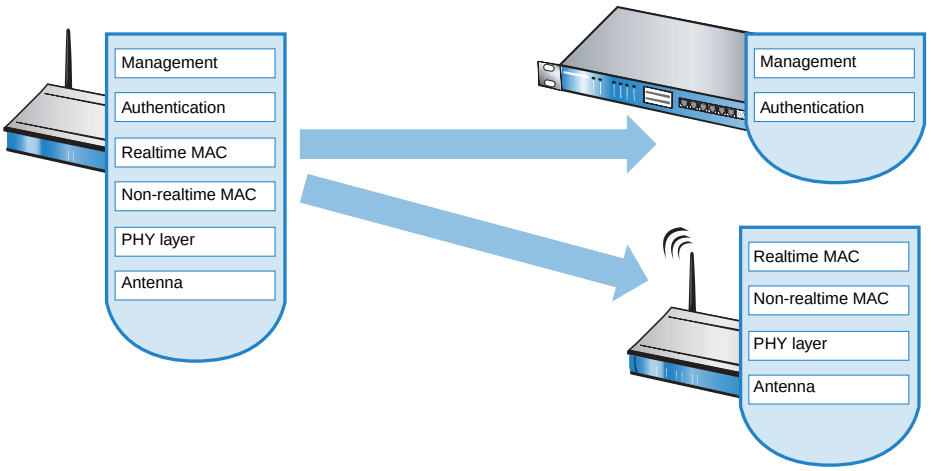
- Remote MAC: In this case, all of the WLAN functions are transferred from the AP to the WLC. Here, the APs only serve as "extended antennas" without independent intelligence



- Split MAC: With this variant, only a portion of the WLAN functions are transferred to the WLC. Normally, realtime applications will continue to be processed in the AP; the non-realtime applications are processed via the central WLC.



- Local MAC: The third possibility provides for complete management and monitoring of the WLAN data traffic directly in the APs. The only information exchanged between the AP and the WLC is for network management and ensures that the APs have a uniform configuration.



Smart Controller Technology from LANCOM uses the local MAC procedure. Thanks to the reduction of centralized tasks, these WLAN infrastructures offer optimum scalability. At the same time, infrastructure of this type prevents the WLC from becoming a central bottleneck that has to process large portions of the overall data traffic. In remote MAC and split MAC architectures, all payload data is forced to run centrally via the WLC. In local MAC architectures the data can alternatively be broken out from the APs directly to the LAN to provide high-performance data transfer. With break-out into the LAN, data can also be directly routed into special VLANs. This makes it very easy to set up closed networks, such as for guest access accounts.

Layer 3 tunneling and layer 3 roaming

WLCs with LCOS also support the transfer of payload data through a CAPWAP tunnel. This allows selected applications such as VoIP to be routed via the central WLC, for example. If WLAN clients change to a different radio cell, the underlying IP connection will not be interrupted because it continues to be managed by the central WLC (layer-3 roaming). In this way, mobile SIP telephones can easily roam between Ethernet subnets, even during a call.

Managing data streams centrally can also make configuring VLANs at the switch ports unnecessary in environments with numerous VLANs because all CAPWAP tunnels are centrally managed on the WLC.

14.2.4 Communication between access point and WLAN controller

Communication between an AP and the WLC is always initiated by the AP. In the following cases, the devices search for a WLC that can assign a configuration to them:

- When shipped, the WLAN modules in LANCOM APs are set to the 'Managed' operating mode. In this mode, APs search for a central WLC that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLC or until the operating mode of the WLAN module is changed manually.
- While the AP searches for a WLC, its WLAN module is switched off.
- Ex-factory, the WLAN modules in LANCOM wireless routers are set to the 'access point' operating mode. In this mode, wireless routers function as standalone access points with a configuration that is stored locally in the device. For integration into a WLAN infrastructure that is centrally managed by WLAN controllers, the operating mode of the WLAN modules in wireless routers has to be switched into the 'managed' mode.

Communication between the access point and the WLAN-Controller takes place via **CAPWAP** as well as via **SCEP**. For **CAPWAP** the **UDP port 1027** is used in the default configuration (can be changed in the WLAN-Controller configuration). For the communication via **SCEP** the protocol **HTTP** (**TCP port 80**) is used.

The AP sends a "discovery request message" at the beginning of communication to find the available WLCs. This request is sent as a broadcast. However, because in some structures a potential WLC cannot be reached by a broadcast, special addresses from additional WLCs can also be entered into the configuration of the APs.

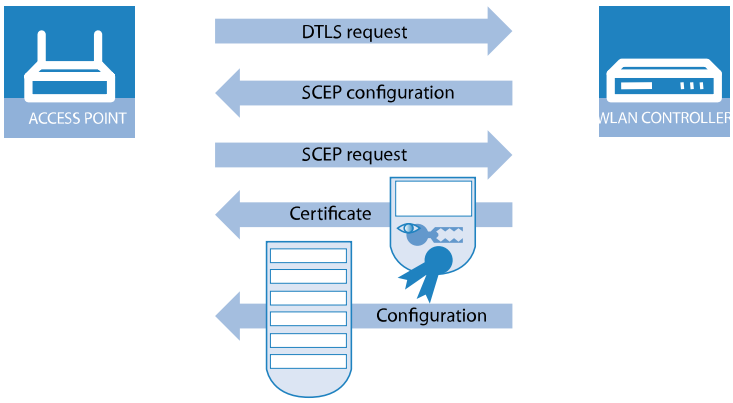
The DNS names of WLCs can also be resolved. All APs with LCOS 7.22 or higher have the default name 'WLC-Address' preconfigured so that a DNS server can resolve this name to a WLC. The same applies to the DHCP suffixes learned via DHCP. This also makes it possible to reach WLCs that are not located in the same network, without having to configure the APs.

From the available WLCs, the AP selects the best one and requests it to establish the DTLS connection. The "best" WC for the AP is the one with the least load, i.e. the lowest ratio of managed APs compared to the maximum possible number of APs. In case of two or more equally "good" WLCs, the AP selects the nearest one in the network, i.e. that with the fastest response time.

The WLC then uses an internal random number to determine a unique and secure session key, which it uses to secure the connection to the AP. The CA in the WLC issues a certificate to the AP by means of SCEP. The certificate is protected by a one-time-only "challenge" (password). The AP uses this certificate for authentication at the WLC to collect the certificate.

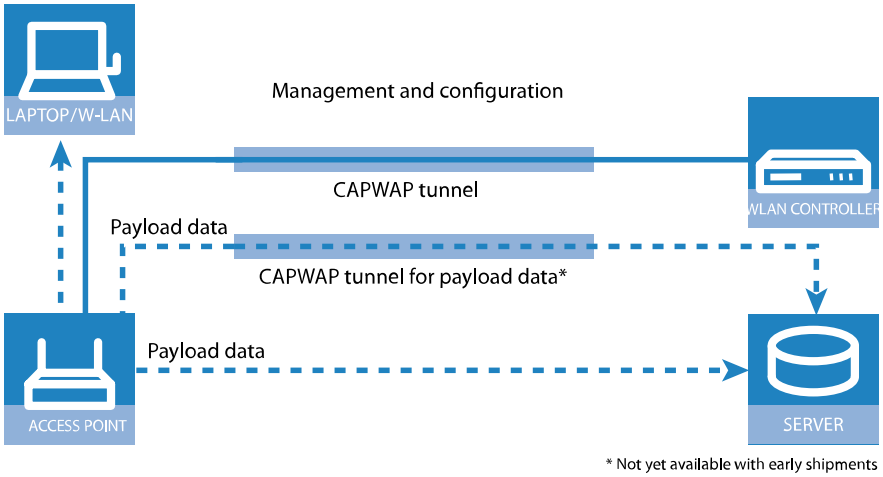
The AP is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the AP uses the SCEP to retrieve its certificate from the SCEP CA. Once this is done, the assigned configuration is transferred to the AP.

SCEP stands for Simple Certificate Encryption Protocol, CA for Certification Authority.



Authentication and configuration can both be carried out either automatically or only with a corresponding entry of the AP's MAC address in the AP table of the WLC. If the AP's WLAN modules were deactivated at the beginning of the DTLS communication, these will be activated after successful transfer of the certificate and configuration (provided they are not explicitly deactivated in the configuration).

The management and configuration data will then be transferred via the CAPWAP tunnel. The payload data from the WLAN client is then released in the AP directly into the LAN and transferred, for example, to the server.



14.2.5 Zero-touch management

With their ability to automatically assign a certificate and configurations to the requesting APs, WLCs implement true "zero-touch management". Simply connect new APs to the LAN—no further configuration is necessary. This simplification to only having to install devices reduces the workload for IT departments, especially in decentralized structures, because no special IT or WLAN expertise is required for the setup at the remote locations.

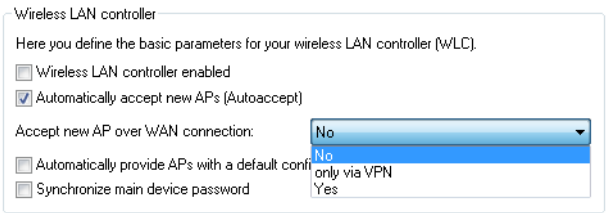
14.2.6 Split management

APs are able to search for their WLC in remote networks—a simple IP connection, such as via a VPN path, is all you need. As the WLCs only influence the WLAN part of the configuration in the AP, all other functions can be managed separately. This division of the configuration tasks makes WLCs ideal for establishing a company-wide WLAN infrastructure that is based at the headquarters and includes all of the branch and home offices connected to it.

14.2.7 Protection against unauthorized CAPWAP access from the WAN

The WLC or LANCOM router with activated WLC option handles CAPWAP requests from the LAN and the WAN in the same way. In the case of requests from WAN remote stations, it accepts the APs into its AP management and, under certain circumstances, it sends a default configuration. If configured appropriately, the CAPWAP service is no longer available to WAN remote stations, meaning that for WAN remote stations, APs are no longer accepted and configurations are not provisioned.

The configuration is done under **WLAN Controller** > **General** in the section **Wireless LAN controller**. If the automatic acceptance of new APs is enabled, you can use the feature **Accept new AP over WAN connection** to control whether the CAPWAP service is available to WAN remote stations.



No

The device accepts no new APs over the WAN connection.

Only via VPN

The device only accepts new APs if the WAN connection is via VPN.

Yes

The device accepts all new APs over the WAN connection.

14.3 Basic configuration of the WLAN controller function

To get started, a WLC requires the following two pieces of information to carry out the mainly automated configuration of the APs:

- Current time information (data and time) for checking the validity of the necessary certificates.
- A WLAN profile that the WLC can assign to the APs.

Further optional examples for configuration include setting up redundant WLC, the manual disconnection and connection of APs, and backing up any necessary certificates.

By default the WLC listens for connections on the UDP port 1027 (configurable). The certificates are distributed by SCEP, which uses the TCP port 80 (HTTP).

14.3.1 Setting the time information for the WLAN controller

The management of APs in a WLAN infrastructure is based upon the automatic distribution of certificates via the Simple Certificate Enrollment Protocol (SCEP).

The WLC can only check the temporal validity of these certificates if it is set with the current time. If the time is not set in the WLC, the WLAN LED illuminates in red and the device is not operational.

Routers with the WLC option do not have a WLAN LED.

To set the time in the device start LANconfig, click on the entry for the WLC with the right-hand mouse key and select **Set date/time** from the context menu. Alternatively in WEBconfig you can click on **Extras** and then **Set date and time**.

Alternatively, WLCs can automatically retrieve the current time from a time server by means of the Network Time Protocol (NTP). Information on NTP and its configuration can be found in the LCOS reference manual.

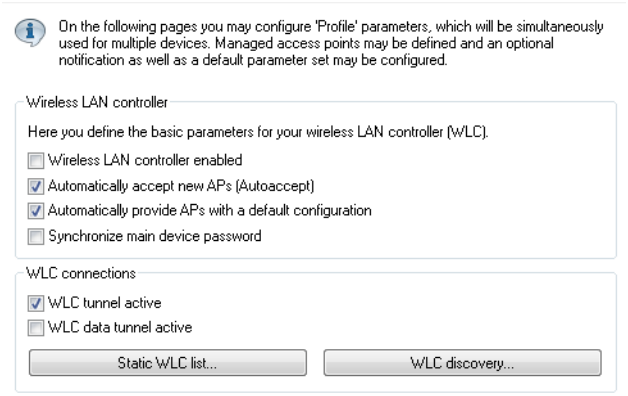
As soon as the WLC has valid time information it begins with the generation of the certificates (root and device certificate) and it determines a random number. Once the necessary certificates have been generated, the WLC indicates that it is operational and the WLAN LED blinks red.

Once operational, you should make a backup copy of the certificates (*Backing up the certificates*)

14.3.2 Example: Default configuration

1. Open up the configuration of the WLC by double-clicking on its entry in LANconfig.

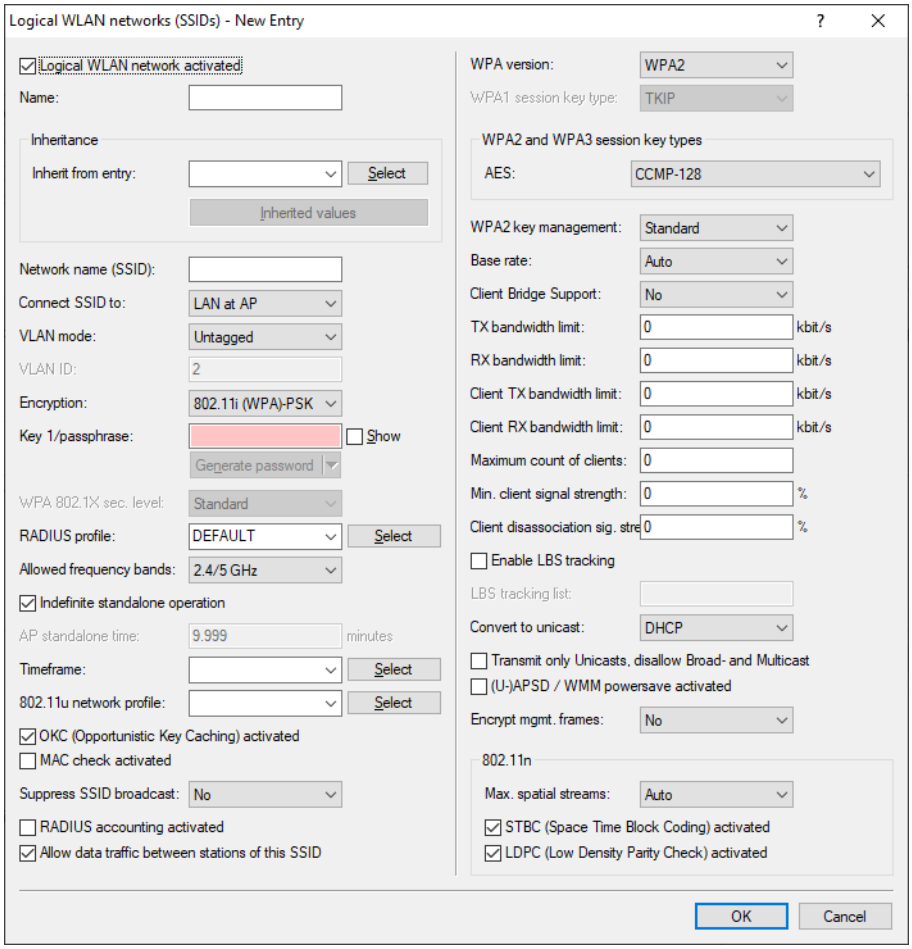
2. Activate the options for the automatic acceptance of new APs and the provision of a default configuration under **WLAN controller** > **General**.



- **Automatically accept new APs (Auto-accept)** Enables the WLC to provide a certificate to all new APs without a valid certificate. To this end, either a configuration for the AP has to be entered into the AP table, or 'Automatically provide APs with a default configuration' has to be activated.
- **Automatically provide APs with a default configuration**: This enables the WLC to assign a default configuration to any new AP, even if no explicit configuration has been stored for it.

By combining these two options, the WLC can automatically integrate any managed-mode AP found in the LAN into its WLAN infrastructure. This may, for example, be a temporary measure during the rollout phase of a WLAN installation.

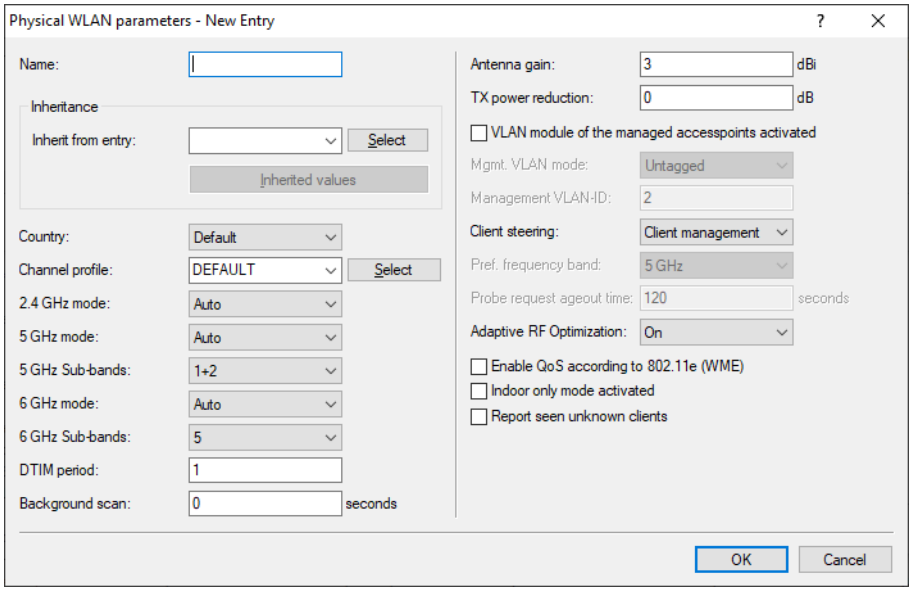
3. On the **Profiles** page, move to the logical WLAN networks. Add a new entry with the following values:



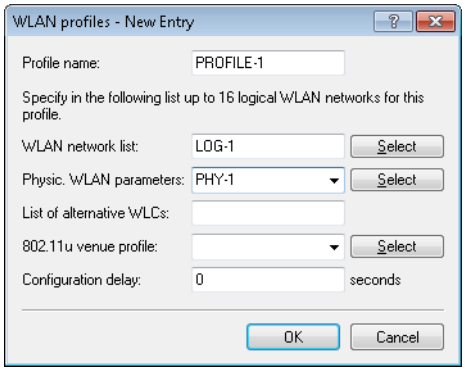
- **Name**: Give the WLAN a name. This name is used only for administrative purposes in the WLC.
- **SSID**: This SSID is used for the WLAN clients to connect.
- **Encryption**: Select the encryption method suitable for the WLAN clients being used, and enter a key or passphrase, as applicable.
- Deactivate the MAC check. Instructions on the use of MAC filter lists in managed WLAN infrastructures can be found under *Checking WLAN clients with RADIUS (MAC filter)*.

4. A new entry also has to be added to the physical WLAN parameters. In most cases involving the default configuration, just entering a name is sufficient. Adjust the other settings to meet your needs, if necessary.

For normal AP applications you should use only the 5-GHz subbands 1 and 2. Subband 3 is for special applications only (e.g. BFWA, Broadband Fixed Wireless Access).

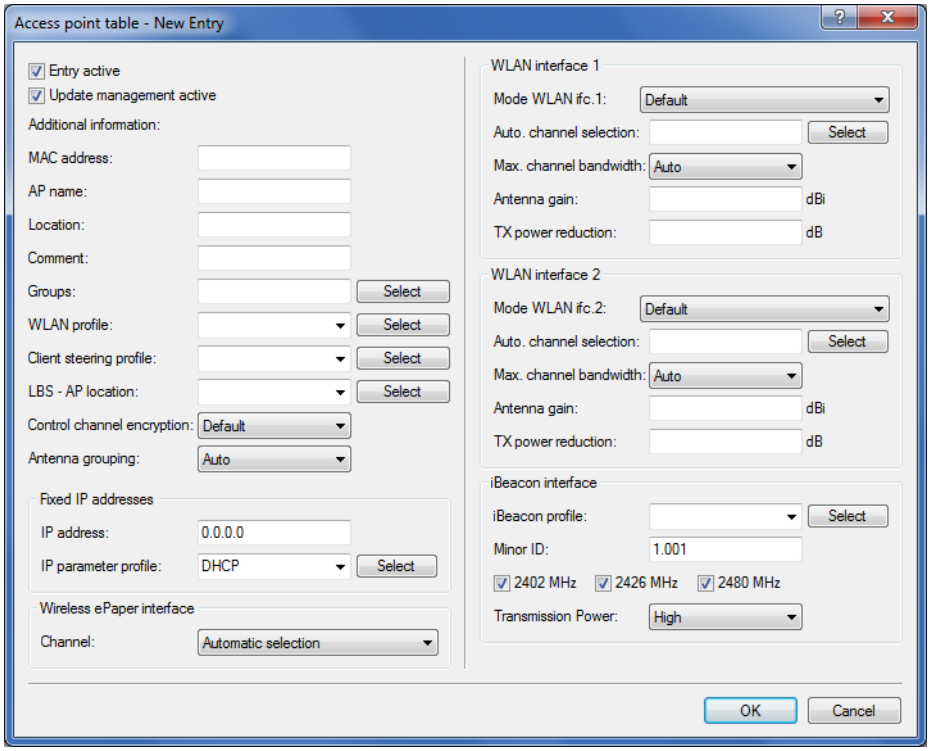


5. Create a new WLAN profile, give it an unique name, and assign the above logical WLAN network and physical WLAN parameters to it.



6. Change to the **AP configuration** view, open the **Access point table** and add a new entry by clicking on the **Default** button. Assign the WLAN profile to it as defined above. Leave **AP name** and **Location** empty.

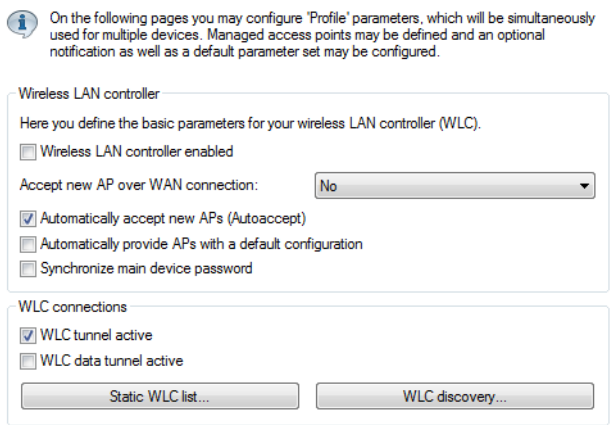
The **MAC address** is set to 'ffffffffffff' for the default configuration and it cannot be edited. This entry is thus a standard for any AP that is not explicitly listed in this table with its MAC address.



14.3.3 Assigning the default configuration to the new access points

With these settings you have defined all of the necessary values for the WLC to provide the APs with the required WLAN parameters. Upon assignment of the configuration, the APs change their status in the WLC management from "New access point" to "Expected access point", and they are listed in the device display under **Exp. APs**. Once the default configuration has been assigned to all new APs, the New APs LED switches off.

After the initial start-up phase, the option **Automatically accept new APs** can be deactivated again so that no further APs are automatically accepted into the network.



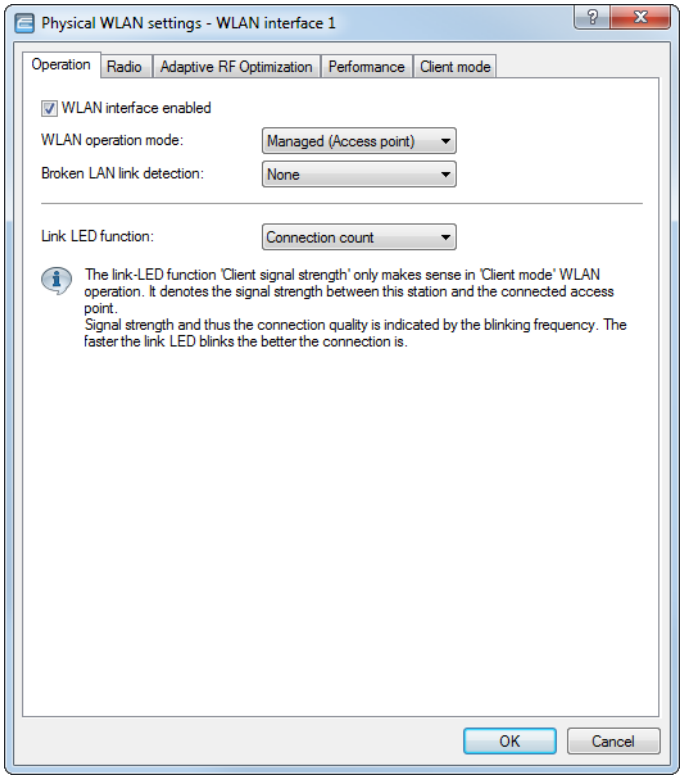
14.3.4 Configuring the access points

LANCOM access points and LANCOM wireless routers differ with regard to the ex-factory default settings in the WLAN modules.

- When shipped, the WLAN modules in APs are set to the 'Managed' operating mode. In this mode, APs search for a central WLC that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLC or until the operating mode of the WLAN module is changed manually.
- Ex-factory, the WLAN modules in wireless routers are set to the 'access point' operating mode. In this mode, wireless routers function as standalone APs with a configuration that is stored locally in the device. For integration into a WLAN infrastructure that is centrally managed by WLCs, the operating mode of the WLAN modules in wireless routers has to be switched into the 'managed' mode.

The operating mode can be set separately for every WLAN module. For models with two WLAN modules, one module can work with a local configuration and the second module can be centrally managed with a WLC.

For individual devices, the operating mode of the WLAN modules can be found in LANconfig under **Wireless LAN** > **General** > **Physical WLAN settings** > **Operation mode**:



If you need to change the operating mode for multiple devices, you can use a simple script on the devices with the following lines:

```
# Script
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

14.4 Configuration

Most of the parameters for configuring the WLAN controller correspond with those of the access points. For this reason, this section does not explicitly describe all of the WLAN parameters, but only those aspects necessary for operating the WLAN controller.

14.4.1 General settings

This area is for the basic settings of your WLC.

- Automatically accept new APs (auto accept)

  Enables the WLC to provide all new APs with a configuration, even those not in possession of a valid certificate.

  Enables the WLC to provide a certificate to all new APs **without** a valid certificate. a valid certificate. One of two conditions must be fulfilled for this:

  - A configuration for the AP is entered into the AP table under its MAC address.
  - The option 'Automatically provide APs with the default configuration' is enabled.

- Automatic provision of the default configuration

  This enables the WLC to assign a default configuration to every new AP (even those **without** a valid certificate), even if no explicit configuration has been stored for it. In combination with auto-accept, the WLC can accept all managed-mode APs which are found in the WLAN infrastructure managed by it (up to the maximum number of APs that can be managed by one WLC). Any APs accepted by default are also entered into the MAC list.

  This option can also lead to the acceptance of unintended APs into the WLAN infrastructure. For this reason this option should only be activated during the start-up phase when setting up a centrally managed WLAN infrastructure.

Combining the settings for auto-accept and default configuration can cater for a variety of different situations for the setup and operation of APs:

Auto accept	Default configuration	Suitable for
On	On	Rollout phase: Use this combination only if you can be sure that **no APs can unintentionally** connect with the LAN and thus be accepted into the WLAN infrastructure.
On	Off	Controlled rollout phase: Use this combination if you have entered all of the approved APs into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.
Off	Off	Normal operation: No new APs will be accepted into the WLAN infrastructure without the administrator's approval.

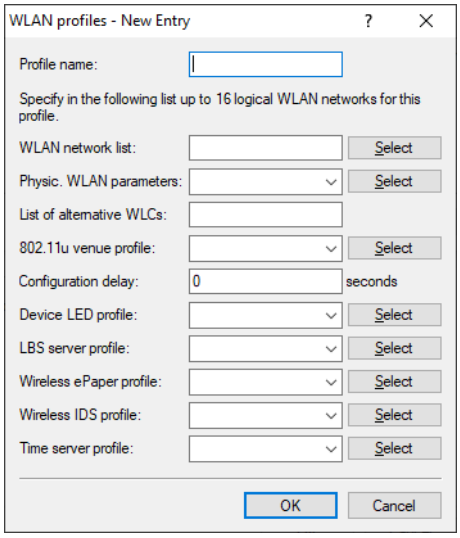
14.4.2 Profiles

The profiles area is used to define the logical WLAN networks, physical WLAN parameters, and the WLAN profiles which combine these two elements.

14.4.2.1 WLAN profiles

The WLAN profiles are collections of the various settings that are to be assigned to the APs. The allocation of WLAN profiles to the APs is set in the AP table.

For each WLAN profile you can specify the following parameters under **WLAN controller** > **Profiles** > **WLAN profiles**:



Profile name

Name of the profile under which the settings are saved.

Log. WLAN network list

List of the logical WLAN networks that are assigned via this profile.

From this list, APs use only the first 16 entries that are compatible with their own hardware. This means that 16 WLAN networks for purely 2.4-GHz operations and 16 for purely 5-GHz operations can be defined in a profile. Consequently, each AP—be it a model offering 2.4 GHz or 5 GHz support—can choose from a maximum of 16 logical WLAN networks.

Physic. WLAN parameters

A set of physical parameters that the AP WLAN modules are supposed to work with.

IP address of alternative WLCs

A list of WLCs that the APs should attempt to connect with. The AP starts searching for a WLC with a broadcast. Defining alternative WLCs is worthwhile when a broadcast cannot reach all WLCs (e.g.if the WLC is located in another network).

802.11u venue profile

Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

Configuration delay

Here you specify a time delay before an AP managed by the WLAN controller activates the configuration transmitted to it.

A rule of thumb for calculating the delay is (regardless of the topology): One second per managed AP, e.g. 200 seconds for 200 APs.

The delay does not apply to transmitted scripts.

Device LED profile

The device LED profile selected here applies to the WLAN profile. To manage the devices LED profiles, see **WLAN controller** > **Profiles** > **Advanced profiles** > **Device LED profiles**.

LBS general profile

The general LBS profile selected here applies to the WLAN profile. You select the general LBS profile under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **LBS - General**.

Wireless ePaper profile

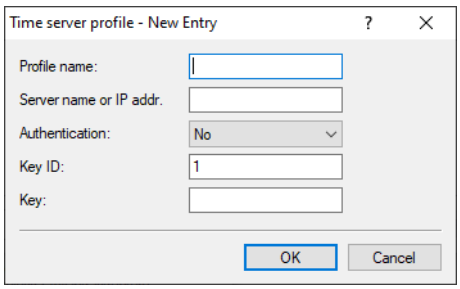
The Wireless ePaper profile selected here applies to the WLAN profile. You manage the Wireless ePaper profiles under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **Wireless ePaper profiles**.

Wireless IDS profile

The Wireless IDS profile selected here applies to the WLAN profile. You manage the Wireless IDS profiles under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **Wireless IDS profiles**.

Time server profile

The Time server profile selected here applies to the WLAN profile. You manage the Time server profiles under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **Time server profiles**.



Profile name

The name of this NTP profile.

Server name or IP addr.

The server name or IP address of the NTP server.

Authentication

Enables or disables MD5 authentication for the server.

Key ID

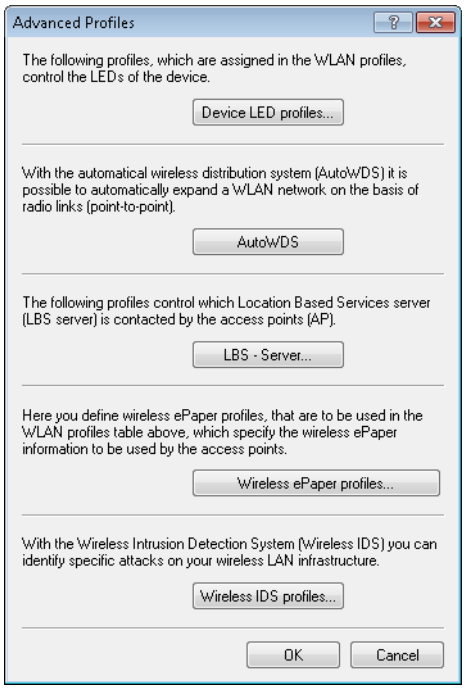
Identifies the key used for MD5 authentication for the server.

Key

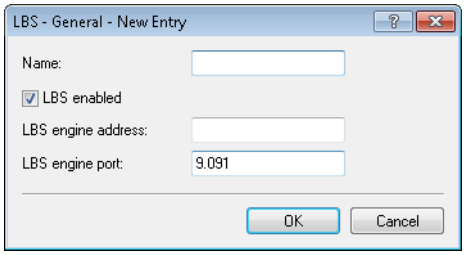
The value of the key for authentication with the NTP server.

14.4.2.2 General LBS profile and device location profile

In order to conveniently manage the settings for location-based services servers (LBS) and the AP locations by means of a WLC, you create the appropriate profiles for LBS servers via the menu **WLAN Controller** > **Profiles** and the button **Advanced profiles**.



The button **LBS - Server** opens the dialog for creating a general LBS server profile.



Name

Enter a descriptive name for the profile.

LBS enabled

Enable or disable LBS.

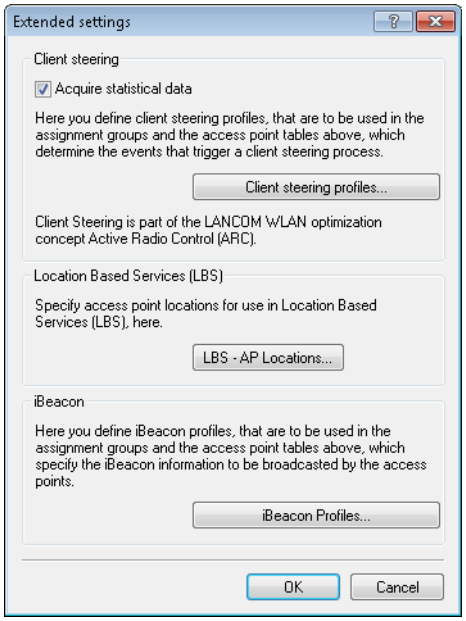
LBS server address

Enter the address of the LBS server.

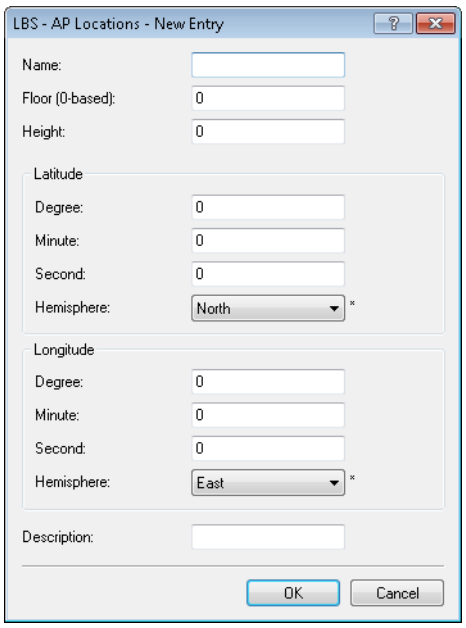
LBS server port

Enter the port used by the LBS server (default: 9091).

You create the corresponding profile for locations of the LBS APs under **WLAN controller** > **AP configuration** with the button **Extended settings**.



The button **LBS - AP locations** opens the dialog for creating a location profile for the LBS APs.



Name

Enter a descriptive name for the profile.

Floor (0-based)

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Degrees (latitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (latitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (latitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (latitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical latitude:

- North: Northerly latitude
- South: Southerly latitude

Degrees (longitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (longitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (longitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (longitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical longitude:

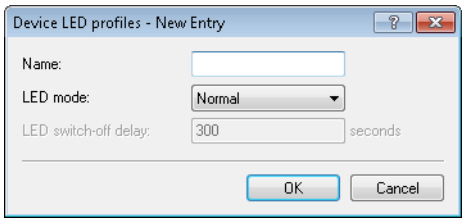
- East: Easterly longitude
- West: Westerly longitude

Description

Enter a description of the device.

14.4.2.3 Device LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile under **WLAN Controller** > **Profiles** > **Device LED profiles** and assign this to a WLAN profile.



Name

Give a name to the device LED profile here.

LED mode

The following options are available:

- **Normal**: The LEDs are always enabled, also after rebooting the device.

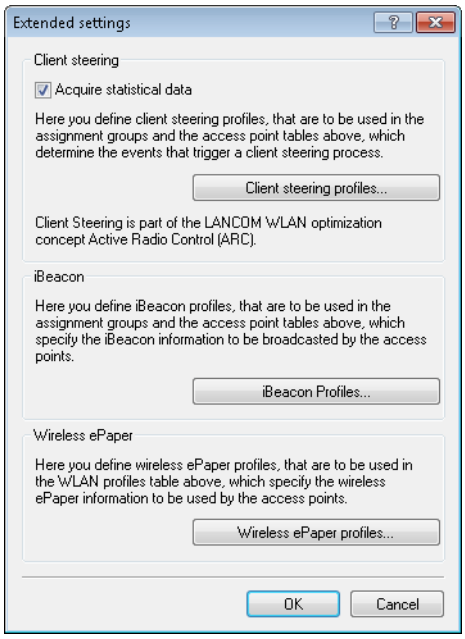
- **Timed off**: After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.
- **All off**: The LEDs are all off. Even after restarting the device, the LEDs remain off.

LED switch-off delay

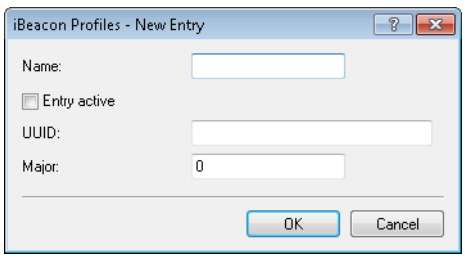
The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

14.4.2.4 ESL- and iBeacon profiles

In order to use a WLC to manage the settings of the Wireless ePaper information and iBeacon information of the individual APs, you create the corresponding profiles for Wireless ePaper and iBeacon via **WLAN-Controller** > **AP-Configuration** with the button **Extended settings**.



The button **iBeacon profiles** is used to create iBeacon profiles for the assignment groups and the AP table, which specify the iBeacon information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

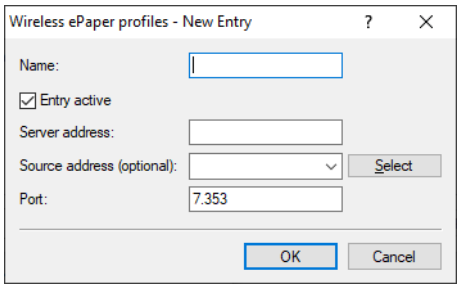
UUID

Unique identification of the transmitter

Major

Specifies the Major value of the iBeacon.

The button **Wireless ePaper profiles** is used to create Wireless ePaper profiles for the WLAN-profiles table, which specify the Wireless ePaper information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

Server address

IP address of the Wireless ePaper Server.

Source address (optional)

Enter loopback address here.

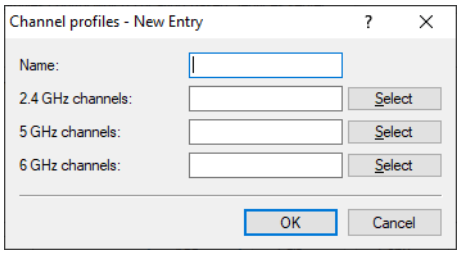
Port

Specifies the port.

14.4.2.5 Channel Profile Table

You create the configuration of the WLAN channels via **WLAN Controller** > **Profiles** > **Advanced Profiles** > **Channel Profiles**. Within the channel profile, the WLAN channels can be defined for each frequency band. In this way, you can also uniquely define channels whose numbering is repeated in different frequency bands (e.g., at 2.4 GHz and 6 GHz). Then link newly created channel profiles within the physical WLAN profile.

The DEFAULT profile activates all allowed channels.



Name

Name of the profile.

2.4 GHz channels

Select the 2.4 GHz channels for this profile.

5 GHz channels

Select the 5 GHz channels for this profile.

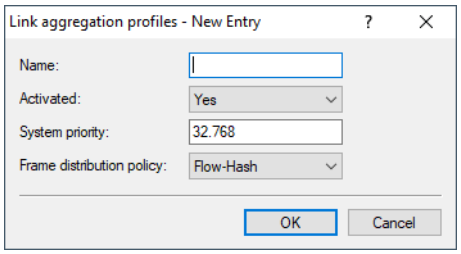
6 GHz channels

Select the 6 GHz channels for this profile.

14.4.2.6 Link Aggregation profiles

LACP according to IEEE 802.1AX allows several Ethernet connections to be bundled in a so-called LAG (Link Aggregation Group) in order to increase the achievable data throughput within the LAG. For this purpose, the outgoing packets on the sending side are distributed to the various individual links within the LAG on the basis of the configured frame distribution policy.

You create the configuration of the link aggregation profiles under **WLAN Controller** > **Profiles** > **Advanced Profiles** > **Link aggregation profiles**.



Name

The name of this LAG (Link Aggregation Group).

Activated

Enables or disables this LAG (Link Aggregation Group).

System priority

The system priority of this LAG (Link Aggregation Group).

Frame distribution policy

Frame distribution policy of this LAG (Link Aggregation Group). Possible options:

Flow-Hash

For outgoing packets, a flow hash is formed over the IP addresses and TCP/UDP ports contained and the packets are distributed to the individual links of the LAG on the basis of this. This achieves a distribution at session level, so that sessions of a single client can also be distributed to multiple links. This setting is recommended for most scenarios.

Source-Dest-MAC

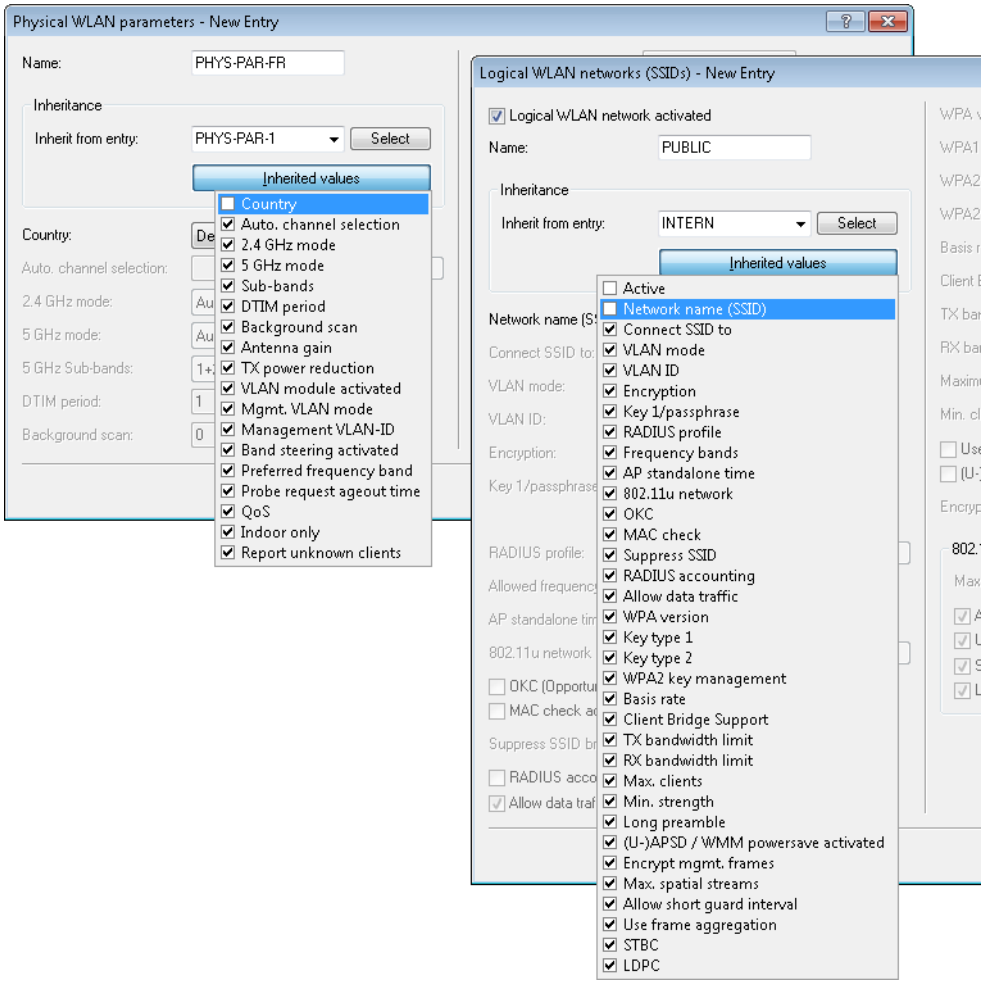
Outgoing packets are distributed to the individual links of the LAG based on the contained pair of source MAC address and destination MAC address.

14.4.2.7 Inheritance of parameters

A WLC is capable of managing a wide range of different APs at different locations. However, WLAN profiles include settings that are not equally suitable for every type of AP that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for countries or device types, it is possible to "inherit" selected properties from the logical WLAN networks and the physical WLAN parameters.

1. You should initially generate the basic settings that are valid for the majority of the managed APs.
2. You can then start to generate entries for the more specific values, e.g. physical settings for a certain country, or a logical WLAN network for public access by mobile clients.



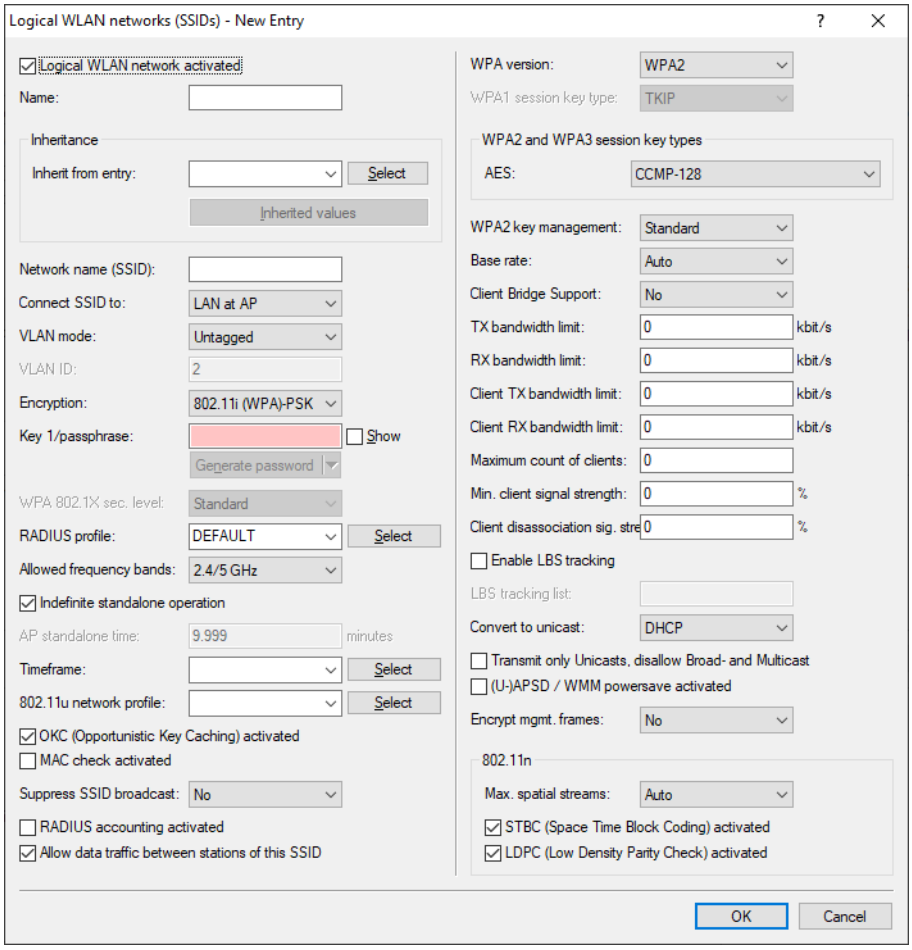
3. Select the entry from which the values are to be inherited and mark the values for inheritance. Parameters inherited in this way are displayed in the configuration dialog in gray and they cannot be edited.
4. Depending on the application, the WLAN settings collected in this way are then grouped into separate profiles, and these are then assigned to their respective access points.

Inheritance fundamentally allows chains over multiple stages (cascading). This means, for example, that country and device-specific parameters can be grouped for convenience.

Recursion is also possible—profile A inherits from profile B, and at the same time B inherits from A. However, the parameters available for inheritance are limited to one "inheritance direction" per parameter.

14.4.2.8 Logical WLAN networks

Under **WLAN Controller** > **Profiles** > **Logical WLAN networks** you set the logical WLAN network parameters that the WLC assigns to the APs. The following parameters can be defined for each logical WLAN network:



Logical WLAN network activated

Enable the logical WLAN network by clicking on this option.

Name

Here, specify a name which uniquely identifies the logical WLAN network.

Inheritance

If you wish to create entries that differ only slightly from existing ones, you can choose a "parent" entry here and select the parameters which are to be applied each time it is used.

A "parent" entry itself can contain inherited entries. Try to ensure that the structure of inherited entries is not too complex, otherwise they may be difficult to understand and configure.

Network name (SSID)

Enter the SSID of the WLAN network here. All stations that belong to this WLAN network must use the same SSID.

SSID connect to

Here you select which of the AP's logical interfaces is to be associated with the SSID, i.e. where the AP sends the data packets for this SSID.

- "LAN": The AP forwards the data packets locally into the LAN (LAN-1) by default. It must be configured appropriately to do this.
- "WLC-Tunnel-x": The SSID is connected to a WLC bridge layer-3 tunnel. The AP sends all data packets to this tunnel and thus to the WLC. This tunnel must be configured on the WLC.
- "L2TP-ETHERNET-x": The SSID is connected to an L2TPv3-Ethernet tunnel. This enables the automatic break-out of WLAN SSIDs through L2TP-Ethernet tunnels. General information on the topic of L2TPv3 is available in the section *Layer-2 tunneling protocol (L2TP)* on page 833. L2TPv3 tunnels are recommended as an alternative to the classic WLC layer-3 tunnel if the latter limits the WLAN throughput. Higher maximum throughputs can be achieved with L2TPv3. Then adjust the usage of the L2TP-ETHERNET-x interface used on the WLC, e.g. for further use on the IP router or LAN bridge.

  Both the WLC and the managed access points must support LCOS 10.50 or higher.

Note that although forwarding all data packets to the WLC allows you to define routes and filters centrally, this creates a heavy load on the WLC. This model demands a correspondingly high bandwidth in order to transfer all of the data traffic of this and any other SSIDs that are connected to this WLC via WLC tunnel.

VLAN mode

This item sets the AP VLAN mode for packets belonging to this WLAN network (SSID). VLAN IDs are used if the VLAN module is enabled in the physical WLAN parameters of the AP. Otherwise the AP ignores all VLAN settings in the logical networks. Even with VLAN activated, it is possible to operate the network untagged.

- "Untagged": The AP does not tag data packets from this SSID with a VLAN ID.

  Even with VLAN activated, it is possible to operate a WLAN network untagged. The VLAN ID '1' is reserved internally for this.
- "Tagged": The AP marks the data packets with the VLAN ID specified as follows.

VLAN-ID

VLAN ID for this logical WLAN network

Please note that to use VLAN IDs in a logical WLAN network, you must set up a management VLAN ID (see physical WLAN parameters).

Encryption

This item sets the encryption method or, in the case of WEP, the key length for packet encryption in this WLAN.

Key 1 / passphrase

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "0x". The following character string lengths result for the formats used:

- WPA-PSK: 8 to 63 ASCII characters
- WEP128 (104 bit): 13 ASCII or 26 hex characters
- WEP64 (40 bit): 5 ASCII or 10 hex characters

RADIUS profile

Specify which RADIUS profile the AP should receive for this network, so that it can connect directly to the RADIUS server if necessary. Leave this field blank if the WLC is to handle RADIUS requests.

You configure the RADIUS profiles in the corresponding table.

Allowed frequency bands

Here you set the frequency band used by network participants for transmitting data on the wireless network. You can select the 2.4-GHz band, the 5-GHz band, or both bands. In addition, the 6 GHz band is available.

Indefinite standalone operation

If the standalone operation for the WLC is configured so that the WLAN networks are broadcast indefinitely (value: 9999), this applies to networks with local break-out on the LAN as well as to networks connected via WLC tunnel. If the WLC fails, both types of network will continue to be broadcast: However, this only makes sense for local break-out networks on the LAN, since networks connected via the WLC tunnel have lost their end point (the WLC) and are therefore out of operation.

This option allows the two types of networks to be treated separately.

- With this option enabled, local break-out networks will indefinitely operate standalone. In contrast, networks that break-out via a WLC tunnel are only broadcast if the WLC can be reached.
- Without this option enabled, the time specified under **AP standalone time** applies.

AP standalone time

The time in minutes that a managed-mode AP continues to operate in its current configuration.

The configuration is provided to the AP by the WLC and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLC be interrupted, the AP will continue to operate with the configuration stored in flash for the time period entered here. The AP can also continue to work with this flash configuration after a local power outage.

If there is no connection to the WLC after this time period has expired then the flash configuration is deleted and the AP goes out of operation. As soon as the WLC can be reached again, the WLC transmits the configuration to the AP again.

This represents an effective measure against theft as the AP deletes all security-related configuration parameters after this time has expired.

If the AP establishes a backup connection to a secondary WLC then the countdown to the expiry of standalone operation stops. The AP and its WLAN networks remain active as long as there is a connection to a WLC.

Please note that the AP only deletes the configuration in flash memory after the time for standalone operation has expired, and not when the power is lost!

Timeframe

Select one of the time frames defined in **WLAN controller** > **General** > **Time frame**. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times. The time frame for the WLAN controller is configured in the same way as the settings in *Timeframe* on page 1669.

802.11u network profile

Select the Hotspot 2.0 profile from the list.

OKC activated

This option enables the opportunistic key caching. OKC makes it easy for WLAN clients to quickly and conveniently roam between WLAN cells in wireless environments with WPA2-Enterprise encryption.

MAC check activated

The MAC addresses of the clients that are allowed to associate with an AP are stored in the MAC filter list (**Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

Suppress SSID broadcast

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

- **No**: The AP publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the AP responds with the SSID of the radio cell (public WLAN).
- **Yes:** The AP does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the AP similarly responds with an empty SSID.
- **Tightened:** The AP does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the AP does not respond.

Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the AP, this transmits the SSID in cleartext so that it is briefly visible to all clients in the WLAN network.

RADIUS accounting activated

Select this option if you want to enable the RADIUS accounting in this logical WLAN network.

Allow traffic between stations of this SSID

Check this option if all stations logged on to this SSID may communicate with one another.

WPA-Version

Here you select which WPA version the AP is to offer to the WLAN clients for encryption.

- WPA1: WPA2 only
- WPA2: WPA2 only
- WPA3: WPA3 only
- WPA1/2: WPA1 and WPA2 in one SSID (radio cell)
- WPA2/3: WPA2 and WPA3 in one SSID (radio cell)
- WPA1/2/3: WPA1, WPA2 and WPA3 in one SSID (radio cell)

WPA1 session key type

If you use "802.11i (WPA)-PSK" for encryption, the method for generating a WPA1 session or group key can be selected here:

- AES: The AP uses the AES method.
- TKIP: The AP uses the TKIP method.
- AES/TKIP: The AP uses the AES method. If the client hardware does not support the AES method, the AP will change to the TKIP method.

WPA2 and WPA3 session key types

The method for generating the session or group key for WPA2 and WPA3 is selected here.

Basis rate

The defined basis rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster". By setting the transmission rate to auto, the AP collects information about the transmission rates of the various WLAN clients. Clients automatically notify the AP of this rate with each unicast communication. The AP takes

the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

Client bridge support

Enable this option for an AP if you have enabled the client-bridge support for a client station in WLAN client mode.

Client-bridge mode is only available between two LANCOM devices.

TX bandwidth limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID. A value of `0` disables the limit.

RX bandwidth limit

With this setting, you define the overall bandwidth that is available for reception within this SSID. A value of `0` disables the limit.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Maximum count of clients

Here you set the maximum number of clients that may associate with this AP. Additional clients wanting to associate will be rejected by the AP.

Min. client signal strength

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the AP stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the AP and cannot associate with it. This ensures that the client has an optimized list of available APs, as those offering only a weak connection at the client's current position are not listed.

Client disassociation signal strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

This threshold only works if the value **Minimum client signal strength** is also set and the **Client disassociation signal strength** is less than this value.

Enable LBS tracking

This option specifies whether the LBS server is permitted to track the client information.

This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

Use long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the AP. "Long preamble" should only be set when the clients require this setting to be fixed.

(U)APSD / WMM Power Save activated

Enable this option to signal stations that the power saving function (U)APSD ([Unscheduled] Automatic Power Save Delivery) is supported.

(U)APSD is established in the 802.11e standard, and helps VoWLAN devices to increase their battery life. The related devices switch to power saving mode after login on a (U)APSD-capable AP. If the AP receives data packets for the related devices thereafter, it temporarily stores the data and waits until the VoWLAN device is available again. It then forwards the data. Afterwards, (U)APSD increases the latency time of the radio module, whereby it ultimately consumes less power. The individual rest periods may be so short that a VoWLAN device can still use the power saving function in the call state itself. However, the relevant devices must also support (U)APSD.

WWM (Wi-Fi Multimedia) Power Save is a power saving function of the Wi-Fi Alliance and is based on U-APSD. Certain LANCOM APs are WMM® Power Save CERTIFIED by the Wi-Fi Alliance.

Max. spatial streams

The spatial multiplexing function allows the AP to transmit multiple data streams over separate antennas in order to increase the data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

In the 'Auto' setting, the AP uses all of the spatial streams supported by this WLAN module.

Allow short guard interval

This option is used to reduce the transmission pause between two signals from 0.8 s (default) to 0.4 s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

Use frame aggregation

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This procedure reduces the overhead of the packets to increase the throughput.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

STBC (space time block coding) activated

Activate the space time block coding here.

STBC is an encoding method according to IEEE 802.11n. The “STBC” (Space Time Block Coding) function varies the transmission of data packets over time in addition to space to minimize temporal effects on the data. The temporal offset of transmissions provides the receiver with an even better chance of receiving error-free data packets, regardless of the number of antennas. This results in improved reception conditions in a MIMO system.

LDPC (low density parity check) activated

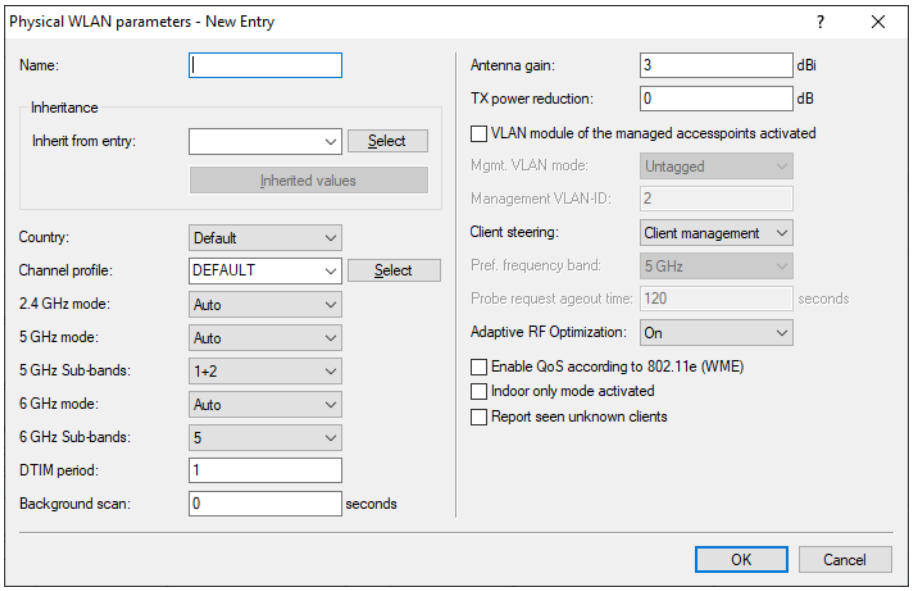
Activate the low density parity check here.

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

14.4.2.9 Physical WLAN parameters

Here the physical WLAN parameters are set for assignment to the access points. For each set of physical WLAN parameters you can specify the following parameters under **WLAN controller** > **Profiles** > **Physical WLAN parameters**:



Name

Unique name for this combination of physical WLAN parameters.

Inheritance

Selection of a physical WLAN parameter set defined earlier and from which the settings are to be inherited.

Country

The country in which the access points are to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

Channel profile

Select a channel profile. See *Channel Profile Table* on page 1131.

The DEFAULT profile activates all allowed channels of the set country.

DTIM period

If just one mobile client operates power-saving mechanisms, broadcasts and multicasts are no longer transmitted in the radio cell immediately. Instead, they are buffered and sent after the beacon that is transmitted regularly by the access point. The clients are informed about their next relevant beacon so they can synchronize with the broadcasts and multicasts, and this allows them to leave their radio module switched off for most of the time and to activate it only when necessary.

The DTIM period specifies how many beacons are sent before the buffered broadcast and multicasts are transmitted. Higher values allow clients to save more power, but also increase the latency of delivering these packets.

The default value is 1, i.e. buffered broadcasts and multicasts are sent after every beacon.

Management VLAN-ID

The VLAN ID of the management network used to manage the APs.

The Management VLAN ID **must** be set to a value not equal to zero in order for VLANs to be used over the WLAN networks. This also applies when the management network itself is not to be tagged with VLAN IDs (Mgmt-VLANID=1).

VLAN activation only applies to WLAN networks which are connected by means of these physical WLAN parameters.

Client steering

This entry sets the method used for client steering and whether the AP should activate band steering. In this case, a dual-port access point can forward a WLAN client to a preferred frequency band.

With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLAN controller. Managed access points constantly report the current values to the WLAN controller, which uses these criteria to decide which access points may respond to requests from WLAN clients. For this reason, client steering is only possible with access points that are centrally managed by a WLAN controller.

Off

Client steering is deactivated.

On

The AP lets the WLC handle the client steering.

Client management

The client steering is handled decentrally by the APs. See *Client Management* on page 978.

AP-based band steering

The AP independently steers the WLAN client to a preferred frequency band.

Report seen unknown clients

By default, the access point only reports associated clients to the WLC. If all other seen clients should be reported, i.e. unassociated clients as well, you can activate this switch. This will increase the traffic on the network. You should therefore activate this switch only temporarily or for test purposes.

If you have a large number of unknown clients (e.g., with a Public Spot or in areas with lots of traffic), you should not activate this switch, otherwise you will be flooded by inbound messages.

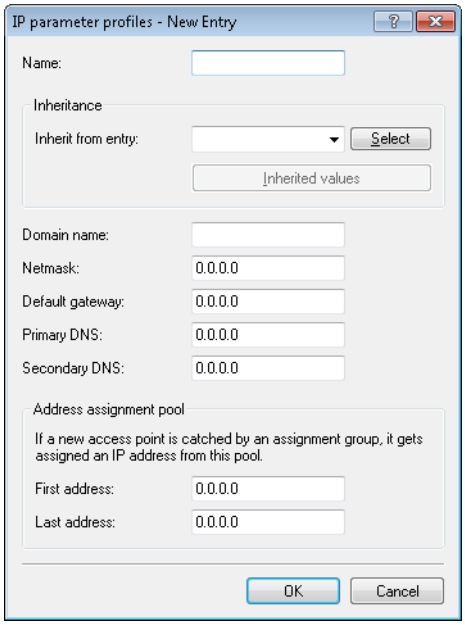
All other physical WLAN parameters correspond to those for the standard configuration of APs.

To successfully acquire a profile, HTTP access to the WLC from the local network must be allowed.

14.4.3 Access point configuration

14.4.3.1 IP parameter profiles

This table is used to configure specific network profiles that are assigned with APs that must not be automatically configured by the WLC by means of DHCP. In this way you set which specific IP parameters are used by an AP.



Name

Name of the IP parameter profiles.

Inheritance

Selection of an IP parameter profile defined earlier and from which the settings are to be inherited (see *Inheritance of parameters* on page 1132).

Domain name

Name of the domain (DNS suffix) which is to use this profile.

Netmask

Netmask of the profile

Default gateway

The gateway used by the profile as standard.

DNS default

The DNS (Domain Name System) to be used by the profile.

DNS backup

Second, alternative DNS if the first is unavailable.

Start address

The start of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

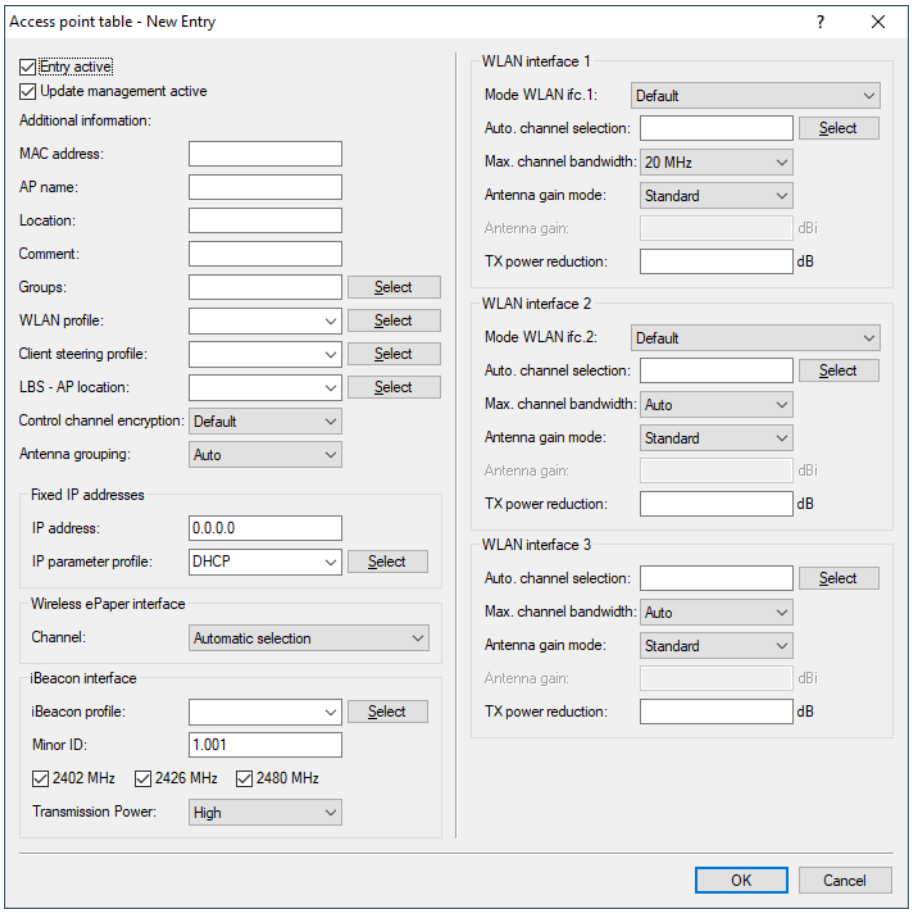
End address

The end of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

For further information on assignment groups, please refer to the section *IP-dependent auto configuration and tagging of APs* on page 1177.

14.4.3.2 List of access points

The access point table is a central element of the configuration for WLCs. Here, the WLC assigns WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) to the access points via their MAC addresses. Furthermore, the mere existence of an entry in the access-point table for a particular access point affects its ability to establish a connection to a WLC. Under **WLAN Controller** > **AP Configuration** > **Access point table** you can define the following parameters for each access point:



Active

Activates or deactivates this entry.

Update management active

Activating update management for this access point enables it to download the latest firmware and script versions automatically. All other settings are adjusted under access point update (*Central firmware and script management*).

MAC address

MAC address of the access point

AP name

Name of the access point in managed mode.

Location

Location of the access point in managed mode.

Comment

Enter a comment for this entry.

Groups

Assigns the access point to one or more groups

WLAN profile

WLAN profile from the list of defined profiles.

Client steering profile

Client-steering profiles control how the WLC decides which access points are to accept a client at the next login attempt.

LBS AP location profile

LBS location profile from the list of defined profiles.

Control channel encryption

Encryption for the communication over the control channel. Without encryption, access points and WLC exchange their control data in cleartext. In both cases authentication is by certificate.

Antenna grouping

Antenna grouping can be configured in order to optimize the gain from spacial multiplexing.

IP address

Here you specify a fixed IP address of the access point.

IP parameter profile

Here you specify the profile name used by the WLC to reference the IP settings for the access point. If you retain the default setting DHCP, the WLC ignores the setting for the fixed IP address and the access point is forced to obtain its IP address via DHCP.

Channel (Wireless ePaper interface)

Here you specify how the channel is selected for the Wireless ePaper interface.

iBeacon profile (iBeacon interface)

Select an iBeacon profile from the list of profiles created.



You create iBeacon profiles under **WLAN Controller** > **AP configuration** > **Extended settings** > **iBeacon profiles**.

Minor

Set a minor ID for the iBeacon module.

2402 MHz, 2426 MHz, 2480 MHz

Specify here which channels the iBeacon module uses to transmit.

Transmission power

Specify the power used by the iBeacon module to transmit. The following values are possible:

- **High**: The module sends with maximum power (default).
- **Medium**: The module sends with medium power.
- **Low**: The module sends with minimum power.

Mode WLAN ifc.1 1

This setting allows you to configure the frequency band in which the access point operates the 1st physical WLAN interface. When set to **Default**, the access point independently selects the frequency band for the physical WLAN interface. The access point prefers the 2.4 GHz band, if available.

Mode WLAN ifc.1 2

This setting allows you to configure the frequency band in which the access point operates the 2nd physical WLAN interface. When set to **Default**, the access point independently selects the frequency band for the physical WLAN interface. The access point prefers the 5 GHz band, if available.

If a managed access point only has one physical WLAN interface, the access point ignores the settings for the 2nd physical WLAN interface.

Auto Channel selection

Access points automatically carry out channel selection for the frequency band available in the country of operation, assuming that no entry is made here.

Enter the channels to be available for automatic selection by the first WLAN module. If you enter just one channel here, the access point uses this channel only and no automatic selection takes place. For this reason you should ensure that the channels entered here are legal for use in the defined country of operation. The access point ignores channels that are invalid for the frequency band.

Max. channel bandwidth

Enter how and to what extent the access point specifies the channel bandwidth for the physical WLAN interface(s). The following values are possible:

- **Automatic**: The access point automatically detects the maximum channel bandwidth (default).
- **20 MHz**: The access point uses channels bundled at 20 MHz.
- **40 MHz**: The access point uses channels bundled at 40 MHz.
- **80 MHz**: The access point uses channels bundled at 80 MHz.
- **80+80 MHz**: The access point uses two channels bundled at 80 MHz.
- **160 MHz**: The access point uses channels bundled at 160 MHz.
- **320 MHz** (Only WLAN interface 3): The access point uses channels bundled at 320 MHz.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Antenna gain mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard

antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is transmitted to the WLAN controller and used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

Possible values:

Standard

The antenna gain value preset in the access point is used.

Userdefined

The value entered in the field **Antenna gain** is used.

Antenna gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, as well as depending on the country where the system is operated and the frequency band, the access point calculates the maximum permitted transmission power.

If you leave the field blank, the access point uses the default setting from the configuration group in the relevant WLAN profile.

You can reduce the transmission power to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band.

Be sure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

The current transmission power is displayed by WEBconfig or telnet under **Status** > **WLAN-statistics** > **WLAN-parameters** > **Transmission-power** or with LANmonitor under **System information** > **WLAN card** > **Transmission power**.

TX power reduction

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your access point to the level permitted on the frequency band in the country of operation.

If you leave the field blank, the access point uses the default setting from the configuration group in the relevant WLAN profile.

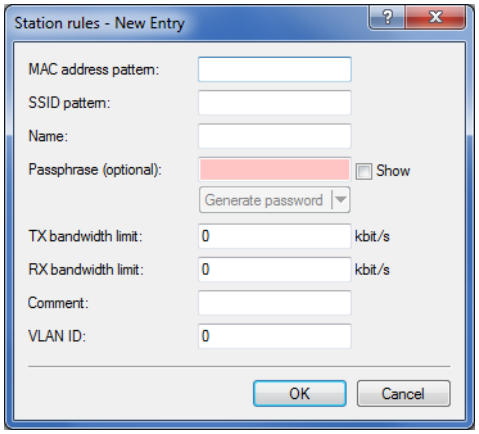
The same values and constraints apply as for the field **Antenna gain**.

14.4.3.3 Stations

The station rules define which WLAN clients can associate with the WLAN networks of the APs that are centrally managed by the WLC. Furthermore, the method offers a convenient way to give each WLAN client an individual authentication passphrase and a VLAN ID.

To use the station rules, it is imperative that the RADIUS server is activated in the WLC under **WLAN Controller** > **Stations/LEPS** > **LEPS-MAC** > **Station rules**. As an alternative, requests can be forwarded to another RADIUS server. More information on RADIUS is available under *RADIUS*.

For every logical WLAN in which WLAN clients are authenticated by RADIUS, the MAC check has to be activated.



MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

It is possible to use wildcards.

SSID pattern

WLAN clients with the corresponding MAC addresses have access that is limited to this SSID.

The use of wildcards makes it possible to allow access to multiple SSIDs.

Name

You can enter any name you wish and a comment for any WLAN client. This enables you to assign MAC addresses more easily to specific stations or users.

Passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

TX bandwidth limit

Transmission-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

RX bandwidth limit

Reception-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

The RX bandwidth restriction is only active for WLAN devices in client mode. For value is not used by normal WLAN clients.

Comment

You can enter a comment here.

VLAN-ID

The ID of the VLAN that this client belongs to. Consequently the client can only be reached by packets originating from the same VLAN. Packets sent by the client are marked with this VLAN ID. You only need to set this value if you want this client to belong to a different VLAN than the logical WLAN (SSID) that it is connected to. Valid VLAN IDs are in the range 0 to 4094. 0 means that the client belongs to the VLAN of its logical WLAN (SSID), if this belongs to a VLAN at all.

If you use IPv6, or if multicast is operating on a VLAN, different group keys must be assigned to the different VLANs of an SSID. Otherwise the different multicasts are not be assigned to the correct clients. When using IPv6, for example, clients are informed of IPv6 prefixes that do not function on the VLAN ID. The group keys are configured under **Wireless LAN** > **Encryption** > **VLAN group key mapping**.

If filter rules contradict, the individual rule has a higher priority: A rule without wildcards in the MAC address or SSID takes precedence over a rule with wildcards. When creating these entries, the user should ensure that filter rules do not contradict. The definitions in the filters can be checked in a Telnet session with the trace command `trace WLAN-ACL`.

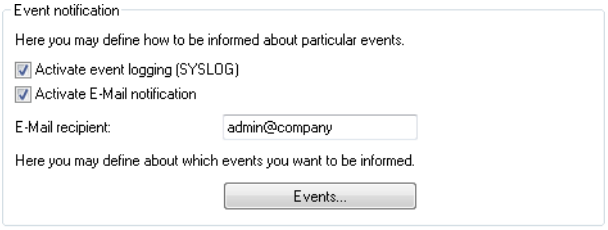
The filter criteria in the station list either allow or deny WLAN clients to access your wireless network. The entries **Name**, **Bandwidth limit**, **VLAN ID** and **Passphrase** are meaningless if the device uses valid filter criteria to deny access to the WLAN.

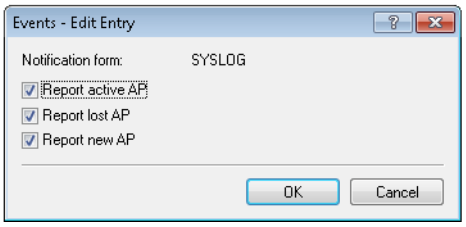
14.4.3.4 Options for the WLAN controller

The **Options** area in the WLC configuration is used to define notifications in case of events and to set various default values.

Event notification

Notifications can be sent via SYSLOG or e-mail. You can define the following parameters:





LANconfig: **WLAN Controller** > **Options**

Activate event logging (SYSLOG)

Activates notification by SYSLOG.

Activate e-mail notification

Activates notification by e-mail.

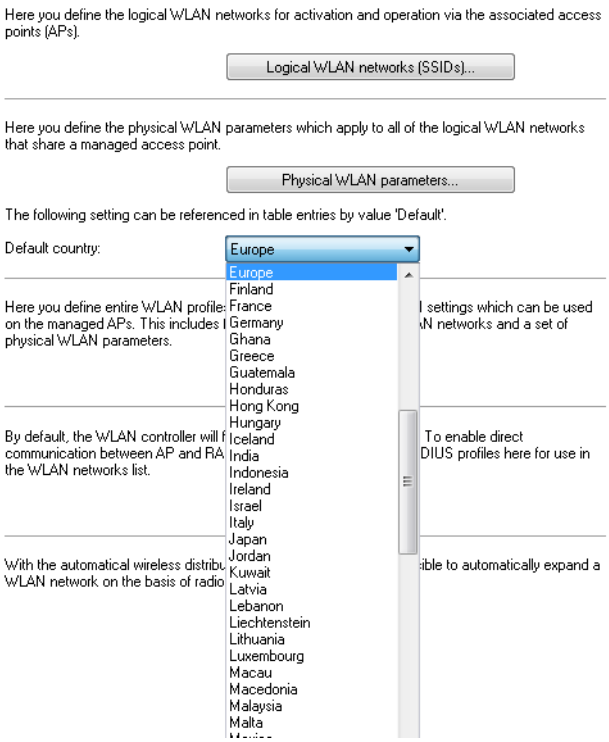
Events

Selects the events that trigger notification. Possible values:

- Report active AP
- Report lost AP
- Report new AP

Default parameters

For some parameters, default values can be defined centrally and these serve as reference default values for other parts of the configuration.



LANconfig: **WLAN Controller** > **Profiles** > **Default country**

› **Default country**

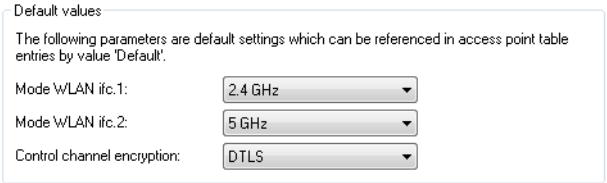
The country in which the access points are to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

› Possible values:

› Selection from the list of available countries

› Default:

› Europe



LANconfig: **WLAN controller** > **AP configuration** >

WEBconfig: **LCOS menu tree** > **Setup** > **WLAN-Management** > **AP-Configuration**

› **WLAN-Interface 1**

Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

› **WLAN-Interface 2**

Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

- **Encryption**

  Encryption for the communication over the control channel. Without encryption the control data is exchanged as cleartext. In both cases authentication is by certificate.

14.4.3.5 Virtualization and guest access via WLAN controller with VLAN

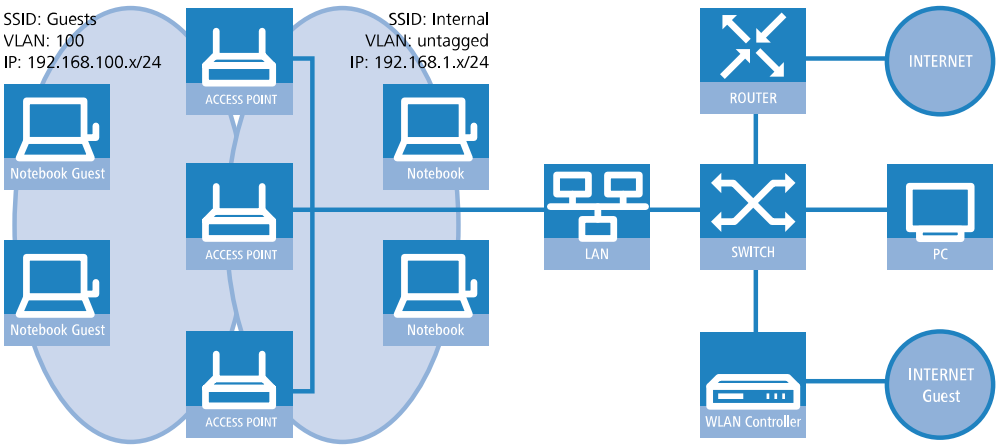
Many companies wish to offer Internet access to their visitors via WLAN. In larger installations the required settings apply to multiple access points, and these can be programmed centrally in the WLAN controller.

Targets

- Wireless LAN infrastructure available to internal employees and guests
- Shared physical components (cables, switches, access points)
- Separation of networks with VLAN and ARF
- Break-out of data streams to certain target networks:
  - Guests: Internet only
  - Internal employees: Internet, all local devices and services
- Guests login to the WLAN with a Web form.
- Internal employees use WLAN encryption for authentication.

Establish

- Management of the access points is handled by the WLC.
- The WLC serves as the DHCP server for the WLAN clients in the guest network.
- The guest network is provided with Internet access via the WLC (e.g. separate DSL access or Internet access via the company DMZ).
- The wired infrastructure is based on managed VLAN-capable switches:
  - Access point VLAN management is handled by the WLC.
  - The VLAN management of the switches is handled separately by the switch configuration.
- The access points operate within the internal VLANs.



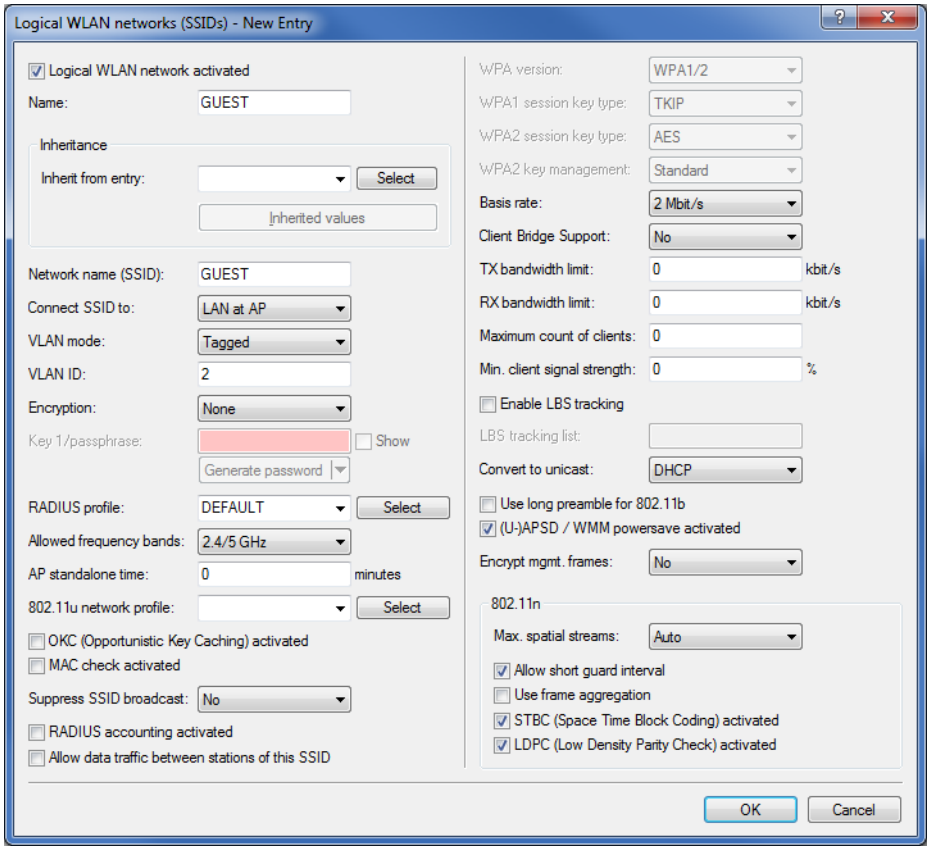
Wireless LAN configuration of the WLAN controllers

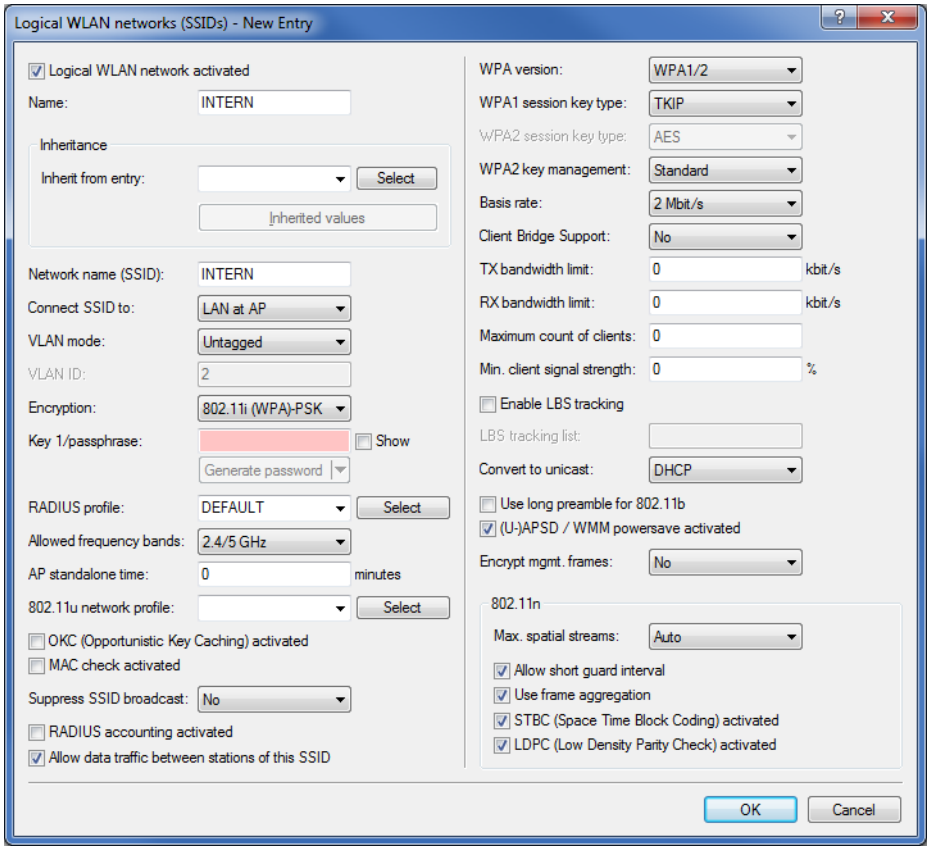
During the configuration of the WLAN, the necessary WLAN networks are defined and, along with the physical WLAN settings, are assigned to the access points managed by the controller.

1. Create a logical WLAN for guests and one for the internal employees:

- The WLAN with the SSID `GUESTS` uses the VLAN ID `100` (VLAN operating mode **Tagged**) and uses **no** encryption.
- The WLAN with the SSID `INTERNAL` receives no VLAN ID (VLAN operating mode **untagged**, i.e. packets are transferred in the Ethernet without a VLAN tag) and uses WPA encryption, e.g. **802 11i (WPA)-PSK**.

› LANconfig: **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**

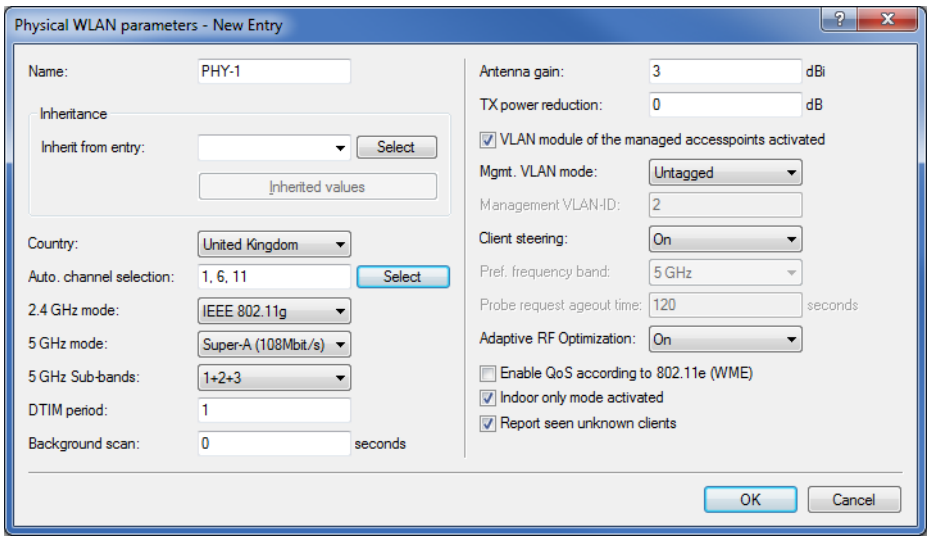




If you set the **VLAN mode** to **untagged**, LANconfig will gray-out the **VLAN ID** input field in the add/edit dialog shown above. However, the corresponding table **Logical WLAN networks (SSIDs)** still displays the assigned VLAN as a value in the grayed-out box. This entry is only of internal significance, as the acceptable range is between 2 and 4094. Ultimately it is the VLAN operating mode which is decisive: If this is set to **untagged**, then a VLAN ID is not transmitted under any circumstances.

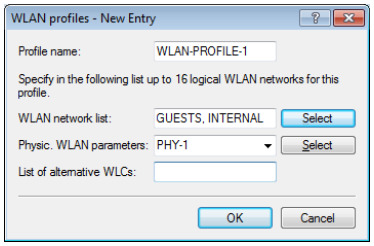
2. Create a set of physical parameters for the access points.
The management VLAN ID is set to `1`, which serves to activate the VLAN function (but without a separate management VLAN for the device; the management data traffic is transmitted untagged).

   › LANconfig: **WLAN-Controller** > **Profiles** > **Physical WLAN parameters**



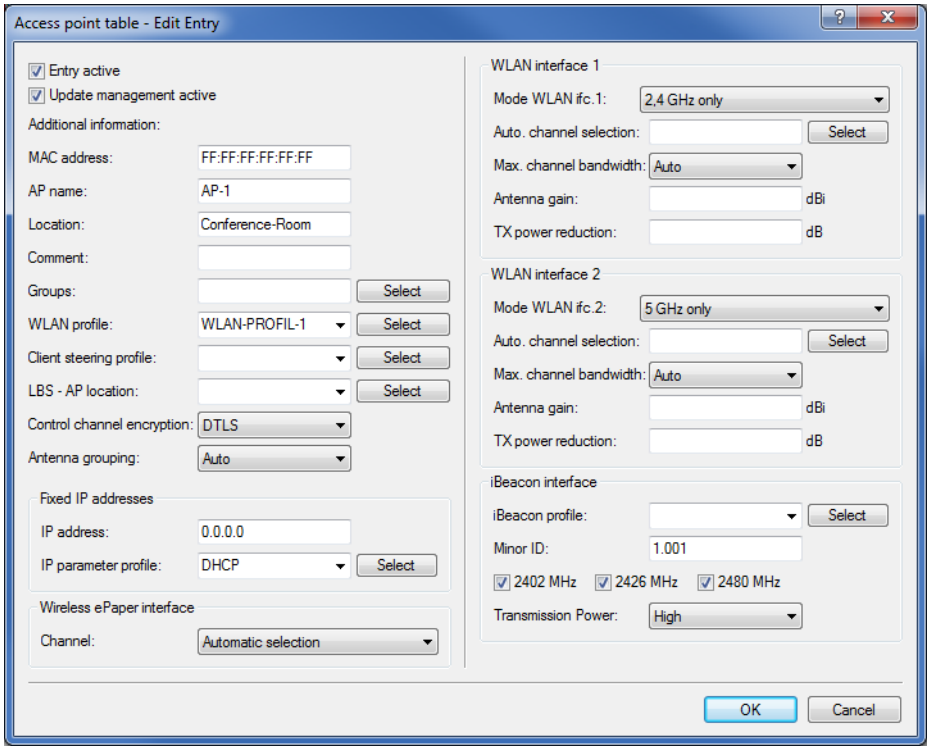
3. Create a WLAN profile that you can assign to the access points.
   The two logical WLAN networks and the set of physical parameters defined earlier are collected into this WLAN profile.

   › LANconfig: **WLAN-Controller** > **Profiles** > **WLAN-Profiles**



4. Assign this WLAN profile to the access points managed by the controller.
   Do this by entering each access point with its MAC address into the access point table. Alternatively you can use the **Default** button to create a default profile, which applies to all access points.

   › LANconfig: **WLAN controller** > **AP configuration** > **Access point table**



Configuring the switch (LANCOM GS-2326P)

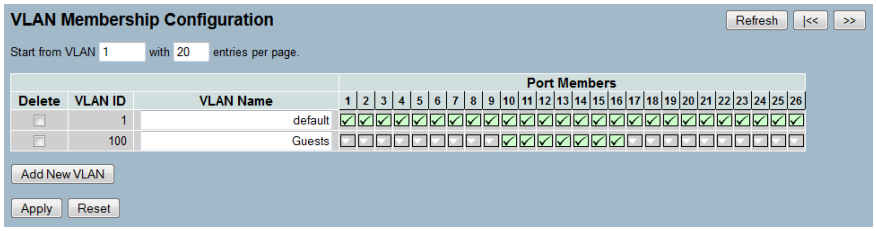
In this section we describe the configuration of the switch using the LANCOM GS-2326P as an example.

1. Under **Configuration** > **VLAN** > **VLAN-Membership**, create an additional VLAN group for the guest network.

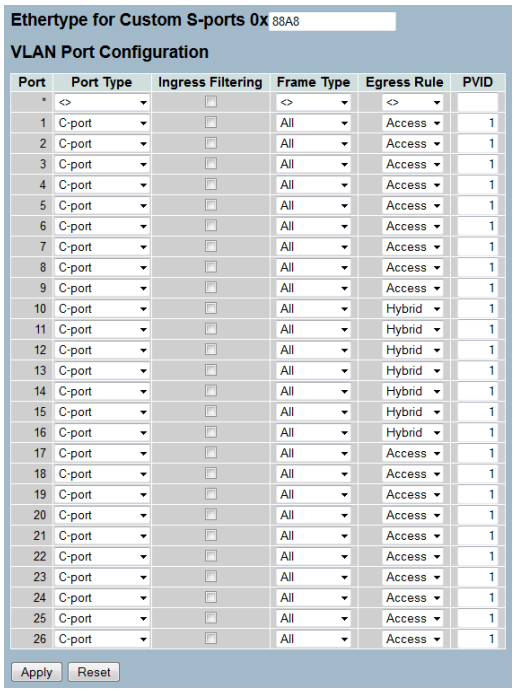
   To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the group `default`, and that for the guests is mapped to the group `guests`.

   › The VLAN group for the internal employees uses the default VLAN ID `1`. This VLAN ID used for internal administration applies on all ports and is operated untagged, i.e. all untagged incoming data packets are given the VLAN ID 1 for internal routing, and this is removed again from outgoing data packets (see also "PVID" in the next step).

› The VLAN group for the guests uses the VLAN ID `100`, which you entered earlier when configuring the WLAN in the controller. This ID applies only to the ports which the WLAN controller and the access points are connected to (in this example: Port 10 to 16, green checkmarks for **Port members**). The switch does not remove tags from outgoing data packets. i.e. all tagged incoming packets with VLAN ID 100 retain this tag and are routed only to the ports that are members of the corresponding group.



2. Under **Configuration** > **VLAN** > **Ports** set the **Port Type** for all ports to **C-port**. See the documentation about your switch for details about this setting.
3. Configure the **Egress rule** for each port.
   › All ports except port 10 to 16 are given the **Access** rule. As a result, these ports forward only tagged packets and all others are dropped.
   › The ports 10 to 16 are given the rule **Hybrid**. As a result, these ports forward both untagged and tagged packets.



Ensure that the **PVID** (port VLAN ID) for each port is set to a value of `1`. The PVID is the VLAN ID that a port assigns to incoming data packets which do not already have a VLAN tag; Therefore, the PVID corresponds to the VLAN ID of the `default` group.

4. OPTIONAL: If you wish to allow access to the guest network via Ethernet, go to **Configuration** > **VLAN** > **Ports** and, for example, set the **PVID** to `100` for ports 17 to 20 and, under **Configuration** > **VLAN** > **VLAN-Membership**, assign these ports to the group `Guests`. All untagged incoming data packets arriving at these ports are given VLAN ID 100.

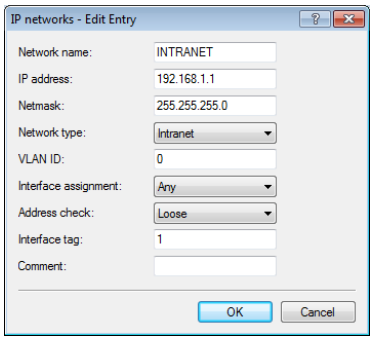
Note that these data packets can only leave the switch via the ports of the guest network.

Configuring the IP networks in the WLAN controller

To separate the data streams on layer 3, two different IP networks are employed (ARF – Advanced Routing and Forwarding).

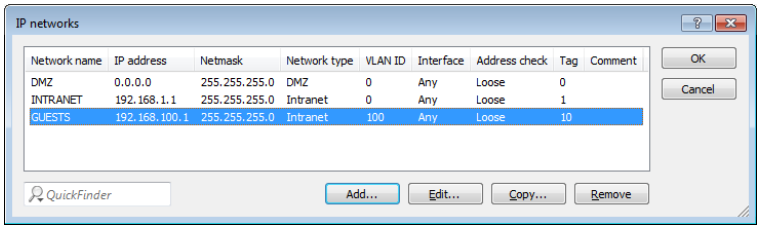
1. For the internal network, set the **INTRANET** to the address `192.168.1.1`.
   This IP network uses the **VLAN ID** `0`. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The **interface tag** `1` is used for the subsequent break-out of data in the virtual router.

   › LANconfig: **TCP/IP** > **General** > **IP networks**



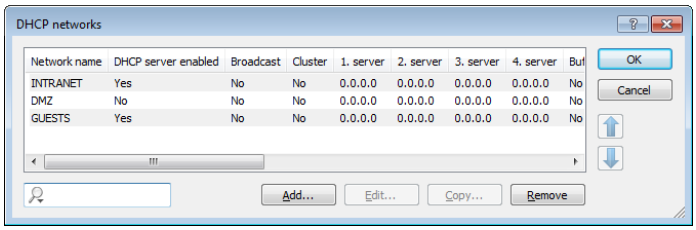
2. For guests, create a new IP network with the address `192.168.100.1`.
   This network uses the **VLAN ID** `100`. In this way, all data packets with this ID are assigned to the guest network. Here, too, the **interface tag** `10` is used later by the virtual router.

   › LANconfig: **TCP/IP** > **General** > **IP networks**

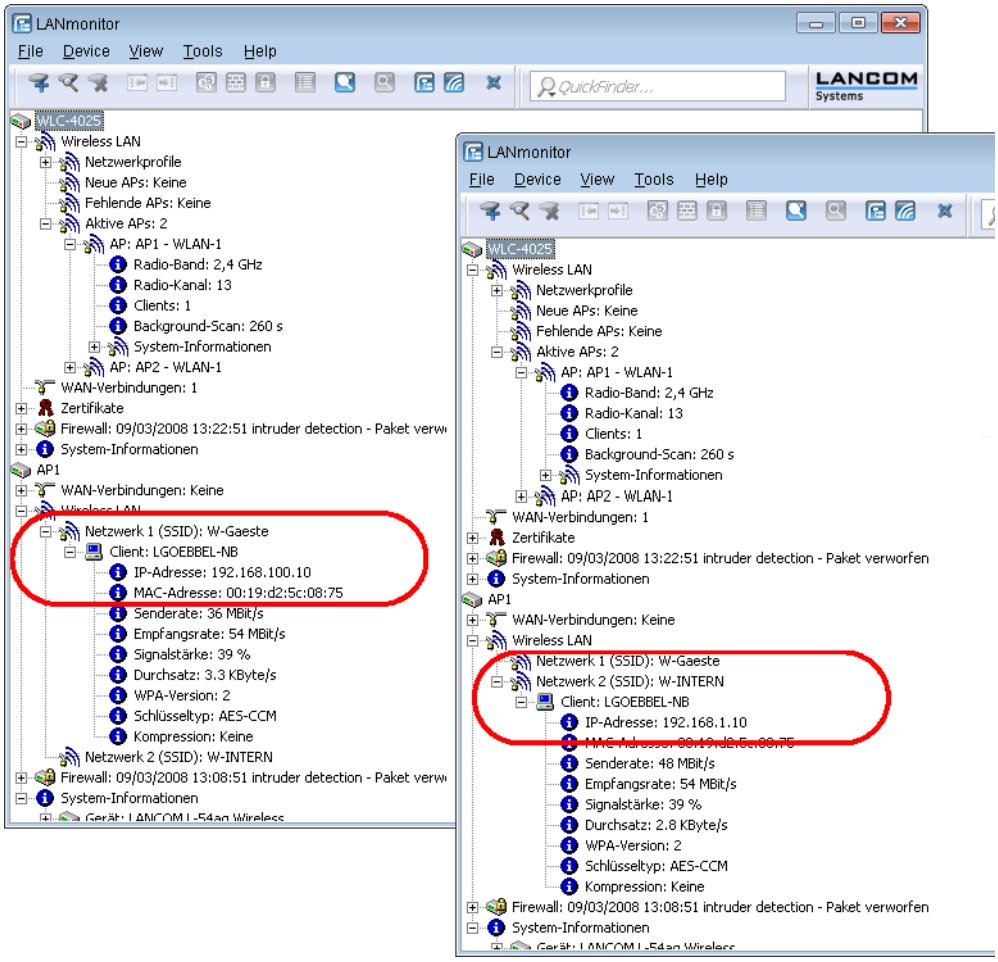


3. Enable the DHCP server for both IP networks.

   › LANconfig: **TCP/IP** > **General** > **IP networks**



With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.

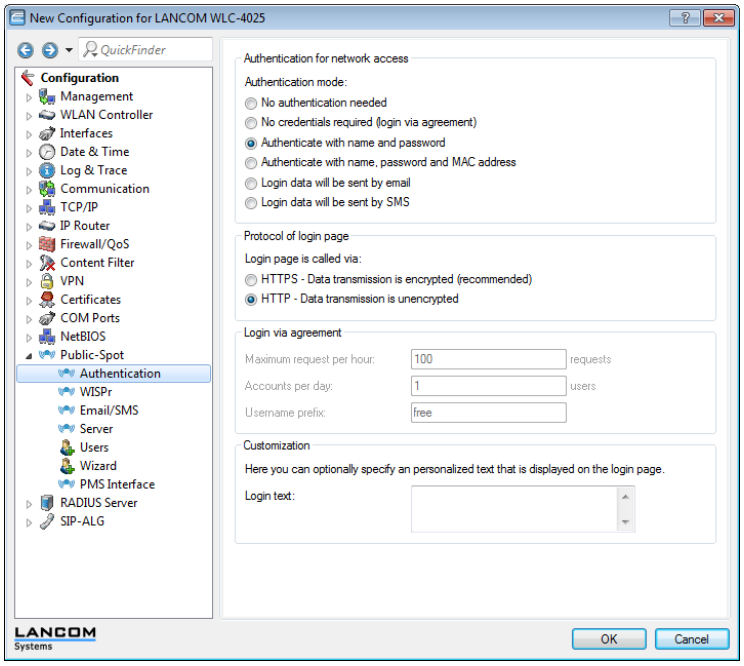


Configuring Public Spot access accounts

The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. Authentication is performed by requesting user information via a web interface. If necessary, you can can set a time limit for the access.

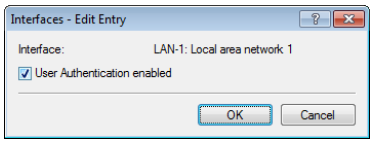
1. You should activate authentication for network access by name and password.

› LANconfig: **Public Spot** > **Authentication** > **Authentication for network access**



2. Activate user authentication for the controller's interface that is connected to the switch.

› LANconfig: **Public Spot** > **Server** > **Operation settings** > **Interfaces**

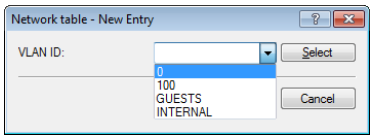


3. Restrict access to the Public Spot.

   You restrict use of the Public Spot to data packets from this virtual LAN by entering the VLAN ID of "100" for the guest network into VLAN table. Other data packets from other VLANs will be forwarded to the Public Spot without a login. Note that access to WEBconfig via the Public Spot interface is restricted to the authentication pages only (see *Limit configuration access*).

   If the interface is not restricted to the VLAN ID, the controller will no longer be reachable at the specified physical Ethernet port!

   › LANconfig: **Public Spot** > **Server** > **VLAN table**



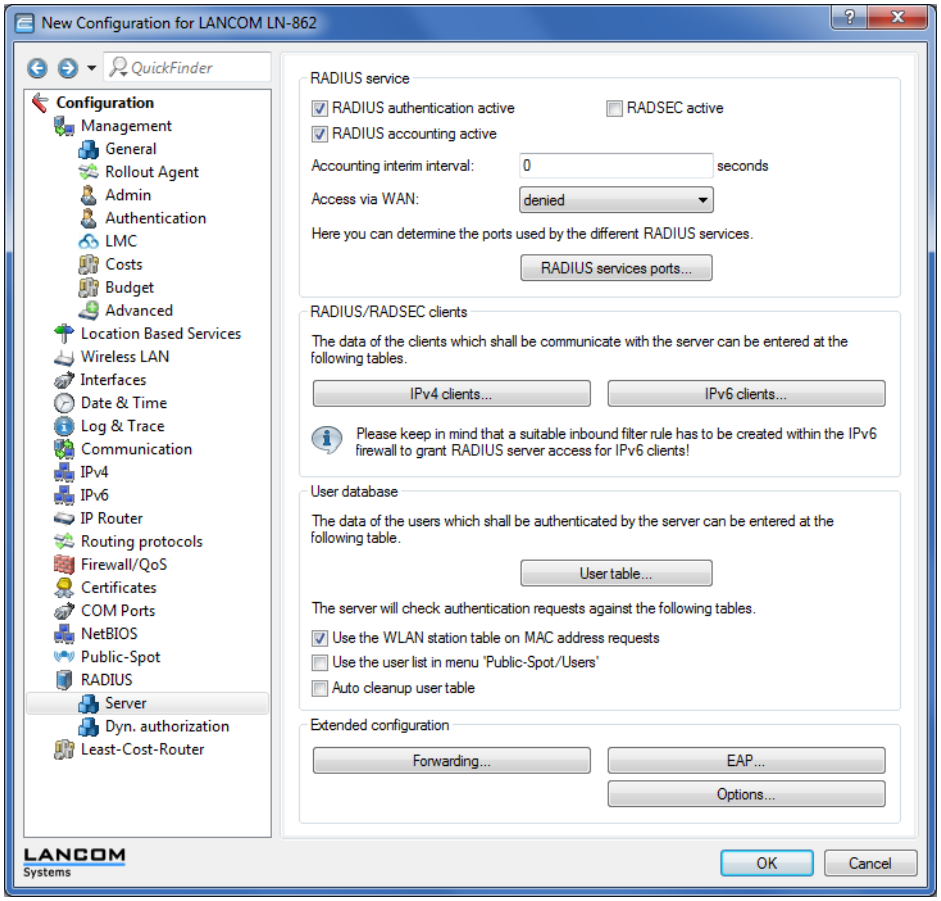
4. Enable the option to clean up the user table so that your device automatically deletes entries that are no longer needed.

   › LANconfig: **RADIUS** > **Server** > **User table** > **Auto cleanup user table**

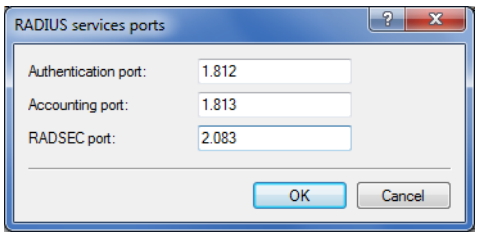
Configuring the internal RADIUS server for Public Spot operation

The Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. In order to use these Public Spot access accounts, the internal RADIUS server has been preconfigured with default values. You can inspect this setup in **LANconfig** as follows:

1. Navigate to **RADIUS** > **Server** > **RADIUS service**.
2. Ensure that checkmarks have been set for **RADIUS authentication active** and **RADIUS accounting active**.



3. Click the button **RADIUS services ports**.



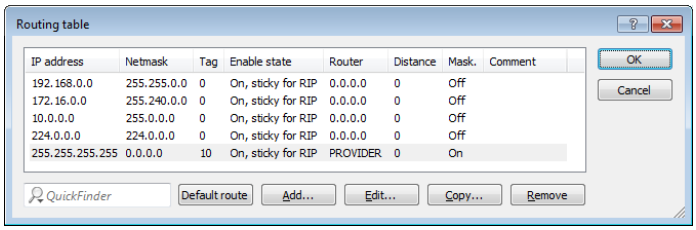
The default settings are available here for inspection.

Configuring Internet access for the guest network

1. In order to provide Internet access for guest network users, there is a wizard to set up access to a provider network.
2. Limit access to the provider network.
   In order for this access to be available to users of the guest network only, set the routing tag "10" for the corresponding route. This ensures that only data packets from the IP network "GUEST" with the interface tag "10" are transmitted

to the provider's network. The different routing tag values ensure that data cannot be routed between the guest network and the internal network.

› LANconfig: **IP router** > **Routing** > **Routing table**



3. Optional: If necessary, use **Device** > **Configuration Management** > **Upload certificate or file** in LANconfig to upload an HTML template and an image as a template to the device for output of the voucher.
The image can be a GIF, JPEG or PNG file of max. 64 KB in size.

14.4.3.6 WLAN layer-3 tunneling

Introduction

The CAPWAP standard for centralized WLAN management offers two different channels for transmissions:

› The obligatory control channel transports administrative data between the managed AP and the WLC.
› The optional data channel transmits the payload data from the various WLAN networks (SSID) between the managed AP and the WLC.

The decision whether to use of the optional data channel between the managed AP and the WLC depends on the route to be taken by the payload data:

› If you deactivate the data channel, the AP forwards the payload data directly to the LAN. In this case, you control the allocation of WLAN clients to specific LAN segments, for example by assigning VLAN IDs. The advantage of this application lies in the low load on the WLC and on the network as a whole, because the AP transmits only the management data via the CAPWAP tunnel and it transmits the payload data over the shortest available route.
› If you activate the data channel, the AP additionally forwards the payload data to the central WLC. This approach has the following advantages:
  › The APs can provide access to networks that are only available on the WLC, such as a central Internet access for a Public Spot.
  › The WLANs provided by the APs (SSIDs) can be separated from one another without the use of VLAN. Avoiding the use of VLAN reduces the effort required for the configuration of other network components such as switches, etc.
  › WLAN clients associated with the APs and in different IP networks can roam to other APs without interruption to their IP connections, because the connection is continually managed by the central WLC and not by the APs (layer-3 roaming).

The use of data channels forms additional logical networks on the basis of the existing physical infrastructure. These logical networks are known as overlay networks.

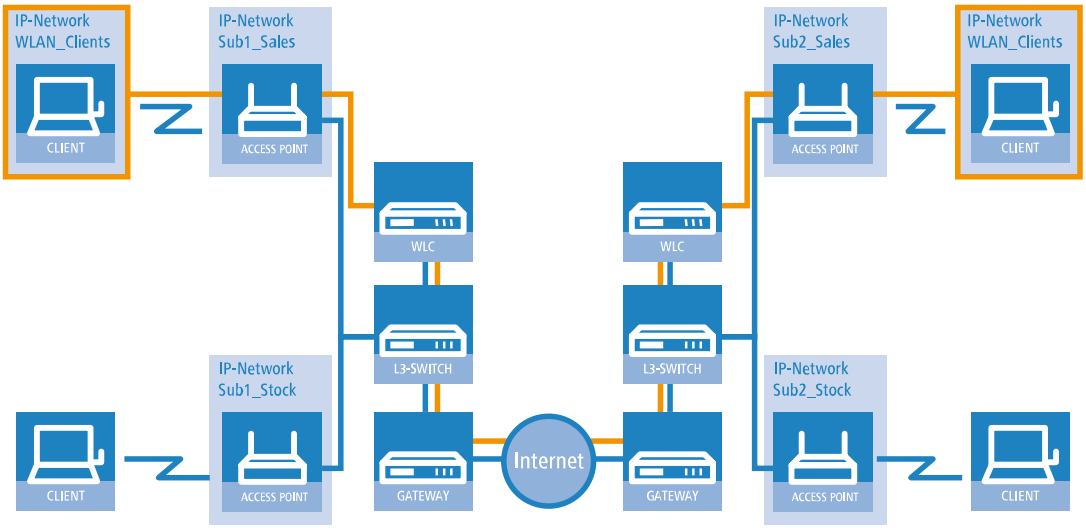


Figure 20: Overlay network across multiple IP networks

Using the data channel even allows you to span logical overlay networks across multiple WLCs.

Several WLCs within a single broadcast domain can support the same overlay network. Disable the WLC data channel between these WLCs (WEBconfig: LCOS Menu Tree > Setup > WLAN-Management > WLC-Cluster > WLC-Data-Tunnel-active). Otherwise the multiple reception of the broadcast messages would give rise to loops. Since routers drop broadcast messages, you can activate the CAPWAP data channel for WLCs in separate networks.

The APs use virtual WLC interfaces (WLC tunnels) to manage each SSID's data channels between AP and WLC. Depending on the model, each WLC provides 16 to 32 WLC tunnels that you can use when configuring the logical WLANs.

Virtual WLC interfaces are available for selection in all dialogs used to select logical interfaces (LAN or WLAN), such as in the port table of the LAN and VLAN settings or for the definition of IP networks.

Tutorials

The following sections present specific scenarios with step-by-step instructions for a number of standard situations when operating WLCs.

Overlay network: Separating networks for access points without using VLAN

In many cases, networks in a shared physical infrastructure are separated by using VLANs. However, this method assumes that the switches operated in the network are VLAN-capable and that these are configured for VLAN operations. Consequently, the administrator has to rollout the VLAN configuration for the whole network.

WLCs enable you to separate the networks while minimizing the use of VLANs. The APs use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the WLC, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the WLC and a single, central switch. All of the other switches in this example work without a VLAN configuration.

With this configuration, you reduce the VLAN to the core of the network structure (illustrated with a blue background). What's more, only 3 of the switch ports in use require a VLAN configuration.

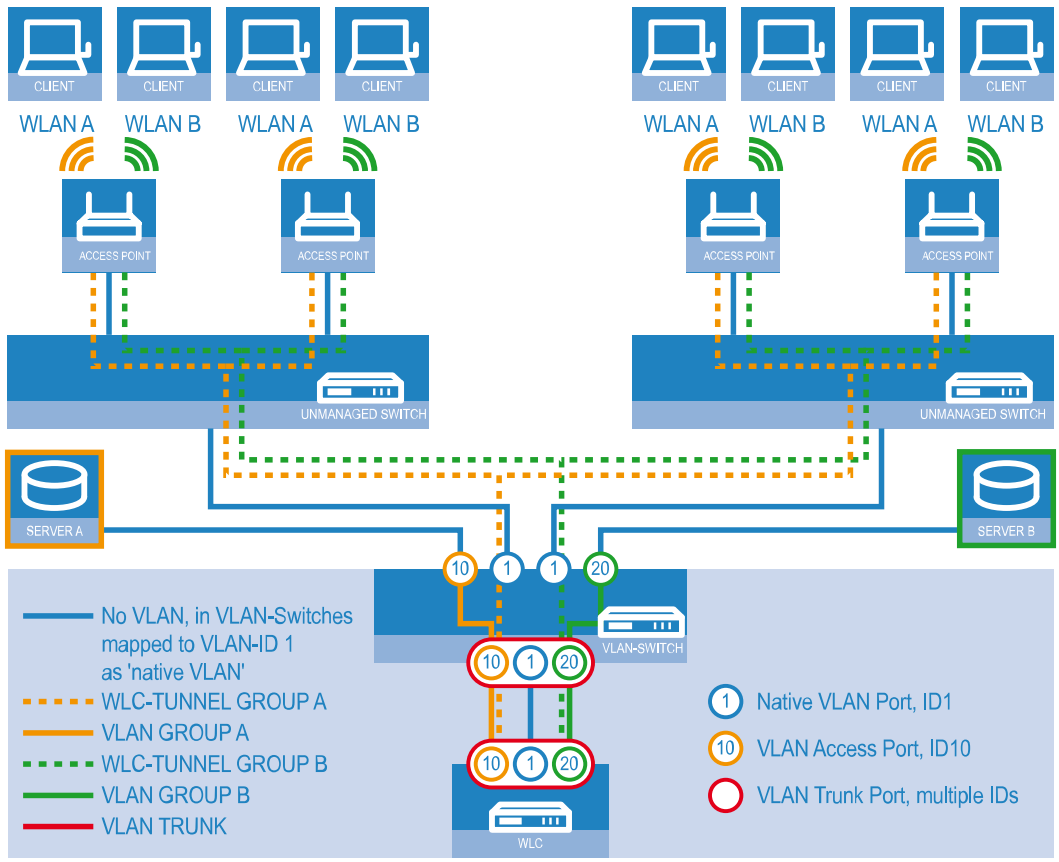


Figure 21: Example application: Overlay network

The diagram shows a sample application with the following components:

- The network consists of two segments, each with its own (not necessarily VLAN-capable) switch.
- Each segment contains several APs, each of which is connected to one of the switches.
- Each AP provides two SSIDs for the WLAN clients in two different user groups, shown in the diagram in green and orange.
- Each user group has access to its own dedicated server that is separated from other user group. The servers can only be accessed via the corresponding VLANs, i.e. through the access ports configured on the switch.
- A single WLC manages all of the APs in the network
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLC.

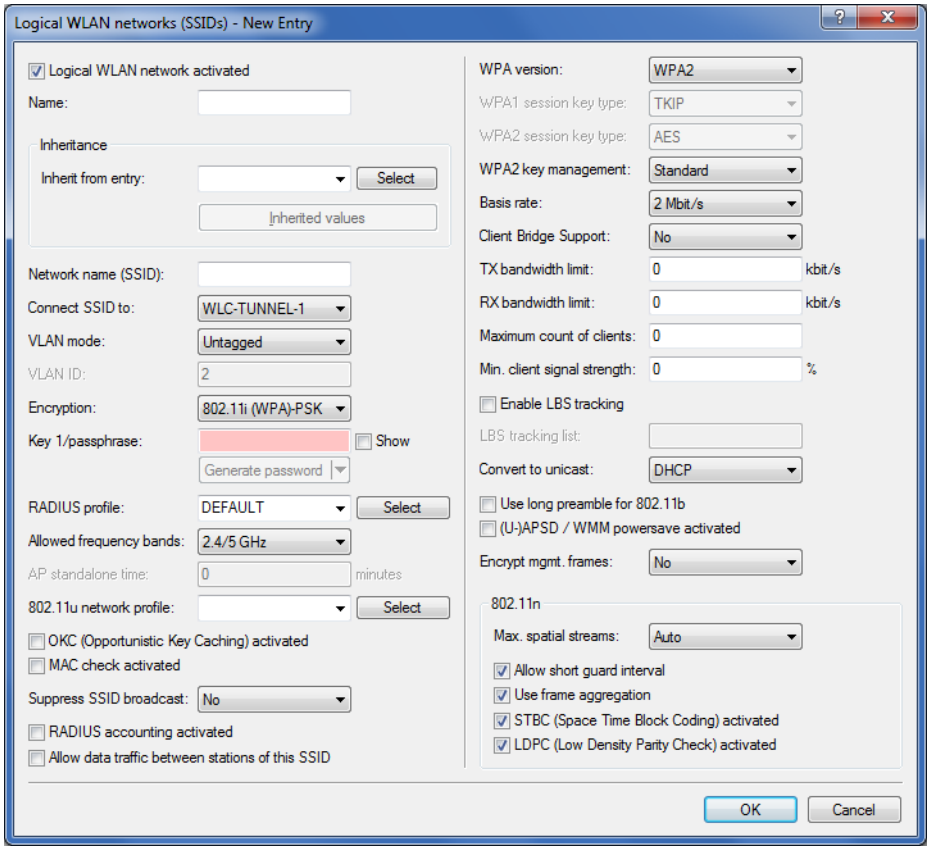
The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which AP is being used and regardless of the segment in which the client is located.

The following description assumes a working basic configuration of the WLC. The configuration of the VLAN switch is not part of this description.

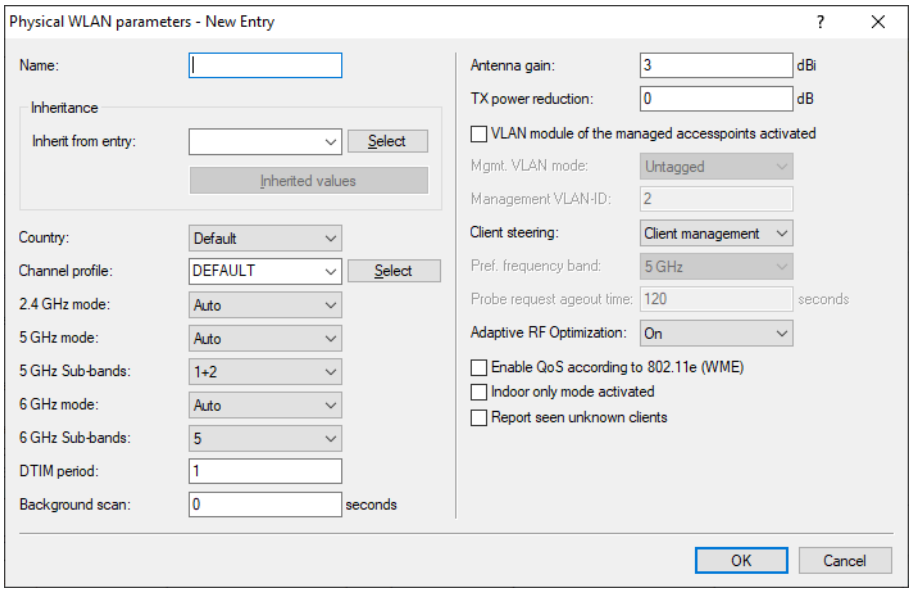
Configuring the WLAN settings

1. For each SSID, create an entry in the list of logical networks, each with a suitable name and the corresponding SSID. Connect the SSID to a WLC tunnel, for example the first SSID to "WLC-TUNNEL-1" and the second to "WLC-TUNNEL-2 '. Set the VLAN mode to 'tagged', set the VLAN ID '10' for the first logical network and the VLAN ID '20' for the

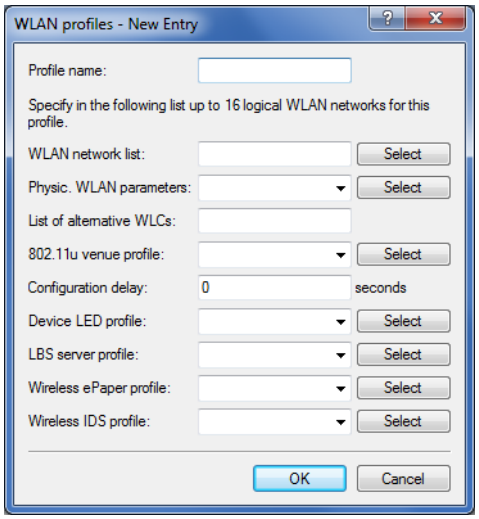
second logical network. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.



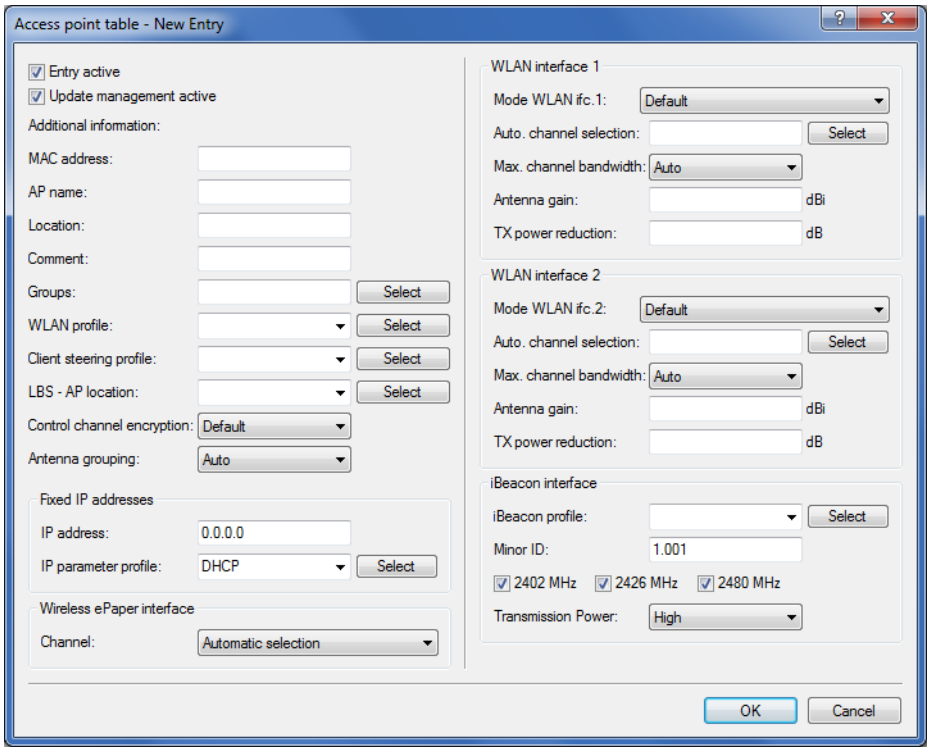
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. For this profile in the physical WLAN parameters, enable the option to turn on the VLAN module on the APs. Set the operating mode for the management VLAN in the APs to 'Untagged'. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.

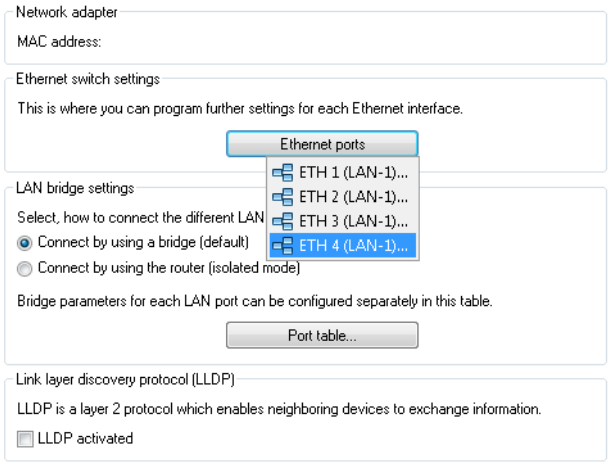


4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.

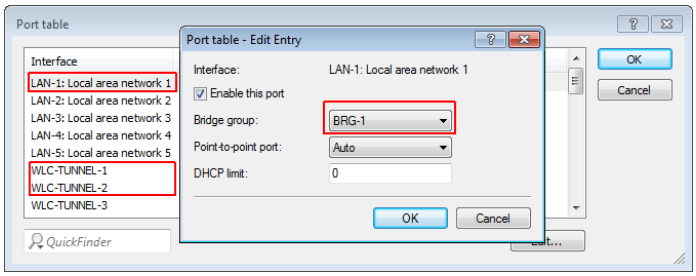


Configuring the interfaces on the WLC

5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Make sure that the other Ethernet ports are not assigned to the same LAN interface. In LANconfig you find these settings under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.

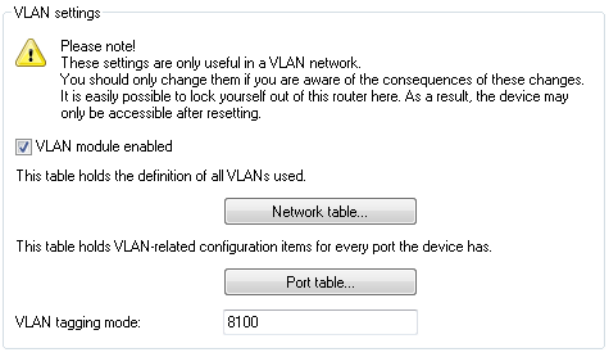


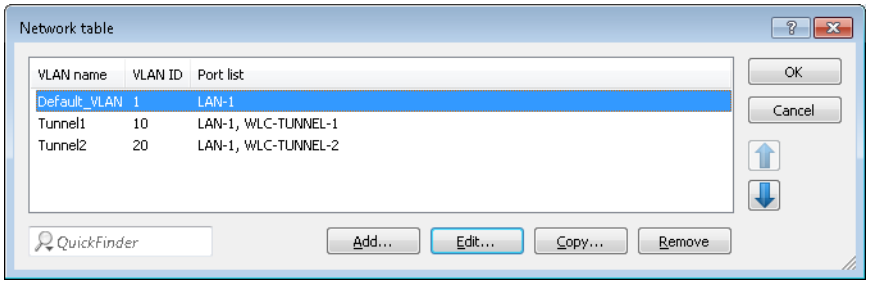
6. Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.



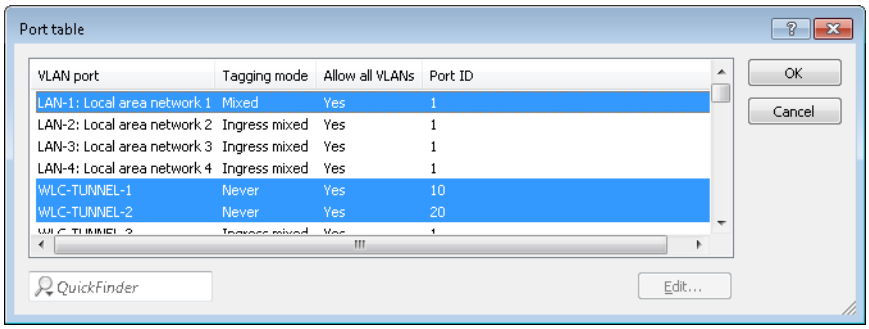
By default, the LAN interfaces and WLC tunnels do not belong to a bridge group. By assigning the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-Tunnel-1' and 'WLC-Tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

7. Activate the VLAN module of the WLC under **Interfaces** > **VLAN** and, under **VLAN table**, assign the LAN port you selected above (LAN 1) and also the corresponding WLC tunnel to the desired VLAN.





8. Under **Interfaces** > **VLAN** > **Port table**, set the Tagging mode of the tunnel interface and the LAN interface, and set the corresponding port VLAN ID.



Depending on how the switch is configured, set the Tagging mode of the LAN interface to 'Mixed' or 'Always'.

In most cases the tunnel interfaces are operated with the mode 'Never', because packets here (from the WLAN) always arrive untagged and the WLC marks them with the port VLAN ID

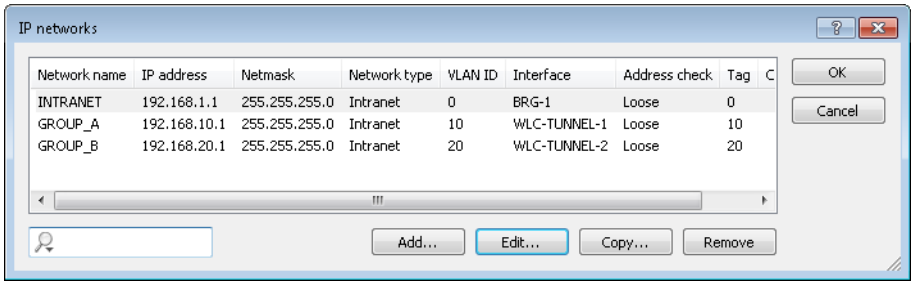
When you activate the VLAN module, please observe that the ARF networks configured on the WLC must be given a VLAN ID. In the VLAN configuration outlined above, you need to set the VLAN ID for the IP network to '1' in order for the WLC to reach the network without a VLAN tag.

A similar configuration is achieved by making the access point set a VLAN tag for packets that are to be sent via the tunnel, in which case the VLAN module of the WLC is not used.

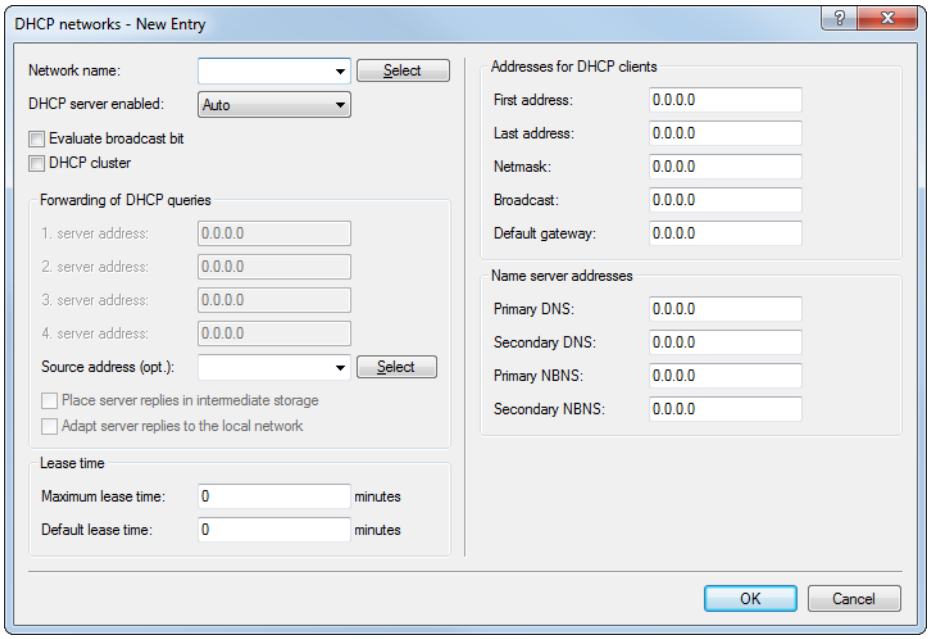
However, this bridging of the various WLC tunnels with one another causes broadcasts to be redirected into all of the tunnels; with a certain number of tunnels/SSIDs and APs, this can lead to load problems on the network and on the WLC. The VLAN module configuration presented here prevents this.

9. In addition you configure the IP settings for the networks that are separated on layer 2 under **IPv4** > **General** > **IP networks**.

To prevent the device from connecting these networks via layer 3, a separation must also be configured on layer 3, for example by using a port tag or by means of the firewall.



10. The WLC optionally acts as a DHCP server for the APs. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **IPv4** > **DHCPv4** > **DHCP networks**.



"Layer 3 roaming"

Allowing payload data from the wireless LAN to pass-through the WLC tunnel to the WLC enables roaming even beyond the limits of broadcast domains. In this example application, a layer-3 switch between the floors prevents the transmission of broadcasts, and thus separates the broadcast domains.

In this example, two user groups A and B each have access to their own WLAN (SSID). On all floors of the building, the APs provide two SSIDs, 'GROUP_A' and 'GROUP_B'.

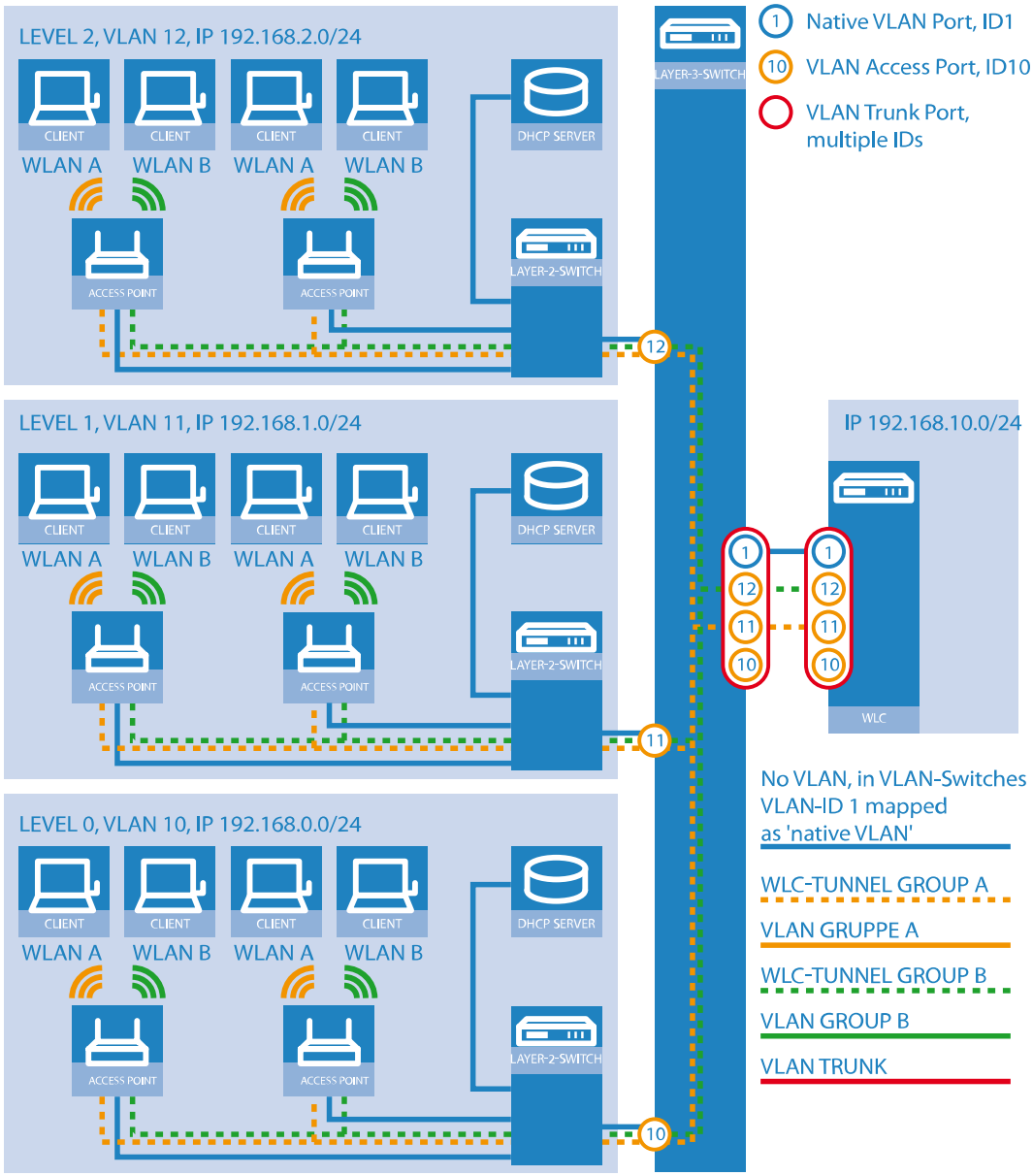


Figure 22: Example application for layer-3 roaming

The diagram shows a sample application with the following components:

- The network consists of three segments on separate floors of a building.
- A central layer-3 switch connects the segments and divides the network into three broadcast domains.
- Each segment uses its own IP address space and its own VLAN.
- Each segment operates a local DHCP server, which transmits the following information to the APs:
  - IP address of the gateway
  - IP address of the DNS server
  - Domain suffix

  This information enables the APs to contact the WLC in another broadcast domain.

The aim of the configuration: When moving to another floor, a WLAN client that associates with a particular SSID is to retain access to its "own" WLAN, regardless of which AP is being used and regardless of the segment in which the client is located. Since the segments in this example use different IP address ranges, this scenario can only be implemented by managing the APs directly with the central WLC via layer 3 and across the boundaries of the VLANs.

The configuration corresponds to the example *Overlay network: Separating networks for access points without using VLAN* on page 1162.

WLAN controller with Public Spot

This scenario is based on the first scenario (overlay network) and enhances it to include specific settings for user authentication.

The configuration of a Public Spot can be greatly simplified if the payload data sent from the WLAN to the WLC is routed through a WLC tunnel. A Public Spot can, for example, provide guests with Internet access in parallel with, but separated from, an internal wireless LAN.

In this example, the employees of a company have access to a private WLAN (SSID), while the guests use a Public Spot to access the Internet. In all areas of the building, the APs provide two SSIDs, 'COMPANY' and 'GUESTS'.

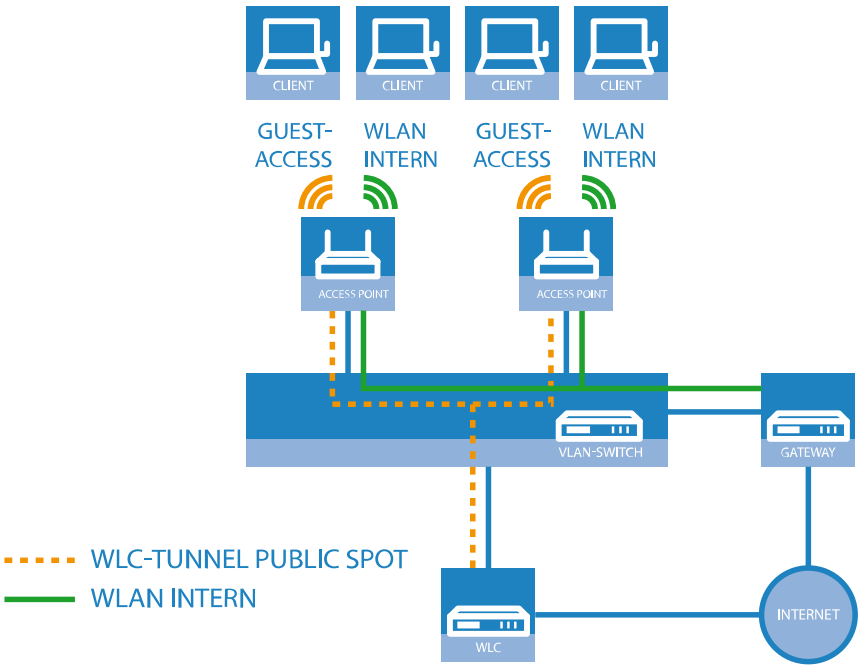
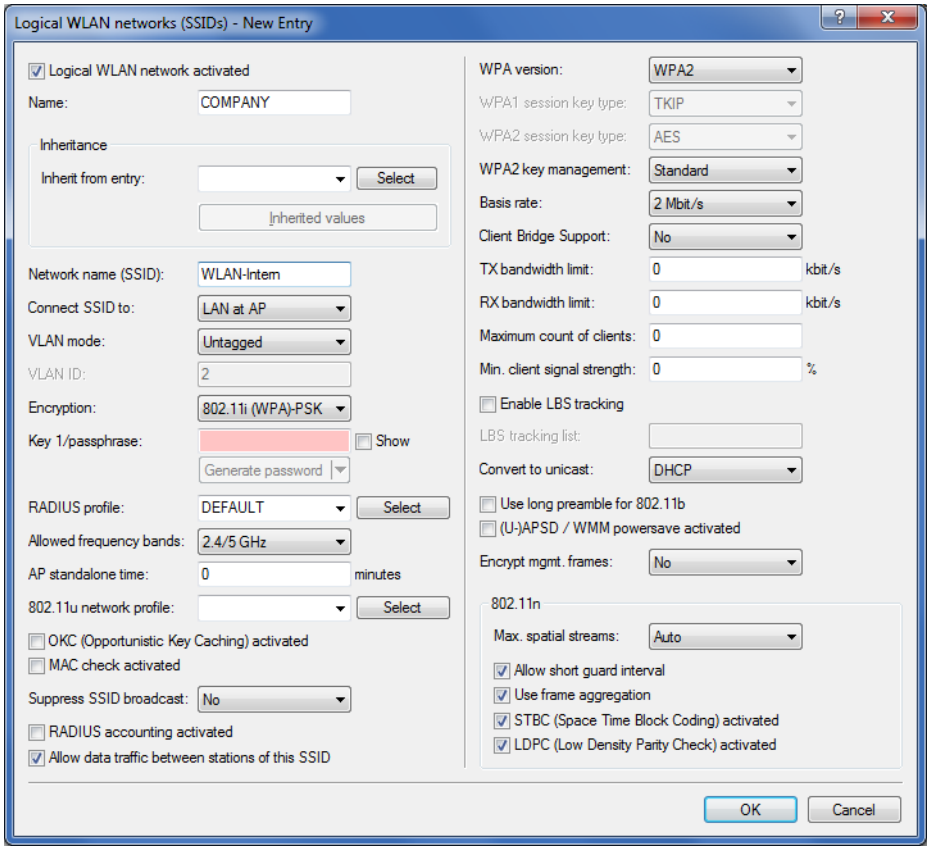


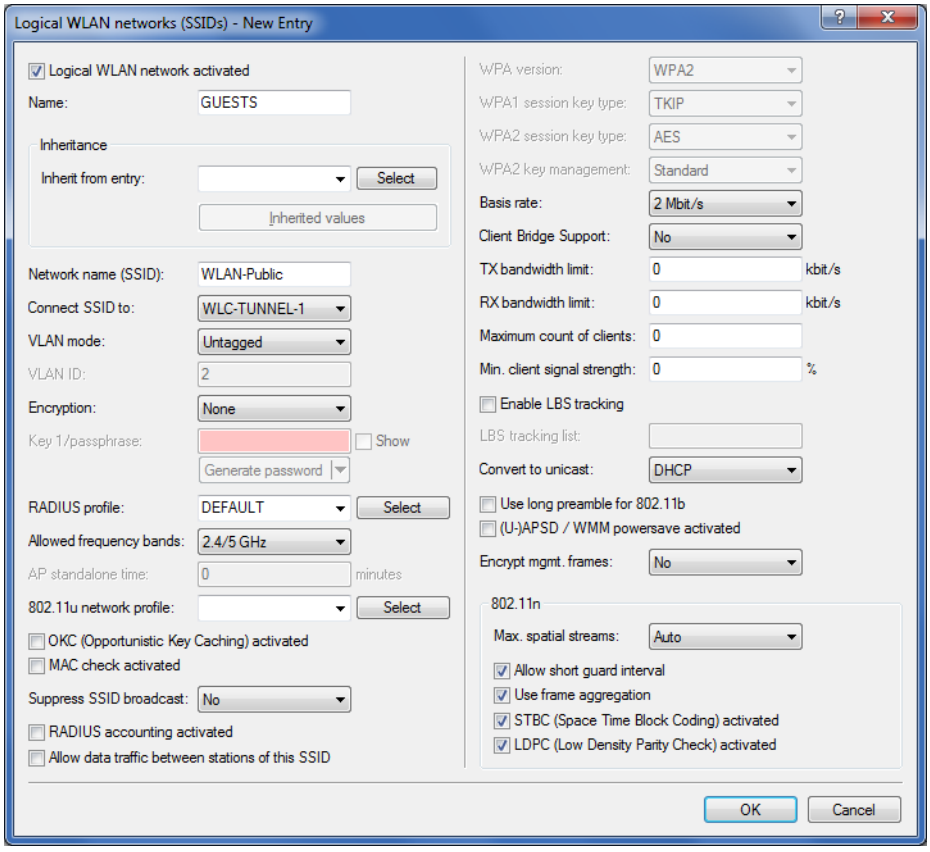
Figure 23: Example application: WLAN controller with Public Spot

The aim of the configuration: A WLAN client that associates with the internal SSID should have access to all internal resources and the Internet via the central gateway. The APs break-out the payload data from the internal clients locally and pass it on directly to the LAN. The guests' WLAN clients associate with the Public Spot. The APs send the payload data from the guest clients through a WLC tunnel directly to the WLC, which uses a separate WAN interface for Internet access.

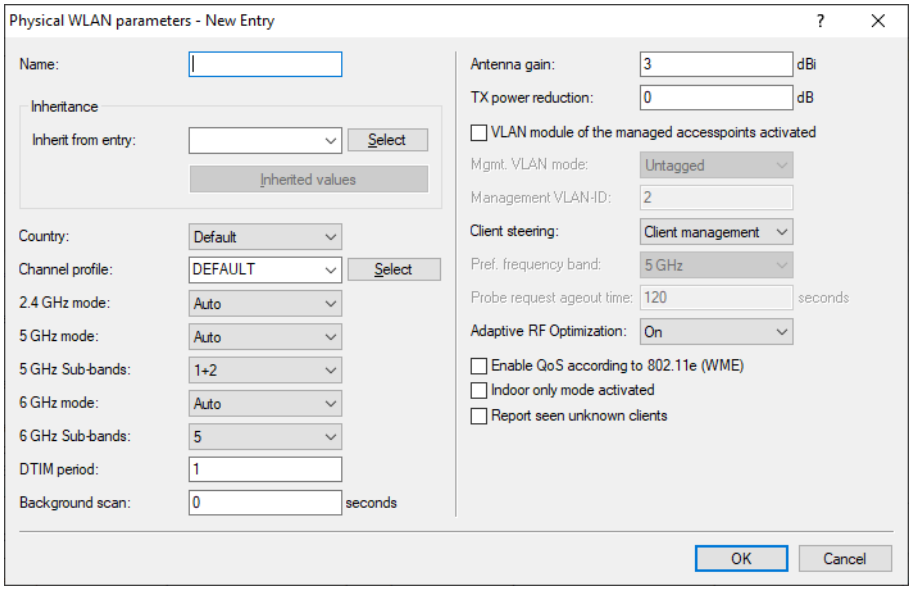
1. The internal WLAN and the guest WLAN each require an entry to be created in the list of logical networks, each with a suitable name and the corresponding SSID. Link the SSID for internal use with the 'LAN at AP', and the SSID for guests with (for example) 'WLC-TUNNEL-1'. Disable encryption for the guest network SSID so that the guests' WLAN

clients can associate with the Public Spot. You should also prevent inter-station traffic for this SSID. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.

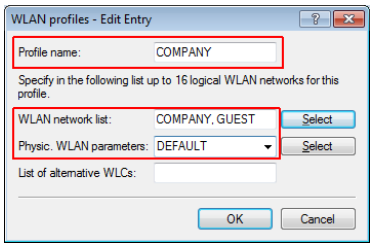




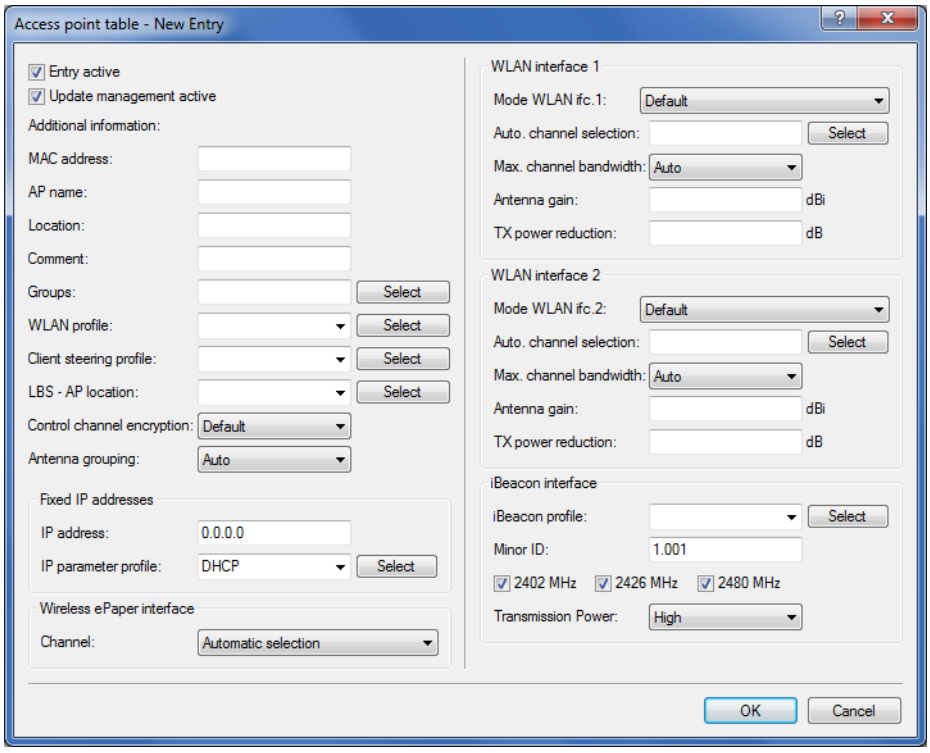
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



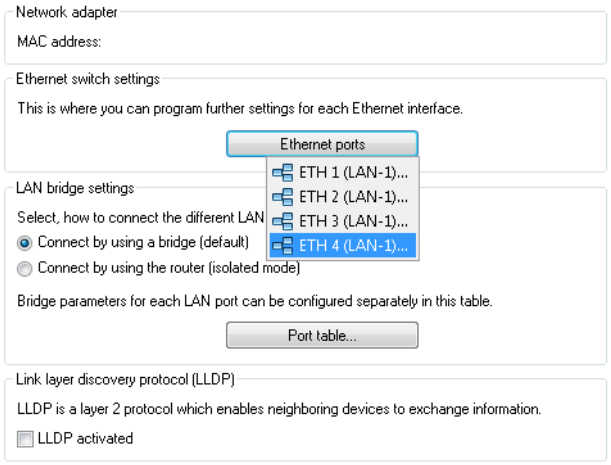
3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.



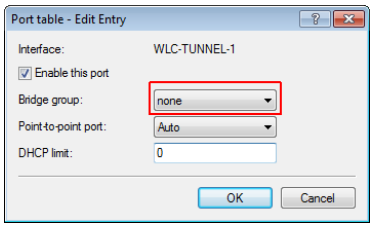
4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.



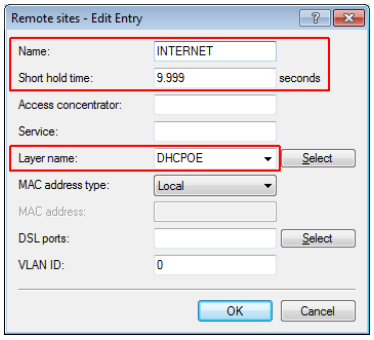
5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical LAN interface 'DSL-1'. The WLC then uses this LAN interface for the guest network Internet access. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.



6. Verify that the logical LAN interface 'WLC-tunnel-1' is not allocated to a bridge group. This ensures that the other LAN interfaces do not transmit any data to the Public Spot. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.

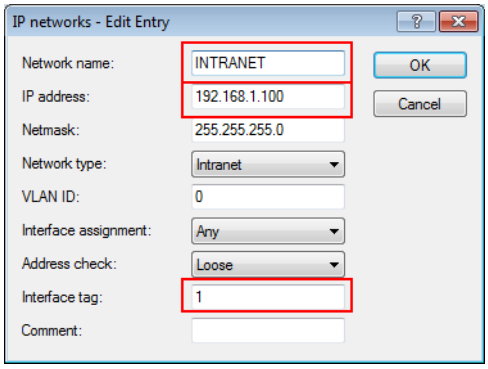


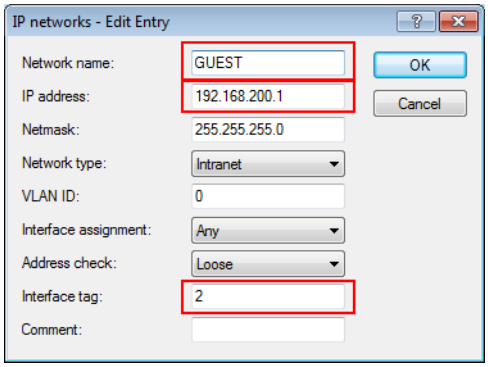
7. For the guest Internet access, create an entry in the list of DSL remote sites with the hold time '9999' and the pre-defined layer 'DHCPOE '. This example assumes that Internet access is provided by a router with DHCP server. In LANconfig you find this setting under **Configuration** > **Communications** > **Remote sites** > **Remote sites**.



8. For internal users, create the IP network 'INTRANET' with (for example) the IP address '192.168.1.100' and the interface tag '1'. For the guest access, create the IP network 'GUEST-ACCESS' with (for example) the IP address of

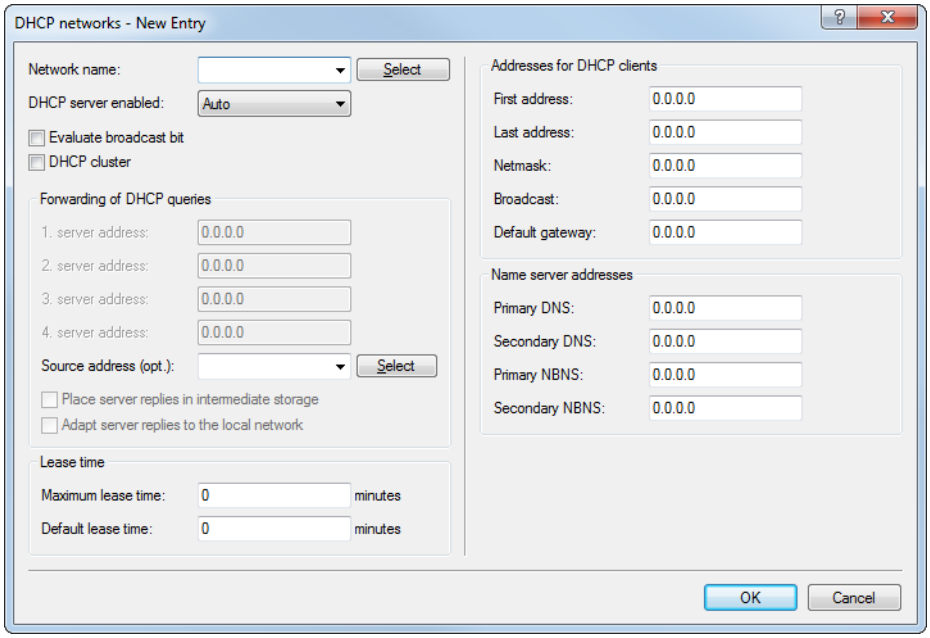
'192.168.200.1' and the interface tag '2'. The virtual router in the WLC uses the interface tags to separate the routes for the two networks. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **General** > **IP networks**.



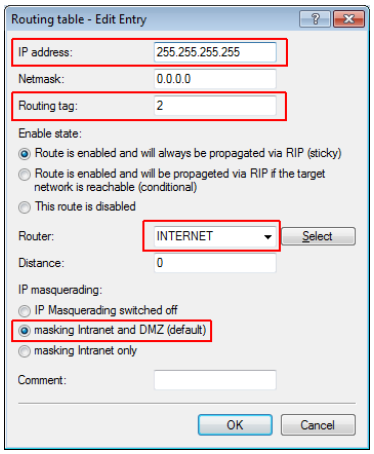


9. The WLC is able to act as a DHCP server for APs and the associated WLAN clients. To set this up, activate the DHCP server for the 'INTRANET' and the 'GUEST-ACCESS'. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **DHCP** > **DHCP networks**.

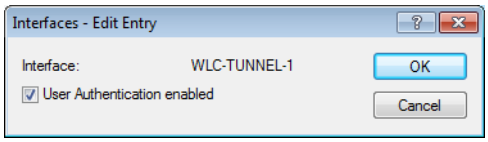
Activation of the DHCP server is obligatory for the guest network and optional for the internal network. There are other ways of realizing a DHCP server for the internal network.



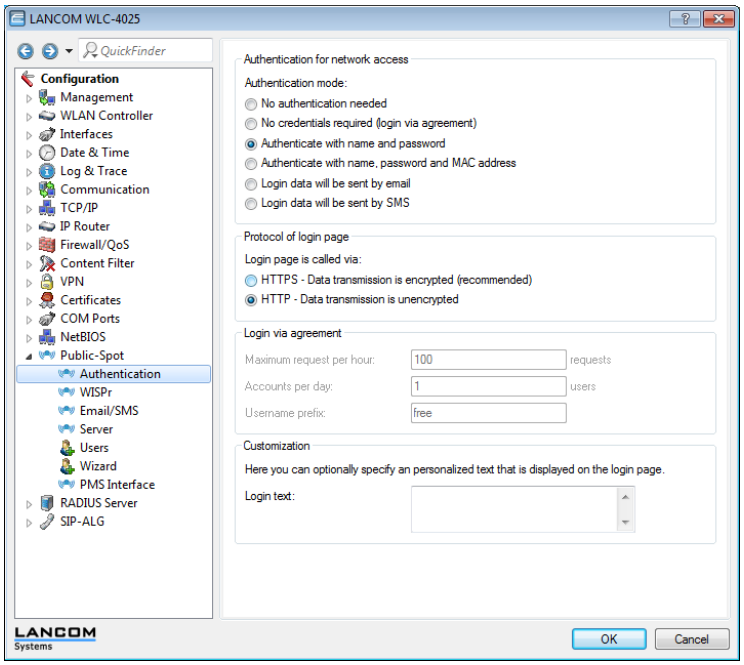
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLC. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under **Configuration** > **IP router** > **Routing** > **Routing table**.



11. Activate the Public Spot user authentication for the logical LAN interface 'WLC-Tunnel-1'. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Server** > **Operational settings** > **Interfaces**.



12. The final step is to enable authentication via the Public Spot for the WLC. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Authentication**.



In addition to configuring the WLC, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

14.4.4 IP-dependent auto configuration and tagging of APs

The easiest way to manage all of the APs that you add to a managed network is to use a flat hierarchy. However, in the largest installations with hundreds of APs across several locations, this type of organization quickly becomes confusing and creates a high level of administrative effort. Setting up **Assignment groups** can help to simplify the management of distributed APs. The WLC can automatically to configure each new AP based on the IP addresses it receives. Manual assignment of an IP parameter profile, a WLAN profile and a Client-steering profile by an administrator is no longer required.

The following describes how an assignment group is used when an unassociated AP registers with a central WLC: After the new APs are installed on site (e.g. at a company or branch network), they try to establish a connection to the specified WLC and obtain a configuration via CAPWAP. The WLC detects the connection requests and, for each new AP, it checks the AP table for a suitable AP profile (e.g., the default profile) and/or whether a suitable assignment group has been defined. If one or more configuration options are available, the WLC checks them for the following states:

1. For a new AP there is an assignment group but no AP profile. In this case, the WLC assigns the profile specified in the assignment group to the new AP.
2. For a new AP there is both an assignment group as well as an AP profile. In this case, the WLC ignores the assignment group and assigns the profile defined in the AP profile to the new AP.
3. For a new AP, there is an AP profile but no assignment group. The behavior is the same as point (2).

If a new AP has neither an AP profile nor an assignment group, the WLC issues an alarm to notify the administrator of the incorrect configuration.

After successful group assignment, the WLC automatically creates an AP profile for every new AP in the access point table. In the **Groups** field, the WLC references the assignment group used when it added the new AP.



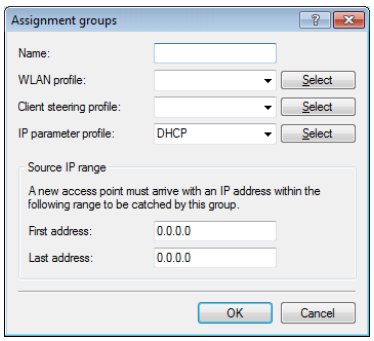
An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups overlap, LCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status** > **WLAN-Management** > **AP-Configuration**.

The group field also gives you the the option of assigning individually definable tags to an AP. For example, these **Tag groups** can be used to act as filter criteria in order for the WLC to restrict the actions it performs to a selection of APs.

14.4.4.1 Setting up assignment groups for IP-dependent auto configuration

The following tutorial shows you how you setup assignment groups on a WLC for the IP-dependent automatic configuration of new APs.

1. Open the configuration dialog for your device and select **WLAN controller** > **AP configuration** > **Assignment groups**
2. Click on **Add** to create a new group.



3. Enter under **Name** a unique descriptor for the assignment group, for example, `Berlin_branch`.
4. Select the **WLAN profile** that the WLC automatically assigns to a new AP if the IP address of the new AP is within the source IP range.

5. Enter the **IP parameter profile** if the new AP should receive a manual network configuration. Otherwise, leave the value as **DHCP**, whereby the AP automatically gets a network configuration from the DHCP server. The DHCP server must be configured to do this.

   If you wish to assign a manual network configuration in which a new AP receives a different IP address, you specify the corresponding address range in the **IP parameter profile** under **Address assignment pool**.

6. **Optional**: Specify a **Client-steering profile** in order to forward future WLAN clients to the ideal AP in case there are several new APs within transmission range.

   If you activate client steering, this must be activated for every AP in the managed infrastructure. Refer to section *Client steering by WLC* on page 1196 for further information on this.

7. Enter the start and end of the **Source IP range** relevant to the assignment group.
   A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.
8. Close all dialog windows with **OK** and save the configuration to your device.

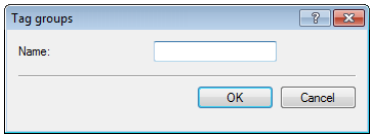
From now on, the WLC assigns the profiles referenced in the assignment groups to all new APs. The LCOS console can now provide you with information about the categorization, see *Overview of CAPWAP parameters with the show command* on page 75.

Please ensure that the access point table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.

14.4.4.2 Setting up tag groups for the detailed selection of APs

The following tutorial shows you how a tag group can be added to an AP configuration on a WLC. To do this, you first create a tag group and then assign it to a WLAN profile.

1. Open the configuration dialog for your device and select **WLAN controller** > **AP configuration** > **Tag groups**
2. Click on **Add** to create a new group.



3. Under **Name** you enter the new tag and save the entry with **OK**.
4. Navigate to the dialog with **WLAN controller** > **AP configuration** > **Access point table**.
5. Select an existing AP profile with **Edit** or add a new one, if necessary.
6. Under **Groups** select the tag group(s) created earlier.
   Multiple tag groups can be specified in a comma-separated list.

   The tag groups are independent of the assignment groups, the assignment of which is specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. The manual allocation of an assignment group has no effect on the AP configuration, which is in line with the state check described under *IP-dependent auto configuration and tagging of APs* on page 1177. The only effects are on the filtering in the command `show capwap group` at the console

   The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

7. Close all dialog windows with **OK** and save the configuration to your device.

From now on the WLC gives the tags in the edited WLAN profile to those APs that received it.

14.5 Access point administration

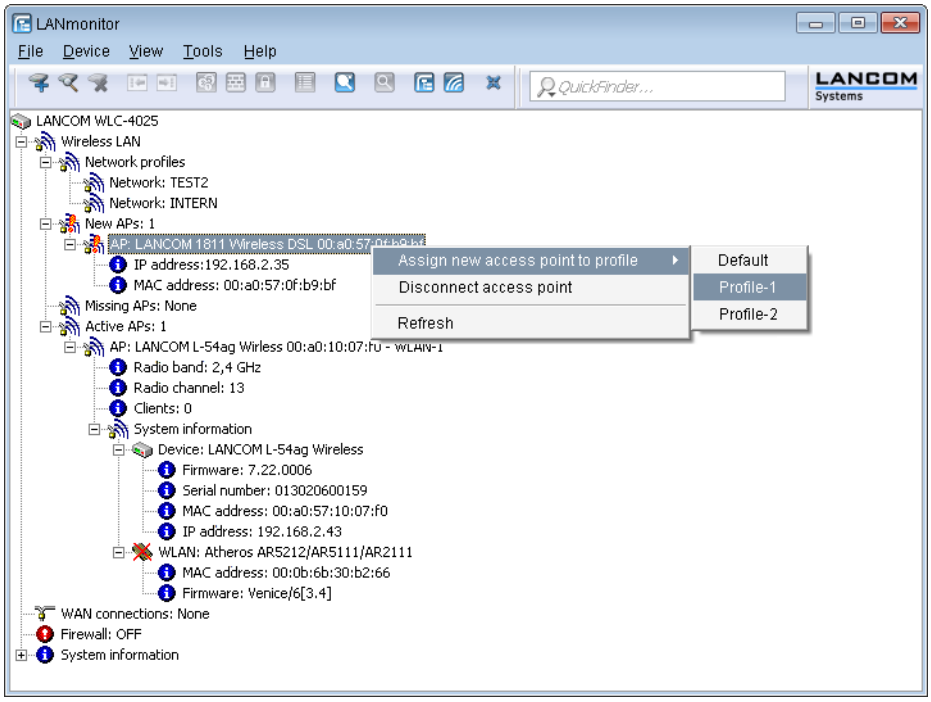
14.5.1 Accepting new access points into the WLAN infrastructure manually

If you prefer not to accept APs into the WLAN infrastructure automatically, you can also manually accept APs.

14.5.1.1 Using LANmonitor to accept access points

It is very easy to accept new APs with LANmonitor. A configuration is selected that will be assigned to the AP after transmission of a new certificate.

In LANmonitor, click on the new AP with the right-hand mouse key. From the context menu that pops up, you select the configuration which is to be assigned to the device.



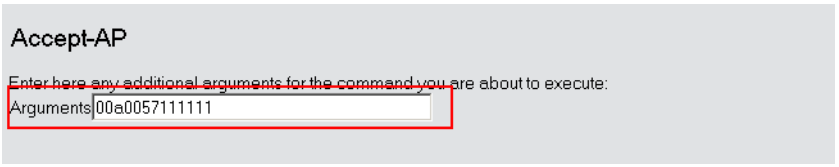
Assignment of the configuration causes the AP to be entered into the AP table in the WLC. It takes a few seconds for the WLC to assign a certificate to the AP and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted AP is briefly signaled as a "Lost AP" by the red Lost AP LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

14.5.1.2 Accepting access points via WEBconfig with provision of a certificate

New APs that do not have a valid certificate but do have an entry in the AP table can be manually accepted with WEBconfig.

1. Open the WLC configuration with WEBconfig.
2. Under **Extras** > **LCOS menu tree** > **Setup** > **WLAN-Management** select the action **Accept AP**.

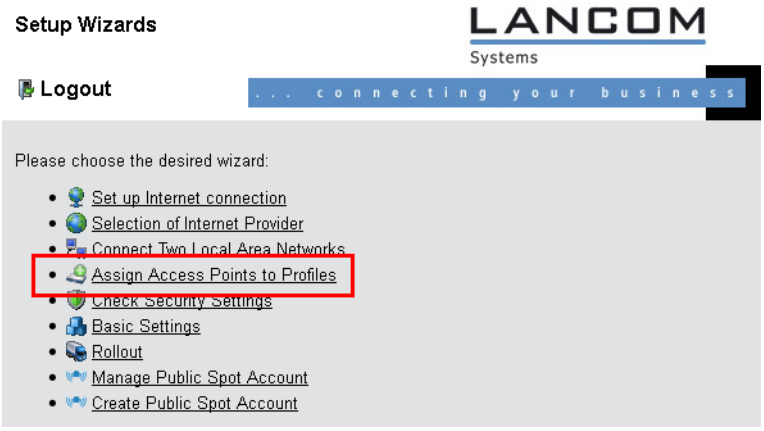
3. When requested for additional arguments, enter the MAC address of the AP to be accepted and confirm with **Execute**.



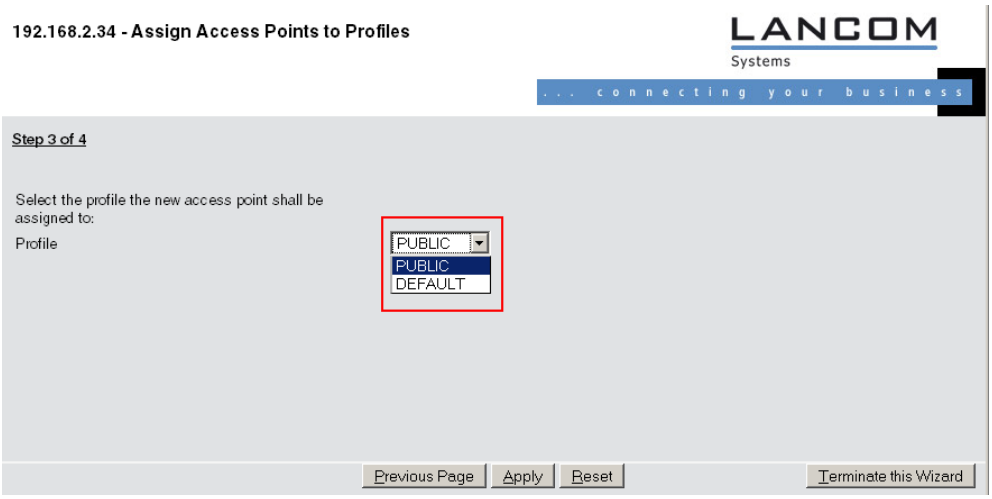
14.5.1.3 Accepting access points via WEBconfig with provision of a certificate and configuration

New APs that do not have a valid certificate and do not have an entry in the AP table can be manually accepted by means of a wizard in WEBconfig. A configuration is selected that will be assigned to the AP after transmission of a new certificate.

1. Open the WLC configuration with WEBconfig. Click on **Setup Wizards** and select the wizard **Assign access points to profiles**.



2. Click on the link to start the wizard. Select the desired AP by means of its MAC address and choose the WLAN configuration that is to be assigned to it.



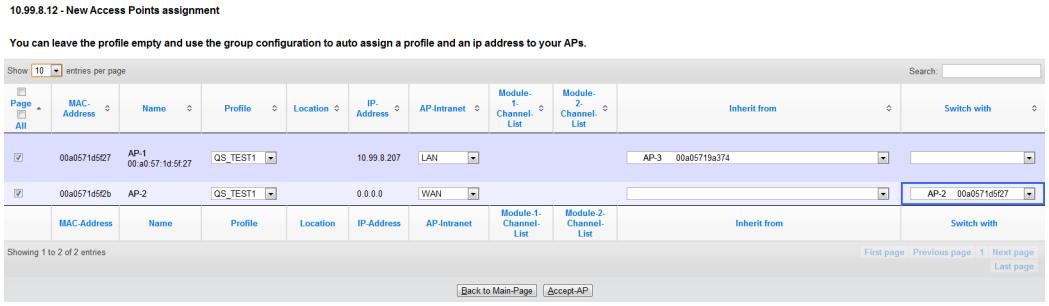
Assignment of the configuration causes the AP to be entered into the AP table in the WLAN controller. It takes a few seconds for the WLC to assign a certificate to the AP and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted AP is briefly signaled as a "Lost AP" by

the red "Lost AP" LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

14.5.1.4 Adding new APs with the WEBconfig Setup Wizard

As of LCOS 9.00, WLCs have a revised Setup Wizard **Assign Access Points to Profiles**, which makes it easier to add new APs via WEBconfig. Just a few mouse clicks with the new Setup Wizard allows you to

- Make a targeted search for a new AP;
- Accept one or more new APs at the same time;
- Assign a WLAN profile or a channel list to a new AP;
- Allow a new AP to inherit the configuration from an accepted AP;
- To exchange the configuration in a new AP for that of an accepted missing AP. When exchanging a configuration, the new AP receives the complete configuration of the accepted missing AP (except for its MAC address). When the new AP has been integrated, the WLC then deletes the configuration of the accepted missing AP.



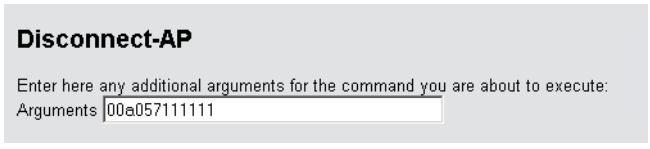
Click **Accept AP** to include the new AP with its new settings into the network.

If you have allowed an AP to be configured via assignment groups, there is no need for any further settings for this AP in the Setup Wizard. The WLC automatically assigns the settings for the appropriate groups to the AP.

14.5.2 Manually removing access points from the WLAN infrastructure

The following actions are required to remove an AP under management of the WLC from the WLAN infrastructure:

1. In the AP, switch the WLAN operating mode of the WLAN module from 'Managed' to 'Client' or 'Access Point'.
2. In the WLAN controller, delete the configuration for the AP and/or deactivate **Automatically provide APs with a default configuration** via **Extras** > **LCOS menu tree** > **Setup** > **WLAN-Management** > **Autoaccept-AP**.
3. Disconnect the AP in WEBconfig by selecting **Extras** > **LCOS menu tree** > **Setup** > **WLAN-Management** and the action **Disconnect AP**, or alternatively in LANmonitor.
4. When requested for additional arguments, enter the MAC address of the AP to be disconnected and confirm with **Execute**.



14.5.3 Deactivating access points or permanently removing them from the WLAN infrastructure

Occasionally it is necessary to temporarily deactivate or even permanently remove a WLC-managed AP.

14.5.3.1 Deactivating an access point

To deactivate an AP, set its corresponding entry in the AP table to 'inactive' or delete the entry from the table. In the AP, the WLAN modules in managed mode are switched off and the corresponding SSIDs are deleted.

The WLAN modules and the WLAN networks (SSIDs) are still switched off even if standalone operation is activated.

An AP deactivated in this way remains connected to the WLC and the certificates are retained. The WLC can reactivate the AP and its managed-mode WLAN modules at any time simply by activating the entry in the AP table or by making a new entry in the AP table along with the appropriate MAC address.

If the connection to a deactivated AP is broken (either unintentionally due to a failure or intentionally by the administrator) then the AP begins a new search for a suitable WLC. Although the former WLC can check the validity of the certificate, due to the fact that there is no (active) entry in the AP table the AP treats it as a secondary WLC. If the AP finds a primary WLC then it will register with it.

14.5.3.2 Permanently removing an access point from the WLAN infrastructure

In order to permanently remove an AP from a centrally managed WLAN infrastructure, the certificates in the SCEP client have to be either deleted or revoked.

- If you have access to the AP, the certificates are quickly deleted by resetting the device.
- If the device has been stolen and consequently needs to be removed from the WLAN infrastructure, then the certificates in the WLC's CA have to be revoked. This is done in WEBconfig by navigating to **Extras** > **LCOS menu tree** > **Status** > **Certificates** > **SCEP-CA** > **Certificates** and accessing the **Certificate status table**. Here you delete the certificate for the MAC address of the APs which are to be removed from the WLAN infrastructure. The certificates are not actually deleted, but they are marked as expired.

In case of a backup solution featuring redundant WLCs, the certificates have to be revoked in all of the WLCs!

14.6 Central firmware and script management

WLCs allow the configurations of multiple LANCOM WLAN routers and APs to be managed from a central location in a consistent and convenient manner. With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

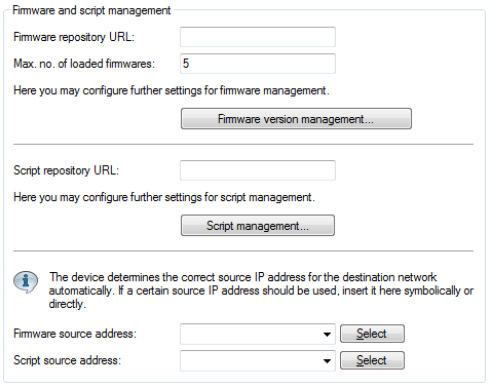
To achieve this, the firmware and script files are stored on a Web server (firmware as *.upx files, scripts and *.lcs files). The WLC checks once daily, or when prompted by a user, to compare the available files with those on the devices. Alternatively, this procedure can be handled by a cron job—overnight, for example. If an update can be carried out, or if the AP is not running the desired firmware version, then the WLC downloads the file from the Web server and uploads it to the appropriate WLAN routers and APs.

The configuration of firmware and script management provides precise control over the distribution of the files. It is possible, for example, to limit certain firmware versions to certain device types or MAC addresses.

An update can be carried out in two possible states:

- When a connection is established; the AP subsequently restarts automatically.
- If the AP is already connected, the device does not restart automatically. In this case the AP is manually restarted with the menu action **Setup** > **WLAN-Management** > **Central-Firmware-Management** > **Reboot-updated-APs** or by a timed cron job.

› The action **Setup** > **WLAN-Management** > **Central-Firmware-Management** > **Update-Firmware-and-Script-Information** updates the script and firmware directories.



The parameters for configuration can be found under the following paths:

LANconfig: **WLAN controller** > **AP update**

WEBconfig: **Setup** > **WLAN-Management** > **Central-Firmware-Management**

14.6.1 General settings for firmware management

› **Firmware-URL**

The path to the directory with the firmware files.

› Possible values: URL in the form `Server/Directory` or `http://Server/Directory`

› Default: Blank

Note that the Web server specified must permit directory listing. The firmware management uses this to retrieve information about the available firmware.

› **Simultaneously loaded FW**

The number of firmware versions loaded simultaneously into the main memory of the WLC.

The firmware versions stored here are downloaded from the server just once and then used for all update processes.

› Possible values: 1 to 10

› Default: 5

› **Firmware loopback address**

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

Default:

› Empty

If the list of IP networks or loopback addresses contains an entry named “INT” or “DMZ”, the associated IP address of the IP network or the loopback address named “INT” or “DMZ” is used.

14.6.1.1 Firmware management table

This table is used to store information about which firmware versions are to be operated with which devices (MAC address) and device types.

Device types

Select here the type of device that the firmware version specified here is to be used for.

- Possible values: All or a selection from the list of available devices.
- Default: All

MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

- Possible values: Valid MAC address
- Default: Blank

Version

Firmware version to be used for the devices or device types specified in this entry. If necessary, an update for the specified devices or device types will be made to this firmware version. This is stated in the form: "xx.yy", e.g. 10.40. Default: Blank

Date

The date allows you to downgrade to a specific firmware version within a release, for example from a Release Upgrade (RU) on an earlier upgrade.

- Possible values: 8 characters from 0123456789. The entry must match the format of the UPX header, e.g. "01092014" for the September 01, 2014.
- Default: Blank

14.6.1.2 General settings for script management

- **Script URL**

  The path to the directory with the script files.

  Possible values:

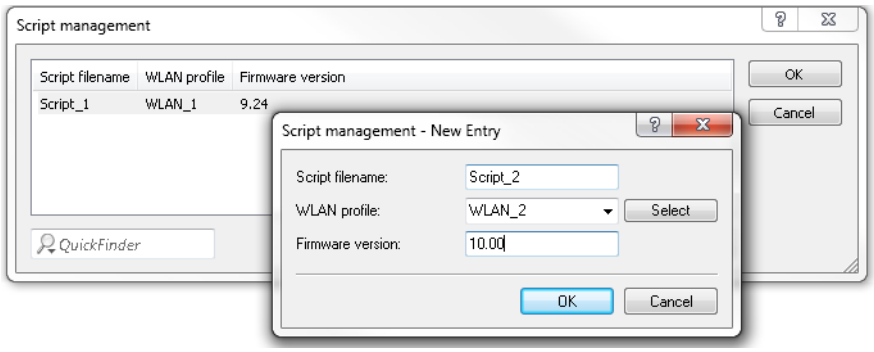
  - URL in the form `Server/Directory` or `http://Server/Directory`
  - Default: Blank

14.6.1.3 Script management table

In this table, scripts are assigned to a WLAN profile depending on the name of the script file.

Configuring a WLAN router and Access Point in the Managed mode is handled via WLAN profiles. A script can be used for setting those detailed parameters in managed devices that are not handled by the pre-defined parameters in a WLAN profile. Distribution is also handled by WLAN profiles to ensure that the wireless routers and APs with the same WLC configuration also use the same script.

As only one script file can be defined per WLAN profile, versioning is not possible here. However, when distributing a script to a wireless router or Access Point, an MD5 checksum of the script file is saved. This checksum allows the WLC to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.



Script filename

Enter the CAPWAP slot you selected for the script upload to the WLAN controller (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs). If the WLAN controller obtains the script from a web server, the script name on the web server has to be entered. Possible values: File name in the form `*.lcs`. Default: Blank.

WLAN profile

Select here the WLAN profile that the script file specified here should be used for. Possible values: Selection from the list of defined WLAN profiles. Default: Blank

Firmware version

By specifying a firmware version, you determine the LCOS version set in the script that is rolled out.

Please enter the firmware version in the form “xx.yy”, e.g. 10.00 or 9.24.

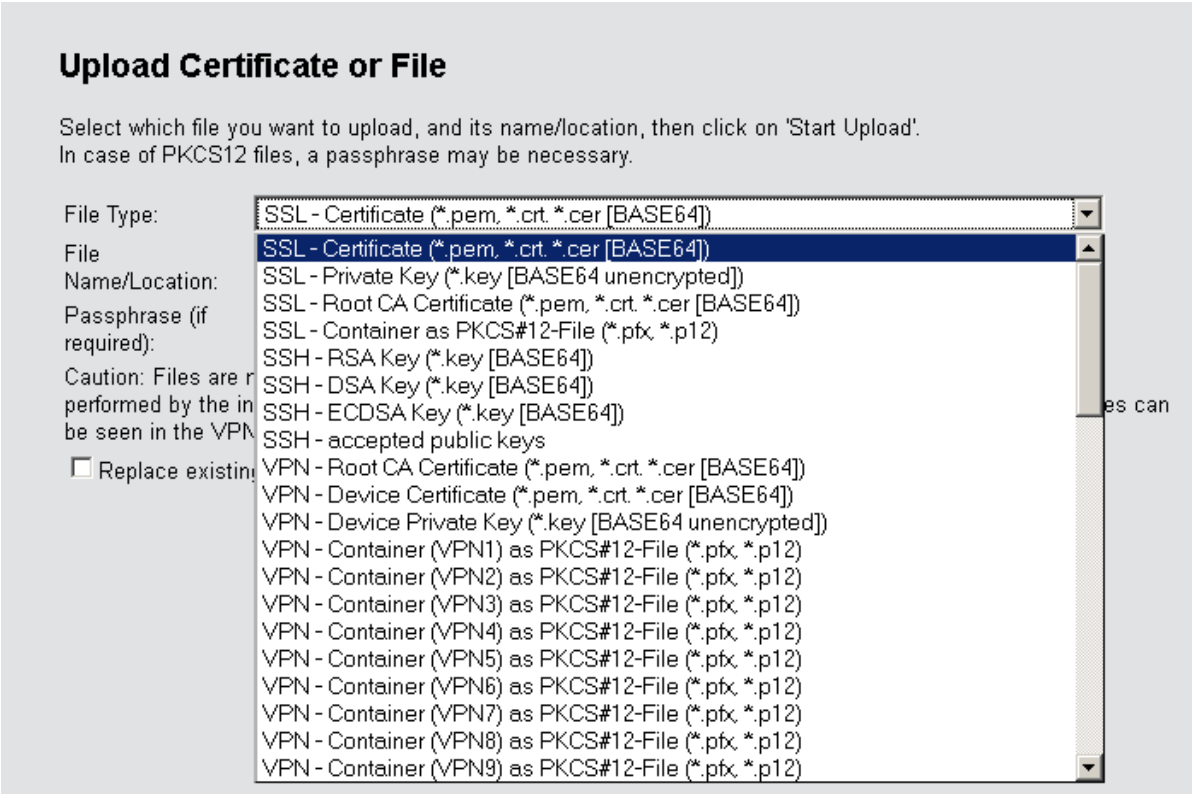
14.6.1.4 Internal script storage (script management without HTTP server)

In contrast to firmware files, script files are very small. The WLC's internal script storage allows the storage of up to three scripts of up to 64KB each. If script requirements do not exceed this volume, an HTTP server does not need to be configured for this purpose.

Script files are simply loaded from the designated storage location using WEBconfig. After upload, the list of available scripts must be updated with **Setup** > **WLAN-Management** > **Central-Firmware-Management** > **Update Firmware and Script Information**.

The internal scripts can be referenced from the script management table using the relevant names (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs).

Please be careful with upper and lower case letters when entering script names.



14.7 RADIUS

RADIUS stands for “Remote Authentication Dial-In User Service” and is referred to as a “triple-A protocol”. The three “A”s stand for

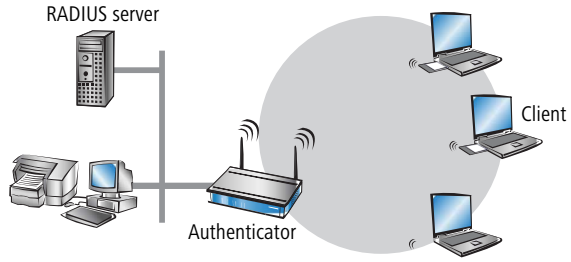
- Authentication
- Authorization
- Accounting (billing)

This protocol allow you to grant users access to a network, to assign them certain rights and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

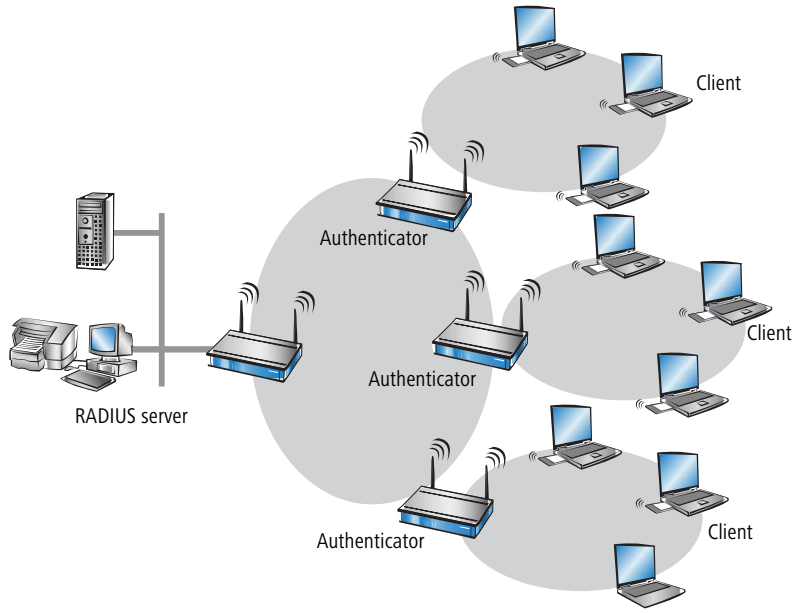
3 different devices are required for RADIUS to work.

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.

- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by an access point, for example. The authenticator is referred to as the Network Access Server (NAS).



- Authentication server: RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of an access point for this task.



The authenticator has no initial information on the clients wanting to register. This is all stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database there and can vary from network to network. The authenticator has just the one task, that of transferring the information between the client and the RADIUS server.

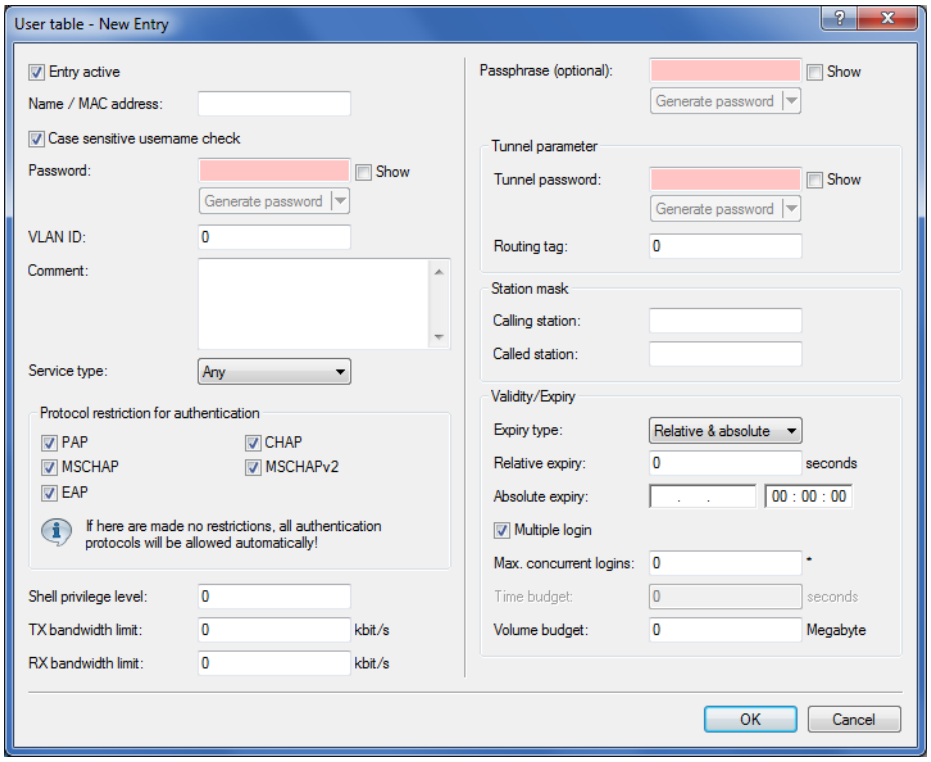
Access to a RADIUS server can be configured in several ways:

- Using PPP when dialing into a network
- Via WLAN
- Via a public spot for users who register using a browser
- Via the 802.1X protocol

14.7.1 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to authenticate WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal user table in the WLC.

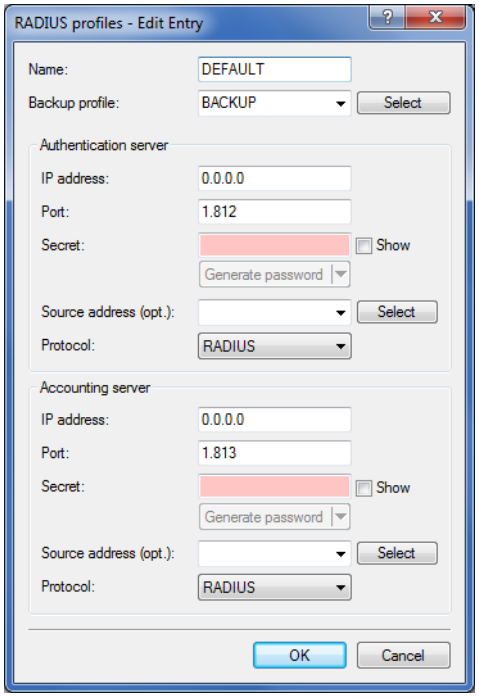
In LANconfig enter the approved MAC addresses into the RADIUS database in the configuration section **RADIUS** > **Server** on the **General** tab. Enter the MAC address as **Name** and as **Password** and select the authentication method **All**.



14.7.2 External RADIUS server

By default the WLC forwards account and access management requests to a RADIUS server. In order for APs to contact the RADIUS server directly, the necessary server information has to be specified here. This ensures that the RADIUS application continues to function even if the WLC is unavailable. However, this means that the RADIUS server requires

settings for each and every AP, and the managed APs must be able to access the RADIUS server from their management network. If the RADIUS server is on another IP network, then it is vital that the gateway is set in the IP parameter profile.



LANconfig: **WLAN controller** > **Profiles** > **RADIUS profiles**

Name

Specify an identifier for this entry.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

Authentication server

IP address

Enter the IP address of authentication server.

Port

Enter the port used by the authentication server.

Secret

This entry contains the shared secret used for authorization.

Show

Enables / disables the display of the key.

Source address (optional)

Enter the loopback address of the device, where applicable.

Protocol

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Accounting server

IP address

Enter the IP address of accounting server.

Port

Enter the port used by the accounting server.

Secret

This entry contains the shared secret used for authorization.

Show

Enables / disables the display of the key.

Source address (optional)

Enter the loopback address of the device, where applicable.

Protocol

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

14.7.3 Dynamic VLAN assignment

Larger WLAN infrastructures often require individual WLAN clients to be assigned to certain networks. Assuming that the WLAN clients are always within range of the same APs, then assignment can be realized via the SSID in connection with a particular IP network. If on the other hand the WLAN clients frequently change their position and logon to different APs then, depending on the configuration, they may find themselves in a different IP network.

For WLAN clients to remain within a certain network **independent** of their current WLAN network, dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID, in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

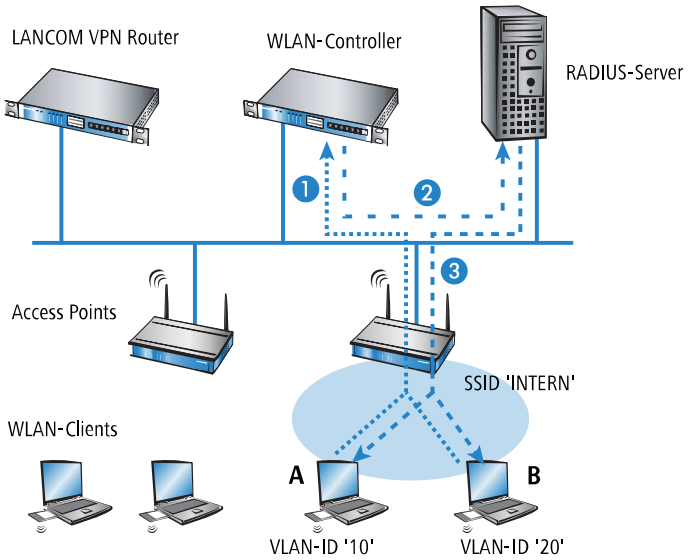
Example:

- The WLAN clients of two employees log into an AP in the WPA2-secured network with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the AP. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests are automatically forwarded to the WLC. This forwards the request in turn to the defined RADIUS server. The RADIUS server can check the access rights of the WLAN clients. It can also use the MAC address to assign a certain VLAN ID, for example for a certain department. The WLAN client in Marketing, for example, receives the VLAN ID '10' and WLAN client from Research & Development receives '20'. If no VLAN ID is specified for the user, the SSID's primary VLAN ID is used.
- The WLAN clients of the guests log into the same AP in the unsecured network with the SSID 'PUBLIC'. This SSID is statically bound to the VLAN ID '99' and leads the guests into a certain network. Static and dynamic VLAN assignment can be elegantly operated in parallel.



Assignment of the VLAN ID by the RADIUS server can be controlled by other criteria, such as a combination of user name and password, for example. In this way the unknown MAC address of a visitor to a company can be assigned a VLAN ID that permits guest access for Internet access only, for example, but that prohibits access to other network resources.

As an alternative to an external RADIUS server, WLAN clients can be assigned with a VLAN ID via the internal RADIUS server or the stations table in the WLC.



1. Activate VLAN tagging for the WLC. This is done in the physical parameters of the profile by entering a value greater than '0' for the management VLAN ID.
2. For authentication via 802.1x, go to the encryption settings for the profile's logical WLAN network and choose a setting that triggers an authentication request.
3. To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

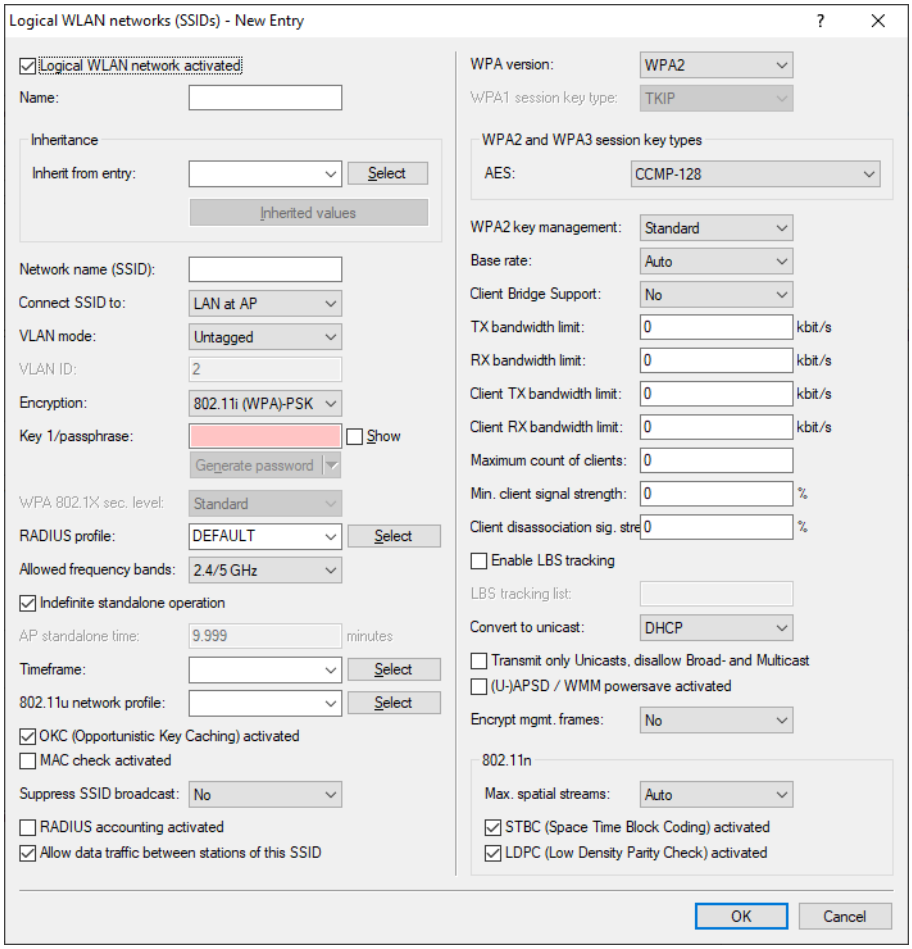
   For the management of WLAN modules with a WLC, a RADIUS server is required to operate authentication via 802.1x and MAC-address checks. The WLC automatically defines itself as the RADIUS server in the APs that it is managing—all RADIUS requests sent to the AP are then directly forwarded to the WLC, which can either process the requests itself or forward them to an external RADIUS server.
4. To forward RADIUS requests to another RADIUS server, use LANconfig to enter its address into the list of forwarding servers in the configuration section 'RADIUS servers' on the **Forwarding** tab. Alternatively, external RADIUS servers can be entered in WEBconfig under **Menu tree** > **LCOS Setup** > **RADIUS** > **Server** > **Forward servers**. Also, set the standard realm and the empty realm to be able to react to different types of user information (with an unknown realm, or even without a realm).
5. Configure the entries in the RADIUS server so that WLAN clients placing requests will be assigned the appropriate VLAN IDs as based on the identification of certain characteristics.

Further information about RADIUS is available in the documentation for your RADIUS server.

14.7.4 Activating RADIUS accounting for logical WLANs in the WLAN controller

The configuration for logical WLAN networks is to be found in the following menu:

LANconfig: **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**



RADIUS accounting activated

This is where you can activate RADIUS accounting for this logical WLAN network.

Possible values:

› Yes, No

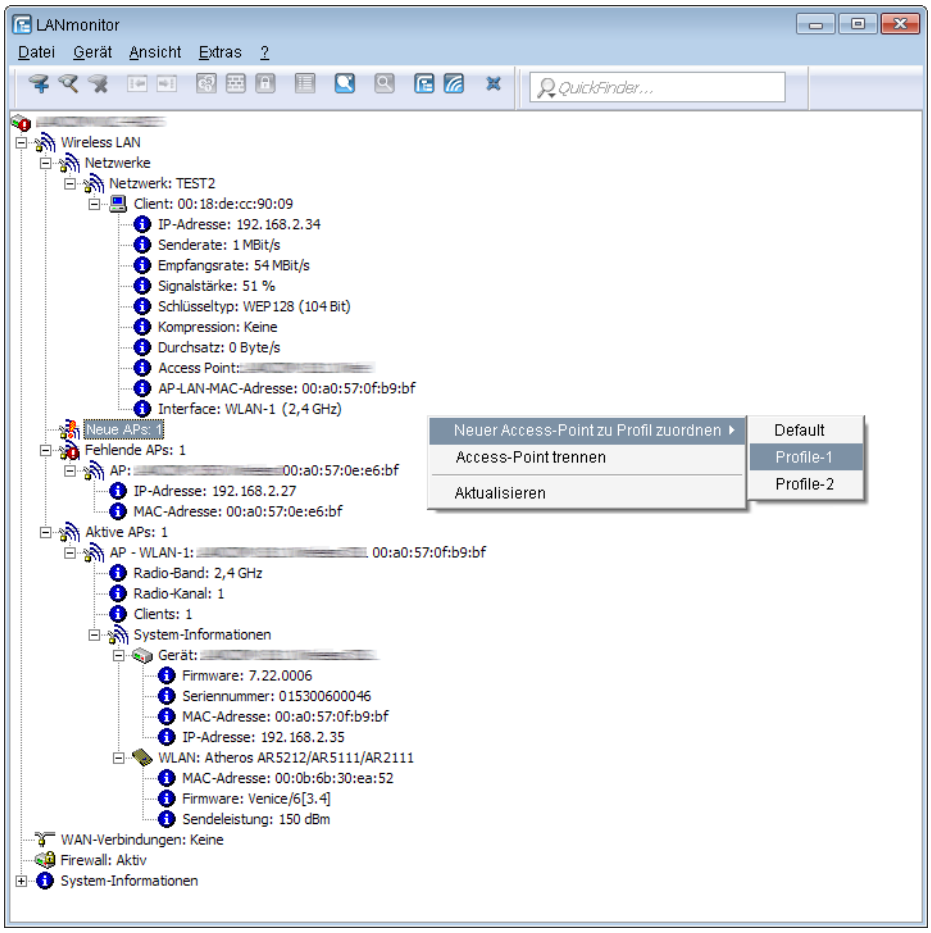
Default:

› No

The APs supporting the logical WLAN network as configured by the WLC must have a LCOS version 8.00 or higher.

14.8 Displays and commands in LANmonitor

LANmonitor gives you a quick overview of the WLCs in your network and the APs within the WLAN infrastructure. LANmonitor displays the following information, among other things:



- Active WLAN networks with the logged-in WLAN clients and the descriptor of the APs that they are associated with.
- Display of new APs with IP and MAC address
- Display of missing APs with IP and MAC address
- Display of managed APs with IP and MAC address, the utilized frequency band, and the channel

> For APs with an older firmware version and unable to transmit this data, the WLC takes the channel and frequency information from the **Active radios** status table under **Status** > **Active-Radios** > **WLAN-Management** > **AP-Status**.

Using the right-hand mouse key, a context menu can be opened for the APs and the following commands are available:

- **Assign new access point to profile**

  Enables a new AP to be allocated to a profile and accepted into the WLAN infrastructure.

- **Disconnect access point**

  Terminates the connection between AP and WLC. The AP then carries out a new search for a suitable WLC. This command can be used after a backup event to disconnect APs from a backup WLC and to redirect them to the correct WLC.

- **Refresh display**

Updates LANmonitor's display.

14.9 RF optimization

Selecting the channel from the channel list defines a portion of the frequency band that an AP uses for its logical wireless LANs. All WLAN clients that need to connect to an AP have to use the same channel on the same frequency band. The 2.4-GHz band works with channels 1 to 13 (depending on the country) and the 5-GHz band works with channels 36 to 64. On each of these channels, only one AP can actually transfer data. In order to operate another AP within radio range with maximum bandwidth, the AP must make use of a separate channel—otherwise all of the participating WLANs have to share the channel's bandwidth.

With a completely empty channel list, the APs could automatically select channels which overlap in some areas, so reducing signal quality. Similarly, the APs might select channels which the WLAN clients cannot use due to the country settings. To steer APs towards certain channels, the non-overlapping channels 1, 6, 11 can be activated in the channels list.

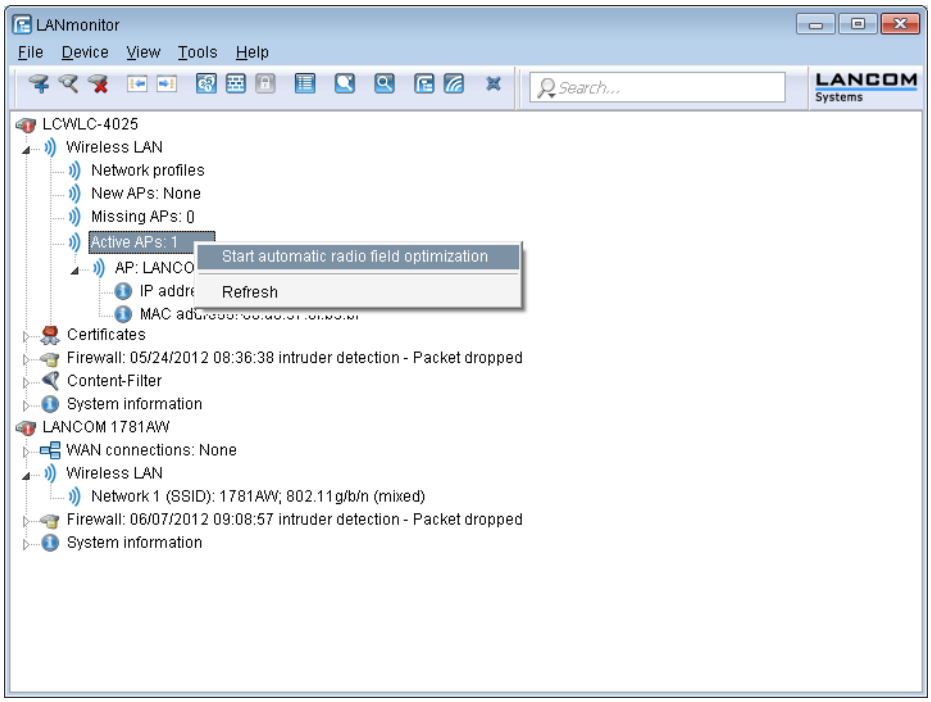
In larger installations with several APs it can be difficult to set a channel for every AP. With automatic radio-field (RF) optimization, the WLCs provide an automatic method of setting the optimum channels for APs that work in the 2.4-GHz band and 5-GHz band.

You should ensure that APs transmitting in the 5-GHz band are set to the "indoor only" mode.

Command line: **Setup** > **WLAN-Management** > **Start-automatic-radio-field-optimization**

You can invoke optimization for a particular AP by entering its MAC address as a parameter for the action.

LANmonitor: Right-click on the list of active APs or on a specific device, and in the context menu select **Start automatic RF optimization**.



Optimization is then carried out in the following stages:

1. The WLC assigns the same channel to all APs. The selected channel is the one being used by the majority of APs.
2. The APs carry out a background scan and report the results to the WLC.
3. Based on the devices found by the background scan, the WLC sets an interference value for each AP.
4. It then deletes the AP channel list for all APs. With the channel list now empty, each AP receives a configuration update with a new channel list for its respective profile.
5. The WLC disables the radio modules of all APs.
6. The individual APs now go through the following sequence. This begins with the AP with the highest interference value being the first to select a channel.
7. In the order of the interference values the WLC enables the radio modules in the APs, which then start their automatic calibration. Each AP automatically searches for the best channel from the channel list assigned to it. To determine which channel is the best, the AP scans for interference in order to allow for the signal strengths and channels occupied by other APs. Because the former list in the WLC configuration was deleted, this is now the profile channel list. If the profile channel list is empty, then the AP has freedom of choice from the channels that are not occupied by other radio modules. The selected channel is then communicated back to the WLC and entered into the AP channel list there. For this reason, the AP receives the same channel the next time a connection is established. The AP channel list has a higher weighting than the profile channel list.



If an AP has multiple radio modules, each module goes through this process in succession.



Radio-field optimization is a component of the *LANCOM Active Radio Control (ARC)*.

14.9.1 Group-related radio field optimization

A WLC allows the grouping of APs by location information, device properties or network structure. This grouping can also be used as a basis for radio field optimization. Instead of performing a radio field optimization either for all APs or just for one of them, you can address all of the APs within a building tract, with a particular name, or with a particular firmware version.

Groups can be addressed via WEBconfig and also via the console by means of the Group parameters:

```
do /Setup/WLAN-Management/start optimization <Group>
```

The APs can be filtered with the following group-parameter options:

`-g <Group name>`

APs, which belong to the group. Multiple group names can be separated by commas.

`-l <Location>`

APs with the corresponding location setting.



The combination of `-l` and one of the location options `-c` to `-r` is not useful.

`-c <Country>`

APs with the corresponding country setting.

`-i <City>`

APs with the corresponding city setting.

`-s <Street>`

APs with the corresponding street setting.

-b <Building>

APs with the corresponding building setting.

-f <Floor>

APs with the corresponding floor setting.

-r <Room>

APs with the corresponding room setting.

-d <Device name>

APs with the corresponding device name.

-a <Antenna>

APs with the corresponding number of antennas.

A combination of the options `-d` and `-a` is not useful.

-v <Firmware>

APs with this firmware version only.

-x <Firmware>

APs with a firmware version less than that specified here.

-y <Firmware>

APs with a firmware version less than or equal to that specified here.

-z <Firmware>

APs with a firmware version greater than that specified here.

-t <Firmware>

APs with a firmware version greater than or equal to that specified here.

Combinations are possible, e.g. to address APs with a firmware version between two versions.

-n <Intranet-Address>

APs located on the intranet with the address specified here.

-p <Profile name>

APs included in the WLAN profile specified here.

14.10 Client steering by WLC

With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLC. Managed APs constantly report the current values to the WLC, which uses these criteria to decide which APs may respond to requests from WLAN clients. For this reason, client steering is only possible with APs that are centrally managed by a WLC.

In managed networks a WLC centralizes the client steering for all connected APs. In this case, client steering works as follows:

1. The WLC collects the data about the associated WLAN clients from the APs connected to it. These data are the basis for the WLC to control the client steering.
2. All APs are configured so that client steering is handled by the WLC.
3. An unassociated WLAN client sends a probe request to the APs within its range.
4. Using CAPWAP, the APs transmit the request and the signal strength of the WLAN client to the WLC.
5. For each AP within range of the WLAN client, the WLC calculates a value from three factors:
   - Signal strength value
   - A value calculated from the number of clients associated at the AP
   - Frequency band value

   The WLC weights these factors and multiplies them together to derive the final value.
6. APs with the highest value, or a value that deviates from it within a specified tolerance level, receive a message from the WLC that they may accept the WLAN client at the next login attempt.
7. WLAN clients attempting to connect to an AP before it has received the response from the WLC are rejected.
8. If a WLAN client is acting "sticky", i.e. it does not attempt to connect to another AP with a good connection quality even though its current connection is of a lower quality, the WLC can prompt the current AP to log off the WLAN client. The WLAN client is then forced to connect with the AP offering the better connection.

If an AP loses connection to the WLC which is responsible for client steering, the AP accepts all connections from authenticated WLAN clients.

In order to optimize managed client steering, all APs require the installation of LCOS9.00 or later. If you have mixed operations with APs using earlier versions of LCOS, your WLAN will not be capable of optimizing the distribution of clients.

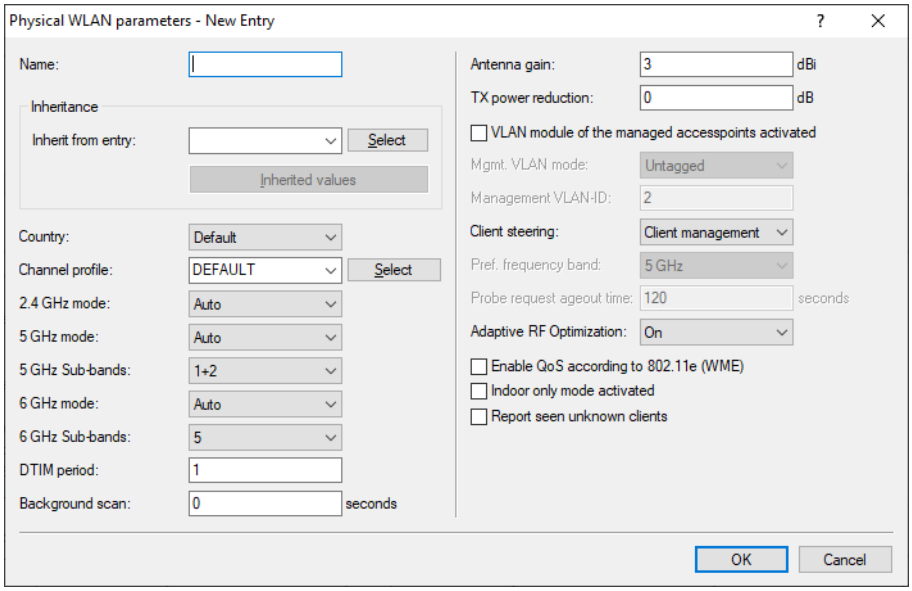
In scenarios with time-critical roaming, such as with VoIP phones, you should not use client steering, as this can delay the client's login process.

14.10.1 Configuration

You configure client steering with LANconfig as follows:

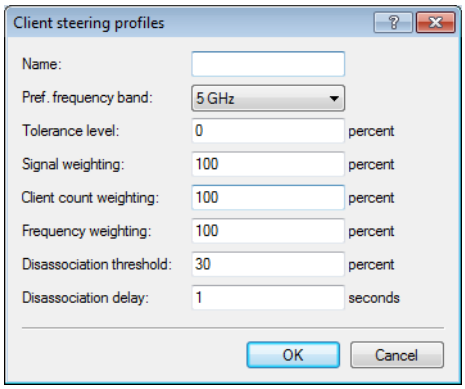
1. First, in the WLC you activate client steering for an AP under **WLAN controller** > **Profiles** > **Physical WLAN parameters** using the selection list **Client steering**.
   - **Off**: Client steering is deactivated.
   - **AP-based band steering**: The AP independently steers the WLAN client to a preferred frequency band.

› **On**: The AP lets the WLC handle the client steering.



2. The menu **WLAN-Controller** > **AP-Configuration** > **Client steering profiles** contains two preconfigured default profiles (high density, default), which are sufficient for most use cases. Optionally, you create a new client steering profile by clicking on **Add**.

   Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.



The items have the following meanings:

Name

Name of the client-steering profile.

Pref. Frequency band

Specifies the frequency band to which the WLC steers the WLAN client.

› **2.4GHz**: The WLC steers the WLAN client to the 2.4-GHz frequency band.
› **5GHz**: The WLC steers the WLAN client to the 5-GHz frequency band.

Tolerance level

The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

Signal-Strength-Weighting

Specifies the percentage weighting of the signal-strength value used to calculate the final value.

Associated-Clients-Weighting

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Frequency-Band-Weighting

Specifies the percent weighting of the value for the frequency band used to calculate the final value.

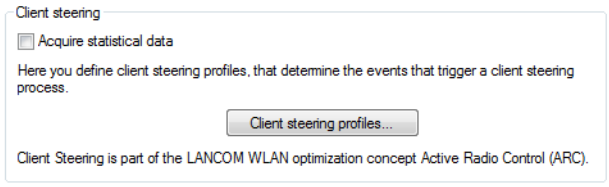
Disassociation threshold

Specifies the percentage of the maximum signal strength. If the current signal strength falls below this value, the client is disconnected.

Disassociation delay

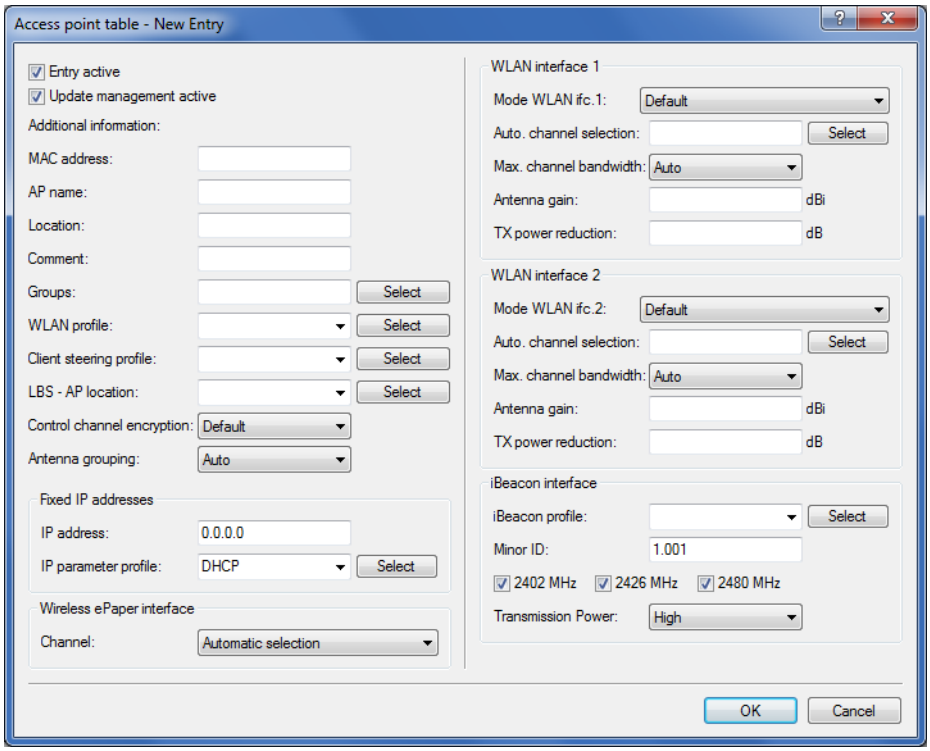
Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

3. Optional: Enable the capture of client-steering statistics with the parameter **Acquire statistical data**. This statistical data is suitable for analysis by LANmonitor, for example.

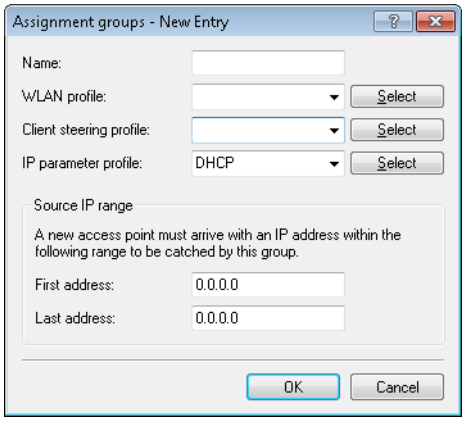


Statistics capture increases the load on the WLC. LANCOM does not recommend the permanent recording of statistics.

4. Now assign one of the client-steering profiles to the corresponding AP in the AP table under **WLAN controller** > **AP configuration** > **Access point table**.



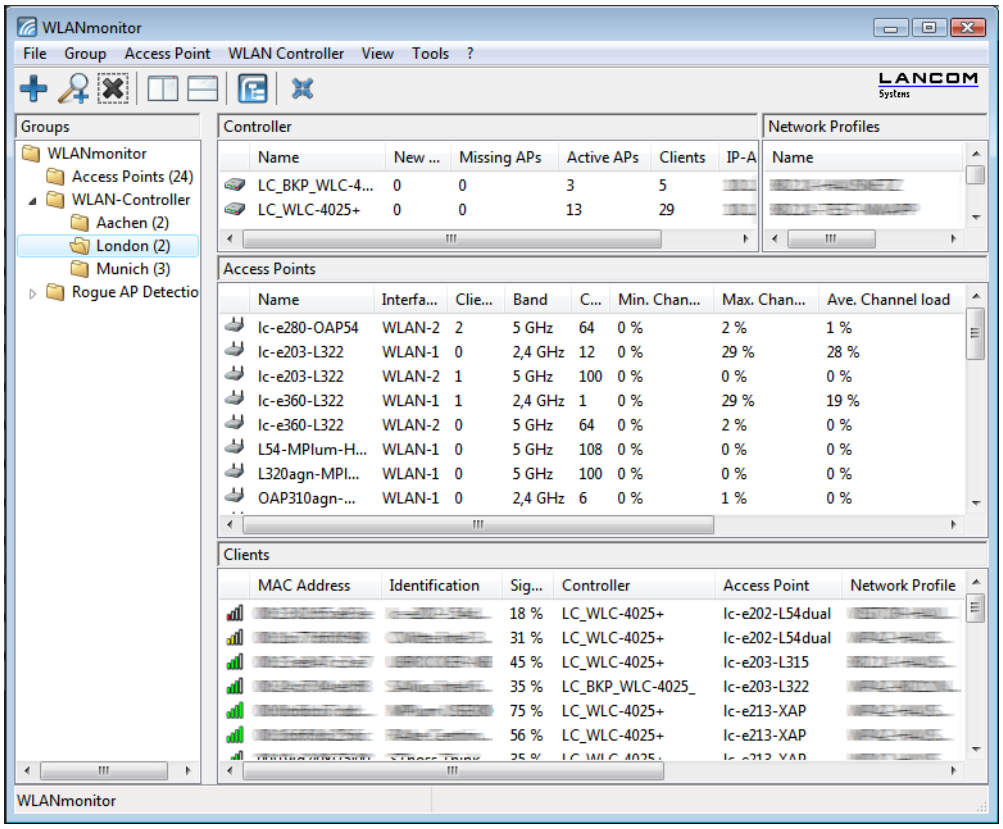
5. Optional: If necessary, assign a suitable client-steering group to the defined assignment groups.



You have now completed the configuration of the client steering.

14.11 Channel-load display in WLC mode

The loads on the various channels used by each AP which is managed by a WLC are displayed as three values, the minimum, maximum and average channel load. The values displayed are measured every three minutes. Consequently, the first values are displayed after three minutes at the earliest.



14.12 Backing up the certificates

At system startup, a WLC generates the basic certificates for the assignment of certificates to the APs, including the root certificates for the CA (Certification Authority) and the RA (Registration Authority). Based on these two certificates, the WLC issues device certificates for the APs.

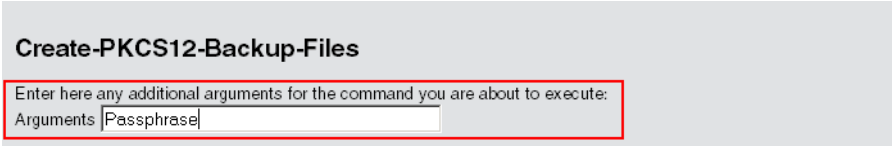
If multiple WLCs are employed in parallel in the same WLAN infrastructure (for load balancing) or if a device is being replaced or reconfigured, the same root certificates should always be used to avoid problems operating the managed APs.

14.12.1 Create backups of the certificates

To restore the CA or RA, the relevant root certificates with private keys will be required as generated automatically when the WLC was started. Furthermore the following files with information on issued device certificates should also be backed up. To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PCKS12 container.

WEBconfig

1. Open the configuration of the WLC in WEBconfig and go to **Extras** > **LCOS menu tree** > **Setup** > **Certificates** > **SCEP-CA** > **CA-certificates**.
2. Select the command **Create PKCS12 backup files** and enter the passphrase for the PKCS12 container as the additional argument.

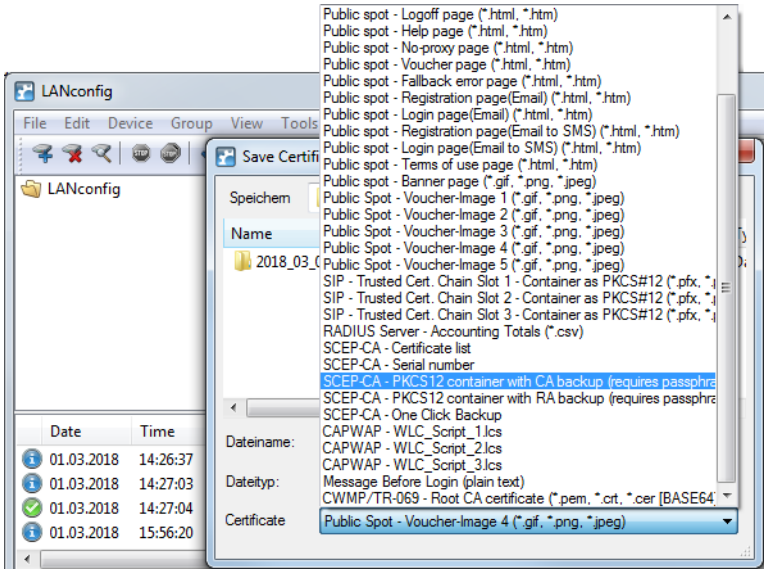


This command backs up the certificates and private keys to the PKCS12 files and these can then be downloaded from the device.

LANconfig

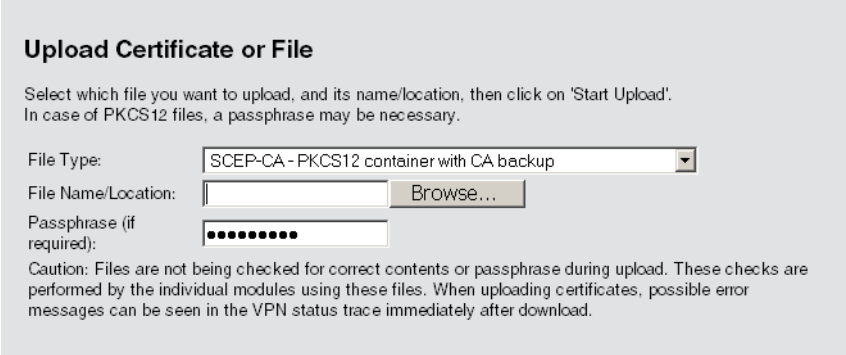
1. Highlight the WLC in the device view section and in the menu **Device** > **Configuration management** select the item **Save certificate as file**.

2. Set the **Certificate type** to PKCS12 container and click **Save**.



14.12.2 Uploading a certificate backup into the device

1. Click on **Extras** > **File management** > **Upload certificate or file**.
2. Select the two entries for SCEP-CA as data type one after the other:
   - PKCS12 container with CA backup
   - PKCS12 container with RA backup
3. For each upload, enter the file name, storage location, and the passphrase that was defined when the backup file was created. Confirm with **Start upload**:



4. After loading the CA backup, the file `controller_rootcert` in the directory **Status** > **File-System** > **Contents** must be deleted.
   Enter the following commands in the console:

```
cd /Status/File-System/Contents
del controller_rootcert
```

5. After restoring the backup, delete all files that start with `controller_` or `eaptls_`.
6. After that, access the directory **Setup** > **Certificates** > **SCEP-Client** and execute the command `Reinit`:

```
cd /Setup/Certificates/SCEP-Client
do Reinit
```

14.12.3 Backing up and restoring further files from the SCEP-CA

To be able to fully restore the SCEP-CA, it is important to have the information on the device certificates issued for the individual APs by the SCEP-CA.

If the root certificates only were backed up, then any issued device certificates can no longer be revoked!

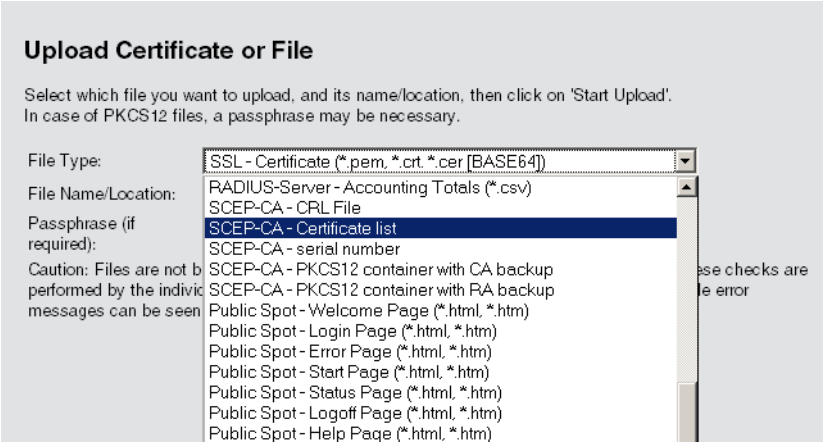
For this reason the following files have to be saved in addition to the certificates themselves:

- SCEP certificate list: List of all certificates ever issued by the SCEP-CA.
- SCEP serial numbers: Contains the serial number for the next certificate.

1. Click on **Extras** > **File management** > **Download certificate or file**.
2. Select the entries listed above as data type one after the other and then confirm with **Start download**:



3. To upload these files to the device, go to the entry page of WEBconfig and select the command **Upload certificate or file**.
4. Select the entries listed above as data type one after the other, enter each file name and storage location and confirm with **Start upload**:



After installing a new certificate list, expired certificates are removed and a new CRL is created. Furthermore, the CA reinitializes itself automatically if certificates and keys are successfully extracted after loading the certificate backup.

14.12.4 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.

These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in LCOS. If you cannot wait until the individual services request

new certificates, a manual resolution requires deleting the SCEP files from the LCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, LCOS performs the necessary steps automatically.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup** > **Certificate** > **SCEP-CA** > **CA certificate**. This action generates a ZIP file within the LCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password, unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **Extras** > **File management** > **Download certificate or file** > **SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **Extras** > **File management** > **Upload certificate or file** > **SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.

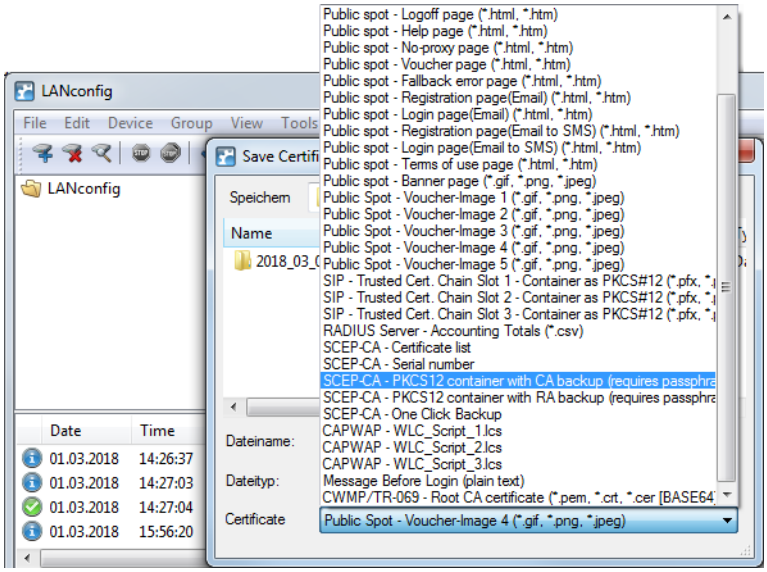
If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action *2.39.2.2.11 Restore-certificates-from-Backup* in order for the device to restore the certificate record.

14.12.5 Using LANconfig to backup and restore certificates

Certificates are stored and uploaded with LANconfig as follows:

Save

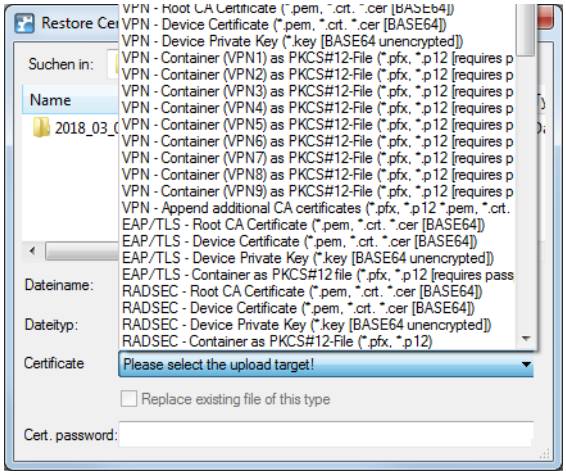
1. Highlight the WLC in the device view section and in the menu **Device** > **Configuration management** select the item **Save certificate as file**.
2. Set the **Certificate type** to PKCS12 container and click **Save**.



Upload

1. Highlight the WLC in the device view section and in the menu select **Device** > **Configuration management** and the item **Upload certificate or file**.
2. Set the **Certificate type** to PKCS12 container.

3. Now navigate to the desired file, enter the password if necessary and click **Open**.



One Click Backup

For the One Click Backup, select the entry "SCEP-CA - One Click Backup" from the dialog list.

14.13 Backup solutions

WLCs manage a large number of APs, which in turn may have a large number of WLAN clients associated with them. WLCs thus play a crucial role in the functioning of the entire WLAN infrastructure—for which reason the organization of a backup solution in case of temporary WLC failure is in many cases indispensable.

In case of a backup event, a managed AP should connect to an alternative WLC. Because this connection will only function if the certificate in the AP has been authorized by the backup controller, it is essential that all WLCs sharing a backup solution have identical root certificates.

14.13.1 WLC cluster

If you are operating multiple WLCs in your network, you can collect these devices into a cluster. The APs in a managed WLAN are no longer managed by a single, central WLC but by multiple, synchronized WLCs. For large networks in particular, a WLC cluster provides numerous advantages:

- Automatic network “load balancing” between the individual APs and WLCs;
- Increased failover reliability through the provision of backup WLCs (“hot standby”) and automatic redistribution of the APs in the case of a WLC failure;
- Setting up a certificate hierarchy: Management of certificates by a central certification authority (CA), represented either by a master WLC or an external station (such as a server).

As of LCOS 9.00, the cluster function received numerous enhancements described below.

14.13.1.1 Enabling/disabling CAPWAP in the WLC

In order to operate multiple WLCs in a cluster, they must all have identical configurations. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master WLC's configuration.

Learn more about mirroring a configuration in the section *Config-Sync*.

14.13.1.2 WLC tunnel for internal communication

The use of WLC tunnels is essential for a WLC cluster. The WLCs in the WLC cluster use this tunnel to communicate with one another and keep their status information aligned. With the feature extensions as of LCOS 9.00, the way that LCOS deals with WLC tunnels is also improved:

- WLCs are able to find one another automatically.
- You have the option to statically configure WLC tunnels.
- WLCs disconnect a WLC tunnel only after a timeout.
- WLC tunnels can be switched on or off globally.

The settings for the WLC tunnels and other WLCs (remote WLCs) are located in the section **WLAN controller** > **General** > **WLC cluster**. The setting **WLC tunnel active** allows you to disable the usage of WLC tunnels, which in effect causes the clustering feature to be switched off.

14.13.1.3 Finding the ideal WLC

The algorithms implemented in LCOS ensure that the APS are intelligently distributed between the individual WLCs. This allows the APs to equally distribute the network load between all of the WLCs in a cluster, or to select an alternative WLC if one should fail. For this, an AP first sends out a discovery request on the network to identify all available WLCs. The WLCs then respond with a discovery response which an AP uses to create a prioritized list of WLCs. This AP prioritizes the list based on various criteria.

An AP works through the different criteria sequentially: If multiple WLCs appear to be ideal candidates after applying a criterion, the AP uses the next criteria to prioritize. This process ends when a WLC finally identifies just one WLC as being ideal after the prioritization described in the following.

Criteria for prioritization

- **Specificity of the AP configuration**: An AP evaluates whether a WLC can provide it with a configuration, and whether this contains a specific AP profile or a default profile. The AP prioritizes a specific AP profile as highest, followed by a default profile. If a profile is missing, it is given the lowest priority.
- **The preference value**: The AP evaluates the preference value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

If there still remain several WLCs which are considered to be ideal, the prioritization process continues by evaluating the connection status and the type of selection process (automatically vs. manually initiated):

- When the **calculation is triggered for the first time**, an AP calculates a weighted value for each of the remaining WLCs by taking the number of APs connected to each WLC and comparing this with the maximum possible number of APs (**license usage**). Ultimately, the ideal WLC is taken as that with the lowest license usage.

  If a WLC has reached the maximum possible number of AP connections (license quota exhausted), an AP no longer considers the affected WLC for the current selection.
- In the case of **automatic checking** of the ideal AP distribution, an AP stays with the WLC it is connected to if this WLC is included in the list of the remaining WLCs. Otherwise, a **randomized algorithm** causes the AP to select an arbitrary AP.
- In the case of a **manually triggered check**, a **randomized algorithm** ensures that the APs distribute the available license quotas as evenly as possible across the network.

14.13.1.4 Determining the ideal AP distribution

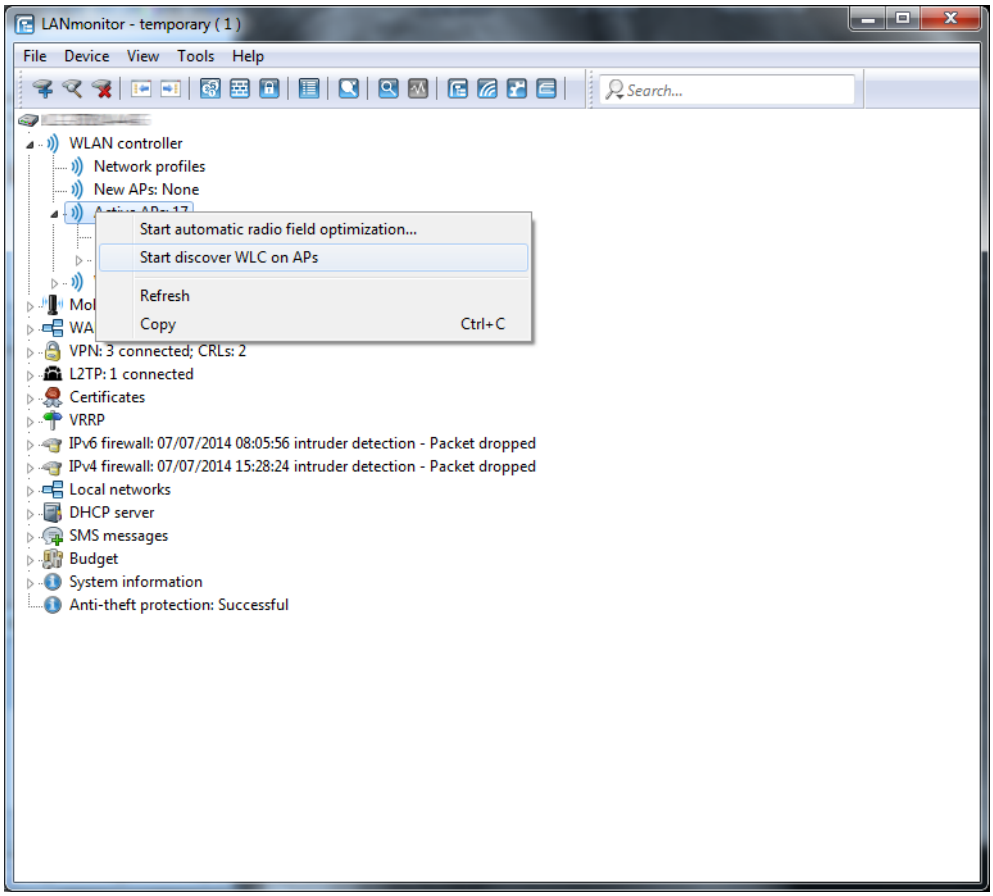
The identification of the ideal AP distribution in a WLC cluster and any redistribution that may be triggered by it occur automatically. Every AP automatically performs the *Finding the ideal WLC* process at irregular intervals between 30 and 60 minutes. If the result of the process is positive for the WLC which is already connected, no redistribution takes place. If a different WLC has a higher priority, the AP attempts to connect to this WLC.

However, as an administrator you can use LANmonitor to manually trigger a calculation of the ideal AP distribution and the resulting redistribution of the APs (see *Manually initiate ideal AP distribution* on page 1207).

14.13.1.5 Manually initiate ideal AP distribution

The following steps show you how to start the recalculation of an ideal distribution, and if necessary to trigger a redistribution.

1. Start LANmonitor and select a WLC.
2. Navigate to the menu item **Wireless LAN** > **Active APs**.
3. Open the context menu on any AP and select **Start WLC search on APs**.



The access points each find their optimum WLC and distribute themselves across the WLC cluster according to the specifications.

14.13.1.6 Setting up a CA hierarchy

In order to operate multiple WLCs in a WLC cluster, they all need to have identical configurations. This also includes the certificates used within the WLC cluster. The solution lies in establishing a certificate hierarchy, also known as a CA hierarchy: This involves defining the CA of a WLC as the root-CA. The other WLCs retrieve this certificate for their (sub-) CA.

The following scenario shows you the configuration steps which are necessary for setting up a CA hierarchy. As examples, the configuration is done using two WLCs:

- WLC-MAIN represents the device with the root-CA;
- WLC-SUB is the device which obtains a certificate from the root-CA in order to issue further certificates as a sub-CA.

Configuring the root-CA

The following section describes how to set up a root CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** > **CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

   Example: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

3. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Operating** to **Yes**.

You have now completed the configuration of the root CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly.

Configuring the sub-CA

The following section describes how to set up a sub-CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Root-CA** to **No**.
3. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** > **CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

   Example: `/CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE`

4. Switch to the menu **Setup** > **Certificates** > **SCEP-CA** > **Sub-CA** and enter the distinguished name of the root-CA under the parameter **CADN**.

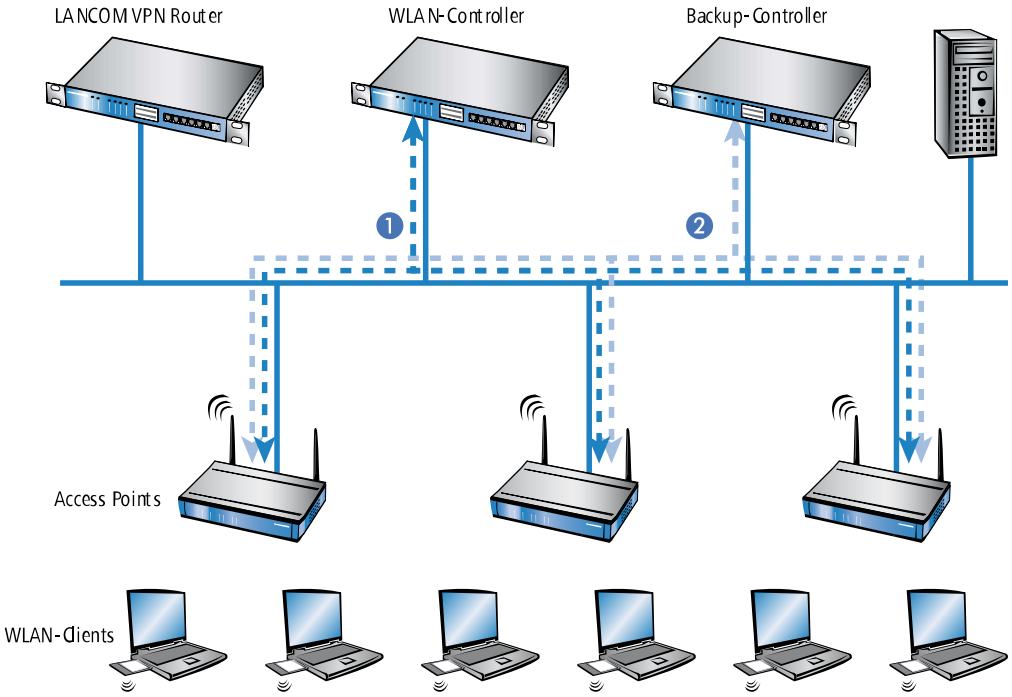
   Example: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

5. For the parameter **Challenge-Pwd** , enter the challenge password that is stored on WLC-MAIN under **Setup** > **Certificates** > **SCEP-CA**.
6. Enter the URL (address) to the root CA in the **CA-Url-address** parameter.
   If another WLC with the LCOS operating system provides the root CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached. Example: `http://192.168.1.1/cgi-bin/pkiclient.exe`.
7. Optional: Specify the **Ext-Key-Usage** and **Cert-Key Usage** to restrict the functions of the sub-CA. For more information, see the Menu Reference Guide.
8. Set the parameter **Auto-generated-request** to **Yes** to activate the sub-CA.
9. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Operating** to **Yes** to enable the CA server with SCEP.

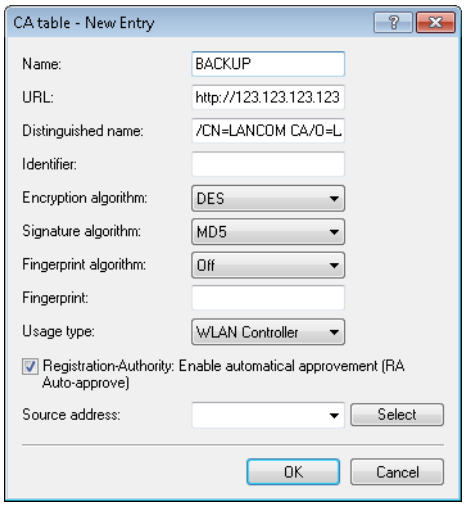
You have now completed the configuration of the sub-CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly. The hierarchy of certificates must be visible here: The WLC first displays the certificate of the root CA and then the certificate of the sub-CA.

14.13.2 Backup with redundant WLAN controllers

This is worthwhile for backing up a WLC with a second WLC, the aim being to maintain full control over all managed APs at all times. The backup WLC is configured in such as way that it obtains the necessary certificates from the backed-up primary WLC via SCEP.



1. Set the same time on the two WLCs **1** and **2**.
2. Switch off the CA on the backup WLC (WEBconfig: LCOS menu tree > Setup > Certificates > SCEP-CA > SCEP-Operating).
3. In the configuration of the SCEP client in the backup WLC, create a new entry in the CA table (in LANconfig under **Certificates** > **SCEP client** > **CA table**). The CA of the primary WLC is entered here.

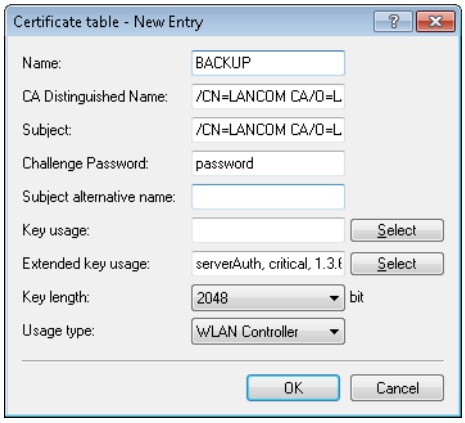


4. The URL is to be entered as the IP address or the DNS name of the primary WLC followed by the path to the CA `/cgi-bin/pkiclient.exe`. For example `10.1.1.99/cgi-bin/pkiclient.exe`'.

   › **Distinguished-Name**: Standard name of the CA (/CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE) or the name given on the primary Controller

- Enable **RA auto-approve**
- **Usage type**: WLAN controller

5. Then create a new entry in the certificate table with the following information:



- **CA-Distinguished-Name**: The standard name under which the CA is entered, e.g. /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE
- **Subject**: Specification of the primary WLAN controller's MAC address in the form: /CN=00:a0:57:01:23:45/O=LANCOM SYSTEMS/C=DE
- **Challenge password**: The general challenge password of the CA on the primary WLAN controller or a password for the Controller specified manually.
- **Extended key usage**: critical,serverAuth,1.3.6.1.5.5.7.3.18
- **Key length**: 2048 bits
- **Usage type**: WLAN controller

6. If a SCEP configuration was previously active on the backup controller, the following actions must be executed under WEBconfig (**LCOS Menu Tree** > **Setup** > **Certificates** > **SCEP client**):

- Clear-SCEP-Filesystem
- Update (2x: the first time, the SCEP client retrieves the new CA/RA certificates only; the second time the device certificate is updated)

7. Configure the first WLC **1** according to your requirements with all profiles and the associated AT table. The APs then establish connections to the first WLC. Each AP receives a valid certificate and a configuration for the WLAN module from the WLC.
8. Transfer the configuration from the first WLC **1**, for example using LANconfig, to the backup controller **2**. The profiles and the AP tables with the MAC addresses of the APs are transferred to the backup WLC at the same time. All APs remain logged on to the first WLC. Once the configuration is transferred, you need to give the backup controller a new IP address.

Should WLC **1** fail, the APs will automatically search for another WLC and they will find the backup WLC **2**. Because this has the same root certificate, it is able to check the validity of the APs' certificates. Because the APs are also entered into the backup WLC's AP table along with their MAC addresses, the backup WLC can fully take over the management of the APs. Changes to the WLAN profiles in the backup WLC will directly affect the managed APs.

In this scenario, the APs remain under the management of the backup WLC until this itself becomes unavailable or is manually disconnected.

If the APs are set up for standalone operation they will remain operational while searching for a backup WLC, and the WLAN clients will remain associated.

14.13.3 Backup with primary and secondary WLAN controllers

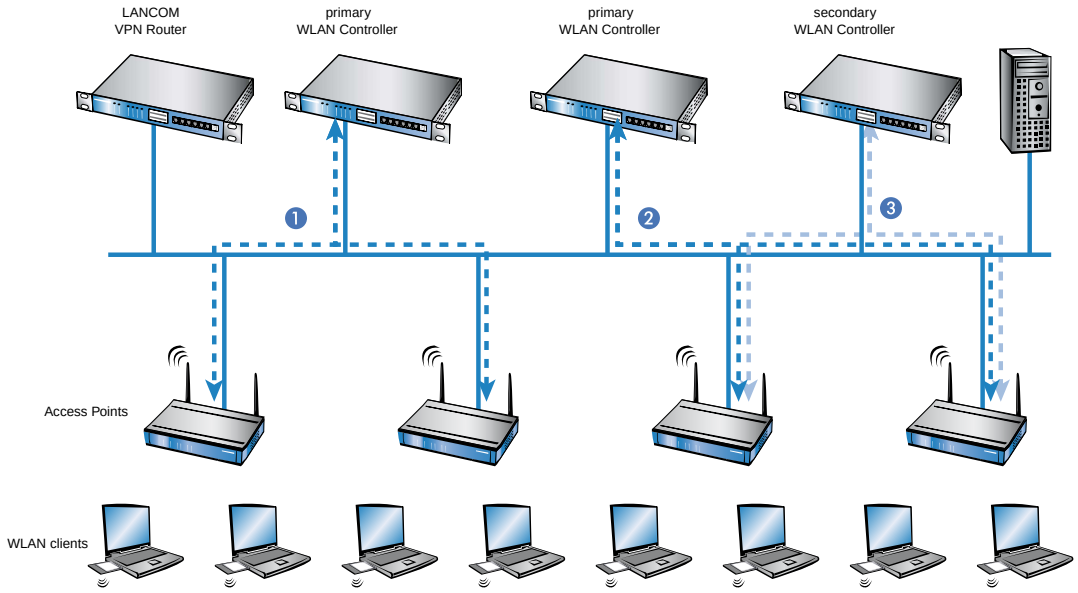
This second type of backup you can provide a larger number of "primary" WLCs with one common "secondary" backup WLC. In case a WLC should fail, the APs remain operational but they work with the current configuration of the WLAN modules. As a secondary WLC, the backup WLC cannot assign any configuration changes to the APs.

14.13.4 Primary and secondary controllers

The establishment of a WCL/AP connection is always initiated by the AP. An AP in managed mode will search the LAN for a WLC that will provide it with a configuration. During this search the AP may find various suitable WLCs:

- The WLC can authenticate the **certificate** in the AP and it has a **configuration** stored for the MAC address of the AP. A WLC of this type is described as a "primary" WLC.
- A WLC can authenticate the **certificate** of an AP, but it has **neither a configuration** stored for the MAC address of the AP, **nor does it have a default configuration**. A WLC of this type is described as a "secondary" WLC.

This is an example of a backup solution with three WLCs for 50 managed APs: Two of the WLCs each manage 25 APs and the third is available as a backup WLC:



A WLC is now able to accommodate five times the maximum number of APs that it can manage by itself. For each five WLCs (identical models), just one additional WLC is sufficient to provide a full backup WLC in case of failure.

1. Set the same time on all of the WLCs **1**, **2** and **3**.
2. Transfer the CA and RA certificates from the first primary WLC **1** to the second primary WLC **2** and to the secondary "backup WLC" **3**.
3. Configure the first WLC **1** according to your requirements with the profiles and the associated AP table for one half of the APs. This WLC becomes the primary WLC for the APs entered into it.

For a backup solution using a secondary WLC, be sure to set the time for standalone operations such that the AP has time to find a backup WLC. This is because the backup WLC is not able to provide a new configuration for the AP.

Once the AP has established a backup connection to a secondary WLC the countdown until expiry of standalone operation is halted. The AP and its WLAN networks remain active as long as there is a connection to a WLC.

1. Configure the second WLC **2** for the other half of the APs, which subsequently treat this WLC as their primary WLC.
2. For the backup WLC **3** the time and the root certificates are set up only. No further configuration is required.

3. After being started, the APs search for a WLC by emitting a discovery message. In this case, all three WLCs respond to this message—the APs select "their" primary WLC for the DTLS connection that follows. One half of the APs decides on WLC **1** and the other half chooses WLC **2**. Because WLC **3** does not function as primary WLC for any of the APs, none of the APs log on to it.
4. Should WLC **2** fail, the APs will automatically search for another WLC. They discover the WLC **A** and **C**, whereby **A** is already under full load with its 25 APs. Backup controller **C** is able to check the validity of the certificates, i.e. it can authenticate the APs and accept them as managed APs. However, because the APs are **not** entered with their MAC numbers into the backup WLC's AP table, the backup WLC cannot manage the APs any further; they simply continue to operate with their current WLAN configurations.

If WLC **A** is not under full load, for example because some of "its" APs are switched off, then some of the searching APs could log on here. WLC **A** remains a "secondary" controller for these APs because it does not have their configuration profiles. If in this case one of the APs with an entry in the AP table of WLC **A** is switched on again, then **A** accepts this reactivated AP and, in exchange, it disconnects one of the backup-event APs.

If the APs are set up for standalone operation they will remain operational while searching for a backup WLC, and the WLAN clients can continue to use all of their functions.

14.13.5 Automatic search for alternative WLCs

As of LCOS 9.00, an AP no longer attempts to reconnect to the last known WLC in case of a disconnection. Instead, the AP searches in the network for an available WLC which corresponds to the criteria for the *Finding the ideal WLC*.

14.13.6 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.

These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in LCOS. If you cannot wait until the individual services request new certificates, a manual resolution requires deleting the SCEP files from the LCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, LCOS performs the necessary steps automatically.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup** > **Certificate** > **SCEP-CA** > **CA certificate**. This action generates a ZIP file within the LCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password, unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **Extras** > **File management** > **Download certificate or file** > **SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **Extras** > **File management** > **Upload certificate or file** > **SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.

If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action *2.39.2.2.11 Restore-certificates-from-Backup* in order for the device to restore the certificate record.

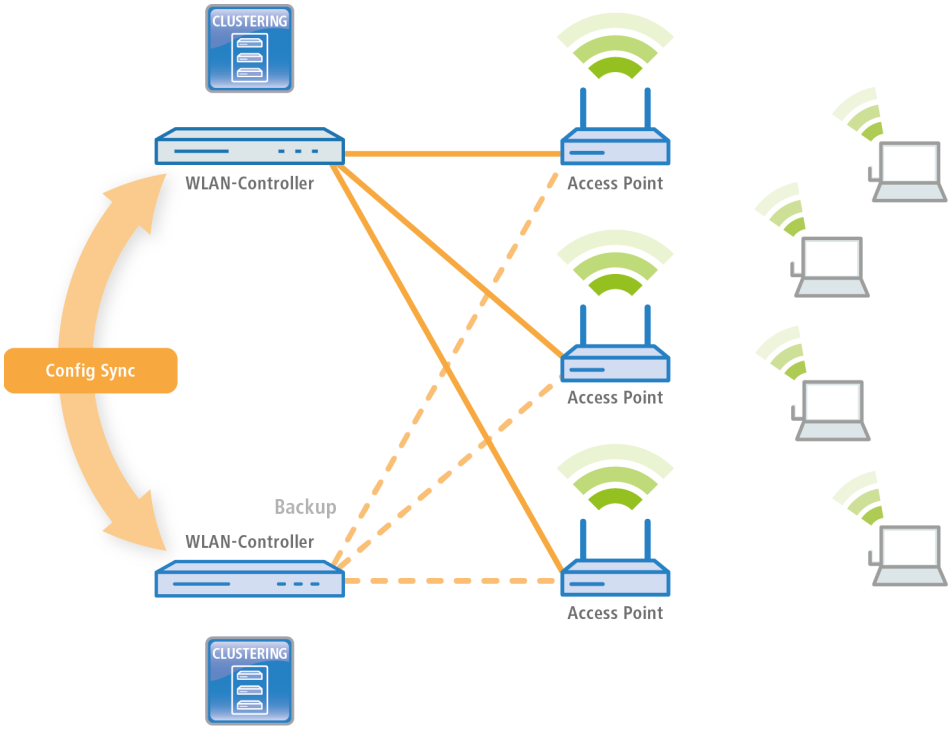
14.14 Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option

Example application, WLAN controllers:

WLAN infrastructures have become an integral part of modern corporate networks. In the age of the "all wireless office", the increasing demands on the availability of a WLAN solution make it essential to have a reliable backup and high-availability solution. In WLAN infrastructures with a single WLAN controller, any failures or maintenance downtimes (such as a firmware update) of the WLC until now caused the APs connected to it to switch to standalone operation. Consequently, the APs in standalone mode were no longer able to access the features that are provided centrally by the WLC such as a Public Spot, IEEE 802.1X authentication, or Layer-3 tunnels.

In order to avoid this and to maintain the full operation of all WLAN capabilities even if a WLC should be temporarily unavailable, one or more redundant or backup WLCs should be employed. In the backup event, the APs automatically switch from the temporarily unavailable WLC to a backup WLC. The backup WLC has the same configuration (e.g. AP table or WLAN profiles) as required by the primary WLC of the APs. The initial setup of the WLCs and any subsequent configuration changes must be carried out separately and identically on each device—a huge effort for the administrator. Manual maintenance of the configurations between multiple identical devices could lead to outdated or non-synchronous configurations on the backup WLCs, which in the case of a backup event could lead to a critical state for the entire WLAN infrastructure. The resulting troubleshooting usually turns out to be a real challenge. The users of the WLAN clients experience a loss of productivity, which could have major consequences company-wide.

New with the LANCOM WLC High Availability Clustering XL option: This software option allows multiple WLCs to be grouped into a highly-available cluster. In this way, configuration changes, features and enhancements made on one WLC are automatically transferred between the other WLCs in the cluster, without having to make manual changes on each individual device. Common parameters in a cluster (e.g. WLAN profiles, AP tables, or Public Spot settings) remain synchronized, individual parameters (such as the IP address of the WLC) are not exchanged.



The LANCOM WLC High Availability Clustering XL option offers greatly simplified administration and huge time savings because you only need to configure one WLC in the cluster. The WLC then transfers the changes to the other cluster devices automatically. In the case of maintenance downtime (e.g. for a firmware update) or even the failure of a WLC,

the APs automatically connect to another WLC which, thanks to Config Sync, already has the identical configuration without any intervention by the administrator. The result is a convenient way to high availability.

The prerequisites for a device to be a valid member of a cluster are:

- The LANCOM WLC High Availability Clustering XL option (as of LCOS version 9.10) must be available.
- IP communications must be available to all other devices, e.g. via LAN, WAN, or VPN.
- It must be in the list of group members that is stored in each device.
- A valid certificate must be available
- It needs to authenticate itself by certificate as a member of the cluster.

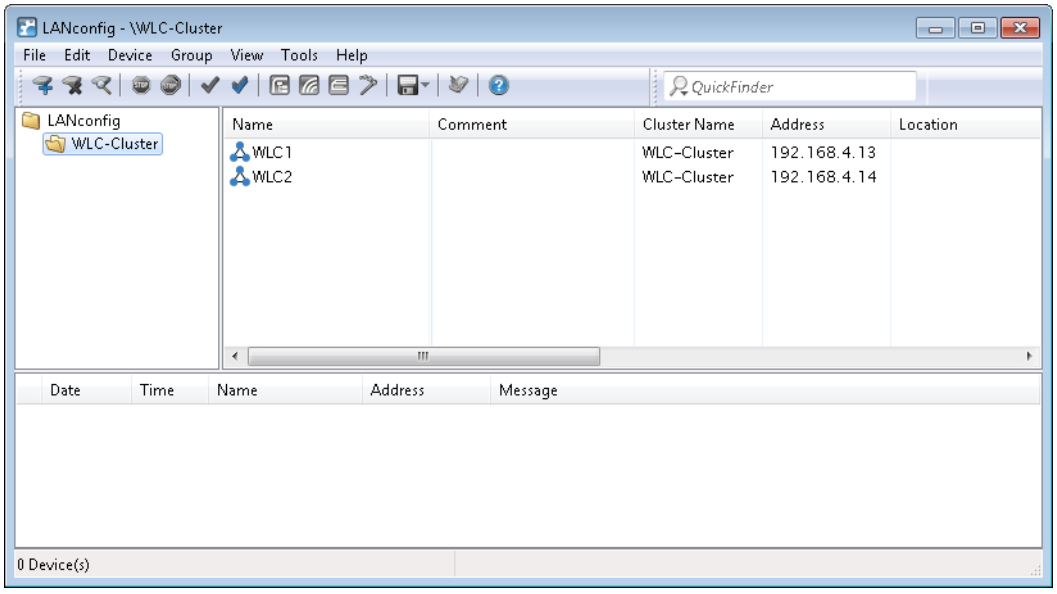
14.14.1 Special LANconfig icon for devices in a cluster or using Config Sync

LANconfig has a specific icon to mark devices that share their configuration via Config Sync. Furthermore, the **Config Cluster** column shows the configuration group for each device. LANconfig is thus able to sort and edit the device listing according to cluster name.

If you try to make changes to the configuration of a cluster member, you will receive following warning:

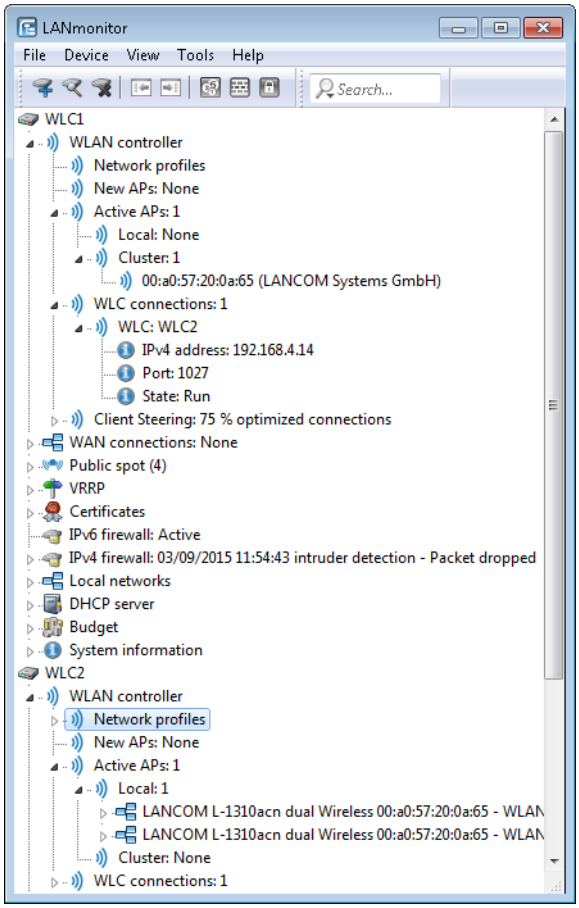
"This device belongs to the Config Cluster: [cluster name]. Editing this configuration also affects the following devices: [Listing of all devices in the same cluster]"

You can bypass this message if necessary. To do this, enable the option **Don't show again** in the displayed window.



14.14.2 Special LANmonitor icon for devices in a cluster or using Config Sync

LANmonitor has a specific icon to mark devices that share their configuration via Config Sync. Also, the name of the configuration group (cluster name) is shown after the device name. LANmonitor thus makes it easier to see which devices share the same configuration.



15 Public Spot

15.1 Introduction

This chapter provides answers to the following two questions:

- What is a Public Spot?
- Which functions and properties apply to the Public Spot module?

15.1.1 What is a Public Spot?

Public Spots, also called hotspots, are places where users can connect their terminals – such as smartphones, tablet PCs or laptops – to a publicly accessible network. Normally, these networks provide connections to the Internet; however a Public Spot can also be limited to a local network in order to offer extra information to users visiting a museum or a trade show, for example. The term is usually synonymous to the devices with which the user can connect to the network, which is also why this manual does not differentiate between the location and the device.

15.1.1.1 The solution: (W)LAN technology

Public Spot scenarios make use of the widespread (W)LAN technologies based on the internationally established IEEE 802.11/802.3 standards:

- Access via WLANs provides fast, uncomplicated network access by radio. WLAN adapters are standard equipment for mobile devices and they support bandwidths that even allow the smooth playback of HD videos.
- With automatic address allocation via DHCP, access via LAN is similarly uncomplicated: Most notebooks feature a LAN adapter for the network cable.

When accessing via LAN the user loses mobility and uninterrupted flexibility. However, this access – assuming that a corresponding infrastructure is available – also provides stable network operation with the highest network load (for example, for multimedia content such as video-on-demand) and a higher number of users (for example, in a large hotel), where connections via WLAN may reach their limits sooner. It is also possible to add a Public Spot offering to an existing cable infrastructure (for example, in a college) with the use of a Public Spot via LAN.

Noteworthy issues of access using (W)LAN

Operating conventional WLAN access points or LAN routers as a Public Spot is made more difficult by the fact that user authentication is only possible by RADIUS/802.1X, which requires a corresponding configuration. For this reason, the use of devices without the Public Spot function is not practical, since these devices are not able to separate and log the specific network usage of authorized and unauthorized users of publicly accessible networks.

15.1.1.2 User authorization and authentication

As soon as an end device moves within range of an access point, the user can spontaneously established a connect to this access point. The same is true for open LAN connections. However, the problem is that access should not be available to the public in general, but only to certain selected users. Setting up restrictions of this type is the task of a Public Spot.

For this purpose, a Public Spot must be in a position to control access to the (W)LAN on a user basis. For simple Public Spot installations, user data can be locally stored and managed in the router or access point – or alternatively on a WLAN controller. Instead, complex installations employ a direct database connection to a central authentication server in the interests of detailed accounting or direct management. Central servers of this type generally work with RADIUS technology.

15.1.1.3 Accounting

If the Public Spot operator does not want to offer this service free of charge, connection data has to be collected and billed for each user. Typical methods include: Purchase of a limited amount of online time (pre-paid model), retrospective payment of consumed resources (post-paid model), or unrestricted access until a certain time (e.g. checking out of a hotel).

For smaller Public Spot installations, accounting functions should be as simple as possible, and they should be implemented locally in the device. Larger installations offer the facilities for billing via an external RADIUS server. For each application scenario, the connection to an external system can also be implemented using a software interface which has access to the accounting data and can control the user authentication (e.g. hotel reservation systems).

15.1.1.4 Logging

The Public Spot module provides suitable functions for recording user data with RADIUS accounting and SYSLOG.

Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations. You can also find information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

15.1.2 Application scenarios

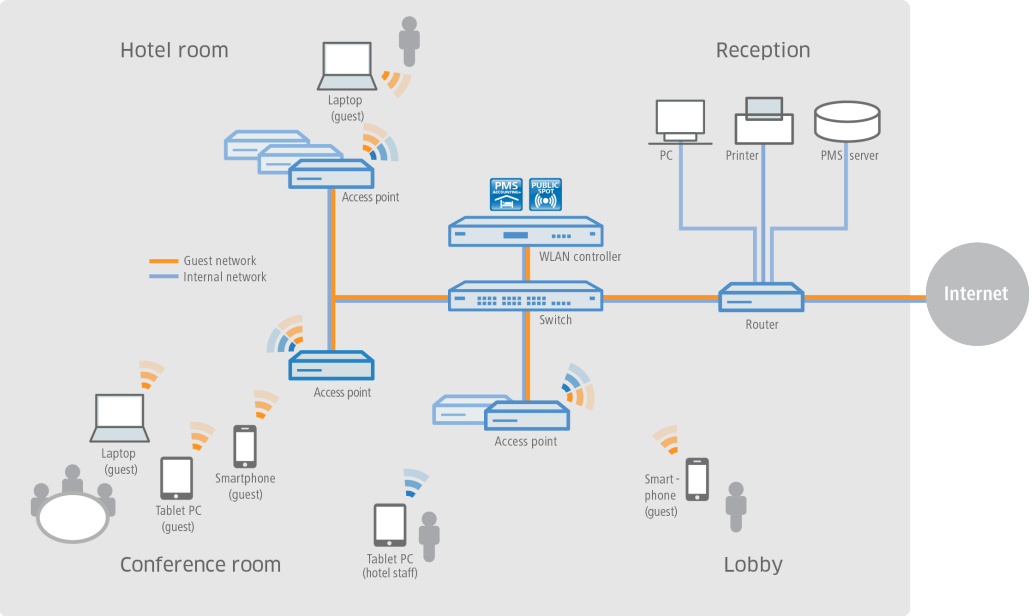
15.1.2.1 Guest access accounts in hotels

Wireless LAN makes it easier than ever for hotel operators to offer their guests convenient Internet access. Quick and easy to install, hotspot solutions from LANCOM enable guests to use their own laptop, tablet or smartphone to access the Internet via WLAN. Whether in the lobby, the conference room or in the hotel rooms—securely separated from the internal network, guest access can be provided anywhere it is desired.

The option LANCOM Public Spot PMS Accounting Plus is ideal for straightforward accounting: All Public Spot logins are automatically sent to the central PMS server where the hotel's accounting system is installed. In this way, guests can login to the hotspot using their room number and last name. For fee-based Internet access, the usage fees can be billed directly to the room. Needless to say, it is easy to set up free guest-access accounts in hotels, if desired.

- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 1227.
- **No access by unauthorized persons to internal data** – secure separation of the in-house and guest networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. Also, data can be securely encrypted on the wireless interface so that guests cannot penetrate the hotel network over the WLAN. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 1151.
- **Simplified guest login on the WLAN** – The integrated Smart Ticket function ensures that the guest receives the login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Alternatively, vouchers can also be printed out or guests can login with their room number and/or last name. For more details see the chapter *Alternative login methods* on page 1274.

- **Simple billing of fee-based Internet access** – with the addition of the LANCOM Public Spot PMS Accounting Plus option, it is possible to connect to hotel accounting systems such as Micros Fidelio. For more details see the chapter *Interface for property management systems* on page 1303.

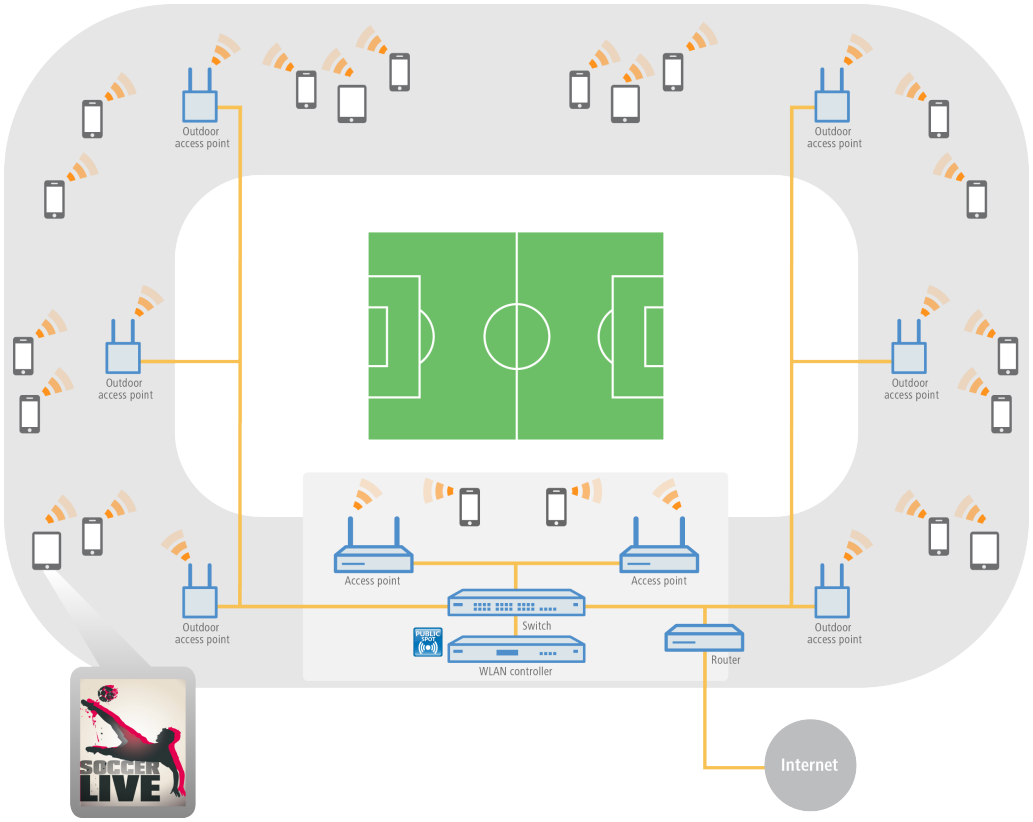


15.1.2.2 Guest access in sport arenas

Stadiums that host large sporting events increasingly offer a range of modern services. For example, they should allow very large numbers of spectators to use Internet access with their own end devices, for example to view live content about the event, or to surf online. In order to offer spectators an Internet connection that is faster than the overloaded cellular networks, a promising solution is to offload the data to the stadium Wi-Fi with the aid of LANCOM solutions. By connecting the clients to the stadium WLAN, the stadium operator has the possibility to create additional advertising space for sponsors—and thus additional sources of income. For example, the hotspot login page can be customized or sponsor websites can be invoked.

- **Multi-media fan experience** – with a WLAN Internet access, fans have the attractive option of watching current sports news live, and looking up information as well as watching replays.
- **New advertising spaces generate additional income** – additional, attractive advertising spaces can be made available to stadium operators by using the individual configuration options of the hotspot login page and also the configuration of pre-defined websites which do not require a login (walled garden function). For more details see the chapter *Open access networks (no login)* on page 1253.

- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 1227.



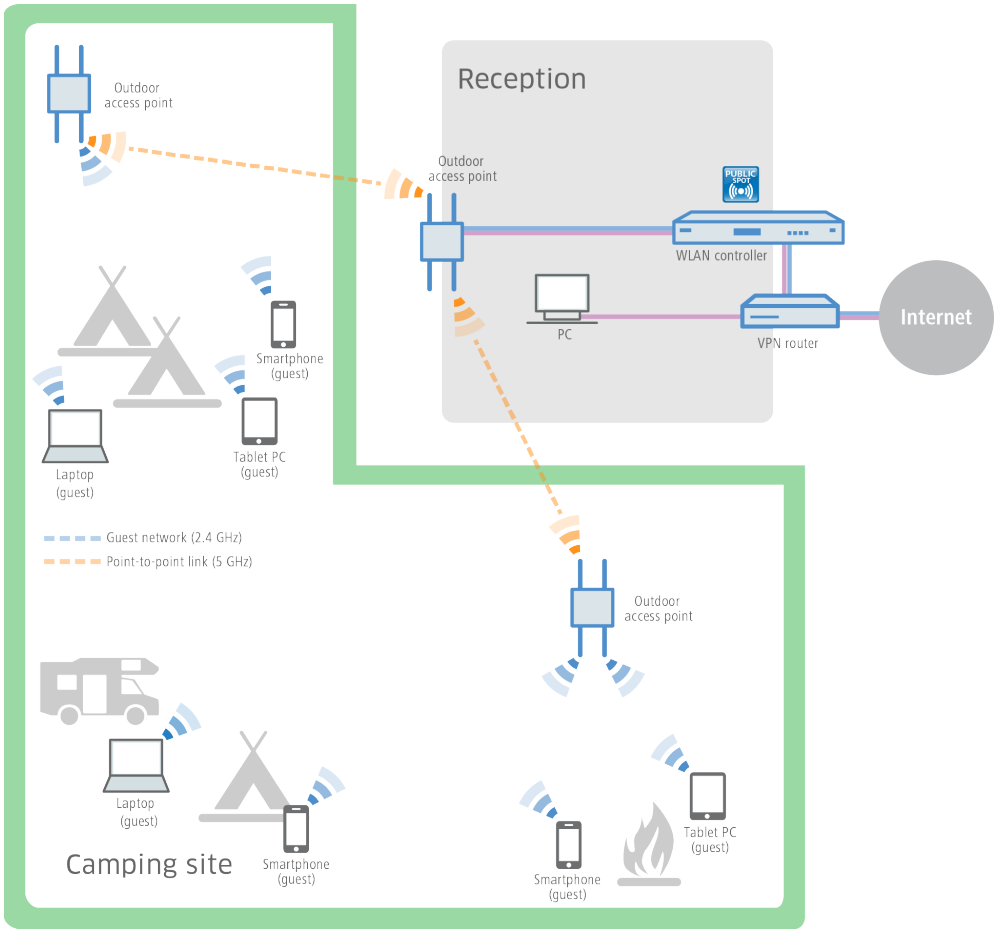
15.1.2.3 Guest access at camping grounds

Camping grounds are exposed to the weather and are often quite large. Nevertheless, people vacationing at modern camping grounds expect to have the convenience of Internet access from their own laptop, tablet or smartphone. Whether in a tent, a camper, or around the campfire, ubiquitously available Internet access is a real competitive advantage for camping ground operators.

With the robust, weather-proof outdoor devices from LANCOM and the LANCOM Public Spot option, even these demanding scenarios are implemented with ease—and without the laborious and costly need to lay cables. For example, in administration buildings for camping grounds, a WLAN controller (incl. LANCOM Public Spot option) is connected to a LANCOM dual-radio outdoor access point. This sends the signal via point-to-point connections in the 5-GHz frequency band to further outdoor access points, which provide WLAN coverage in the 2.4-GHz frequency band to the desired areas—such as campsites or recreational areas for guests. The secure separation of the guest and administrative networks is assured throughout, thanks to VLAN assignment.

- **Online convenience without laying cables** – even in wide-open areas, guests can be connected to the Internet without a costly and complicated installation.
- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 1227.
- **Simplified guest access** – The integrated Smart Ticket function ensures that the client receives the login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Or as an alternative, vouchers can be printed out. For more details see the chapter *Alternative login methods* on page 1274.

- **Reliable even in extreme conditions** – thanks to the robust IP66 outdoor housing and an extended temperature range, LANCOM outdoor devices are reliable and defy even extreme weather conditions from -33° to +70°C.



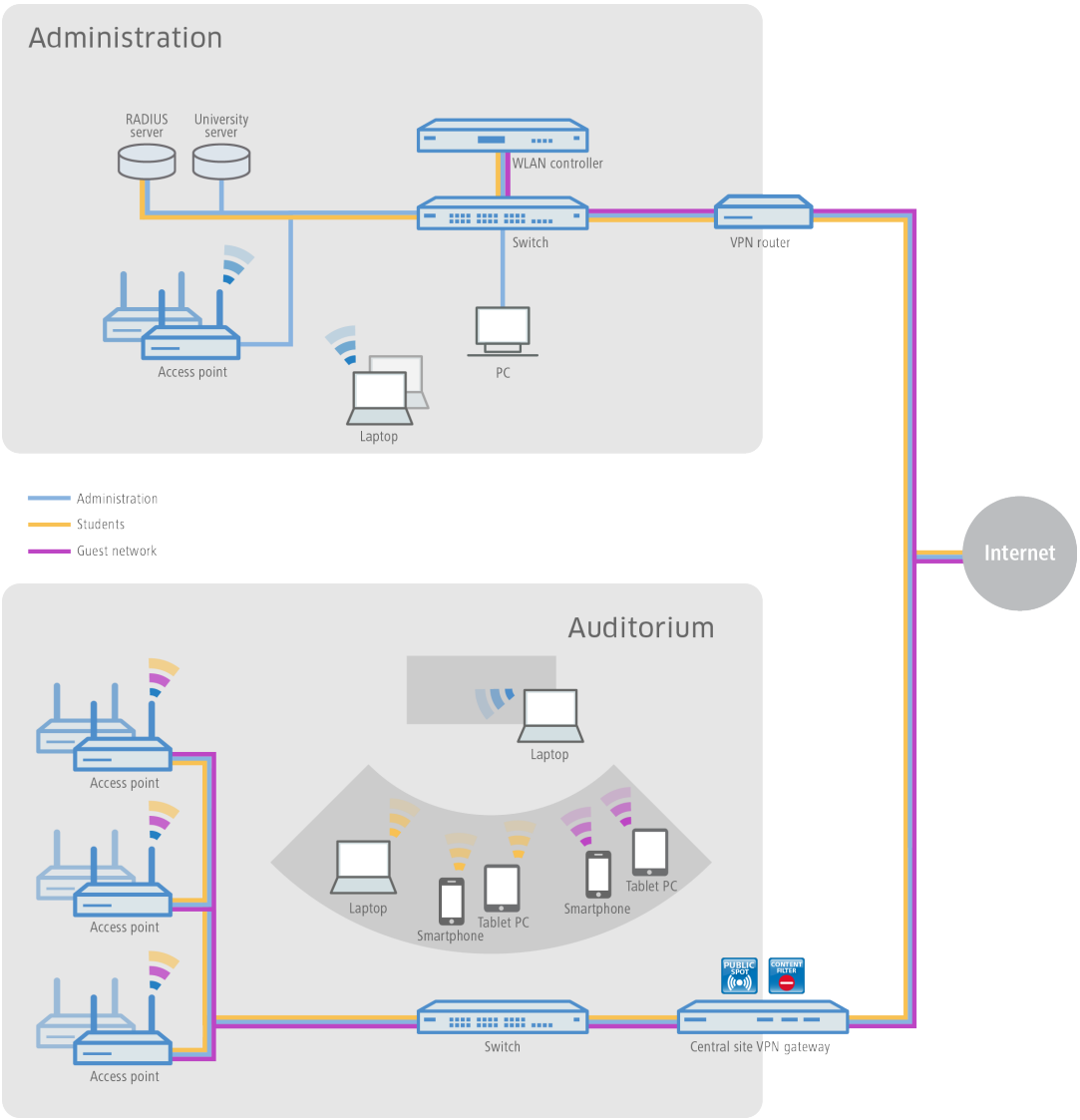
15.1.2.4 Guest access in schools and universities

Researching at home, learning for tests, preparing classes, or interactive design: The potential of Internet usage for students and pupils as well as teachers and staff of modern schools and universities is indispensable today—including at isolated buildings, preferably wireless, and with the users' own end devices.

With the help of LANCOM WLAN solutions, this is easy to implement. By configuring separate networks, the Internet access of the pupils and students is securely separated from the administrative access. Thanks to dynamic VLAN access, the different user groups are assigned to the VLANs that are intended for them, using just one SSID. For example, only staff have access to the university servers. At the same time, school and university students have the convenience of an extensive WLAN guest access, which is so important these days. The authentication in the pupil and student networks (e.g., Eduroam) can be implemented with IEEE 802.1X. This makes it possible for guest students from partner universities to connect to the WLAN of the host university. And even conference guests can be provided with a temporary guest access by means of a voucher.

- **Secure login for university affiliates** – professors, students and staff of universities can have access to the Internet and various online libraries over the securely encrypted WLAN.
- **No access by unauthorized persons to internal data** – secure separation of the administrative, students', and professors' and guests' networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 1151.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.

- **Comfortable, cable-free Internet access** – even in large open areas, guests have Internet access with their WLAN-enabled end devices without a costly and complicated installation.



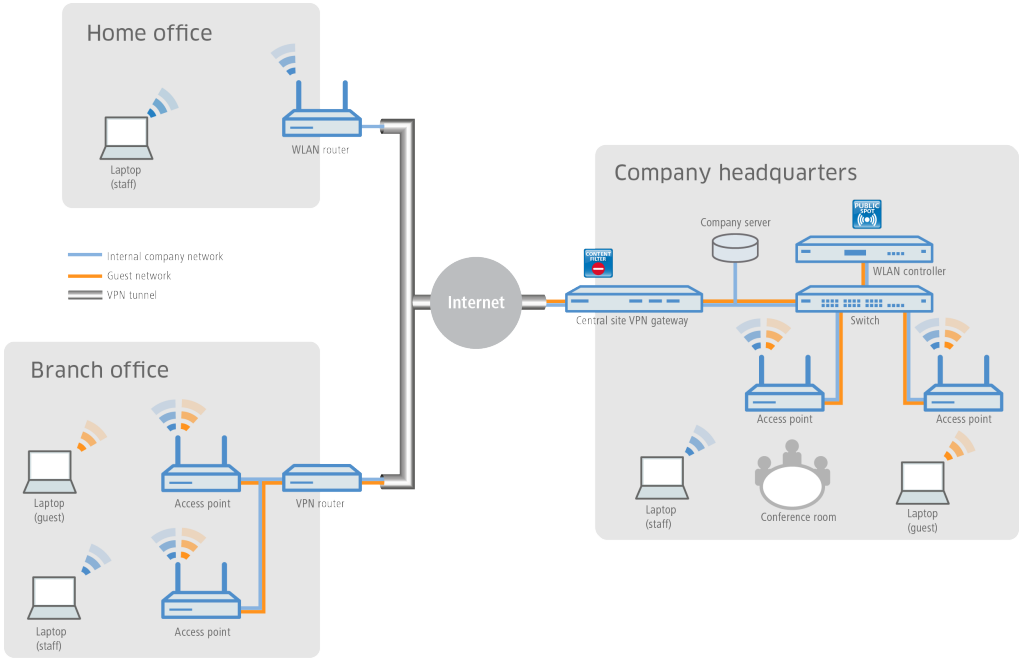
15.1.2.5 Guest access in companies

At any company with a complex network structure, the flexibility and stability of Internet access is vitally important. Branch offices must have cross-site access to the company network, and home office employees also need access to e-mail accounts and databases. In addition, customers and visitors should be offered a separate guess access.

With devices from LANCOM and the LANCOM Public Spot option, these scenarios are easy to implement. The sites are connected using a VPN tunnel. Companies can provide access to the Internet for their external guests on their own mobile devices ("Bring Your Own Device") using a separate guest network in the company main office and even at networked branch offices. Access to the company's internal data is reserved for authorized employees only.

- **Secure separation of company and guest networks** – the secure separation of employee and guess networks within a single infrastructure is achieved by using VLAN or a Layer 3 tunnel. This keeps internal data safe from unauthorized access. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 1151.
- **User-friendly setup and configuration** – a LANCOM WLAN controller allows different user profiles to be defined and configurations to be uploaded to the different WLAN devices – including those at remote sites.

- **Easy guest access** – using vouchers, it is a simple task for your reception desk to provide guests with login data for the Public Spot so that they can use their own mobile clients ("Bring Your Own Device"). In this way, only registered users have access to the Internet and e-mail.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.



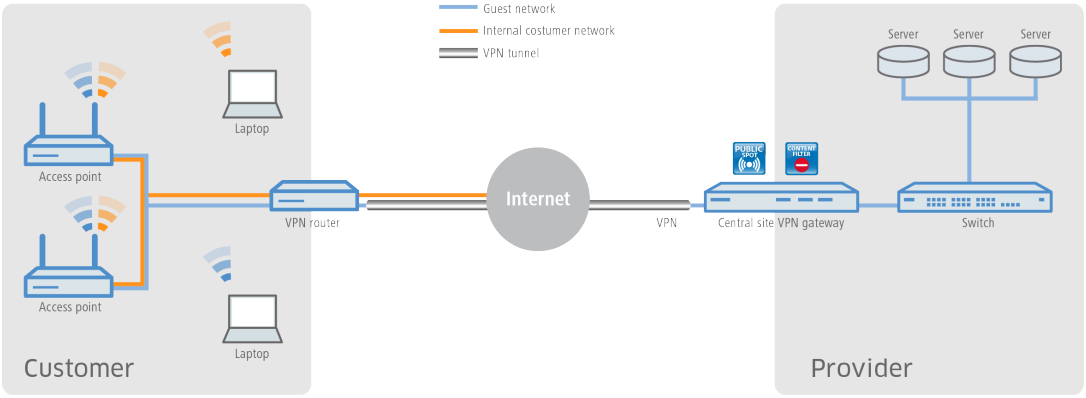
15.1.2.6 Guest access for providers

With the solutions from LANCOM, it is very easy for Internet providers to offer their customers a network with guest access. The provider receives all necessary network products from one source, LANCOM, and manages the networks of its clients centrally and conveniently—without a technician on site.

For the implementation, LANCOM access points are installed behind a LANCOM VPN router at the site of the provider's client (for example, a hotel, hospital or business). A separate internal network is given direct Internet access. The guest access is provided over a secure VPN tunnel to the central-site VPN gateway at the provider, who can log incoming requests on their internal servers. With the LANCOM Content Filter, the provider can also limit or block access to undesirable or illegal websites for customer guest-access accounts.

- **Simple and central management and roll-out** – even without a technician on site, the provider can centrally monitor and configure the networks for the customer. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 1227.
- **Different redirect options** – network separation means that the hotspot services can be designed and implemented in various ways. For example, services offered to end customers can be limited to hotspot administration only, or they can include full-service administration, whereby all data traffic from the end customer is forwarded to the provider via a tunnel.
- **Connection of proprietary AAA systems** – LANCOM provides different interfaces (RADIUS, XML, FIAS) which can be combined with proprietary AAA servers. Custom authentication and login to the hotspot, as well as accounting, can be implemented specific to each provider. For more details see the chapter *Alternative login methods* on page 1274.
- **Multi-provider support** – LANCOM devices are not locked into access via a specific provider. Hotspot service providers who cooperate with different providers can combine their software solutions over a variety of interfaces with the help of LANCOM devices. For more details see the chapter *Alternative login methods* on page 1274.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.

- **Data offloading** – WLAN hotspots can provide effective relief for cellular networks by offloading data traffic to different infrastructures.

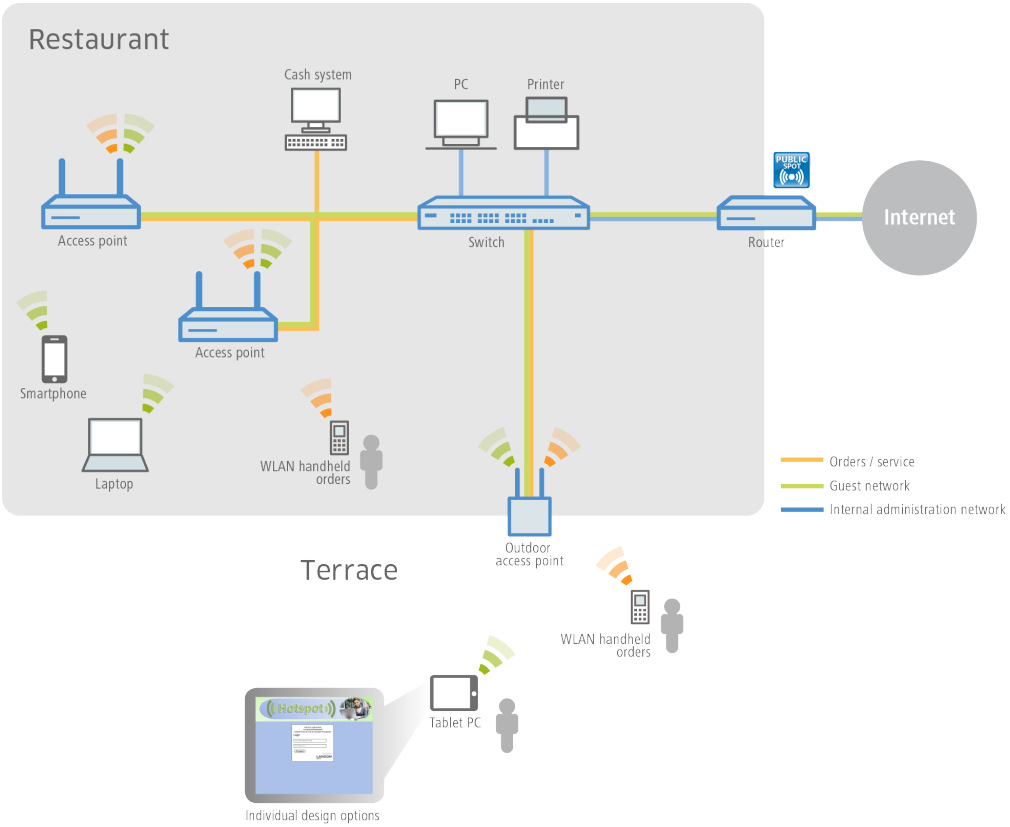


15.1.2.7 Guest access in gastronomy

Providing guests in a modern restaurant or café with a hotspot can significantly increase the appeal of any location. With the WLAN solutions from LANCOM, visitors benefit from a WLAN guest network in that they can make convenient use of the Internet with their mobile smartphones, tablet PCs or laptops—while being securely and completely separated from the internal administrative network. For a significant increase in efficiency in work processes, wait staff also have the option of taking orders with the help of a WLAN-enabled hand-held device, and transmitting the order directly to the checkout system, kitchen, or drink serving station. Needless to say, WLAN access for the guests and for taking orders can also be made available on the patio or outdoor areas of the restaurant, since a robust LANCOM outdoor access point is ideal for outdoor areas.

- **Customizable and flexible creative leeway** – whether with proprietary logos, texts or images—the welcome page of the Public Spot can be easily tailored to your own requirements. Even displaying pre-defined websites is possible (walled garden feature), so that, for example, the menu of the restaurant or its own website is shown to the guest without a prior login to the hotspot by the guest. For more details see the chapter *Internal and customized voucher and authentication pages (templates)* on page 1307.
- **No access by unauthorized persons to internal data** – secure separation of the networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 1151.
- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees the easy setup of hotspots. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 1227.

› **Simplified guest access** – The integrated Smart Ticket function ensures that guests receive their login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Or as an alternative, vouchers can be printed out. For more details see the chapter *Alternative login methods* on page 1274.



15.1.3 Overview of the Public Spot module

The demands placed on devices operating Public Spots are as varied as the environments they are employed in. A Public Spot offers various functions which are described in more detail in the following sections.

15.1.3.1 Open User Authentication (OUA)

Open User Authentication (OUA) provides Web-based authentication by means of an online form and is ideal for Public Spot installations.

Typical procedure for an online session with OUA

1. The user of a W(LAN)-enabled end device is within reach of an access point or a network outlet in a Public Spot mode.
   - › WLAN: After system startup, the WLAN adapter automatically logs on to the appropriate access point.
   - › LAN: After system startup the user connects to the network with a suitable cable and is assigned an address by the DHCP server.

   Internet access or the use of chargeable services is not yet possible at this stage.
2. The user starts a web browser. The device offering the Public Spot service automatically directs the user to the login page of the Public Spot. This page provides detailed information on using the services.

   Alternatively, the user's client device automatically performs captive portal detection and presents the login page of the Public Spot immediately after associating with the WLAN.

Generally, the user purchases a voucher with login data that grants a limited amount of access time. Other login methods are also possible, such as login after confirming the provider's terms of use or independently requesting login data via e-mail or a text message (SMS).

3. In the case of a login using a voucher, the user enters his login data (username and password) on the login page. Depending on the configuration, the RADIUS server on the device (internal) or an external one checks the login data that was entered. If the login is successful, the user gains access to the Public Spot. Otherwise an error message will be displayed. If a prepaid model is employed, i.e. access is to be granted for a limited period of time only, then the RADIUS server additionally informs the Public Spot about the user's time credit.
4. The user can log off from the Public Spot at any time. The Public Spot can terminate a session itself if the time credit has expired, if a specified expiry date is reached, or if contact is lost for an extended period.

   During and at the end of a session the Public Spot provides the user with an overview of the session data. If required, the Public Spot can simultaneously transmit all important accounting information to the RADIUS server. This can be the device's internal server or an external server.

15.1.3.2 Security in the (W)LAN

Wireless LANs are potentially a significant security risk. Public Spots present similar risks to the operator and users.

Security for the operator

Operators of Public Spots are primarily interested in the security of their own network infrastructure. A Public Spot module provides operators with a range of security technologies and methods:

- **Multi-SSID** (only WLAN)**, VLAN and virtual routers**
  - The safe separation of public access can be achieved using one or more different radio cells for an access point (Multi-SSID).
  - VLAN technology can separate public access from the private network of the operator.
  - Virtual routing technology ARF (Advanced Routing and Forwarding) from LANCOM Systems supplies one SSID with its own security and QoS settings and only specific destinations are routed on it.

  This ensures that guest access over a Public Spot is securely and effectively separated from the productive network, even though they share the same infrastructure. The device's internal firewall can, for example, limit the available bandwidth in the WAN to max. 50 %, and access can be restricted to web pages (HTTP, port 80) and name resolutions (UDP 53).

  Further information on Multi-SSID, VLANs and ARF is available in the LCOS Reference Manual.

- **Traffic limit**

  To avoid denial-of-service (DoS) and brute-force attacks on the Public Spot you can restrict the permissible data transfer for non-authenticated Public Spot participants to a harmless volume.

- **Locking access to the configuration**

  You can lock access from your Public Spot network to device configurations (e.g., your access points, WLAN controllers or routers) so that access to configurations is only possible using other specified management interfaces.

Security for the user

The primary security concern for users of Public Spots is the confidentiality of their data. Users are also interested in security of user data to avoid misuse. Users are protected by the following security technologies:

- **Intra-cell blocking** (WLAN Only)

  Prevent communication between the WLAN clients in your Public Spot network. Along with the user's existing security mechanisms, this measure helps to prevent unauthorized access to the resources of your Public Spot users.

- **Encryption during the login phase**

If you have a digital certificate, you can load it on your device in order to secure usernames and passwords using an encrypted HTTPS method. The digital certificate should be signed by a recognized public authority so that browsers classify it as trustworthy and do not display security errors to the users. If there is no certificate, data is sent unencrypted.

The certificate merely secures the login process, as the data within a Public Spot network are normally not encrypted. This is true for LAN as well as WLAN connections. If your users wish to secure their regular data traffic as well, they will have to use their own encryption methods.

An exception to this are the WLAN connections via HotSpot 2.0: Since the HotSpot 2.0 standard is based on WPA2 (802.1X/802.11i), EAP and 802.11u, data packets are always encrypted for transmission, both for authentication and during the session.

LANCOM strongly recommends that sensitive user data should only ever be transferred via encrypted connections, such as the IPSec-based VPN tunnel with the LANCOM Advanced VPN Client or over normal encrypted data connections based on HTTPS. In addition to this, Public Spot users should ensure that a personal firewall is active on their end devices.

15.1.3.3 Setup wizard for Public Spots

The **Setup Public Spot** wizard helps you to setup and perform the initial configuration of your Public Spot. You can set up a functional Public Spot network with just a few clicks. The wizard groups the necessary settings together (e.g. assign an interface, choose an IP range, specify the access format and login procedure, logging) and offers you the option to create an administrator with limited rights who can only create and manage Public Spot users.

15.1.3.4 Wizard for creating and managing users

Using the setup wizard **Create Public Spot account** you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can immediately use to login to the Public Spot network for the specified period.

Alternatively, a stock of vouchers can be created and printed out to speed up the voucher issue at peak times or to allow employees without access to the device to issue vouchers. In this case the Public Spot account is created with an online time duration that starts when the user logs in for the first time. You also set a maximum validity period for the access. After this time, the Public Spot automatically deletes the access account, even if the online time was not used up yet.

The setup wizard **Manage Public Spot account** displays all registered Public-Spot access accounts in a table on a web page. This gives you an overview of your most important user data, as well as a user-friendly way to extend or reduce the validity of an access account with a single click, or even delete user accounts completely. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the user account.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-in.

This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

15.2 Setup and operation

This chapter contains the main information required for setting up and operating a Public Spot.

- **1) step: Basic configuration**

  First, we describe the basic configuration. After completing the basic configuration, the Public Spot is operational and preconfigured for a simple application scenario (login using voucher).

- **2nd step: Security settings**

  This chapter describes in detail the security settings that impede attacks on your Public Spot network and promote stable operation. If you have not already made these settings during previous setup steps, you should pay close attention to the following pages.

- **3rd step: Extended functions and settings**

  Finally, we review the wide variety of available extended functions and settings. Detailed descriptions inform you on how to individually adapt your device to its task and its environment. In addition, this chapter informs you on how to keep an overview of the status and activities of your Public Spot.

Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations. You can also find information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

15.2.1 Basic configuration

The instructions for the basic settings are divided into several separate sections:

- The first section describes the setup of an operational Public Spot using a Wireless Router as an example.

  To set up a Public Spot for a simple application scenario, you can start the corresponding wizard, which assists you in configuring the Public Spot.

- The second section describes the configuration of the default values for the user wizard with which new employees can easily create and manage new Public Spot users without the need for general administrator rights. This also includes creating a limited access account with which your employees can access this wizard only.
- The third section describes user administration on the local RADIUS server, either using the user wizard or manually with LANconfig.

To a certain extent these sections are dependent on one another, and ideally you should work through them in sequence.

15.2.1.1 Basic installation of a Public Spot for simple scenarios

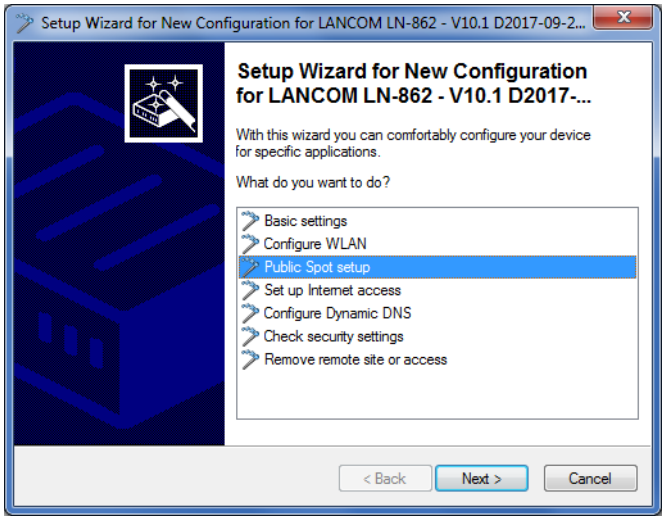
Installation using the setup wizards

The following tutorial describes how to use LANconfig's Public Spot setup wizard to perform a basic Public Spot installation.

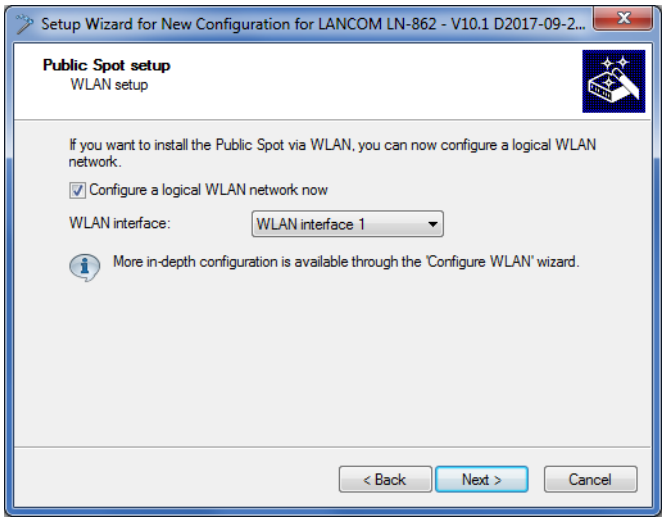
The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.

1. To do this, start LANconfig and select the device on which you wish to set up the Public Spot, for example, an access point.

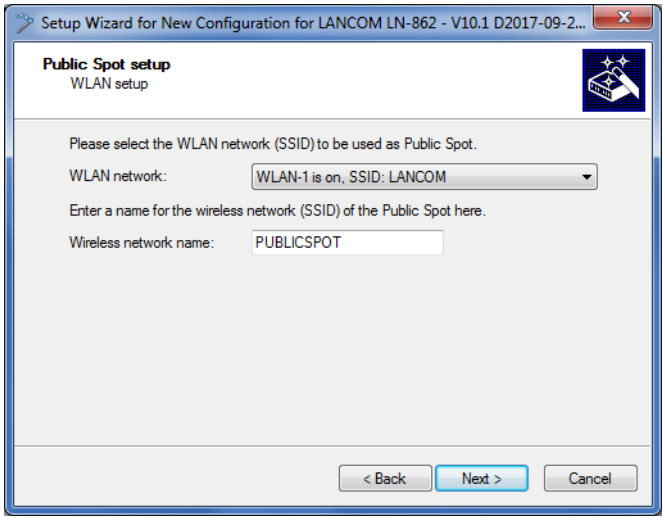
2. Start the Setup Wizard with **Device** > **Setup wizard**, select the action **Setup Public Spot** and then click **Next**.



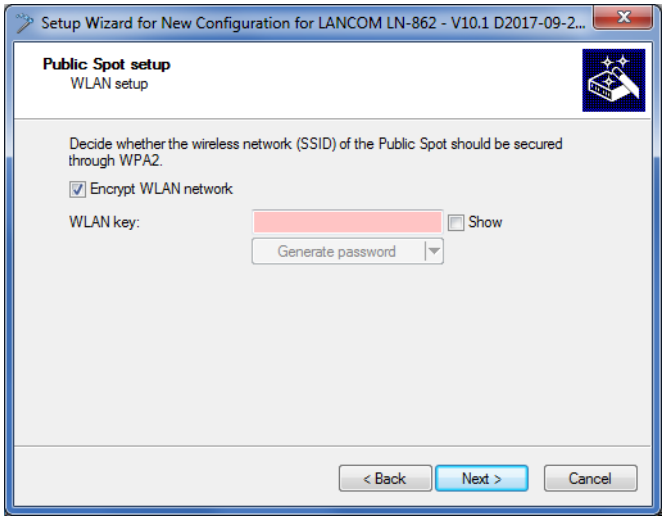
3. If you want the Public Spot to be available over WLAN, enable the corresponding option and then click **Next**.



4. Select the logical interface from the drop-down menu which the Public Spot should offer (e.g., WLAN-1), and enter a descriptive name for the wireless network (PUBLICSPOT). Click on **Next**.

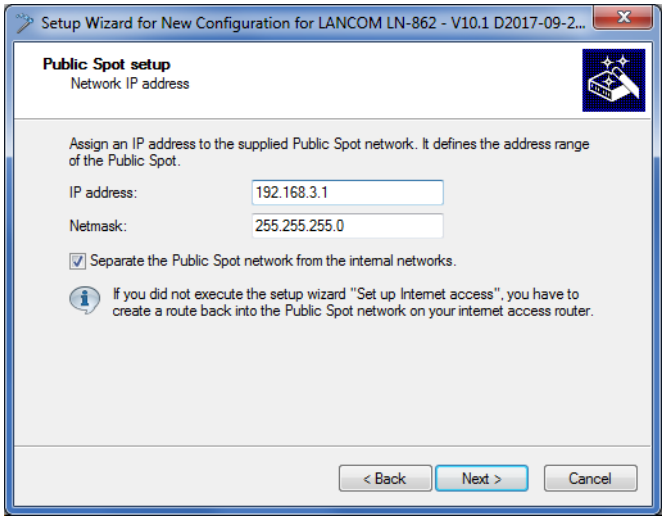


5. Specify whether the wireless network should be encrypted. In this case, specify a WLAN key or have it generated automatically.



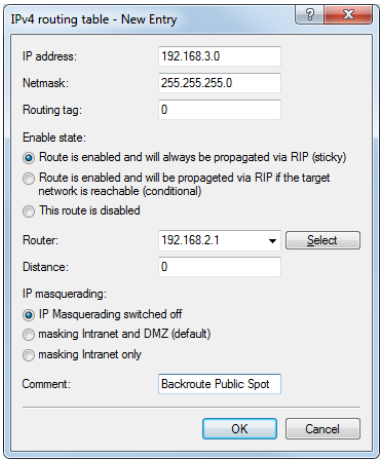
6. Assign the IP address and netmask to the device that your Public Spot network should specify and click **Next**.
   The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere.

If you want to separate the Public Spot network from internal networks for security reasons, make sure that the corresponding option is enabled.



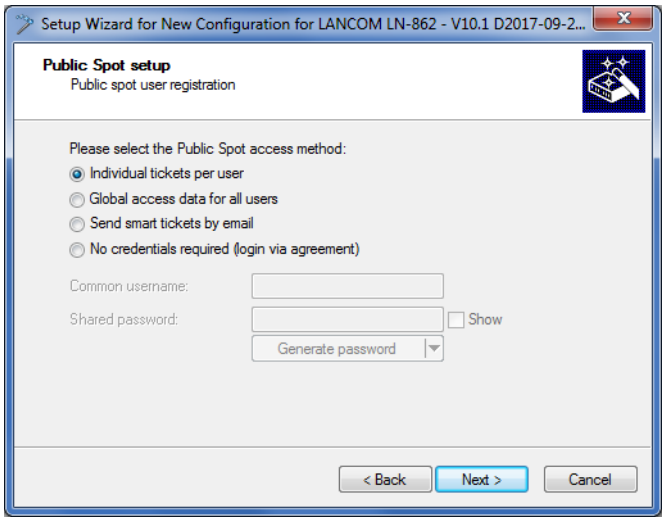
If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you configure this under **IP router** > **Routing** > **IPv4 routing table**. To do this, create a new entry and enter the network address of your Public Spot network under **IP Address** and under **Router** enter the address of the Public Spot in your local network.

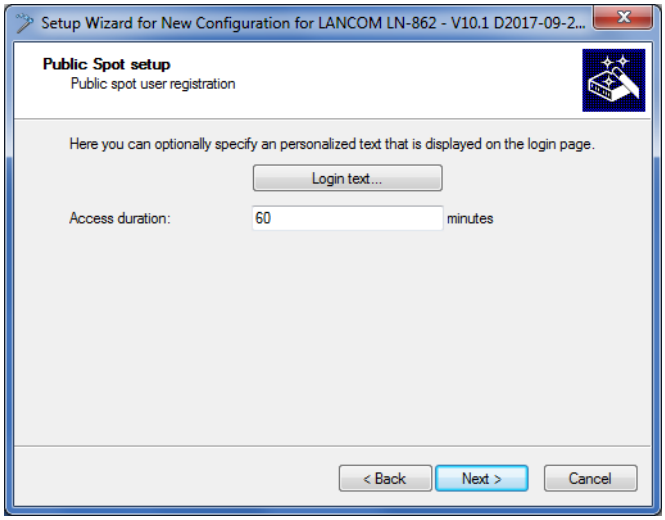


7. Specify which login data your users are to use to login to the Public Spot. Also, you can optionally add customized text to the login page. To continue, click on **Next**.

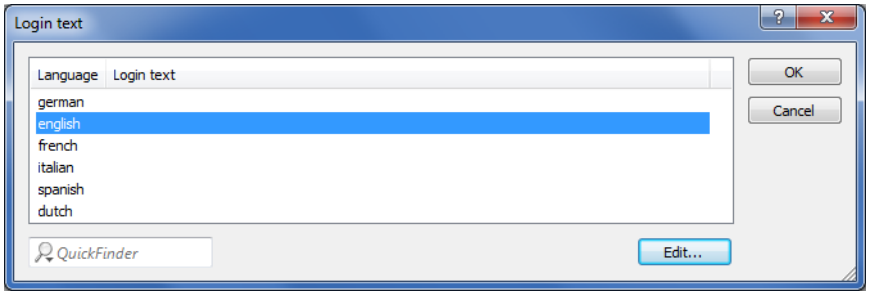
You can either give each user their own login data or set up a general account that all users use to access the Public Spot. If you issue vouchers later and would like to set up permanent user accounts, select the option **Individual tickets per guest**.

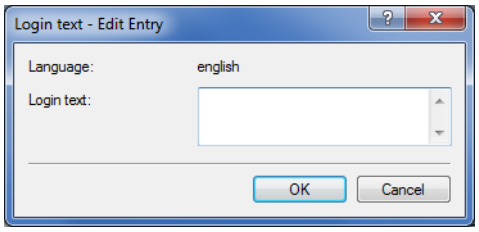


8. Here you can optionally select a login text, you set the access time and click **Next**.



Login text (optional):



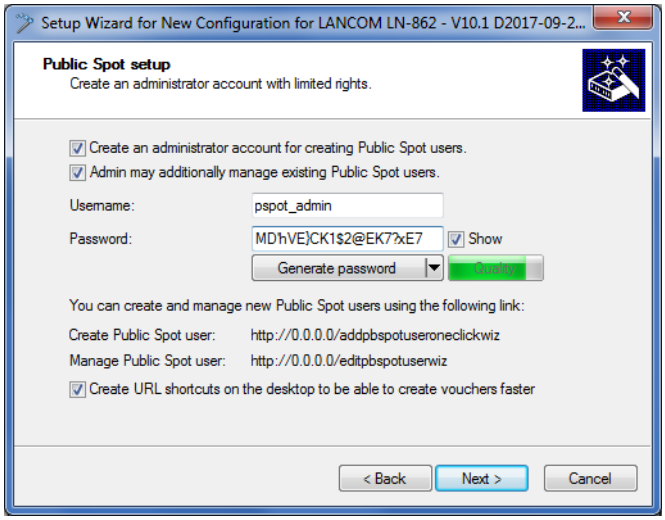


The login text is a customized text entered in HTML format, which appears on the login page inside the box on the registration form. You can manually add or edit this text at a later time (see the section *Customized text or login title for the login page* on page 1310).

9. If necessary, create an administrator with limited rights who can use the setup wizards in WEBconfig to create and manage Public Spot users. To continue, click on **Next**.
   This type of administrator is useful when you want your employees to be able to manage user accounts themselves without the help of a device administrator. The right to create new accounts in WEBconfig enables the Create Public Spot account wizard, and administrator rights enable the Manage Public Spot account wizard.

   Using the user creation wizard **Create Public Spot account**, the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.

   The **Manage Public Spot accounts** wizard enable the administrator to manage the users. The administrator can extend or reduce the validity period of access, or completely delete a specific user account. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the account.

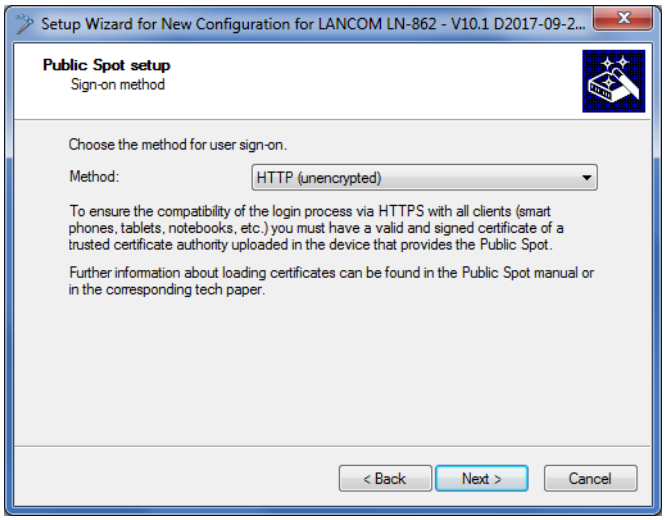


Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to yellow, and when it is very secure the background turns green.

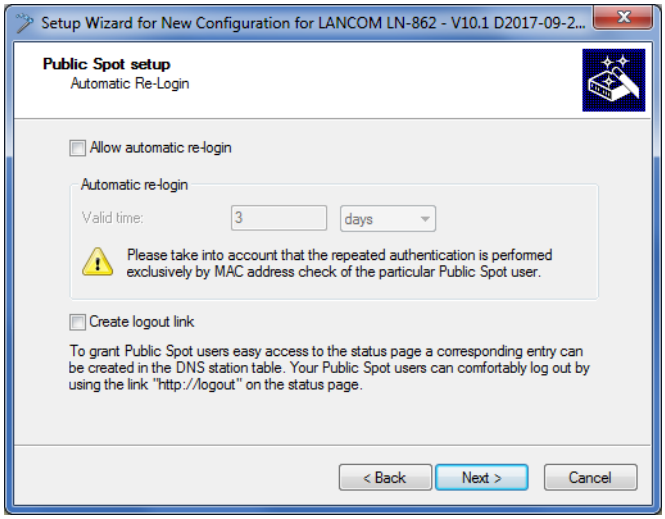
10. Select the procedure for user login. To continue, click on **Next**.

    You can select **HTTP** or **HTTPS** in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.

The use of HTTPS requires the installation of a suitable server certificate. Otherwise the user is presented the device's own certificate, which would cause the browser to issue a certificate warning.

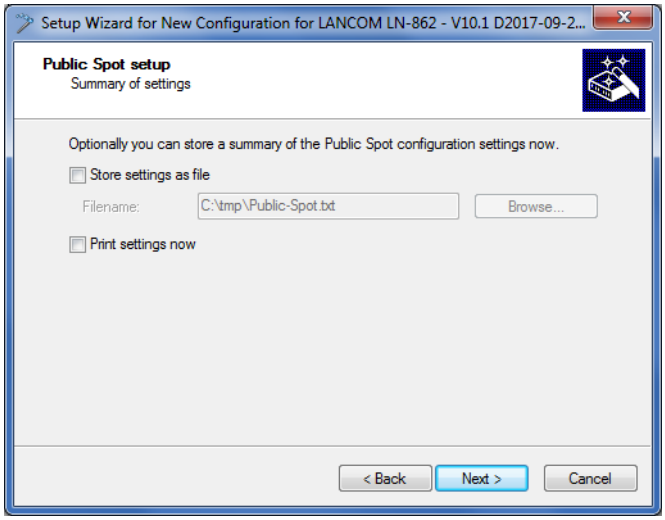


11. Determine whether automatic re-login is allowed for all Public-Spot users, and the maximum absence that is allowed before the user must login again on the Public Spot webpage. To continue, click on **Next**.
    The **Automatic re-login** option is a convenience option that allows the Public Spot to automatically authenticate known users or devices. However, if known devices are to be recognized exclusively from the MAC address of the network adapter, the fact that MAC addresses can be falsified represents a potential security risk. For this reason this option is disabled by default.



12. Save your changes if necessary.

Before you save the configuration to your device, you have the option to save the configuration locally on your PC or to print a summary.



13. The click **Next** and finally **Finish** to complete the basic installation of the Public Spot. The Setup Wizard will now send the settings to the device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

Manual installation

The following configuration steps show you how to manually setup a Public Spot for simple scenarios. For the application scenario described here, you enable the Public Spot on an interface over which there is no other data traffic other than the Public Spot traffic – where Public Spot and normal WLAN users do not share the same network (dedicated SSID).

This tutorial is only an example. Depending on the device type (access point, WLAN controller, etc.) or complexity of the network configuration (e.g., use of VLAN or ARF), setting up a Public Spot may require different or additional steps. Since this type of network configuration can be highly customized, this tutorial concentrates specifically on a simple example, so that you can adapt the steps as needed.

1. To do this, start LANconfig and select the device on which you wish to set up the Public Spot, for example, an access point. Next, open the configuration menu for the device.
2. Check that the time is correct.

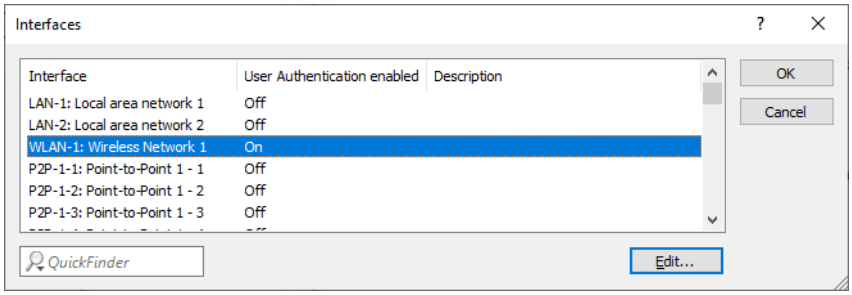
   To check the certificates and correctly record and bill session data, it is important for the Public Spot's time setting to be accurate. First make settings such as time zone and time changes (summer and standard time):

   › LANconfig: **Date/time** > **General**

   In order to ensure that the time of the Public Spot remains correct, the device should be set up as an NTP client. Enter the time server that is necessary for that under **Date/Time** > **Synchronization** > **Time server**. Open the "Add" window to show a list of possible server addresses.
3. Select the interfaces for the Public Spot operation.

   Here you activate the interfaces which will be available to registered users. Along with the logical WLAN interfaces which Public Spot users directly login to, the logical LAN interfaces (LAN-1, etc.), and the point-to-point connections (P2P-1, etc.) can also be selected. When connected via the LAN or P2P interface, additional access points can be integrated into the Public Spot provided by another device. For a single access point, on the other hand, you select, for example, the logical WLAN interface **WLAN-1**.

› LANconfig: **Public Spot** > **Server** > **Operation settings** > **Interfaces**

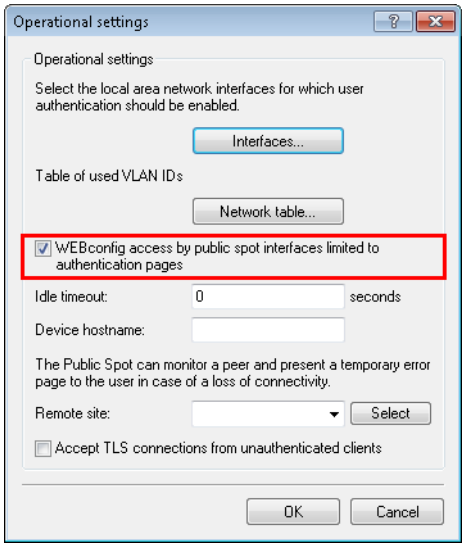


By activating the authentication for a WLAN interface, you automatically release the associated SSID for the Public Spot operation.

On a WLC you can enable certain Ethernet interfaces for the Public Spot. In this manner you can also set up selective restrictions for certain VLANs.

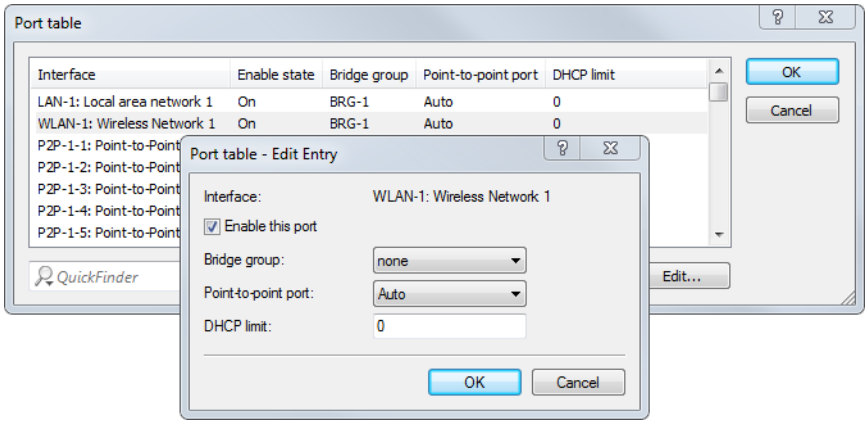
4. Access to your device from the Public Spot network should be restricted to the authentication pages.
If you do not restrict access, Public Spot users will be able to access the configuration interface of your device (WEBconfig). For security reasons you should not permit this.

   › LANconfig: **Public Spot** > **Server** > **Operational settings** > **WEBconfig access by Public Spot interfaces limited to authentication pages**



5. Disconnect the interface which is to be used for Public Spot operations from the other network traffic.
In order for end devices to be able to communicate with one another via the different interfaces of a Public Spot device (e.g., between LAN-1 and WLAN-1), these interfaces are logically connected to one another (bridged) within your device. However, in a Public Spot scenario this type of bridging may not be desirable for security reasons. In order to disconnect the communication between an interface (e.g., WLAN-1) assigned to a Public Spot and the rest of the network, you have to remove bridging. In the **Port table** set the **Bridge group** for the respective interface to `none`.

› LANconfig: **Interfaces** > **LAN** > **Port table**

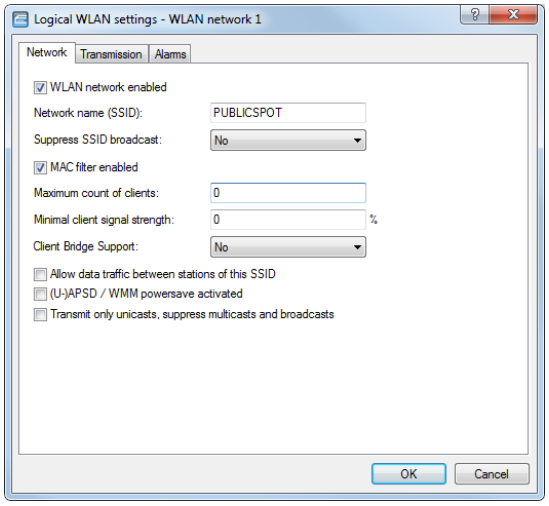


6. Enable the WLAN for the Public Spot.

   This setting does not affect: Routers, WLAN controllers, central-site gateways.

   Activate the logical WLAN which you enabled for the Public Spot login and assign a descriptive name to this network (SSID).

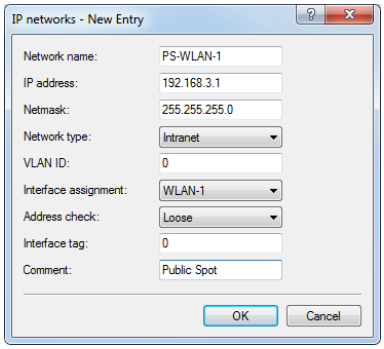
   › LANconfig: **Wireless LAN** > **General** > **Logical WLAN settings** > **WLAN network <number>** > **Network**



   If you do not set up a private WLAN, you should disable the setting **Allow data traffic between stations with this SSID** for security reasons. This prohibits communication between the individual Public Spot users.

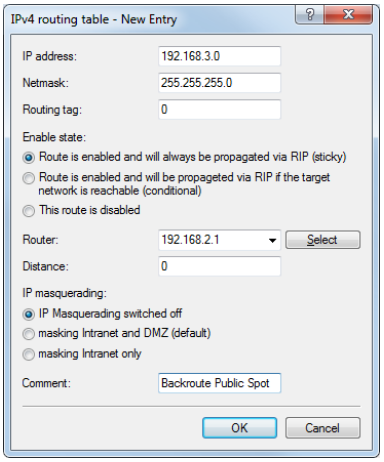
7. Assign the IP address and netmask to the device that your Public Spot network should specify.
   The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere. Select the interface that you chose under **Interface assignment** e.g., `WLAN-1`.

› LANconfig: **IPv4** > **General** > **IP networks**



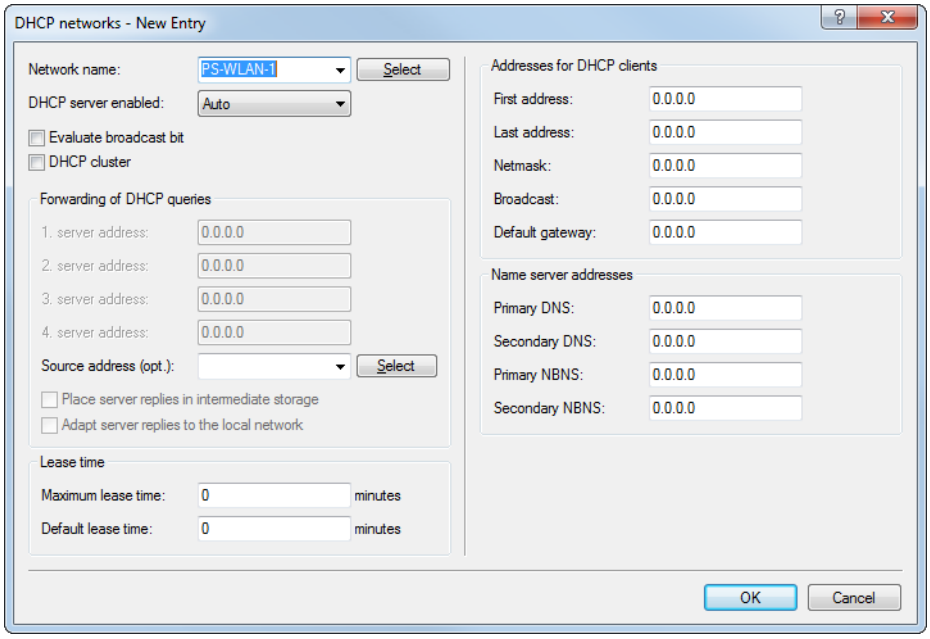
If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you configure this under **IP router** > **Routing** > **IPv4 routing table**. To do this, create a new entry and enter the network address of your Public Spot network under **IP Address** and under **Router** enter the address of the Public Spot in your local network.



8. Configure the DHCP server settings for the Public Spot network.
   Since the device has an IP network that is independent from the network where it is located, you must configure a DHCP server for this network. For the previously set up IP network (e.g., `PS-WLAN-1`), set the value for **DHCP server enabled** to `Yes`.

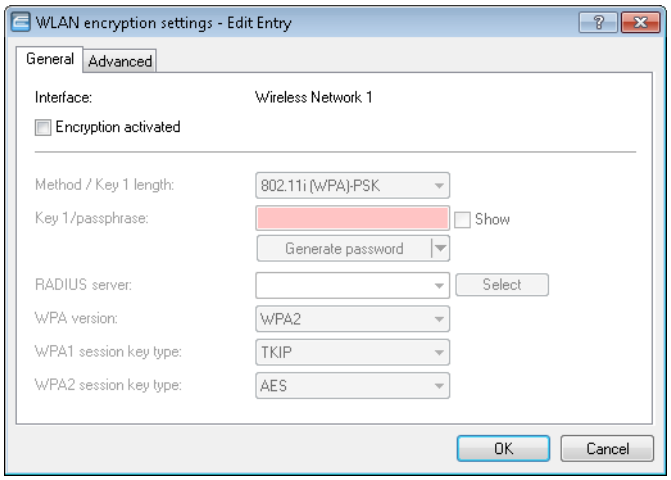
› LANconfig: **IPv4** > **DHCPv4** > **DHCP networks**



9. Disable the encryption for the interface that you are using for the Public Spot.

This setting does not affect: Routers, WLAN controllers, central-site gateways.

Encryption for all logical WLANs is enabled by default. In Public Spot applications, the payload data between the WLAN clients and the access point are usually transmitted unencrypted. For this reason, go to **Wireless LAN** > **Encryption** > **WLAN encryption settings** and disable encryption for the logical WLAN which you previously set up for the Public Spot login.

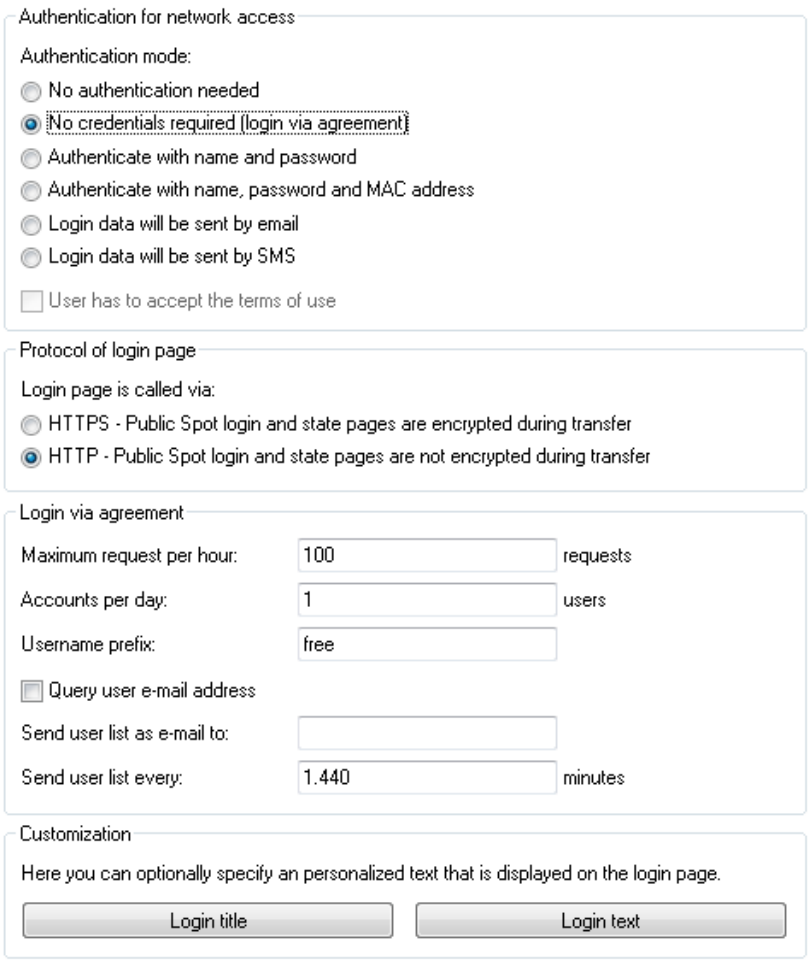


10. Select the authentication mode and the protocol used for the user login.

The authentication method that you select determines the information which users of the Public Spot WLAN must enter when logging in. Select **Authenticate with name and password** to allow your users the option to login with an individual username and password that you have previously assigned them. This setting also allows you to quickly provide Hotspot access to your guests using vouchers (tickets).

Use **HTTPS** as the protocol in order to be able to send encrypted login data to your users during login.

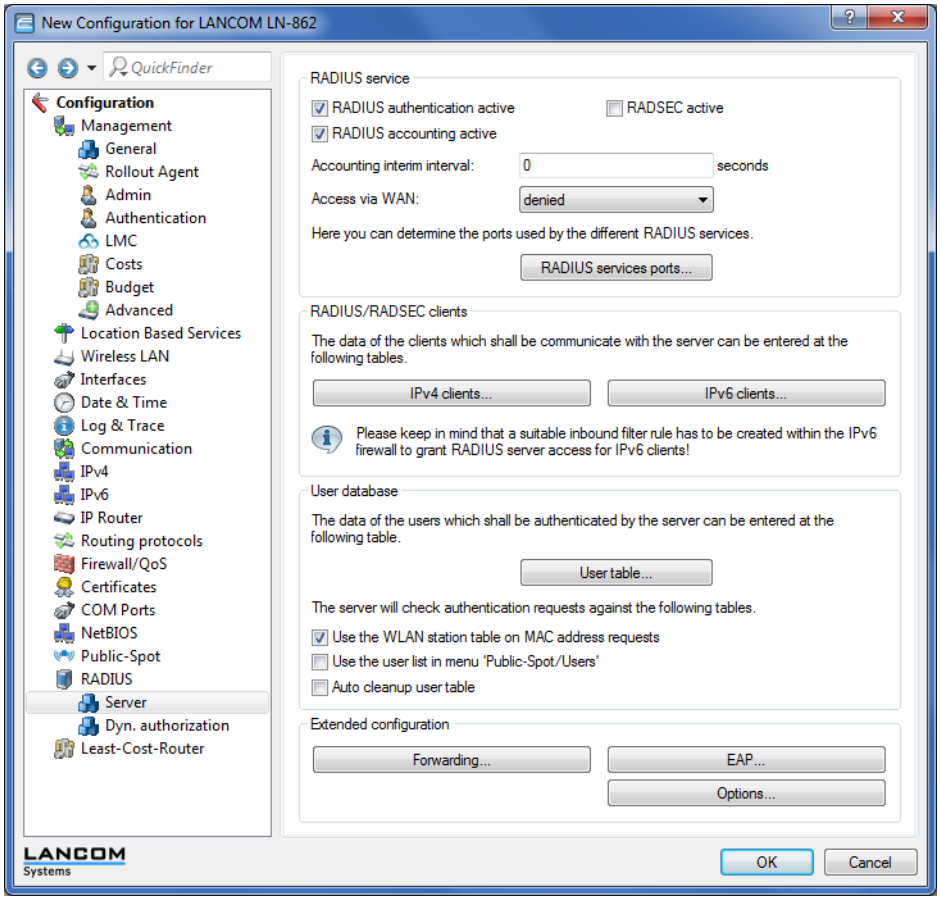
› LANconfig: **Public Spot** > **Authentication** > **Authentication mode**



Pay attention to the fact that, when you select the setting **No authentication needed**, unauthorized persons can have unlimited access to your Public Spot!

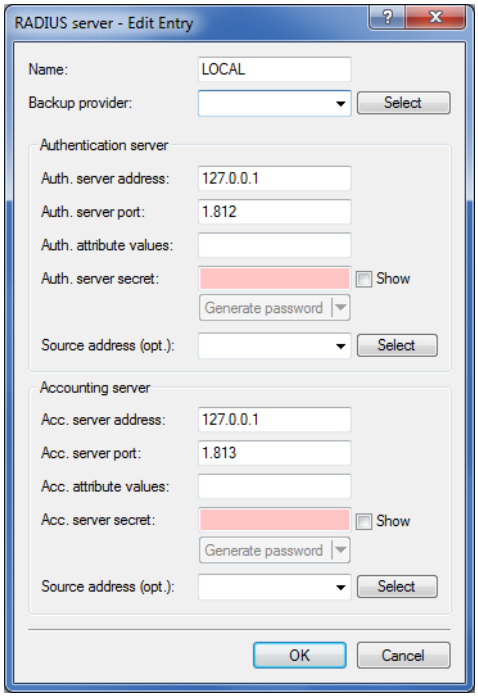
11. Activate the internal RADIUS server for user administration and accounting.
You store Public Spot access accounts in the user database on the device's own RADIUS server.

› LANconfig: **RADIUS** > **Server** > **User database**



12. By default, the Public Spot is preconfigured to use the internal RADIUS server.
The list entry is necessary in order for the Public Spot to recognize the address of the RADIUS server and so that it can authenticate Public Spot access on the internal RADIUS server.

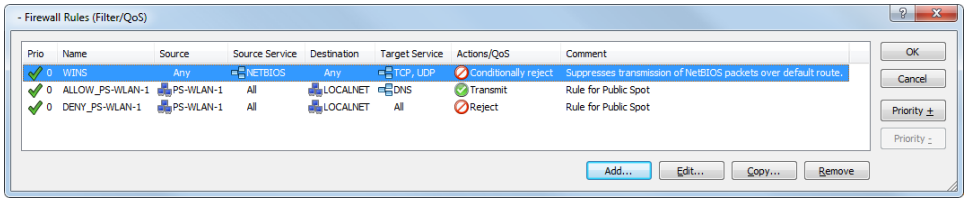
› LANconfig: **Public Spot** > **Users** > **Users and RADIUS servers** > **RADIUS server**

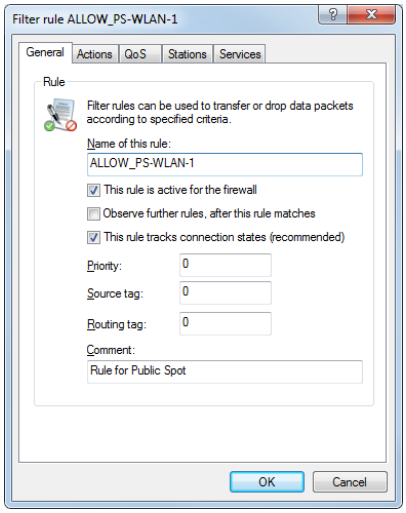


13. Set up filter rules in the Public Spot's firewall to secure your local network. In each case, create an "accept" rule (for example, `ALLOW_PS-WLAN-1`) and a "reject" rule (for example, `DENY_PS-WLAN-1`).

You use the accept rule when devices are to be able to send DNS requests from the Public Spot network to all local networks, e.g., your local intranet. On the other hand, with a reject rule you generally block all access or requests from the Public Spot network to your local network. The order – accept before reject – is essential, since the firewall applies rules from the top to bottom of the list.

› LANconfig: **Firewall/QoS** > **IPv4 Rules** > **Rules…**





› **Settings for the Accept rule:**

a) Enter the name of the rule in **General**, for example, `ALLOW_PS-WLAN-1`.

b) Remove all possible predefined action objects from the list and using **Actions** > **Add..** add an action object of type **ACCEPT**.

c) In **Stations** > **Connection source**, enable the option **Connections from the following stations** and select **Add...** > **Add custom station**.

d) In the Stations window that opens, select the option **All stations in local network** and for **Network name** select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. **Close the dialog with** OK.

e) In **Stations** > **Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.

f) In **Services** > **Protocol/target services** enable the option **Following protocol/target services** and select **Add...** > **DNS**.

g) End the filter rule dialog with a final click on **OK**.
LANconfig then enters the allow rule into the rule table.

› **Settings for the Reject rule:**

a) Enter the name of the rule in **General**, for example, `DENY_PS-WLAN-1`.

b) Remove all possible predefined action objects from the list and using **Actions** > **Add..** add an action object of type **REJECT**.

c) In **Stations** > **Connection source**, enable the option **Connections from the following stations** and select **Add...** > **Add custom station**.

d) In the Stations window that opens, select the option **All stations in local network** and for **Network name** select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. **Close the dialog with** OK.

e) In **Stations** > **Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.

f) End the filter rule dialog with a final click on **OK**.

LANconfig then enters the rejection rule in the rule table.

14. Store the configuration on your device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

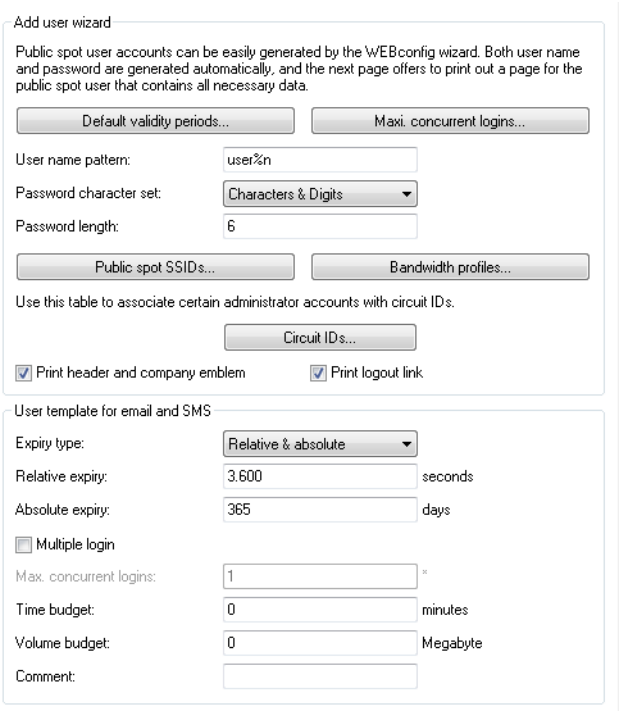
15.2.1.2 Setting default values for the Public Spot wizard

The following section describes how you define default values for the **New user wizard** (setup wizard **Create Public Spot account**) to meet your needs. Public Spot administrators can select the values defined here (e.g. for validity periods, bandwidth profiles, etc.) from selection lists when they are setting up new users and printing out vouchers.

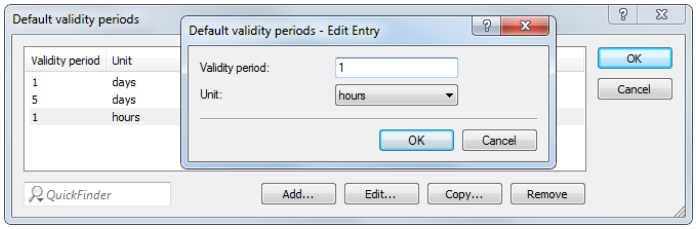
Exceptions to this are the values for User name pattern and Password length shown in the dialog below, which only serve as default values for the device.

1. Start LANconfig and open the configuration dialog for the device.

2. Change the view to **Public Spot** > **Wizard**.

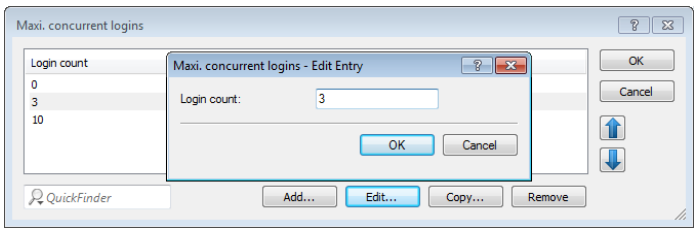


3. In **Default validity periods**, define which default validity periods for user accounts and vouchers are to be available by default.
The new-user wizard takes the shortest validity period as the default.

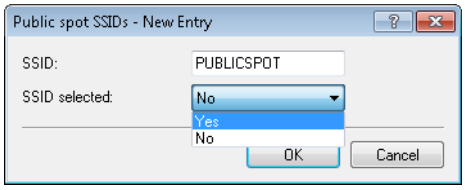


4. Under **Max. concurrent logins** you select the maximum number of devices that have access to the user account simultaneously.

The value `0` stands for 'unlimited'. Whether or not it is generally possible for a user to login with the multiple devices at the same time is determined by the Public Spot administrator with a separate setting in the wizard when creating a new user.



5. In **User name pattern** you specify the pattern used by the new user wizard to create usernames.
   You can enter up to 19 characters, whereby the wizard will automatically create a unique number for every user if you enter "%n". The default description `user%n` will be shown later on the voucher, for example, as `user12345`.
6. Using **Password length** you specify the length of the passwords that the new user wizard generates for Public Spot access.
   The default length is 6 characters. If you would like to have longer passwords, keep in mind that guests can make mistakes when entering them, which can cause unnecessary problems and complaints.
7. Optional: Under **Bandwidth profiles** you set the uplink and downlink limits for each Public Spot user.
   Learn more about this setting under *Manage bandwidth profiles* on page 1260.
8. Public Spot via WLAN only: Using **Public Spot SSIDs** you specify the names of the Public Spot networks taken by default when you create new user accounts using the Create Public Spot account wizard.



   The Create Public Spot account wizard automatically marks the specified network names as **SSID selected** when creating a new Public Spot user. If you employ an access point or WLAN controller, you are able to select several network names as default values in order to give users access to different WLANs. When creating a new user and subsequently printing the voucher, these SSIDs are also printed out on the voucher.

   Using the arrow buttons, you can change the order in which the SSIDs are displayed. In this way, the most popular SSIDs can be placed at the top of the list.

That's it! This concludes the configuration of the default values for the Public Spot wizard.

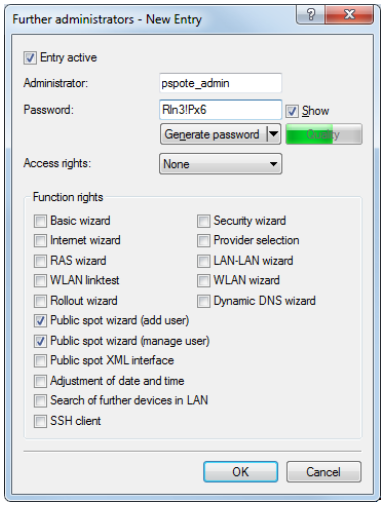
15.2.1.3 Setting up limited administrator rights for Public Spot managers

It is possible to allow employees to create and manage user accounts even though they do not have access rights to the device configuration. This is done by setting up a limited administrator, who only has the right to use the *Public Spot Wizard*. This tutorial describes the steps and the necessary access rights and privileges to do this in LANconfig.

The rights to use the Public Spot Wizards are configurable separately from one another, so it is possible to restrict a limited administrator to any single Wizard. In the case of the Public Spot setup wizard, the restricted administrator logging in to WEBconfig is automatically forwarded to the corresponding input mask.

1. In LANconfig, open the configuration dialog for the device you want to add a Public Spot administrator to.
   The Public Spot option has to be enabled on this device.
2. Navigate to the item **Management** > **Admin**. In the section **Device configuration**, click **Further administrators** and then click **Add**.

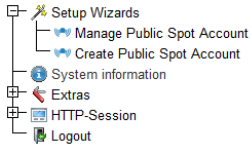
To allow an existing user to perform Public Spot management, you instead select the user's entry in the table and click on **Change**.



3. You activate the profile by checking the **Entry active** box.
4. Assign a descriptive name in the field **Administrator**.
5. Enter a **Password** and repeat it as a check.
6. Set the **Access rights** to **None**.
7. In the section **Function rights** enable the options **Public Spot wizard (add user)**, and **Public Spot wizard (manage user)** for the Public Spot setup wizard.

   The function right **Public Spot XML interface** is not required by a Public Spot administrator. The right is only relevant if you use the XML interface and should not be combined with the function rights described above for security reasons.
8. Save the new or modified administrator profile by clicking on **OK**.

If you have granted the feature rights to several Wizards, the limited administrator can navigate between these using the navigation bar in WEBconfig.



If you have set the function right for the **Public Spot Wizard (create user)** only, then a limited administrator can only navigate within this Wizard, and the navigation bar is hidden. In this case it is not possible to logout of WEBconfig manually. For security reasons, this means that the lifetime of the WEBconfig session is very short. In case of inactivity, the device automatically logs out the limited administrator.

For technical reasons, the Create Public Spot Account wizard does not update automatically after use of the **Create and CSV export** button. A limited administrator who wishes to set up additional users and print vouchers must invoke the Wizard again (e.g. via a URL or by refreshing the web page if the navigation bar is hidden).

15.2.1.4 Setting up and managing Public Spot users for simple scenarios

You can set up and manage Public Spot users either manually or by using the setup wizard. Setting up and managing the configuration options manually offers you more extensive options and allows you, for example, to create self-defined users with an unlimited lifetime.

On the other hand, the setup wizard allows you to create generic Public Spot users with automatically generated login data with limited lifetimes. The respective setup wizard is only accessible using WEBconfig, which allows you to quickly create users without requiring administrator permissions for the entire device. The only requirement is an administrator with limited permissions.

You naturally also have the option to initially create generic users with the aid of the setup wizard and then manually adapt them to your needs (e.g., change the usernames).

Setup and management using the Setup Wizard (WEBconfig)

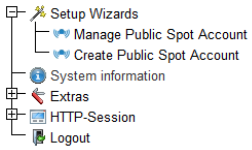
The Setup Wizards provide you with an easy method of managing Public Spot users.

Adding Public Spot users with a single click and voucher printing

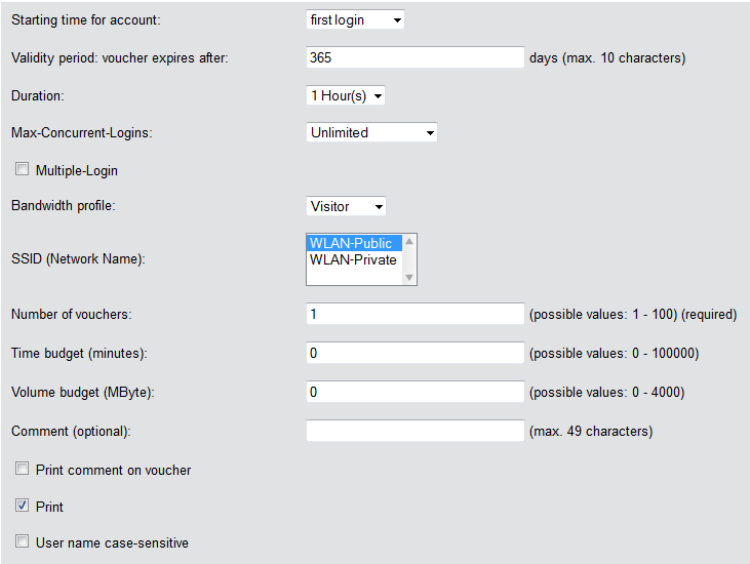
The following section describes the setup of a Public Spot user using WEBconfig and then printing a voucher. You can also prepare vouchers in advance.

You need the permissions for the **Public Spot Wizard (create user)**, in order to create a new Public Spot user.

1. Log on to the WEBconfig home page as an Administrator.
2. Start the setup wizard by clicking on **Setup wizards** > **Create Public Spot account**



3. The new user wizard starts with an input screen. The fields have default values.



The wizard automatically creates a username and a password. In the subsequent printout dialog you can select the voucher printer and print-out the voucher.

4. If necessary, you can change the default values before you print it.

   The following entries affect the appearance as well as the validity of the vouchers:

   - **Starting time for account**: Sets the time when the voucher becomes valid. With the setting **first login**, the access budget runs as of the first login; with the setting **immediately**, it applies as of the time that the user was created.

To a supply of vouchers in advance, select `First login` as the validity of the vouchers. That way the vouchers will still be valid even after a longer period.

- **Validity period: Voucher expires after**: Enter the overall time period within which the voucher can remain valid. If the access is to be valid immediately, it is not possible to enter a validity period.
- **Duration**: Set how long access is to be available after registration or the first login. The values listed here are managed in the **Default validity periods** table.
- **Max-Concurrent-Logins**: Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. The values listed here are managed in the **Max. concurrent logins table**.
- **Multiple login**: Select this option in order to generally allow users to login with several devices using the same login data. The number of devices that can be logged on simultaneously is specified using the drop-down list **Max-concurrent-logins**.
- **Bandwidth profile**: Select a bandwidth profile from the list in order to selectively restrict the amount of bandwidth available to the user (uplink and downlink). Create a bandwidth profile in the **Bandwidth profile** table.
- **SSID (network name)**: Specify which wireless LAN network the access applies to. This SSIDs listed here are managed in the **SSID table**. By pressing the "Ctrl" button you have the option of selecting multiple entries. Default entries are already pre-selected.

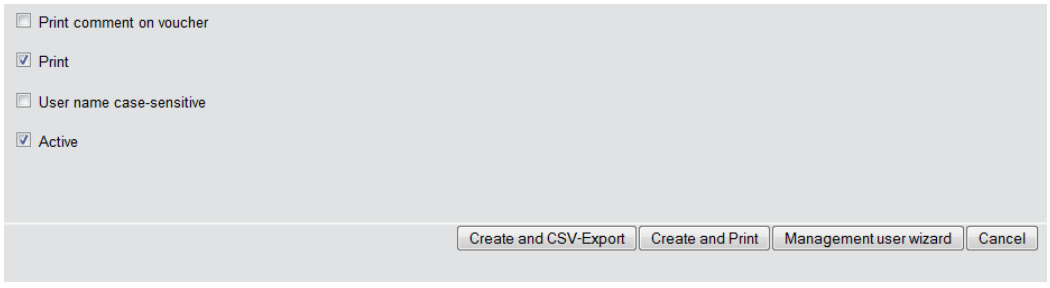
  If you have not defined any entries in the table, the wizard conceals this option.

- **Number of vouchers**: Specify how many vouchers you want to create at a time. If you set the login time as the access start time, you can print-out a supply of vouchers in advance.
- **Time budget (minutes)**: Specify the amount of time after which access to the Public Spot is closed. Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).
- **Volume budget (MByte)**: Specify the available data volume after which access is closed.
- **Comment (optional)**: Enter a comment here. This comment can contain, for example, additional notes about the access duration or the telephone number of the receptionist in case of access problems.
- **Print comment on voucher**: Check this option if the comment is to appear on the voucher.
- **Print:** Check this option to print the vouchers as soon as they are registered.
- **User name case-sensitive**: Enable this option if Public Spot users have to pay attention to capitalization when entering their user name at login.

5. If you want to keep the default values or accept the new values without changing them, you click on **Save and print** at the end.

   If the **Print** option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.

   The button **Manage User Wizard** button takes you to the **Manage Public Spot Account** Setup Wizard.



You have the option to either show or hide this button. It is displayed by default.

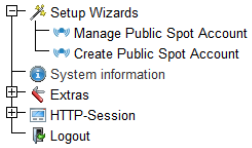
Wizard for Public Spot user management

The following section describes how to use WEBconfig to manage the registered Public Spot users.

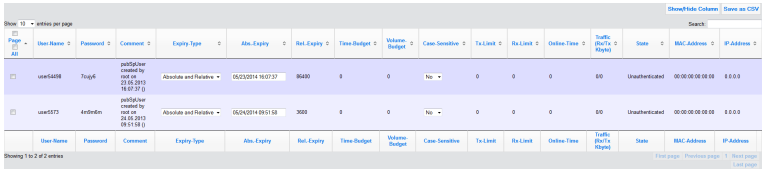
You need the **Public Spot wizard (user management)** permission, in order to manage a Public Spot account.

Unsaved changes are lost once you finish this wizard.

1. Log on to the WEBconfig home page as an Administrator.
2. Start the setup wizard by clicking on **Setup-Wizards** > **Manage Public Spot accounts**



3. The Public Spot wizard starts with a list of registered Public Spot users.



In the **Show... entries per page** drop-down list you set how many entries are displayed per page. The corresponding pages are accessed via the page navigation at the lower right:

- **First page**: Shows the page with the first entries.
- **Previous page**: Returns to the previous page.
- **Page numbers (1, 2, 3, ...)**: Goes directly to the chosen page.
- **Next page**: Goes to the next page.
- **Last page**: Shows the page with the latest entries.

With **Search** you can filter the displayed entries. The filter immediately searches for entered strings.

You export highlighted entries with **Save as CSV**.

The column headers have the following meaning:

- **Page/All**: This column is used to select the user for the desired action (print, delete, save). To select all entries on the current page, select **Page**. To select all of the entries, select **All**.
- **User name**: Manually or automatically displays the username generated by the system.
- **Password**: Manually or automatically displays the password generated by the system.
- **Comment**: Includes the comment entered at registration (in brackets) and any changes to the user data (automatically documented by the system).
- **Expiry type**: Indicates whether the validity period of this user account is absolute (e.g. expires on a set date) or relative (expires after the time has elapsed since the first successful login).
- **Abs.-Expiry**: If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined in this field.
- **Rel.-Expiry**: If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.
- **Time budget**: Specifies the maximum access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.
- **Volume budget**: Specifies the maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.
- **Case sensitive**: Indicates whether the login page takes capitalization of the user name into account.
- **Tx-Limit**: If a bandwidth profile was entered for the user, this entry shows the maximum transmission bandwidth available to that user.

- **Rx-Limit**: If a bandwidth profile was entered for the user, this entry shows the maximum receiving bandwidth available to that user.
- **Traffic (Rx/Tx Kbyte)**: Indicates the data volume in kilobytes that the user has received (Rx) or sent (Tx) so far.
- **State**: Displays the authentication status of each user, i.e. whether the user is currently logged on to the Public Spot (**Authenticated**) or not (**Unauthenticated**).
- **MAC address**: Indicates the physical address of the network adapter for the device with which the user is currently connected.
- **IP address**: This shows the IPv4 address that the system currently has allocated to the user.

The buttons at the bottom of the window have the following functions:

- **Print**: Print out the voucher for the selected user.
- **Delete**: Delete the selected user.
- **Save**: Save the changes.
- **Back to main page**: Return to the main page; all unsaved changes will be lost.

You can edit the following user information by changing the contents of the corresponding fields:

- **Expiry type**
- **Abs.-Expiry**
- **Rel.-Expiry**
- **Case sensitive**

4. Select the account that you want to edit in the first column.
5. Change the corresponding field values and click **Save** to apply the changes. Unsaved changes are lost once you finish this wizard.
6. If you would like to delete a user, mark the corresponding entry in the first column and click **Delete**.

The deletion takes place immediately without confirmation.

Hiding fields in WEBconfig

In the setup wizard "Manage Public Spot Account", the **Show/hide column** button enables you to display or conceal columns of the table. These changes are only temporary. Hidden columns are shown again after a page refresh or in a new session.

If you want to permanently hide specific fields, use the LCOS menu tree and navigate to the view **Setup** > **Public Spot module** > **Manage user wizard**. All of the fields are displayed by default. If you hide certain fields, for example to conceal the time budget, they will stay hidden in the wizard itself and also in the drop-down menu behind the button **Show/hide column** after reloading the page.

In order to delete authenticated Public Spot users, the columns "Calling station ID mask" and "Called station ID mask" need to be visible in the wizard. Unauthenticated users can be deleted even if these two columns are hidden.

Please note that hidden fields are not printed out when you press the **Print** button. On the other hand, exporting a CSV file includes all of the data. The **Save as CSV** button can optionally be hidden. To do this, use the LCOS menu tree to navigate to the view **Setup** > **Public Spot module** > **Add User Wizard** > **Hide CSV export** . Select "Yes" and save your entry.

Manual set up and management

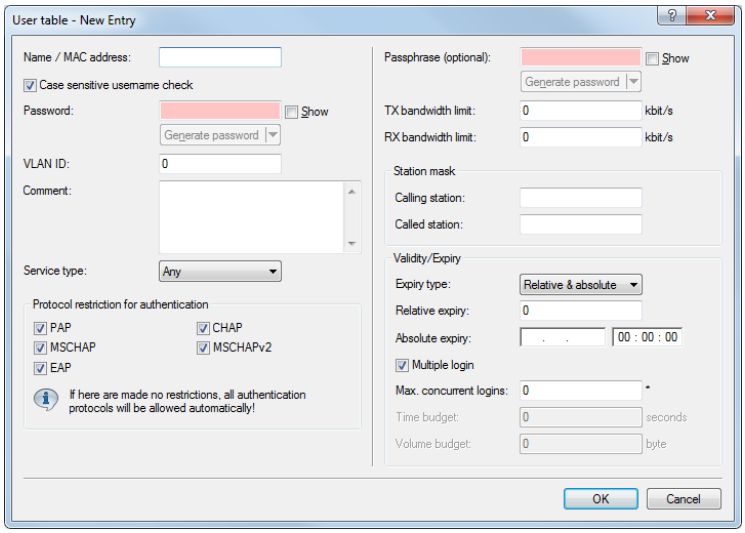
The following configuration steps show you how to use LANconfig to manually setup a Public Spot user for simple scenarios. You create and manage Public Spot users using the **User database** of the device's internal RADIUS server under **RADIUS** > **Server** > **User database**. Here you enter all of the users who should have access to the Public Spot – just as the setup wizard does as well.

For user administration, the Public Spot module also has its own internal list (found under **Public Spot** > **Users** > **User list**). During technical development, this list was replaced as of LCOS 7.70 by the user administration via RADIUS. For compatibility reasons, the device still evaluates the internal user list of the Public Spot module if it is enabled. However, for a new installation you should no longer use this list, since it prevents you from using many features (setup and administration using the wizard, bandwidth restrictions, accounting via RADIUS, VLAN IDs for Public Spot users, etc.).

1. In **Name** you enter the usernames of future users or the **MAC addresses** of their end devices.

   If you selected the authentication mode **Login with name and password**, enter the name of the username that the user employs to authenticate on the Public Spot. Entering a **password** is optional, however it is recommended for the authentication mode above.

   › LANconfig: **RADIUS** > **Server** > **User database** > **User table**



   If the authentication is performed using the MAC address (authentication modus **Authenticate with name, password and MAC address**), you define the MAC address using the field **Calling station** in the format `12:34:56:78:90:AB`.

2. Set the **Service-Type** to `Login`.

3. You remove all protocol restrictions by deselecting all check boxes.
   Two-phase authentication is not performed in a Public Spot scenario. This only makes sense for direct WLAN connections without Public Spot operations and the associated RADIUS users.

   If you do not completely remove the protocol restrictions, a user cannot log in using the login web page of your Public Spot!

4. Optional: On request, you can also, for example,

   › Enter a relative and/or absolute expiry date for the validity of the user account in the section **Validity/Expiry** (relative = validity in seconds after the first login);
   › Limit the uplink/downlink under **TX/RX bandwidth limit**;
   › Enable **Multiple login** and enter the **Max. concurrent logins** of end devices

5. Store the configuration on your device.

That's it! Your Public Spot users can now login with the credentials that you specified.

15.2.2 Security settings

The Public Spot has two additional safety mechanisms that effectively protect it against abuse.

15.2.2.1 Traffic limit option

In order for clients to login to the Public Spot via a browser, it must be possible for unauthorized users to transfer data packets (e.g. for DNS requests) to the access point. By default, there is no limit on this data. The following risks are associated with this:

- **Unauthorized use of the Public Spot:** Certain tools enable a user to pack data into a DNS packet (i.e. to establish a DNS tunnel) and to work with the Public Spot without logging in.
- **Denial-of-Service:** The attacker could send large amounts of data to the device and thus try to block the device or Public Spot.
- **Brute force:** The attacker could repeatedly try to access the base station by guessing the login data until successfully breaking in.

The traffic limit option can effectively eliminate these risks.

You enable the traffic limit option by setting a value other than "0". This value determines the maximum data quantity in bytes that can be transmitted between the base station and an unauthorized terminal device.

- LANconfig: **Public Spot** > **Server** > **Allow access without authentication** > **Maximum data volume**

When a terminal device exceeds this traffic volume, the Public Spot locks this device and drops all data received from it without inspection. This lock expires only when the device entry disappears from the station table.

For WLAN devices, this deletion can follow the general idle timeout, for example:

- WEBconfig: **Extras** > **LCOS menu tree** > **Setup** > **WLAN** > **Idle-Timeout**

Please keep in mind that if station monitoring is active, the lock may be removed earlier. If the mobile station cannot be reached for 60 seconds, the device removes its entry from the station table, and also the block.

The idle timeout for the Public Spot module has the same purpose as the idle timeout for WLANs, but it applies only to connections via Public Spots. If the idle timeout is set and no further data packets are received from a user, the device automatically logs the device out at the end of the specified time period.

- LANconfig: **Public Spot** > **Server** > **Idle timeout**

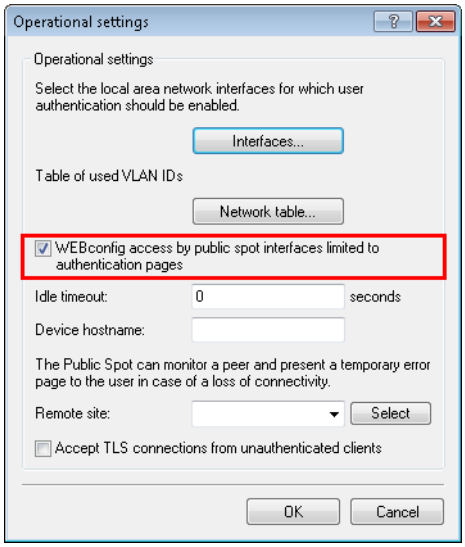
On the one hand the optimal value for traffic limit depends on the data volume of the login page. On the other hand, this value has a significant effect on the potential number of failed login attempts per user. Generally, a traffic limit of 60,000 bytes provides effective protection for a Public Spot but allows a sufficient number of login attempts. You can adjust this value to your individual needs, if necessary. The default value of "0" bytes allows an unlimited volume of data.

The traffic limit option only monitors the traffic before authentication. It does not take into account the traffic to and from a free Web server. This remains unlimited at all times.

15.2.2.2 Restricting access to the configuration

Public Spot access to a Public Spot network's configuration (WEBconfig) should always be prohibited for security reasons. A special switch allows access via the Public Spot interface to be restricted to the Public Spot authentication pages only. All other configuration protocols are automatically blocked.

- LANconfig: **Public Spot** > **Server** > **Operational settings** > **WEBconfig access by Public Spot interfaces limited to authentication pages**



Note that using permissions under **Management** > **Admin** > **Configurations access ways** > **Access rights** you cannot generally limit the access via HTTP(S) to the device.

15.2.3 Extended functions and settings

The Public Spot offers a wide range of extended functions, options and parameters, which can be used to adapt it to the specific requirements of the application at hand.

In the following sections you will find information about:

- Multiple logins

  By default, the use of login data is restricted to login with one device. Find out how you increase this limit or completely remove this limit for a user account.

- Open access networks (no login)

  Setup additional networks so that Public Spot users can also reach them without logging in to the Public Spot to provide the user with additional information (e.g., customer web sites inside the company, event calendars in a hotel).

- User administration using the Web API

  Use URLs to create and administrate Public Spot users with file links or scripts.

- Individual bandwidth limitation

  Individually set uplink and downlink restrictions for each Public Spot user.

- Automatic cleanup of user accounts and mobile stations

  Use the device's own functions to automatically delete expired Public Spot user accounts and improperly logged off mobile stations (WLAN only) from the device's internal databases.

- WLAN handover of sessions between devices

  Find out more about the roaming possibilities of mobile stations between access points, and what special configurations are necessary so that your users benefit from the seamless handover of WLAN sessions.

- Authentication via RADIUS

  Find out how you can provide multiple RADIUS servers for authentication and accounting, and how you can chain them, in order to forward the user data to the appropriate backup system in case individual systems are unavailable.

- Accounting for Public Spot connections for commercial operation

  Learn more about the accounting functions provided by the Public Spot for commercial operations. These billing functions can be roughly divided into two models:

  - Retrospective payment for the resources actually used (credit accounting)
  - Service use on a debit payment basis (PrePaid)

- Using multi-level certificates

  Find out how to load certificate chains on your device.

- Individual assignment of VLAN IDs

  Find out how to assign individual VLAN IDs to specific Public Spot users.

15.2.3.1 Multiple logins

You have the ability to allow Public Spot users to simultaneously sign in using one user account for multiple devices. This can be necessary for a group of people (for example, a family) that has multiple devices, which they would like to use to simultaneously access the Internet.

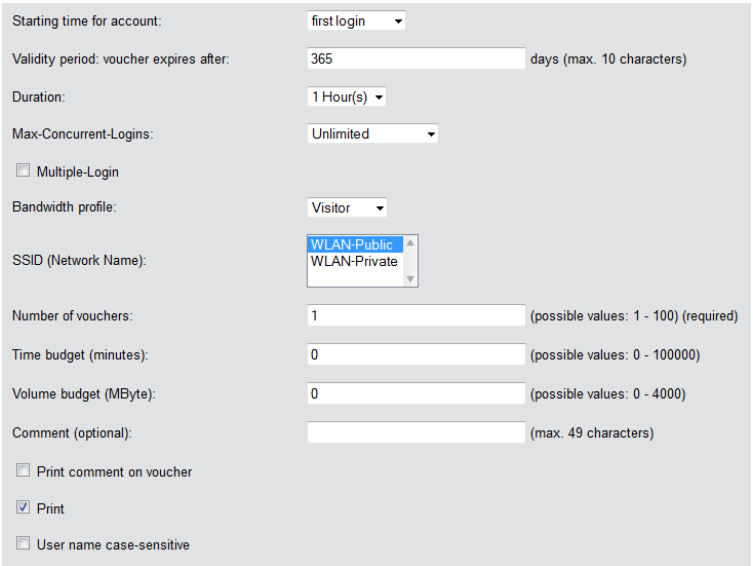
Setting default values

To use this feature, define the number of concurrent devices in the setup menu under **Public Spot module** > **Add user wizard** > **Max. concurrent logins table**. Enter the values here that you assigned in the second step with the **Create Public Spot account**. The value `0` stands for "unlimited".

Enabling multiple logins in the new user wizard

When you invoke the Wizard **Create Public Spot account**, you will see the menu item **Max concurrent logins**. The values shown here correspond to the numbers that you previously entered in the table of the same name. The values are shown within the phrase "Only ... device(s)".

Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. Please note that to enable the feature in the wizard, the option **Allow multiple logins** must also be enabled.



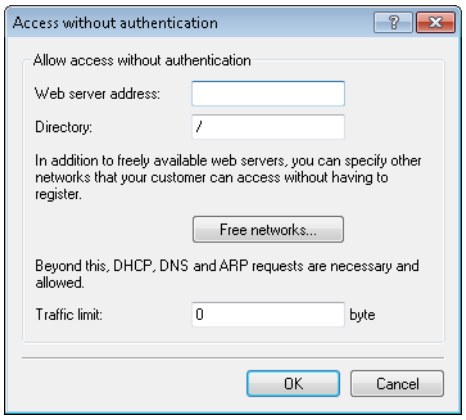
15.2.3.2 Open access networks (no login)

To provide users with access to important information without them having to login (e.g., important contact information) you can define any publicly available Web server.

› LANconfig: **Public Spot** > **Server** > **Access without authentication**

If you do not want to completely release this service, you can optionally define an alternative path to the web server.

› LANconfig: **Public-Spot** > **Server** > **Access without authentication** > **Directory**

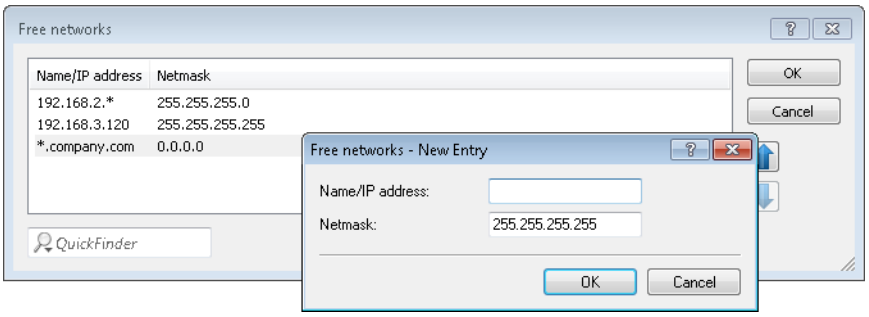


In addition to freely available web servers, you can define other networks and special sites which your customers can access without having to log on.

› **Public-Spot** > **Server** > **Access without authentication** > **Free networks**

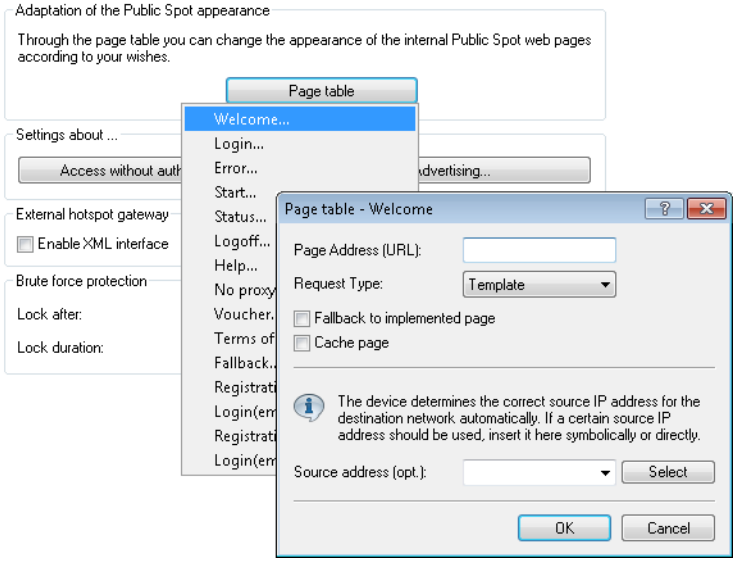
Enter the IP address of the server or of the network with its netmask, that your Public Spot users are to be given access to. Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow free access to all of the subdomains of a particular domain. The entry `*.company.com` allows the addresses `mail.company.com`, and `service.company.com`, etc.

If you wish to authorize a domain or just a single workstation with the address named earlier, set `255.255.255.255` as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value `0.0.0.0`), the device ignores the table entry.



› **Public Spot** > **Server** > **Page table**

Enter the addresses (URLs) of the web pages to be displayed to users on the Public Spot in case of login, error, status display, etc. Read the chapter about *Default and customized authentication pages*.



DNS snooping

Web services with a high number of users distribute the requests for data to multiple servers for better utilization. This means that two DNS queries for the same hostname (e.g. "www.google.com") can lead to to two different IP addresses. If a Public Spot receives more than one valid IP address for the specified host name from the DNS server, it chooses one of them and stores it for future requests by Public Spot users. If a different IP address for the same host name is allocated to the user by a different server for a subsequent request, the Public Spot blocks this connection because this IP address is not stored as the authenticated one.

In order for Public Spot users to be able to connect to the requested host despite changing IP addresses, the Public Spot analyzes the user's DNS queries and stores the returned IP address with the host name, the valid time to live (TTL), the age and the data source as a free destination address in the table **Status** > **Public Spot** > **Free-Hosts** for subsequent use.

The entries in this table will expire after the time period defined in the DNS response (TTL). When the limits are very low (e.g. 5 seconds), you can avoid locking out Public Spot users immediately after a request by setting a minimum validity under **Setup** > **Public Spot-Module** > **Free-Hosts-Minimum-TTL**.

15.2.3.3 Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

URL structure

The URL is structured as follows:

```
http://<Device-URL>/cmdpbspotuser/...?action=actiontodo&parameter1=value1&parameter2=value2
```

The following actions are available:

- **action=addpbspotuser**: Creates one or more new Public Spot users and then prints out the required number of vouchers.
- **action=delpbspotuser**: Deletes the Public Spot user with the specified user ID.
- **action=editpbspotuser**: Displays the Public Spot user with the specified user ID. You can then print out the user's voucher again.

The required parameters and their values depend on the action specified.

The Wizard ignores incorrect parameter information and accepts only the correct parameters. If you omit a required parameter or specify it incorrectly, the wizard displays an input mask. Enter the correct parameter values here.

Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

`comment`

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

```
&comment=<Content1>:<FieldName1>;<Content2>:<FieldName2>;...;<Content5>:<FeildName5>
```

If there is just one comment field per user, then the comment is entered as follows:

```
&comment=<Comment>
```

Special characters such as German umlauts are not supported.

The maximum number of characters for the comment parameter is 191 characters.

`print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

`printcomment`

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

`nbGuests`

Number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

`defaults`

Use default values

The wizard replaces missing or incorrect parameters with default values.

`expirytype`

Combined output of expiry type and, if applicable, the validity period of the voucher.

Specify this parameter as follows:

```
&expirytype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.

- `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

If a parameter is omitted or set with incorrect values the wizard will apply the default values.

`ssid`

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

`unit`

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- `Value1`: LIfetime units. Possible values are: Minute, hour, day
- `Value2`: Duration

`timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

`volumebudget`

Volume budget

The following entries are allowed:

- `k` or `K`: Specified in kilobytes (kB), e.g. `volumebudget=1000k`.
- `m` or `M`: Specified in megabytes (MB), e.g. `volumebudget=1000m`.
- `g` or `G`: Specified in gigabytes (GB), e.g. `volumebudget=1g`.

Without a unit, the specification corresponds to a value in bytes (B).

If this parameter is omitted completely, the wizard uses the default value.

`multilogin`

Multiple logins

If you specify this parameter, the user can login multiple times with his/her user account. If this parameter is missing, multiple logins are disabled by default.

`maxconclogin`

Maximum number of concurrent logins

With this parameter you specify with how many different end devices a user can login to a Public Spot. Valid entries are integers such as `0, 1, 2, ...`.

If this parameter is missing or if the parameter has the value `0`, this means that the number of devices is unlimited.

This parameter requires that multiple logins be enabled. Setting this parameter in isolation has no other effects.

casesensitive

Username case sensitive

If you enter this parameter, the Public Spot user must pay attention to capitalization when entering the user name at login. Valid values are:

- `0`: Case-sensitive username is disabled
- `1`: Case-sensitive username is enabled

If this parameter is omitted, the wizard uses the default value.

bandwidthprof

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under **Setup** > **Public Spot module** > **Add user wizard** > **Bandwidth profiles**, such as

```
&bandwidthprof=1
```

to index the first entry in the table.

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Modifying a Public Spot user

Modify one or more Public Spot users simply by entering the following URL:

```
http://<device-URL>/cmdpbspotuser/...?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

pbspotuser

Name of the Public Spot user

Specify multiple users in the form `&=pbspotuser=<User1>+<User2>+...`.

If the wizard cannot find the specified user, you have the option to search for a user.

After making your changes, accept these and print them out if necessary.

expirytype

Combined output of expiry type and, if applicable, the validity period of the voucher.

Specify this parameter as follows:

```
&expirytype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.
- `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

If a parameter is omitted or set with incorrect values the wizard will apply the default values.

`unit`

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- `Value1`: LIfetime units. Possible values are: Minute, hour, day
- `Value2`: Duration

`timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

`volumebudget`

Volume budget

If this parameter is omitted, the wizard uses the default value.

`print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button. Use this to print out the voucher.

`bandwidthprof`

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under **Setup** > **Public Spot module** > **Add user wizard** > **Bandwidth profiles**, such as

```
&bandwidthprof=1
```

to index the first entry in the table.

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Deleting a Public Spot user

Delete one or more Public Spot users simply by entering the following URL:

```
http://<deviceURL>/cmdpbspotuser/...?action=delpbspotuser&pbSpotuser=<User1>+<User2>+...
```

If the wizard finds the specified user in the user list, the user is deleted and the wizard displays a confirming message.

If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

15.2.3.4 Creating Public Spot users on a remote Public Spot gateway

With Smart Ticket operating, each user is given a Public Spot account on the RADIUS server of the local Public Spot gateway.

However, where multiple Public Spot gateways are in use but the user accounts should be managed by the RADIUS server of just one gateway, Smart Ticket causes the Public Spot account to be created on this central RADIUS server. To

implement this, the remote Public Spot gateway needs to be specified in the LCOS menu tree under **Setup** > **Public Spot module** > **Authentication modules**.

If no remote Public Spot gateway is defined, the Public Spot user accounts are created on the local Public Spot gateway.

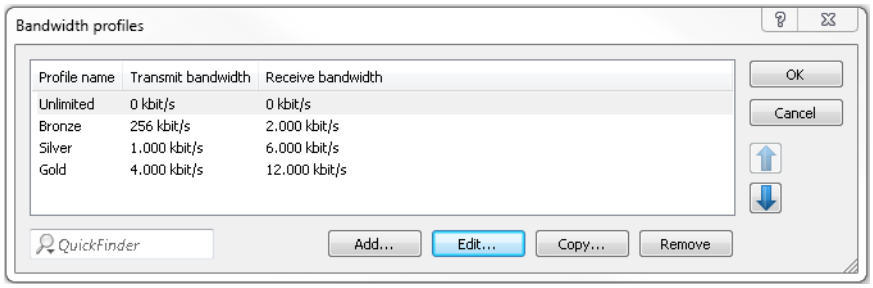
15.2.3.5 Bandwidth profile

Manage bandwidth profiles

Using the window **Public-Spot** > **Wizard** > **Bandwidth profiles**, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. You can select a predefined profile or create your own bandwidth profiles that meet your needs. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Cerate Public Spot account** in WEBconfig.

Integrating predefined bandwidth profiles

From the four predefined profiles, select the bandwidth profile that closest meets your requirements:



Unlimited

No restriction in the transmit and receive bandwidth.

These values refer to the transmit bandwidth (TX) and receive bandwidth (RX) from the perspective of the client.

Bronze

The transmit (TX) bandwidth is 256 kbps, the receive (RX) bandwidth is 2 Mbps.

Silver

The transmit (TX) bandwidth is 1 Mbps, the receive (RX) bandwidth is 6 Mbps.

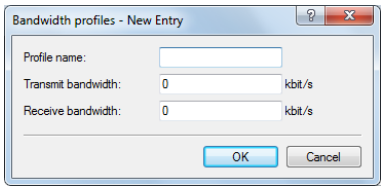
Gold

The transmit (TX) bandwidth is 4 Mbps, the receive (RX) bandwidth is 12 Mbps.

You have the option of customizing the predefined entries to meet your requirements. Select the profile for editing and click the button **Edit**. Alternatively, you can create your own profiles.

Creating your own bandwidth profiles

In order to add manual entries to the table **Bandwidth profiles**, click on the button **Add...**.



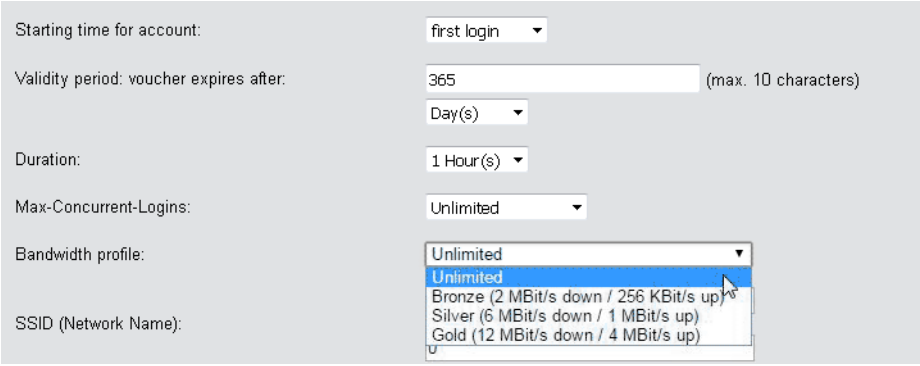
The entries in the edit window have the following meaning:

- **Profile name**: Enter the name for the bandwidth profile here.
- **TX bandwidth**: Enter the maximum uplink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.
- **RX bandwidth**: Enter the maximum downlink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.

Assigning bandwidth profiles

The following steps describe how you assign the available bandwidth profiles to a Public Spot user.

1. Open WEBconfig.
2. Start the add user wizard under **Setup Wizards** > **Create Public Spot account**.
3. Assign the new user an appropriate profile from the selection list **Bandwidth profile**.



When creating a new user, the RADIUS server automatically assigns the upper and lower boundaries of the bandwidth profile (not the bandwidth profile per se) to the associated account.

15.2.3.6 Auto cleanup user table

The device gives you the option to delete expired accounts for Public Spot users automatically.

Users of the Public Spot Wizard are generally administrators with restricted rights who are often unable to delete user table entries themselves. Because the user table has a limited number of entries, outdated entries could limit the capacity of the Public Spot. We strongly recommend that you activate this option.

If you use the internal RADIUS server for the administration of user accounts, enable automatic clean-up under **RADIUS** > **Server** > **User database** > **Auto cleanup user table**.

These settings have no effect on the user table on an external RADIUS server.

The following list offers you a general overview of which capacity limits apply to specific models. If you cannot find your device, please check the exact details in the product description.

Table 31: Size of the user table for specific LANCOM models

LANCOM model	User table size
with **Public Spot** option: - LANCOM LN-17xx serie - LANCOM L(N)-8xx - LANCOM LN-630acn - LANCOM L-3xx series - LANCOM IAP-4G+	64

LANCOM model	User table size
› LANCOM IAP-8xx series › LANCOM IAP-5G › LANCOM OAP-8xx series › LANCOM OAP-5G	
› LANCOM vRouter 50 › LANCOM 178x series › LANCOM 179x series › LANCOM 18xx series	128
› LANCOM 19xx series › LANCOM WLC-4006(+) › LANCOM vRouter 250 › LANCOM 2100 › LANCOM WLC-30 › LANCOM WLC-60	256
› LANCOM vRouter 500 › LANCOM vRouter 1000 › LANCOM vRouter unlimited with **Public Spot XL** option: › LANCOM ISG-1000 › LANCOM ISG-4000 › LANCOM ISG-5000 › LANCOM ISG-8000 › LANCOM WLC-1000 › LANCOM WLC-2000	unlimited*

*) No limitation on the table; however, an upper limit of max. 2,500 users is recommended.

15.2.3.7 Station monitoring

If station monitoring is activated, the Public Spot regularly checks to see if the associated end devices are still available. Lost end devices are automatically deleted from the local user table. If station monitoring is switched off, a user is not logged off until the validity period of the user's authentication expires.

Station monitoring is extremely important for Public Spots operating commercially on a time basis. In installations of this type, users must be assured that they are only paying for the time actually spent using the Public Spot services.

Configuration

Station monitoring for the Public Spot Module is disabled by default. You activate it by entering a value greater than `0` – this value disables the function – under **Public Spot** > **Server** > **Interface selection** > **Idle timeout**. From this point on, all end devices are automatically disconnected from the Public Spot after a specific time.

If your Public Spot device has WLAN, you also have the option of enabling station monitoring globally for all WLAN interfaces. You can find the corresponding settings under **Wireless LAN** > **Security** > **Monitor stations to detect inactive ones**. To do this, the device disconnects mobile stations after 60 seconds (default value). If WLAN station monitoring is disabled, by default this may take up to 15 minutes.

If you offer Public Spot via WLAN, please note that the station monitoring of the WLAN takes priority over that for the Public Spot, and a disconnection can occur earlier if the idle timeout for WLAN (configurable in the Setup menu under **WLAN** > **Idle timeout**) is less than that for the Public Spot.

Monitoring

You can monitor the Public Spot during operation using WEBconfig. The station table in the user authentication menu provides an overview of:

- Users currently logged in to the Public Spot and
- End devices in the WLAN which are not logged in.

You navigate to the Stations table in the Status menu under **Public Spot** > **Stations table**. Using the button **Monitor this table** you automatically refresh the table display at regular intervals.

15.2.3.8 WLAN handover of sessions between devices

Whenever a site equipped with WLAN hotspots expands, it may be necessary to deploy more than one access point to cover the whole area. One option would be to use a central device as an authentication gateway, enable the Public Spot option on this device only, and require all other access points to redirect requests to the central device. In this way, all other access points act as simple, transparent bridges, which connect to the central gateway using the Ethernet backbone. This allows clients to freely roam among the access points since all session information is kept in the central gateway.

This variant has two drawbacks, however:

- The central gateway is a single point of failure, and is not scalable. You can reduce the risk of failures by using VRRP to create a redundancy solution.

  This solution requires an external RADIUS server, since VRRP cannot synchronize configurations, e.g. the user database. However, this means that certain functions (such as the Public Spot wizards in WEBconfig) are no longer available.
- Roaming is only necessary when the Public Spot module is installed on the access points themselves. Using a WLC, the authentication can be forwarded to the central gateway. In this case, the roaming between access points is transparent to the WLAN controller.

An alternative to this type of centralized setup is to enable the Public Spot module in all of the access points. Authentication and page processing handling is thereby distributed over all devices, and a single point of failure is eliminated.

IAPP (inter access point protocol)

Since the Public Spot module is implemented as a "switchable" transparent bridge, there is no need for clients to acquire a new IP address after they roamed to another access point, so there is no need to terminate open connections. This results in the requirement that an already authenticated client does not have to re-authenticate after roaming to a new access point. Thus the authentication information should be carried over from the old to the new access point.

Access points use the IAPP (inter access point protocol) to share information about roaming clients: Whenever a wireless client decides to change to another access point, it has the option of informing the new AP about which AP it was previously connected to. This information, combined with regular Hello packets on the Ethernet backbone, enable the new access point to inform the old access point. The old access point can then remove the client from its station table and acknowledge the handover.

If a client does not use the corresponding Reassociate packet for connecting to the new access point, the new access point sends a handover request as a multicast on the backbone, instead of a directed packet to the old access point. This means that this handover also works for clients that do not support IAPP.

The main task of the IAPP in a WLAN is to tell the old access point not to send any more packets to the corresponding client in its wireless area, since it will no longer receive them. This type of behavior (based on the definition of the 802.11 frame exchange protocol) could otherwise cause problems with other clients that are connected with it.

In case of an enabled Public Spot module, the communication channel provided by IAPP is used to transport the session information of wireless clients. Whenever an access point receives a handover request for one of its wireless clients, and if a session record for this client is available in its station table, it will append state information about this client to the requesting access point. This information includes:

- The client's current state (authenticated or not authenticated)

In case the client is authenticated, it also includes:

- The username used to authenticate
- The amount of data traffic generated by the client so far
- The session duration so far
- The IP address of the client
- Possible limits on the session duration and data volumes
- Possible information about idle timeouts

- If RADIUS accounting was used for the session:
  - The entry used for RADIUS accounting in the authentication server list, referenced by name
  - The accounting cycle used for interim updates

After a successful transfer, the old access point terminates the session, which, in the case of RADIUS accounting, means that it sends an accounting stop request to the RADIUS accounting server. This is necessary since a RADIUS server can use the NAS identification to associate requests with specific sessions, and these requests can no longer be associated with the correct sessions once the data packets for a session come from more than one device. If an access point receives this information in a handover reply, it immediately marks the client as authenticated and starts a new RADIUS accounting session, if possible.

Note that the new access point requires a corresponding entry in its **Authentication server** list in order to receive the necessary information. The specific part of the handover reply for the Public Spot module is protected by a shared secret, which is set in the setup menu under **Public-Spot-Module** > **Roaming-Secret**. These security measures should prevent falsification of handover replies. Without a password configured, the access point does not append the information above on a handover reply, which forces the client to authenticate again.

15.2.3.9 Authentication via RADIUS

RADIUS is an extensively accepted protocol for providing large groups of users access to a server. Although it was originally developed for dial-in server access over telephone lines, the concept is also useful for the hotspot authentication process. For that reason, it can be used in a more complex provider network, for example, to provide access for the same users via dial-in and hotspots. You configure RADIUS servers and their access parameters in the dialog **Public Spot** > **Users** > **Users and RADIUS servers** under **RADIUS server**.

In certain scenarios, it can be feasible to use more than one RADIUS server. In general, a RADIUS server is specified by its IP address, the UDP port the RADIUS service is bound to (typical ports are 1645 or 1812), and a so-called "shared secret". This is a random character string which acts as a password for access to the server. Only clients which know the shared secret can interact with the RADIUS server, since the password for the user account is hashed instead of being sent in cleartext.

If you operate your own external login portal, it is possible to change the attributes of Public Spot sessions after the user has authenticated. This is achieved with dynamic authorization by means of RADIUS CoA (Change of Authorization) (see *Dynamic authorization by RADIUS CoA (Change of Authorization)* on page 1557 and *Enabling the acceptance of RADIUS CoA requests by the Public Spot* on page 1264).

In theory, the simplest possible RADIUS transaction consists of the device sending the entered account data (user name + password) to the RADIUS server and the RADIUS server responding with either "yes" or "no". However, the RADIUS protocol also allows more complex responses and requests where the communication partners use a list of variables—so-called "attributes"—for requests and responses.

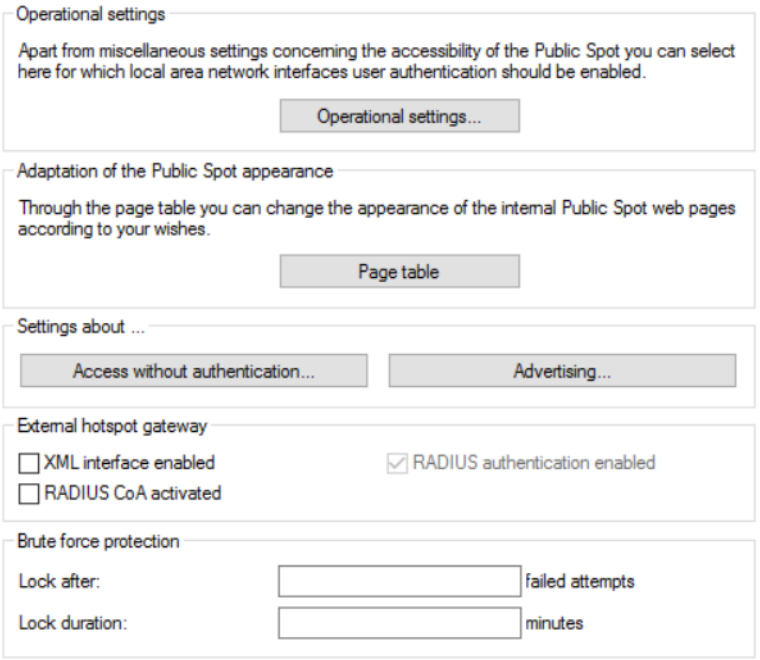
Enabling the acceptance of RADIUS CoA requests by the Public Spot

- The following steps assume that you have a functioning Public Spot that can be connected to an external hotspot gateway.
- The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

The following section explains how you enable RADIUS-CoA support as per RFC3576 in the Public Spot.

1. In LANconfig, open the device configuration and navigate to **Public Spot** > **Server**.



2. Set a checkmark under **RADIUS CoA activated**.
3. Now write the configuration back to the device.

From now on, the Public Spot processes any RADIUS CoA requests received from an external hotspot gateway.

Multiple authentication servers

As mentioned previously, the list of authentication servers can contain more than one entry. There may be situations where the hotspot provides access to the Internet for customers from different service providers. These providers may have separate user databases and their own RADIUS servers. The device must select which provider corresponds to the user based on the username.

Whenever the device does not find an entry for an authenticated user in its local table, it will first search through the authentication server list to find the provider that corresponds to the user. For example, user account names like `John.Doe@mydomain.com` contains the authentication server entry named `MYDOMAIN`. If the first allocation does not work, the device attempts to allocate the entry `DEFAULT` to the user. If this entry also does not exist, the device selects the authentication server that is first in the list. If the device does not find an entry (i.e., the list is empty), the user authentication fails.

Depending on the allocation of a user to a authentication server, your device always transmits the complete username to the selected RADIUS server. The selected RADIUS server is stored as the provider for the subsequent session and used for optional RADIUS accounting.

Chaining of backup servers

Internet access providers wish to provide a very high level of availability, and a common method to achieve this relies on redundancy. This redundancy is achieved using the backup servers which are needed when a request times out on the primary server, for example, because the server or another network component along the way was unavailable.

The requirements for backup servers varies widely among the different providers, which is why the list of authentication servers does not have a specific number of input fields. Instead, the device offers you a series of backup servers (backup chaining). Here, two or more entries in the authentication server table may be chained together to form a list of RADIUS servers. The device looks through the list of RADIUS servers one by one until the end of the list is reached (authentication failure due to server unavailability) or a response from a server (either positive or negative) is obtained.

You chain backup servers using the input field **Backup name** in the add/edit dialog under **Public Spot** > **Server** > **Authentication server**. Whenever a RADIUS request fails (i.e. times out), the device checks the backup field, and continues to try the RADIUS server specified in the entry that is referenced by the backup name. In general, an unlimited number of servers can be connected this way, which makes it possible for several providers to assign the same fallback server. The chain of backup servers is considered to be terminated if one of the following conditions occurs:

- Querying a RADIUS server failed and the corresponding authentication server table entry has an empty backup field.
- Querying a RADIUS server failed and the corresponding provider table entry has an invalid backup field, i.e. the entry referenced is not present in the authentication server list.
- Querying a RADIUS server failed and the corresponding authentication server list entry refers to an entry that has already been used in the query process. This avoids endless RADIUS requests due to circular references. It is possible to specify two RADIUS servers that reference each other as backups, with the primary server being selected by the user account name.



While the device is sending a RADIUS request, the TCP/HTTP connection to the client remains active. If the runtime of the chaining exceeds the lifetime of the TCP/HTTP connection, the client interrupts the login attempt. Therefore, it may be recommended to reduce the number of request retries to the individual backup servers as well as the time intervals between requests. You make these settings in the dialog **RADIUS** > **Server** > **Extended configuration** > **Options**.

15.2.3.10 Billing without a RADIUS accounting server

If user administration is performed using the internal user list of the Public Spot module, and you do not want to use a RADIUS accounting server, your only option is to use the expiry date of the user account for accounting purposes.

The use of the internal user list is no longer recommended. Instead, in order to take advantage of all of the options the Public Spot offers, you should use the internal RADIUS server for new installations.



For the purposes of billing by credit payment, the Public Spot can use SYSLOG to output detailed connection information to any computer in the network. Using the appropriate software on the destination computer allows you to precisely bill the resources that were actually used (such as connection times or transfer volumes).

15.2.3.11 Billing with a RADIUS accounting server

For the purposes of billing via a RADIUS server, you can set up the Public Spot so that it regularly supplies the current connection information for every active user to the specified accounting server. Accounting is started when a client is authenticated using RADIUS and a valid **Accounting server** is configured for the relevant **Authentication server** in the list of **Authentication servers**. It is possible to use different RADIUS servers for authentication and accounting.

Each of the regular message packets to the accounting server contains information about the resources (time, transferred data volumes, etc.) consumed by the user since the last message. This means that, even in the worst case of a Public Spot failure (e.g., due to a power outage or similar), only a small amount of accounting information will be lost.

Periodic messaging of accounting information to the accounting server (interim updates) is deactivated by default. It is activated by setting a value for the accounting cycle which is greater than 0.

- LANconfig: **Public Spot** > **Users** > **Accounting update cycle**



This cycle is defined in seconds. This sets the time interval of when your device regularly sends connection information to the accounting server. Setting the cycle to `0` deactivates this function. If this is the case, your device only sends accounting information at the beginning and end of the session.

When accounting on a prepaid basis, the RADIUS server monitors the restrictions on the users (limits on connection times or transfer volumes, expiry date). As soon as a user has used up the prepaid amount, the RADIUS server locks the user account. Your device rejects future login attempts for the user.

Time limits for prepaid models can be monitored by the Public Spot during active sessions. If a time limit is exceeded, the Public Spot automatically terminates the corresponding session. The monitoring of prepaid amounts is possible if the RADIUS server transmits the user's time credit to the Public Spot as the "Session timeout" attribute at the start of the session.

Request types

Your device is able to send different types of RADIUS requests to an accounting server. These requests differ according to a user's session state:

- An accounting start request is sent after a successful authentication.
- An accounting stop request is sent after a Public Spot session is terminated.
- Optional: Interim updates are sent throughout the session.

There are two types of interim updates: An initial update is sent immediately after the start request since some RADIUS servers need this in order to create a session in the accounting database. All further updates depend on whether an accounting cycle was created for the respective session (see **Public Spot** > **Users** > **Accounting update cycle**).

Alternatively, this value may be included in a RADIUS authentication response: The RADIUS server offers the RADIUS client (for example, your Public Spot) an interim accounting interval, which the client will use if it has the appropriate support for this and as long as no interval was set locally on the device itself.

If a local value was set, it will always be given a higher priority than the one received from a RADIUS server, which the RADIUS RFCs require by default!

Accounting backup

The backup solution for RADIUS accounting is the same as the one for RADIUS authentication, in that your device goes through the entries in the authentication server list one by one (see chapter *Chaining of backup servers*). The backup entries for the accounting server should be chosen with the same care as for the authentication server: If you are using multiple backups, you will probably have to reduce the timeout/try values for the requests in order to achieve reasonable response times for the entire system.

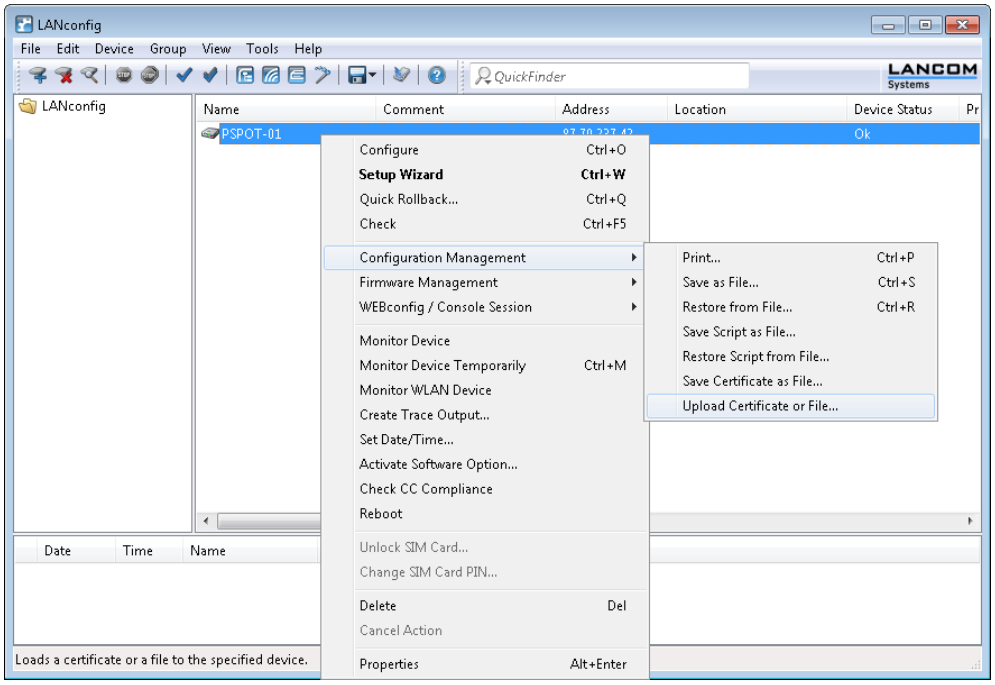
User sessions are not paused while the device sends accounting requests, which consumes additional resources in the device—in contrast to authentication. Please ensure that the time required for the selection of an accounting server* should be less than the length of an accounting cycle for interim update requests. This stops the requests from queuing up, which would result in a stack overflow.

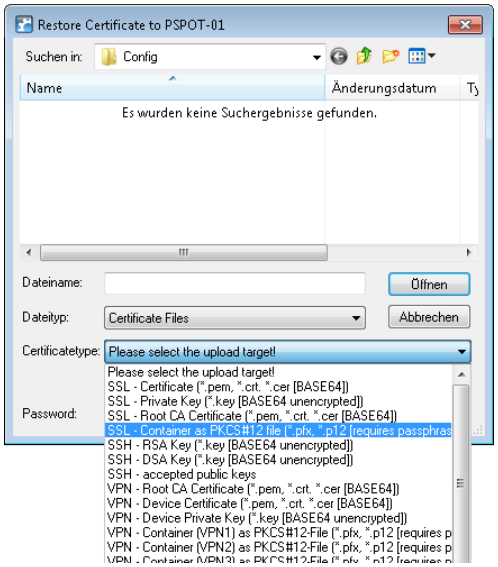
** Number of backups x (idle timeout + number of retries)*

15.2.3.12 Multi-level certificates for Public Spots

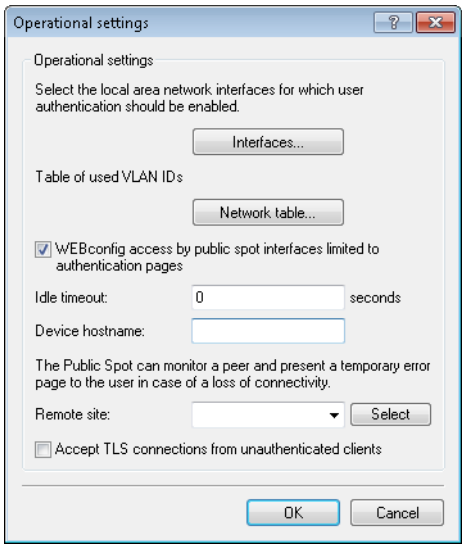
SSL certificate chains can be loaded into the device as a PKCS#12 container. These certificate chains can be used for Public Spot authentication pages by using the HTTPS server implemented in the device. Certificates from recognized trust centers are normally multi-level. Officially signed certificates in the Public Spot are necessary to avoid certificate-related error messages from the browser when authenticating at a Public Spot.

The certificate is loaded into the device for using LANconfig in File Management to upload the individual files of the root CA certificate or a PKCS#12 container:





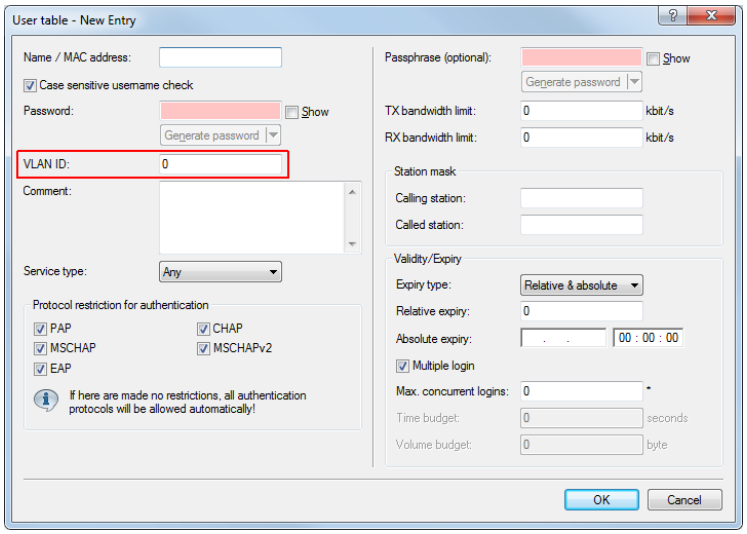
Certificates are normally issued for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address (enter in **Public Spot** > **Server** > **Operational settings** under **Device hostname**). This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.



15.2.3.13 Assigning users to individual VLANs

Regardless of the assignment of a VLAN ID for the entire Public Spot module, the device offers you the option of separately assigning individual VLAN IDs for individual Public Spot users. This ID is automatically assigned by the RADIUS server to your users after successful authentication. In this way it is possible, for example, to classify different Public Spot users in separate networks with different access rights and access options without having them login to separate SSIDs or requiring you to publicize the availability of various networks (e.g., networks for different customer types). The relevant rules can be realized via the firewall by specifying the VLAN ID of the respective user/the relevant user groups as the source tag.

An enabled VLAN module is a prerequisite for the functions described above.



› Open the **User table** in the dialog **RADIUS Server User database** and click **Add...** to create a new user.

› Assign an individual VLAN ID to the new user with the input field **VLAN-ID**. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value `0` disables the assignment of an individual VLAN ID.

For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for the clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server as low as possible under **IPv4** > **DHCPv4**. Possible values (in minutes) include, for example:

› **Maximum lease time:** `2`

› **Default lease time:** `1`

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using an external DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

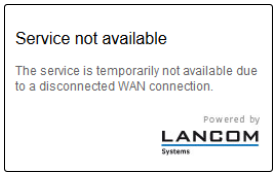
15.2.3.14 Error page in case of WAN connection failure

In addition to the general login error pages, you can also inform non-authenticated Public Spot users of a WAN connection error. Potential users are informed about the lack of network availability beforehand. This **Error** page is displayed whenever the Public Spot module registers a WAN link failure.

In order for the error page to be displayed properly, a corresponding remote site **must** be named, the connection to which is monitored by the Public Spot module. Make an appropriate entry in the dialog **Public Spot** > **Server Remote site**. The **Select** button allows you to assign an existing entry to the input field, or to create a new remote site.

If no remote site is named for monitoring, the Public Spot module disables the display of the connection error page. If the WAN connection fails, unauthenticated will not see an error page and their browsers will timeout instead.

On your custom error page, use the identifier `LOGINERRORMSG` to insert the error message issued by LCOS in case of a WAN link failure. In the event of a WAN link failure, the following error message is displayed:



Users who are already authenticated will see an appropriate error message from their browser.

15.2.3.15 AP-specific login to a central Public Spot

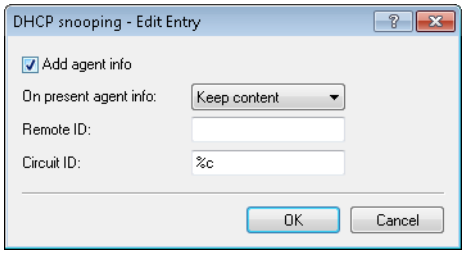
A central WLC manages a Public Spot in a distributed infrastructure. Accordingly, the configuration of the Public Spot (Public Spot SSID, security standards) is identical on all of the participating APs. This allows a Public Spot provider to offer an identical Public Spot at all of the different locations.

After receiving a voucher, customers would have access to this Public Spot at any branch. In order to limit access to the branch where the customer has received the voucher, the AP transmits its own identifier in addition to the user name and password. This identifier enables the voucher to be associated with this AP. To transfer the identifier, the AP attaches

the circuit ID (DHCP option 82) to the DHCP requests. These DHCP packets pass through the central Public Spot, which checks the identifier based on the entries in the RADIUS user table.

The Public Spot only allows a request if the voucher in the RADIUS user table is associated with this AP. Customers who have received a voucher at branch A cannot login to the same Public Spot at branch B, since the two APs transmit different identifiers.

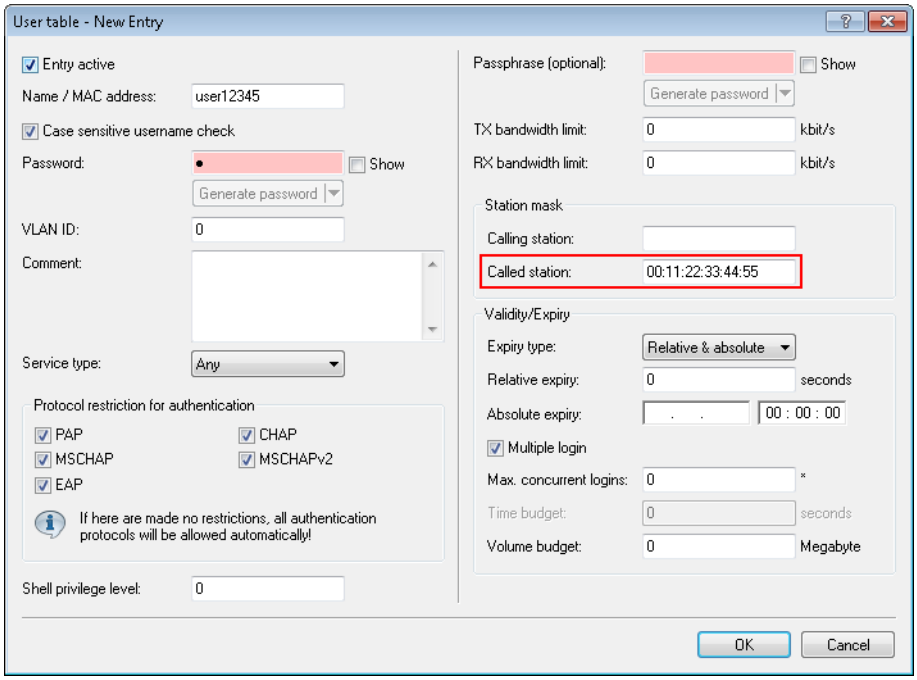
The AP identifier is configured as the circuit ID for the corresponding interface under **Interfaces** > **Snooping** > **DHCP snooping**.



You can use the following variables:

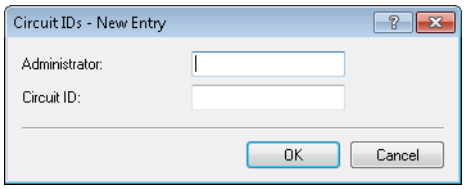
- **%%**: Inserts a percent sign.
- **%c**: Inserts the MAC address of the interface used by the Public Spot user to authenticate. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%c**: Inserts the name of the interface used by the Public Spot user to authenticate.
- **%n**: Inserts the name of the AP as specified under **Management** > **General**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if a WLAN client is used for the authentication. For other clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the AP, to be found for example under **Management** > **General**.

On the WLC, you configure this identifier in the RADIUS user table under **RADIUS** > **Server** > **General** > **User table**.



As the “Called station”, you add the ID of the AP that should enable access by means of the corresponding voucher.

When setting up new Public Spot users, the Public Spot Setup Wizard automatically uses the ID of the device if this is configured under **Public Spot** > **Wizard** > **Circuit IDs**.



When you create a new Public Spot account, the setup wizard checks to see whether this table contains an entry for the logged-in **administrator**. If this is the case, the setup wizard inserts the **circuit ID** into the RADIUS user table as the “called station”.

15.2.3.16 Redirect for HTTPS connections

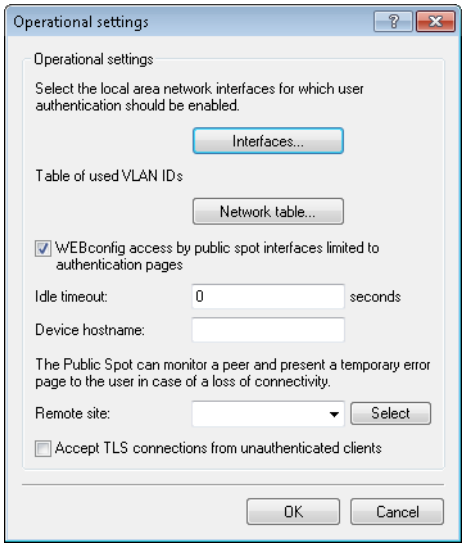
If an unauthenticated client attempts to access an HTTPS website via an interface operated by the Public Spot, the connection request is redirected to the Public Spot gateway itself, which then presents its login page to the user (as is also the case with HTTP). Usually, the user's browser displays a certificate warning, because the name or IP of the requested website is different from the name or IP address of the Public Spot. To prevent this and the increased load on the Public Spot from the HTTPS/TLS connections, this setting allows you to prevent HTTPS connections from being established for unauthenticated clients.

Once the client is authenticated, redirection is stopped and the client can establish any HTTP or HTTPS connection.

Modern clients carry out a "captive portal detection" via HTTP. The client attempts to access a certain URL via HTTP to check for the presence of a login page (from the Public Spot or other solutions). This mechanism is not affected by turning off the HTTPS redirect, since detection is usually via HTTP.

However, if unauthenticated WLAN clients should not perform connect requests over HTTP, this ineffective HTTPS redirect would place unnecessary load on the Public Spot gateway. For this reason it is possible to disable this HTTPS redirect. In this case, the user's browser displays a blank page.

In LANconfig, you configure the HTTPS redirect under **Public Spot** > **Server** > **Operational settings**.



To enable the HTTPS redirect, activate the option **Accept TLS connections from unauthenticated clients**. This option is disabled by default.

15.2.3.17 Protection against brute force attacks

Brute force attacks are the most common type of attack on networks. This method of attack tries out a variety of potential passwords in the shortest possible time, until the right one is found. One form of protection against brute-force attacks is to react to one or more successive failed attempts by delaying the time until the entry is allowed to be attempted again.

Configure the protection against brute-force attacks in LANconfig under **Public Spot** > **Server** in the section **Brute force protection**.



Lock after

Specify how many unsuccessful attempts are permitted before the entry lock takes effect.

Lock duration

Specify for how long the entry lock is to apply.

You can use the console to display the current status of the brute-force protection with the command `show pbbruteprotector`:

`show pbbruteprotector`

Shows all of the MAC addresses that are associated with the Public Spot.

`show pbbruteprotector [MAC address[ MAC address [ ...]]]`

Specifying one or more space-separated MAC addresses shows the status of all of the respective MAC addresses.

MAC addresses are specified in the format `11:22:33:44:55:66`, `11-22-33-44-55-66` or `112233445566`.

15.2.4 Alternative login methods

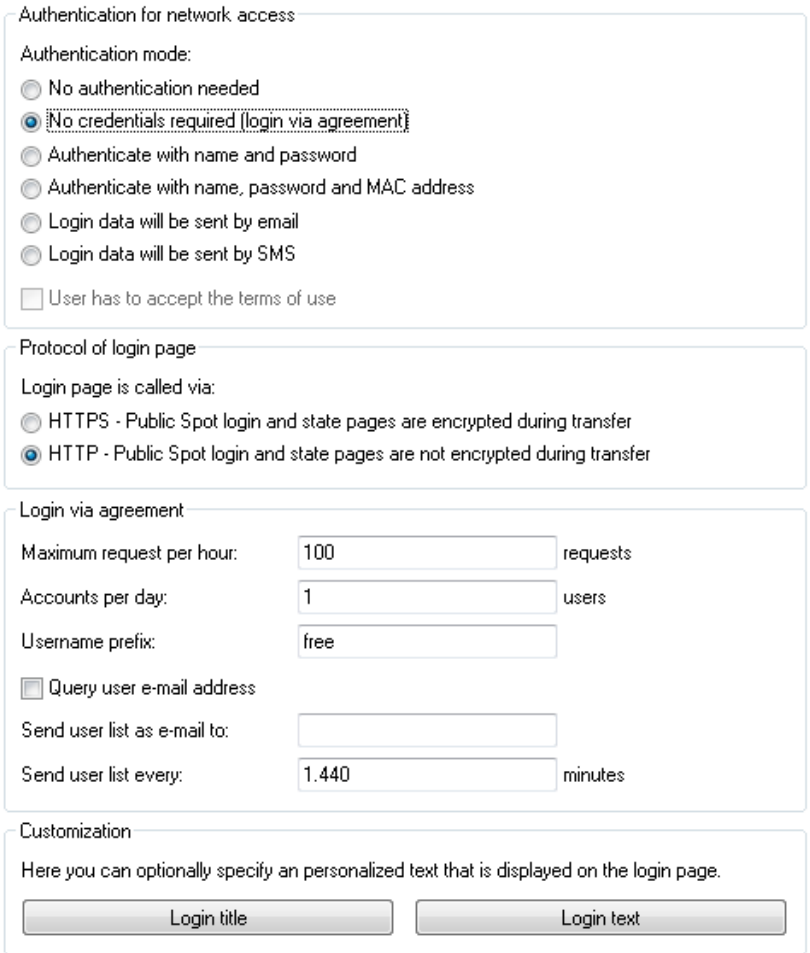
In addition to logging-in with previously provided credentials, your users can also independently request the receipt of login data via e-mail or text message (SMS), or by gaining instant access to the Public Spot by means of Login via agreement. Alternatively, in order to implement more complex or multi-level login scenarios, you can also link your Public Spot to other software systems using the XML or PMS interface (module optionally available).

You can also offer your users additional convenience by allowing, for example, automatic login processes (automatic login as well as re-login using a MAC address, login using WISPr, Hotspot 2.0), and also the related roaming services.

Hotspot 2.0 and roaming features are only available in conjunction with WLAN.

15.2.4.1 Overview of authentication modes

There are various ways to login to the Public Spot. The network access authentication setting is located in the dialog **Public Spot** > **Authentication**.



The following authentication modes are available:

- **No authentication required**

  Users get free access to the Public Spot, authentication is not required.

  Do not use this setting if your device has unlimited access to the Internet.

- **No credentials required (login after agreement)**

  Users get free access to the Public Spot after they agree to the operator's terms. With a RADIUS server, login is completely transparent for the user. The prerequisite is that you have set up an individual template page (a welcome page with a Login via agreement): In this case, the Public Spot initially forwards a user to the Welcome page. After the user agrees to the terms, the device automatically creates a user account in line with the default values set under **Public Spot** > **Wizard** and grants access to the connected network.

  Once you have select this login mode, the dialog section **Login via agreement** becomes available, where you can set additional conditions for the creation of free user accounts by the RADIUS server:

  - **Maximum requests per hour**: Specify how many users per hour can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.
  - **Accounts per day**: Specify how many accounts a user may create per day. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot for the rest of the day.
  - **Username prefix**: Enter a prefix which can be used to identify the user in the RADIUS user table that the device created automatically after confirmation of the terms of use. This prefix is placed directly in front of the **User name pattern** specified under **Public Spot** > **Wizard**.
  - **Query user e-mail address**: Enable this check box in order to query the user's e-mail address as a requirement for using the Public Spot. The device automatically enters the e-mail address specified here into the comments box of the newly created RADIUS user. Once a day a list of all of the available addresses is stored in the flash memory of the device. This list is boot persistent.
  - **Send user list as e-mail to**: Enter the e-mail address where the address list is to be sent. Only new entries that have been added since the last submission are sent. The address list is transmitted as a CSV file.
  - **Send user list every**: This sets the interval at which the updated address list is sent to the specified e-mail address. This value is specified in minutes.

  The terms featured on the Welcome screen are not to be confused with the terms-of-use page itself. The **Terms of use** page is an extra page that becomes available when certain login modes are activated (see *Possible authentication pages* on page 1308). If no Welcome page has been set up (see *Configuration of user-defined pages* on page 1313), the device displays an error message when accessing the Public Spot.

- **Authenticate with name and password**

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher.

- **Authenticate with name, password and MAC address**

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher. For this login mode, the MAC address of the client must also match the one stored in the user list by the administrator.

- **Login data will be sent by e-mail**

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent via e-mail. No action by an administrator is necessary. Learn more about this login mode under *Independent user authentication (Smart Ticket)* on page 1276.

- **Login data will be sent by SMS (text message)**

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent by SMS (text message). No action by an administrator is necessary. Learn more about this login mode under *Independent user authentication (Smart Ticket)* on page 1276.

For some login modes, the option **User has to accept the terms of use** allows you to combine the login with an acceptance of the terms and conditions. In this case, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering or logging in. Users who do not explicitly agree to these terms and conditions are unable to login to the Public Spot.

Remember to upload a page with terms and conditions onto the device before you enable this option. Otherwise, the device will only show the user a placeholder instead of the terms and conditions.

15.2.4.2 Independent user authentication (Smart Ticket)

Devices operating a Public Spot provide users with time-limited access to certain networks, typically the Internet. In many scenarios, a limited administrator account is used for the creation of these accounts: For example, a hotel employee at the front desk can use an account that only has the functional rights to create and manage Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests granting them network access.

However, the convenient voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network, and send it to themselves by e-mail or SMS (login by "Smart Ticket").

Login via agreement

Alternatively, the device gives you the ability to handle the login for Public Spot users transparently using a RADIUS server. In this case, the user login is preceded by a request to consent to the agreement before the user automatically receives access to the Public Spot. The creation of credentials by the user via e-mail or SMS does not apply for this authentication method. Learn more about this in the section under *Overview of authentication modes* on page 1274—the "Login via agreement" is not a part of the Smart Ticket function.

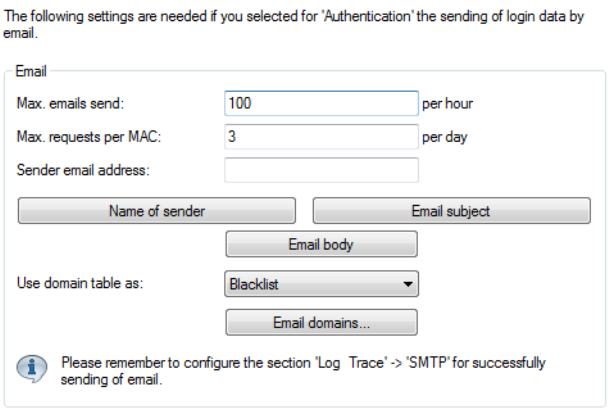
Configuring e-mail authentication

The settings for transmitting the login credentials to the e-mail address specified by the user are adjusted in the dialog **Public Spot** > **Email**. The following steps show you how to correctly configure e-mail authentication.

In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace** > **SMTP account** and **Log & Trace** > **SMTP options**.

In addition, you can specify individual text blocks used by the device to send the login credentials; see *Customizing text message content* on page 1279. By default, the device inserts predefined text modules; for an overview of these see *Standard texts for e-mail sender, subject line and body* on page 1280.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Authentication**.
3. Change the login mode to **Login data will be sent by email**.
4. Change the view to **Public Spot** > **Email**.



5. Under **Max. emails send** you enter the maximum number of e-mails that the Public Spot module may send per hour to users authenticating via e-mail. Lower the value to reduce the number of new users per hour.
6. Under **Max.requests per MAC** you specify how many different sets of credentials the device can provide to a MAC address within one day.
7. Under **Sender e-mail address** enter the return address that your Public Spot users will see when the e-mail is delivered, e.g. `support@providerX.org`.
8. Specify whether the device uses the table **Email domains** as a blacklist or whitelist with the selection item **Use domain table as**.

   This definition sets which e-mail addresses or domains may be entered by your Public Spot users in order to register.

   - **Blacklist**: Registration is permitted on all e-mail domains except those in this table.
   - **Whitelist**: Registration is possible only via the e-mail domains that are present in this table.

   Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

9. Use the **Email domains** table to define the e-mail domains that you allow or prohibit in the case of logins by your Public Spot users via e-mail. Enter domains in the format `web-domain.com`.
10. You can write the configuration back to the device.

Configuring SMS authentication

The settings for transmitting the login credentials as an SMS text message to the phone number specified by the user are adjusted in the dialog **Public Spot** > **SMS**. The choices available to you vary according to the device type:

- The credentials are sent as an SMS text message via the 3G/4G WWAN module in this device.
- The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device.
- The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

LCOS checks the entered phone number for invalid characters. Only numbers between 0 and 9 are allowed. The user must enter 5 to 15 numbers (excluding the country code).

The following steps show you how to correctly configure the different variants of SMS authentication.

In order to send login data as a text message via a 3G/4G WWAN-capable device, the internal SMS module of this device must be set up under **Log & Trace** > **SMS messages**, see *Basic configuration of the SMS module* on page 1685.

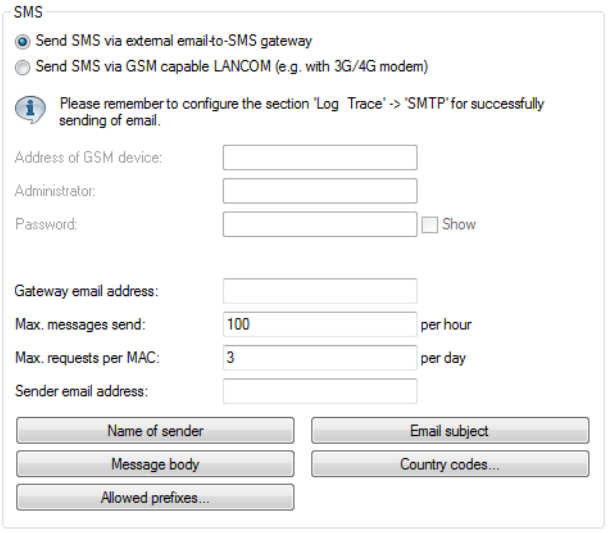
SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace** > **SMTP account** and **Log & Trace** > **SMTP options**.

In addition, you can specify individual text blocks used by the device to send the login credentials; see *Customizing text message content* on page 1279. By default, the device inserts predefined text modules; for an overview of these see *Standard texts for e-mail sender, subject line and body* on page 1280.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Authentication**.
3. Change the login mode to **Login data will be sent by SMS**.

4. Navigate to the menu item **Public Spot** > **SMS**.



5. Specify how the device sends SMS text messages.

   - In order to send the login credentials as an SMS text message via the internal 3G/4G WWAN module, select **Send SMS via internal GSM modem** and then continue with the next main step in the configuration.
   - In order to send the login credentials as an SMS text message via the 3G/4G WWAN module of another device, you first carry out the steps in section *Operating devices with the 3G/4G WWAN module as an SMS gateway* on page 1279 and then continue with the next main step in the configuration.
   - In order to send the login credentials to an external E-Mail2SMS gateway, select the setting **Send SMS via external e-mail-to-SMS gateway** and then continue with the next main step in the configuration.

   a) Under **Gateway e-mail address** you enter the IP address or the hostname of the gateway server, which converts the e-mail into SMS. If the provider expects to find the mobile phone number in the local part of the e-mail, you can use the variable `$PSpotUserMobileNo`.

   b) Under **Sender e-mail address** enter the return address that your Public Spot users will see when the SMS is delivered, e.g. `support@providerX.org`.

6. Under **Max. messages send** you enter the maximum number of SMS text messages that the Public Spot module may send per hour to users authenticating via SMS. Lower the value to reduce the number of new users per hour.
7. Under **Max.requests per MAC** you specify how many different sets of credentials the device can provide to a MAC address within one day.
8. Under **Country codes** you enter the international code numbers that the Public Spot will accept when sending data via SMS.
   Country codes can be entered directly or with a prefixed double-zero, for example for Germany `49` or `0049`.

   This table acts as a whitelist. You must define country codes in order for the login data to be delivered.

9. You can limit the transmission of SMS text messages to certain area codes for each country by entering the permissible codes followed by a '*' into a comma-separated list. An example for German mobile phone providers: `15*, 16*, 17*`.

   If you do not make an entry for a country in this table, all country codes will be allowed. Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

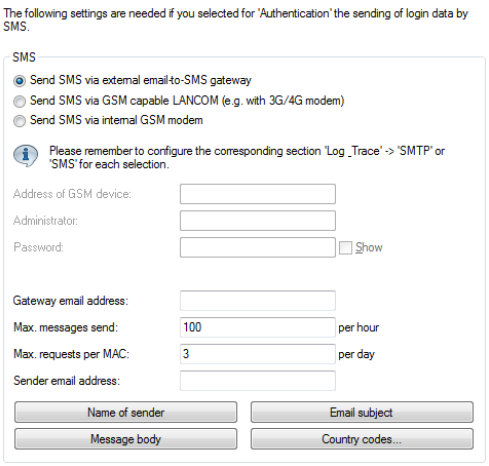
10. You can write the configuration back to the device.

Operating devices with the 3G/4G WWAN module as an SMS gateway

When using Public Spot authentication via SMS (Smart Ticket), you have the option of sending access credentials via the 3G/4G WWAN module in a further device instead of using an external E-Mail2SMS gateway. To use this option, you must store the address and the access credentials for the 3G/4G device on the device that provides the Public Spot. For the purpose of sending the SMS, the Public Spot module uses a URL call to send the credentials and the text message to the external 3G/4G device.

The option is available on devices both with and without their own 3G/4G WWAN module. These options allow you to chain multiple devices together and to set up your own transmitting device if you operate multiple Public Spots or use a device without a 3G/4G WWAN module.

1. Start LANconfig and set up the SMS module on the 3G/4G device that is to serve as an SMS gateway (see *Basic configuration of the SMS module* on page 1685). In addition, we recommended that you create an administrator without access rights (select **None**) and with just one function right, **Send SMS**.
2. Open the configuration dialog for the device that provides the Public Spot.
3. Navigate to the menu item **Public Spot** > **SMS**.



4. Select the setting **Send SMS via GSM-capable device (e.g. with 3G/4G modem)**.
5. Enter the user name and password for the administrator on the other 3G/4G device under **Administrator** and **Password**.
6. In the field **Address of GSM device**, enter the IP address where the Public Spot is to reach the other 3G/4G device.

Customizing text message content

By default, the device uses predefined text modules as the content of the e-mails or SMS text messages. An overview of these standard texts is available under *Standard texts for e-mail sender, subject line and body* on page 1280. You can also define your own texts.

If you do not specify any text for a language, the device automatically enters the internal default text.

1. Start LANconfig and open the configuration dialog for the device.
2. Depending on the selected authentication method, switch to the view **Public Spot** > **E-mail** or **SMS**.
3. Using the button **Name of sender**, enter a customized sender name for the e-mails or SMS text messages sent in the various languages, e.g. `Provider X`.
4. Use the **E-mail subject** button to enter a subject line for the e-mails sent in the various languages by the Public Spot module. Special control characters are available for this, described in more detail in the section *Variables and control characters* on page 1280.

5. Use the **E-mail body** or **Message body** button to enter the content of the e-mails or SMS text messages sent in the various languages by the Public Spot module. Variables and special control characters are available for this, described in more detail in the section *Variables and control characters* on page 1280.
6. Now write the configuration back to the device.

Variables and control characters

The message texts used for the Smart Ticket function can be customized with the use of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user or the SMS gateway.

Variables

The following variables are available in the input field **E-mail body**:

`$PSpotPasswd`

Placeholder for user-specific password for the Public Spot access.

`$PSpotLogoutLink`

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

Control characters

The following control characters may also be used in the text entered into the fields **E-mail subject** and **E-mail body**:

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Standard texts for e-mail sender, subject line and body

If you leave the dialogs **Public Spot** > **Email** or **SMS** blank, then the device automatically reverts to the standard texts in the corresponding language as stored in LCOS to generate the e-mail. The language used depends on the language setting of the browser used by the user for registration. If there are no default texts stored internally for a language, the device uses the English texts.

Table 32: Overview of the internal standard texts for authentication via e-mail/SMS

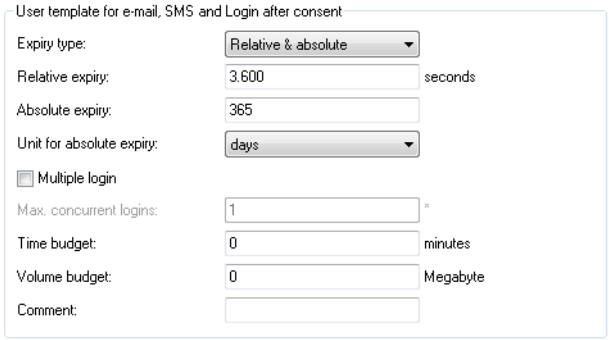
	Name of sender:	E-mail subject:	E-mail body:
Deutsch	Public Spot	Your login credentials for the Public Spot	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

	Name of sender:	E-mail subject:	E-mail body:
English	Public Spot	Your Public Spot account	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

Setting default values for the user templates

The following section describes how you adjust the default values for the **User templates** to meet your needs. The device uses the values set here as defaults when creating new users in Smart Ticket and when users login after confirming the terms and conditions. If you have so opted to send the login credentials via e-mail/SMS or you have activated the login after confirming the terms and conditions, each new user account is equipped with the permissions and constraints as defined by the user template.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Wizard**.



3. Complete the input fields in the section **User template** according to your preferences:

Expiry type

Using this entry you define how an automatically created Public Spot user account expires. You can specify whether the validity period of a user account is absolute (e.g. expires on a set date) and/or relative (elapsed time since the first successful login). If you select both values, the expiry time depends on which case occurs first.

Relative expiry

Using this entry you define the relative expiry time of an automatically created user account (in seconds). The **Expiry-type** that you chose must include `relative` in order for this setting to work. The validity of the account terminates after the time period specified in this field from the time of the first successful login of the user.

Absolute expiry

Using this entry you define the absolute expiry time of an automatically created user account (in days). The **Expiry type** that you chose must include `absolute` in order for this setting to work. The validity of the account terminates at the time specified in this field, calculated from the day of the creation of the account.

Unit for absolute expiry

To configure shorter expiry times, use the drop-down menu to select the unit for absolute expiry. Adjust the value for the absolute expiry if necessary.

Multiple login

This entry allows you to generally allow or prohibit users with an automatically created account to login to the Public Spot using the same credentials with multiple devices at the same time. The number of devices that can be logged on simultaneously is specified using the input field **Max. concurrent logins**.

Maximum number

Using this entry you set the maximum number of devices which can concurrently login to an automatically created account. The value `0` stands for "unlimited". In order for this setting to work, the parameter **Multiple login** must be enabled.

Time budget

Using this entry you define the time budget which automatically created users are assigned. The value `0` deactivates the function.

Volume budget

Using this entry you define the volume budget which automatically created users are assigned. The value `0` deactivates the function.

Comment

Using this entry you specify a comment or informational text which the RADIUS server adds to an automatically created user account.

4. Optional: If necessary, change the **User name pattern** and the **Password length**. In the authentication modes mentioned above, the device uses the relevant *New user wizard default values* to automatically generate a user name and a password.
5. You can write the configuration back to the device.

15.2.4.3 Automatic re-login

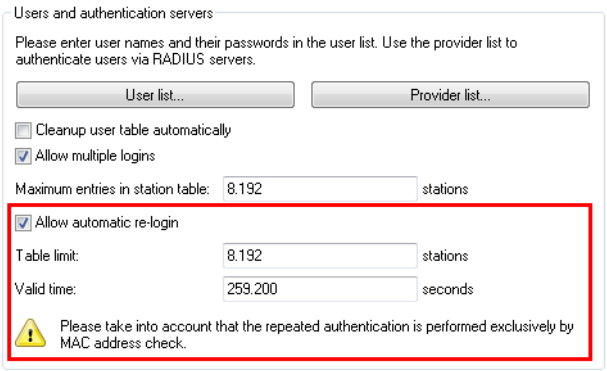
Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) It is similar for mobile LAN clients (e.g., notebooks) which have to be disconnected from the network for a short time for a change of location (e.g., for changes from a lecture hall to a library in a college). In all of these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

With automatic re-login, the user only has to be identified on the Public Spot once. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.

The authentication is only performed on the MAC address of the client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

The settings for automatic re-login can be found in LANconfig in the device configuration under **Public Spot** > **Users** in the section **Users and authentication servers**.



The selection box **Allow automatic re-login** enables this function.

You specify the number of clients (maximum 65536) in the field **Automatic re-login table limit** that the re-login function may use.

In the field **Automatic re-login valid time** you specify how long the Public Spot stores the credentials of a client in the table for a re-login. After this period expires, the Public Spot user must log in again using the login page of the Public Spot in the browser.

15.2.4.4 Automatic authentication with the MAC address

After successful authentication, a Public Spot gives the user access to certain services. The Public Spot usually displays a login website so that users can authenticate. The user enters the authorization credentials into the login page and the Public Spot then redirects the user to the allowed sites.

In some applications, authentication via web site may not be desired or not possible, as the following examples illustrate:

- The end device does not have a browser and therefore cannot open the login page.
- Manually accessing the login page may be undesirable, such as when carrying out a performance test.

Automatic authentication on the Public Spot with a MAC address makes it possible to use the Public Spot without first opening the login page. The administrator enters the MAC addresses of the corresponding end device into the table of permissible MAC addresses under **Public Spot** > **Users** > **MAC authenticated users**.

MAC-address check procedure

When the device receives a request from a client, the Public Spot executes the following steps for the automatic authentication by MAC address:

- If the Public Spot has already authenticated the MAC address of the received data packets, the device forwards the data packets without further delay.
- If the MAC address is in the list of allowed clients, the Public Spot starts a new session for the user and forwards the corresponding data packets.
- If a provider has been defined for verification of the MAC addresses by RADIUS, and a positive, valid MAC address authentication is cached in the Public Spot, then the Public Spot starts a new session for that user and forwards the associated data packets.
- If a provider chooses to check the MAC address with the RADIUS server but there is no valid authentication for the MAC address cached in the Public Spot, the Public Spot initiates the authentication of the MAC address at the corresponding RADIUS server. After a positive response, the Public Spot starts a new session for that user and forwards the associated packets.
- If all of the above checks fail, the Public Spot directs the user to the login page.

Authentication of the MAC address by RADIUS

If the MAC address of a WLAN client requesting to associate is not included in the list of approved addresses, the Public Spot alternatively authenticates the address via a RADIUS server.

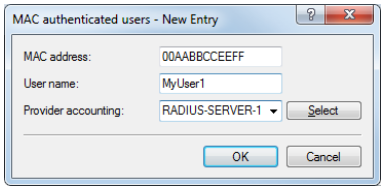
To enable RADIUS authentication, the administrator selects one of the RADIUS servers that has defined in the device and saved to the list of providers.

In addition, the administrator defines a lifetime for the rejected MAC addresses. The Public Spot uses this lifetime to prevent the RADIUS server from being flooded with repeated requests for MAC addresses that cannot be authenticated via the RADIUS server or MAC address table.

If a MAC address authentication is rejected by the RADIUS server, the Public Spot stores this rejection for the lifetime defined here. The Public Spot responds to further requests for the same MAC address directly and without forwarding them to the RADIUS server first.

Configuration by LANconfig

For the configuration in LANconfig, you find the parameters for the authentication of clients by MAC address in the dialog **Public Spot** > **Users** > **MAC authenticated users**.



15.2.4.5 Automatic authentication via WISPr

Your device provides an interface for authentication via WISPr. The **WISPr** standard is the technological predecessor of the 802.11u and Hotspot 2.0 specifications. The acronym stands for **Wireless Internet Service Provider roaming** and designates both a process and a protocol that allow users of WLAN enabled devices to roam seamlessly between the WLANs of different operators – and, therefore, between their Internet service providers. The idea behind it is similar to that of 802.11u and Hotspot 2.0; however, it requires more comprehensive support by the respective users.

Using the WISPr protocol, you can provide logins and network usage on your hotspot in a manner similar to Hotspot 2.0, even for end devices that no longer support Hotspot 2.0. The prerequisite is that your service provider provides the necessary infrastructure. Support for the user's device is provided either by the operating system or a suitable app (smart client). This client handles authentication to the hotspot for the user. If no credentials are available for the relevant network, the client queries the user for valid credentials at the system level. In any case, this eliminates the user having to log in via a login web page in the browser.

Because of its age, almost all current end devices with iOS, Android and Windows 8 support the WISPr protocol. In addition, larger WLAN Internet service providers often have their own apps to make the login for their clients easier: These apps include a preconfigured database of the provider's own hotspots and, optionally, those of their roaming partners. The authentication process corresponds to the following schema:

1. A customer installs his provider's hotspot app to act as a client, which provides a database of preconfigured hotspot SSIDs.
2. The client connects automatically with one of the hotspots and sends a HTTP-GET-Request to a random URL to test if direct Internet access is available or the Public Spot requires authentication.
3. In HTTP-Redirect the hotspot sends a WISPr-XML-Tag with the Login-URL.
4. The client sends its login data to the Login-URL in an HTTP-Post.

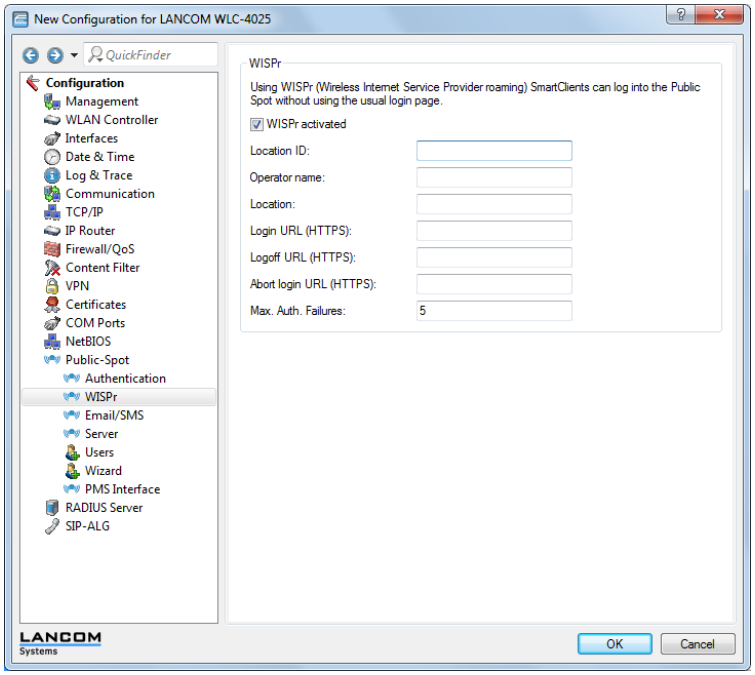
Example for an XML-Tag in redirect:

```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
   </WISPAccessGatewayParam>
</HTML>
```

In order to use WISPr, the device must have an SSL certificate and a private key installed. The certificate must either be signed by a trusted authority or – if it is a self-signed certificate – be imported as a trusted certificate on the client. Otherwise the client will reject the login via WISPr. Further information about loading these objects on your device can be found in the LANCOM techpaper "Certificate Management in Public Spots" available from *www.lancom-systems.com*.

Configuring WISPr

Configure the WISPr function of your device in the menu **Public Spot** > **WISPr**.



In this window you have the following options:

- **WISPr activated**: Enable or disable the WISPr function for the device.
- **Location ID**: Use this ID to assign a unique location number or ID for your device, for example, in the format `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`
- **Operator name**: Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.
- **Location**: Describe the location of your device, e.g., `CafeX_Market3`. This helps to better identify a user in your hotspot.
- **Login URL (HTTPS)**: Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider. Any external URL can be entered or the Public Spot itself. If the Public Spot should authenticate users using WISPr, enter the URL in the format `https://<Device-FQDN>/wisprlogin`. For "wisprlogin" in the example, any freely defined path can be used.
- **Logoff URL (HTTPS)**: Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider. The same rules apply as for the login URL.
- **Abort login URL (HTTPS)**: Enter the HTTPS address to which the device forwards a WISPr client if authentication fails. The same rules apply as for the login URL.

The three URLs must be different, if the Public Spot is used in the device domain, for example:

- Login-URL: https://<Device-FQDN>/wisprlogin
- Logoff-URL: https://<Device-FQDN>/wisprlogoff
- Abort-Login-URL: https://<Device-FQDN>/wisprabort

Finally, for test purposes, you can also configure an URL with IP addresses. In a production system, the client will check the FQDN of the certificate!

- **Max. auth. failures**: Enter the maximum number of failed attempts which the login page of your Internet service provider allows. If the Public Spot is used, the Public Spot rejects further login attempts by the specified client after this number of failed attempts.

15.2.4.6 IEEE 802.11u and Hotspot 2.0

Your device supports WLAN connections according to the IEEE 802.11u standard and the Hotspot 2.0 specification, which is based on it. Using 802.11u you have the option to implement automatic authorization and authentication of your users on a local WLAN network (for example, within your company) or a Public Spot network. The prerequisite for this is that the relevant stations (smartphones, tablet PCs, notebooks, etc.) also support connections for 802.11u and Hotspot 2.0. In detail, the following functions are offered:

- **Automatic network selection**

  In a 802.11u-enabled environment, the user does not have to manually detect and select an SSID. Instead, the client independently searches for and selects a suitable Wi-Fi network by automatically requesting and evaluating the operator and network data of all 802.11u- access points that are in range. A previous login to the access point is not required.

  Hotspot 2.0 stations also have the ability to retrieve information about the services available in a Wi-Fi network. If specific services that are relevant for a user (e.g., connections via HTTP, VPN or VoIP) are not available for a Wi-Fi network, any networks that do not meet the criteria are excluded from further searches. This ensures that users are always connected to the optimal network.

- **Automatic authentication and authorization**

  In 802.11u-enabled environments, the station automatically carries out the user's login if the necessary credentials are available. Authentication can be done, for example, using a SIM card, a username and password, or a digital certificate. Repetitive manual input of the credentials by the user in a login screen is no longer necessary. After successful authentication, the user can immediately use the desired services.

- **Seamless handover**

  Connections according to 802.11u and in conjunction with 802.21 facilitate the uninterrupted exchange of data connections between different network types. This enables users to switch their stations seamlessly from a cellular network to a WLAN network as soon as they get within range of a Hotspot 2.0 zone—and vice versa. The same is true for the transfer between two different operators if, for example, the user goes from one homogeneous network to another during a bus trip

- **Automatic roaming**

  Connections as per 802.11u facilitate roaming between different operator networks. If a user is in range of a Hotspot 2.0 zone of an operator for which he does not have any credentials, his station still has the option to switch to its home network. Authentication at a third-party Hotspot 2.0 zone is handled by the operator's roaming partner, which then allows the user to access the third-party Wi-Fi network. This is interesting not only in areas where there are only single network operators with access points, it is also especially attractive for people traveling abroad.

Example: For example, a user who is in transit in the city with his 802.11u-enabled smartphone (station) can enable the WLAN feature to browse the Internet. The station then starts trying to find all available Wi-Fi networks in the area. If any of the access points offer 802.11u, the station selects the one network that best fits the required service based on the operator and network information that was previously obtained, for example, from a hotspot offering Internet access from its own cellular network company. In this case, the subsequent authentication can be performed automatically via the SIM card so that the user does not need to intervene at any time during the process. The encryption method selected for the connection – e.g., WPA2 – is unaffected.

In summary, connections according to 802.11u and with Hotspot 2.0 enabled combine the security features and performance of classic Wi- Fi hotspots with the flexibility and simplicity of data cellular network connections. At the same time, they relieve the cellular networks by redistributing data traffic (and possibly also telephony) to the network connections and frequency bands offered by access points.

Passpoint® Release 2

As of LCOS 10.40 the extended Hotspot 2.0 feature in your WLAN device can be configured as per Passpoint® Release 2 as specified by the Wi-Fi Alliance. The RADIUS server in the LCOS has been equipped with the necessary features since 10.32 version RU4.

Passpoint® Release 2 simplifies the onboarding of devices into a network using the WPA2-Enterprise (802.1X) encryption method. A dedicated onboarding SSID allows a user with a device that supports Passpoint® Release 2 to install a profile and automatically switch to the encrypted network using the stored credentials. This helps to implement hotspots that provide encrypted wireless communication. An onboarding SSID can be used to give guests temporary access credentials.

Similarly, a mobile service provider can relieve the load on their cellular network by introducing Wi-Fi offloading and allowing mobile devices with a SIM card to automatically log into their WLAN network. Customers' devices find the WLAN network from the mobile service provider and automatically login to the operator's WLAN network using the user data stored on the SIM card.

Passpoint® Release 2 adds the following features to Hotspot 2.0:

- Online Sign-Up (OSU) – with Passpoint® Release 2, companies and network operators can use "Online Sign-Up" servers (OSU servers) to deliver profiles to their users. Using an open OSU SSID, users can identify various OSU servers by their icons and thus select the one that suits them best. The OSU server can optionally ask the user for credentials before providing a profile that best suits the user's device. In addition to the open OSU-SSID, an encrypted SSID can be used to exchange user data by means of "anonymous EAP-TLS". This requires the use of a RADIUS server that supports "anonymous EAP-TLS".

  An OSU server is not included with LCOS. However, solutions are available from LANCOM partners.

- OSU icons – icons corresponding to the supported OSU servers can be uploaded to the LCOS as files using the WEBconfig feature **File management**. We recommend PNG as the file format.
- Notification – the network can notify the user about an imminent logout from the RADIUS server. This may be the case if the user credentials have expired or if the specified connection duration has been reached.
- QoS Map – the "QoS Map Set" function enables an access point to instruct its clients to use a specific QoS map. This defines the values for the contention window (media access via EDCA) of the various access categories (voice, video, best effort and background data packets) and the corresponding DSCP parameters. At the same time, the access points also use the values stored in the QoS map.

  Currently available are the two QoS maps required by the Wi-Fi-Alliance and the default QoS map of the LCOS.

Hotspot operators and service providers

The Hotspot 2.0 specification of the Wi-Fi Alliance differentiates between hotspot operators and hotspot service providers: A **hotspot operator** only operates one Wi-Fi network, while a **hotspot service provider** (SP) provides the connection for the user to the Internet or a cellular network. Of course, it is possible for an operator to also be an SP. However, in all other cases, a hotspot operator requires the corresponding roaming agreements with an SP or a group of multiple SPs (called a roaming consortium). Only when an operator has made these agreements are the various roaming partners' customers able to authenticate with the hotspot operator. Each service provider operates its own AAA infrastructure. A hotspot communicates this list of possible roaming partners and the name of the hotspot operator using ANQP (see functional description).

Functional description

The 802.11u standard is the base standard of IEEE. This standard essentially expands access points or hotspots with the ability to broadcast so-called "ANQP data packets "(Advanced Message Queuing Protocol) in its broadcast signals. ANQP is a query/response protocol that a device can use to request a range of information about the hotspot. This includes both meta-data, such as information about the owner and the venue, as well as information on the underlying network, such as information on operator domains, roaming partners, authentication methods, forwarding addresses, etc. All 802.11u-enabled devices in range have the ability to request these data packets without a prior login to the access point in order to select a network based on the network information.

The Wi-Fi Alliance has added further ANQP elements to the standard, and markets this specification as **Hotspot 2.0**. This Hotspot 2.0 function merely adds additional elements to the standard, which the device can use as criteria for selecting its network. These criteria include, for example, information about the services and WAN metrics available at the hotspot. The associated certification program is called Passpoint®, which is available in different versions. Certain LANCOM access points are Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 and/or 2).

The ANQP data packets are the central information element of the 802.11u standard. However, to signal the support for 802.11u and to transmit data packets, further elements are required for the operation of 802.11u:

- The signaling of 802.11u support in the beacons and probes of a hotspot are done by the element known as the **Interworking element**. In this element, the initial basic network information—such as the network classification, Internet availability (Internet bit) and the OI of the roaming consortium and/or of the operator—are already included. At the same time, it is used by 802.11u-enabled devices as an initial screening criterion when detecting a network.
- ANQP data packets are transferred within the so-called GAS containers. GAS stands for Generic Advertisement Service, and is the name of generic containers that allow a device to request additional internal and external information for the network selection from the hotspot, in addition to the information in the beacons. The GAS containers are transmitted on layer 2 by what are referred to as public action frames.

Login by an 802.11u-enabled client at a Hotspot 2.0

The following functional description schematically illustrates the selection and login process of an 802.11u-enabled device at a Hotspot 2.0.

Login via username/password or digital certificate

1. The hotspots reply with an ANQP response, which contains, among other things, the name of the hotspot operator and a list of NAI realms, which list all available roaming partners (service provider, abbreviated SP).
2. The device loads the locally stored credentials from the WLAN profiles or installed certificates that were set up by the user, and compares the local realms with the NAI realm lists obtained in (2).
   a. If the device successfully finds one, it knows that it can be authenticated successfully on the relevant Wi-Fi network.
   b. If the device successfully finds more than one, the selection of a Wi-Fi network is made based on the user's preference list. This list defines the preferred order of operators in conjunction with the potential roaming partners. In this case, the device compares the operator names listed under (2) with the list, and selects the operator with the highest priority.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate SP. The access point then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for authentication. The authentication is performed using the authentication method determined by the SP. The authentication via username/password uses EAP-TTLS, and authentication via digital certificate uses EAP-TLS.

Login via (U)SIM

1. In contrast to the login via username/password or digital certificate, a device with a (U)SIM does not request the list of NAI realms in its ANQP requests, but rather the 3GPP Cellular Network Information. The ANQP responses contain the cellular network information list of all cellular network providers for which the access point offers authentication.
2. The device loads the parameters for the cellular network from its local (U)SIM card, and compares it with the data retrieved from the cellular network information lists. The list comparison and selection of a preferred provider network is performed analogous to the login via username/password or digital certificate.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate cellular network company. The hotspot then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for the authentication. The presence of a (U)SIM card changes the possible authentication method for the device to EAP-SIM or EAP-AKA.

4. The AAA system verifies the credentials for authentication via the interface MAP (Mobile Application Part) at the HLR server (Home Location Register) of the cellular network company.

If authentication is successful, the device gets access to the WLAN network either via hotspot (credentials for the operator's network are available) or automatic roaming (credentials for the operator's network are not available).

If there are multiple authentication options available for the device (e.g., SIM card and username/password), it has the option of using the preferred EAP authentication method and, therefore, the preferred credentials based on the NAI realm or cellular network information list.

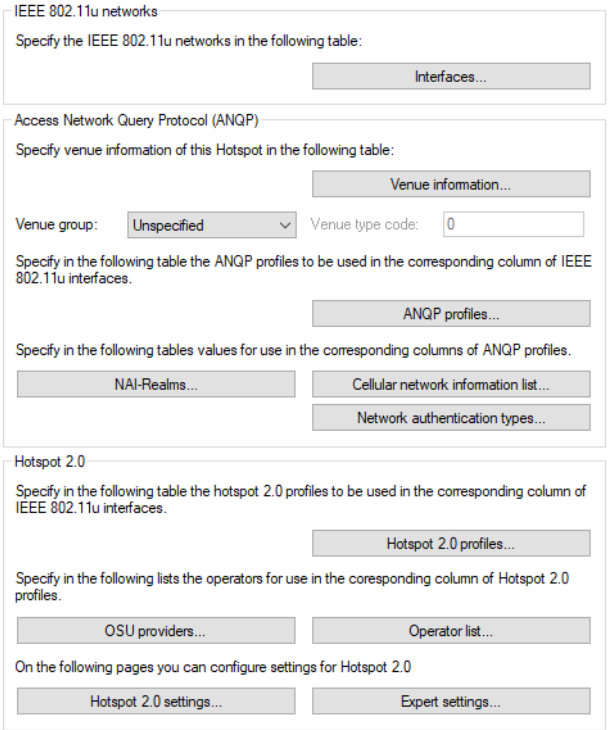
Recommended general settings

The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- WPA2-Enterprise Security (802.1X) enabled
- Authentication using EAP with the corresponding variant:
  - EAP-SIM/EAP-AKA for authentication with SIM / USIM card
  - EAP-TLS for authentication with a digital certificate
  - EAP-TTLS for authentication with a username and password
- Enabled and properly configured ARP proxy
- Disabled multicasts and broadcast in cellular networks
- Non-approved data traffic between the cellular network devices (Layer 2 traffic inspection and filtering). The corresponding settings can be found in LANconfig under **Wireless LAN** > **Security** > **Traffic between different SSIDs**.
- Enabled and implemented firewall on the access router, which provides Internet access

Configuration menu for IEEE 802.11u / Hotspot 2.0

The configuration menu for IEEE 802.11u and Hotspot 2.0 is located under **Wireless LAN** > **IEEE 802.11u**.



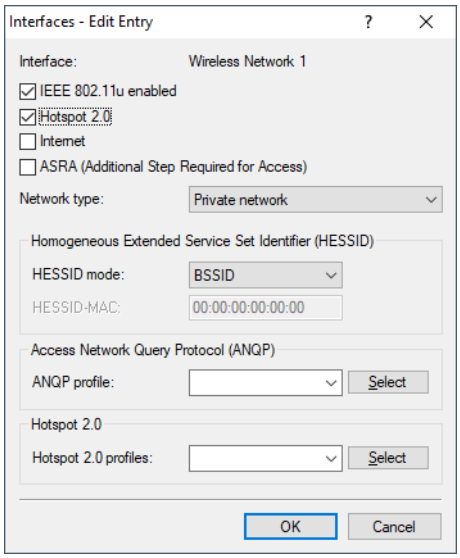
The device offers the ability to individually enable or disable and configure the support the IEEE 802.11u standard as well as the Hotspot 2.0 functionality for each logical WLAN interface using the button **Interfaces**.

Some parameters need to be configured in what are known as “Profiles”. Using profiles, you can group different rows in lists, which you only have to reference from the other windows. Essentially, these are profiles for ANQP data packets and Hotspot 2.0. The relationships between the profile lists is as follows:

```
| -- Interfaces
  |--ANQP profiles
    |--NAI realms
    |--Cellular network information list
    |--Network authentication types
  |--Hotspot 2.0 profiles
    |--Operator list
    |-- OSU providers
```

Activating interfaces

The table **Interfaces** is the highest administrative level for IEEE 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.



Interface

Name of the logical WLAN interface that you are currently editing.

IEEE 802.11u enabled

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Hotspot 2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.

Internet

Select whether the Internet bit is set. The Internet-bit explicitly informs all stations that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

Using this function you only communicate the availability of an Internet connection. You configure the corresponding regulations on the firewall, irrespective of this option.

ASRA – Additional steps for access required

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface. Based on the setting made here, the user has the option to limit network detection of their devices to specific network types. Possible values are:

Private network

Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.

Private with guest access

Similar to **Private network**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

Chargeable public network

Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.

Free public network

Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.

Personal device network

In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.

Emergency services only network

Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

Test or experimental

Describes networks that are set up for testing purposes or are still in the setup stage.

Wildcard

Placeholder for previously undefined network types.

HESSID mode

Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT". Possible values for the HESSID mode include:

BSSID

Select this item to set the BSSID of the device as the HESSID for your homogeneous ESS.

User

Select this item to manually assign a HESSID.

None

Select this item in order to not assign any homogeneous ESS and to isolate it from the device network.

HESSID-MAC

If you selected the setting `user` for the **HESSID mode**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., "008041AEFD7E" for the MAC address 00:80:41:ae:fd:7e.

If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

ANQP profile

Select an ANQP profile from the list. You create ANQP profiles in the configuration menu using the button of the same name.

Hotspot 2.0 profiles

Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

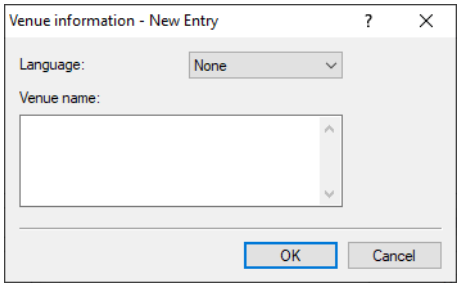
Configuring ANQP data packets

Venue information and group

Information about the access point's location is managed using the table **Venue information** and the subsequent dialogs **Venue group** and **Venue type code**.

In the event of a manual search, additional details on the **Venue information** help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

You can place your device in a predefined category using the **Venue group** and **Venue type code** – as opposed to the user-defined location information.



Language

You have the ability to specify custom information for the location of the access point for each language. The location name that matches your user's language will then be displayed. If a language is not available for a user, its station chooses one based, for example, on the default language.

Location name

Enter a short description of the location of your device for the selected language, for example:

```
Ice Café Valencia
123 Street
City, State 12345
```

The **Venue group** describes the environment where you operate the access point. You define them globally for all languages. The possible values, which are set by the “venue group code”, are specified in the 802.11u standard.

Using the **Venue type code**, you have the option to specify the details for the venue group. These values are also specified by the standard. The possible type codes can be found in the following table.

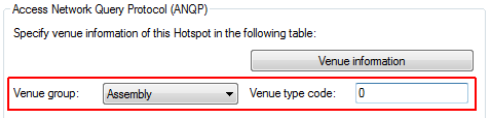


Table 33: Overview of possible values for venue groups and types

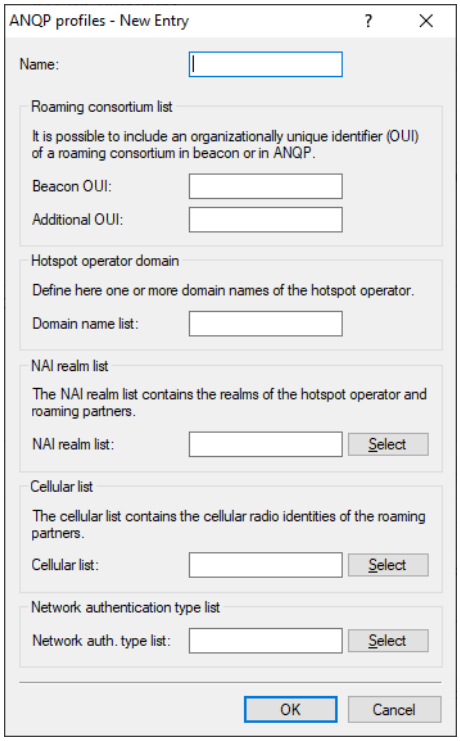
Venue group	Venue type code
Unspecified	
Assembly	› 0 = unspecified assembly › 1 = stage › 2 = stadium › 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) › 4 = amphitheater › 5 = amusement park › 6 = place of worship › 7 = convention center › 8 = library › 9 = museum › 10 = restaurant › 11 = theater › 12 = bar › 13 = café › 14 = zoo, aquarium › 15 = emergency control center
Business	› 0 = unspecified business › 1 = doctor's office › 2 = bank › 3 = fire station › 4 = police station › 6 = post office › 7 = office › 8 = research facility › 9 = law firm
Educational:	› 0 = unspecified education › 1 = primary school › 2 = secondary school › 3 = college
Factory and industry	› 0 = unspecified factory and industry › 1 = factory

Venue group	Venue type code
Institutional	> 0 = unspecified institution > 1 = hospital > 2 = long-term care facility (e.g., nursing home, hospice) > 3 = rehabilitation clinic > 4 = organizational association > 5 = prison
Commerce	> 0 = unspecified commerce > 1 = retail store > 2 = food store > 3 = Automobile workshop > 4 = shopping center > 5 = gas station
Halls of residence	> 0 = unspecified residence hall > 1 = private residence > 2 = hotel or motel > 3 = student housing > 4 = guesthouse
Warehouse	> 0 = unspecified warehouse
Utility and miscellaneous	> 0 = unspecified service and miscellaneous
Vehicular	> 0 = unspecified vehicle > 1 = passenger or transport vehicles > 2 = aircraft > 3 = bus > 4 = ferry > 5 = ship or boat > 6 = train > 7 = motorcycle
Outdoor	> 0 = unspecified outdoor > 1 = municipal WLAN network > 2 = city park > 3 = rest area > 4 = traffic control > 5 = bus stop > 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. **ANQP profiles** offer you the ability to group certain ANQP elements and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These elements

include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.



Name

Assign a name for the ANQP 2.0 profile here. This name will appear later in the interfaces table in the selection for ANQP profiles.

Beacon OUI

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

Additional OUI

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

Domain name list

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is

sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

NAI realm list

Select an NAI realm profile from the list. You specify profiles for NAI realms in the configuration menu by clicking the button **NAI realms**.

Cellular list

Select the cellular network identity from the list. You set the identities for cellular networks – similar to profiles – in the configuration menu using the button **Cellular network information list**.

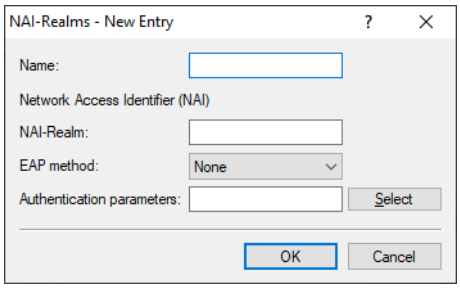
Network authentication type list

Select an authentication profile from the list. You specify profiles for network authentication in the configuration menu by clicking the button **Network authentication types**.

Additionally, the CLI provides the option to show the type of available IP addresses, which they can obtain from the network after successful authentication. You can access the relevant parameters **IPv4-Addr-Type** and **IPv6-Addr-Type** via the path **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.



Name

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. This name will appear later in the ANQP profile in the selection for **NAI realm list**.

NAI realm

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in *RFC 2486* and, in the simplest case, is `<username>@<realm>`. For `user746@providerX.org`, the corresponding realm is `providerX.org`.

EAP-Method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication method Possible values are:

EAP-TLS

Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate that the user has to install.

EAP-SIM

Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.

EAP-TTLS

Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.

EAP-AKA

Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

None

Select this setting when the relevant NAI realm does not require authentication.

Authentication parameters

Click the authentication parameters that match the EAP method, e.g. for EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

or for EAP-TLS `Credentials.Certificate`.

Possible values are:

Table 34: Overview of possible authentication parameters

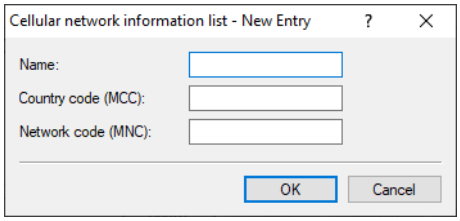
Parameter	Sub-Parameter	Comment
NonEAPAuth		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in *RFC 1994*
	MSCHAP	Implementation of Microsoft CHAP V1, specified in *RFC 2433*
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in *RFC 2759*
Credentials		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password

* The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Parameter	Sub-Parameter	Comment
TunnelEAPCredentials.*	None	No credentials required
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

Cellular network information list

Using this table you manage the identity lists for cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.



Name

Assign a name for the cellular network identity, such as an abbreviation of the network operator in combination with the cellular network standard used. This name will appear later in the ANQP profile in the selection for **Cellular list**.

Country code (MCC)

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.

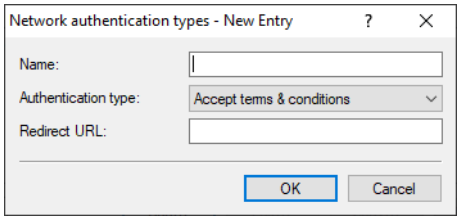
Network code (MNC)

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Network authentication types

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

Please remember to set the ASRA bit in the **Interfaces** table if you set up an additional authentication step.



Name

Assign a name for the table entry, for example `Accept Terms & Conditions`. This name will appear later in the ANQP profile in the selection for **Network auth. type list**.

Authentication type

Choose the context from the list, which applies before forwarding. Possible values are:

Accept terms & conditions

An additional authentication step is set up that requires the user to accept the terms of use.

Online enrollment

An additional authentication step is set up that requires the user to enroll online first.

HTTP redirection

An additional authentication step is set up to which the user is forwarded via HTTP.

DNS redirection

An additional authentication step is set up to which the user is forwarded via DNS.

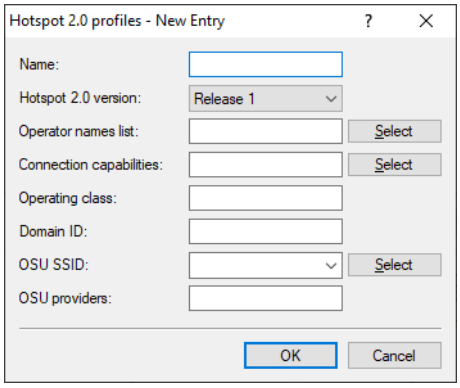
Redirect URL

Enter the address to which the device forwards stations for additional authentication.

Configuring Hotspot 2.0

Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offer you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.



Name

Assign a name for the Hotspot 2.0 profile here. This name will appear later in the interfaces table in the selection for the Hotspot 2.0 profile.

Hotspot 2.0 version

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Operator names list

Select the profile of a hotspot operator from the list. You specify profiles for hotspot operators in the configuration menu by clicking the **Operator list**.

Connection capabilities

Select the connection capabilities for each service. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown". Possible status values for each of these services are "closed" (`-C`), "open" (`-O`) or "unknown" (`-U`):

- `ICMP`: Specify whether to allow the exchange of information and error messages via ICMP.
- `TCP-FTP`: Specify whether to allow file transfers via FTP.
- `TCP-SSH`: Specify whether to allow encrypted connections via SSH.
- `TCP-HTTP`: Specify whether to allow Internet connections via HTTP/HTTPS.
- `TCP-TLS`: Specify whether to allow encrypted connections via TLS.
- `TCP-PPTP`: Specify whether to allow the tunneling of VPN connections via PPTP.
- `TCP-VOIP`: Specify whether to allow Internet telephony via VoIP (TCP).
- `UDP-IPSEC-500`: Specify whether to allow IPsec via UDP and port 500.
- `UDP-VOIP`: Specify whether to allow Internet telephony via VoIP (UDP).
- `UDP-IPSEC-4500`: Specify whether to allow IPsec via UDP and port 4500.
- `ESP`: Specify whether to allow ESP (Encapsulating Security Payload) for IPsec.

If you do not know if a service is available and its ports are open or closed on your network, or you consciously do not want to make any entry for the status, select a `-U` setting.

Using this dialog, you do not define permissions! The stations only use the entries to determine whether to join a network via your device. You configure specific access permissions for your network with other device functions, such as the firewall/QoS.

Operating class

Enter the code for the global operating class of the access point. Using the operating class, you inform a station about the frequency bands and channels that your access point is available on. Example:

- `81`: Operation at 2.4 GHz with channels 1-13
- `116`: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11- 2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at *standards.ieee.org*.

Domain ID

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16- value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

OSU SSID

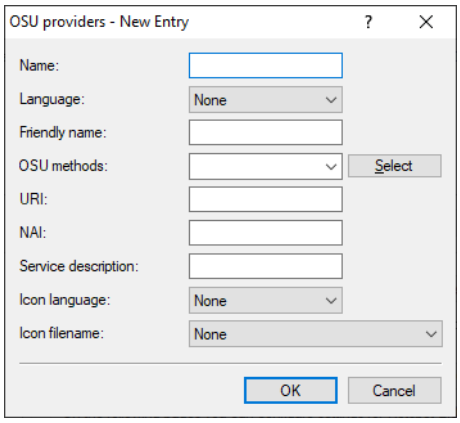
Name of the SSID that provides access to the OSU server.

OSU providers

List of OSU provider names in *OSU providers* on page 1092 that are supported in the profile.

OSU providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.



Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Language

Set the language supported by this OSU provider.

Friendly name

Give this OSU provider a descriptive name.

OSU methods

Set the OSU methods used by this OSU provider. Options are “OMA-DM” or “SOAP-XML-SPP”.

Available methods with the online sign-up server with Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Enter a URI where a client can reach the OSU server.

NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Service description

Enter a descriptive text for this service here.

Icon language

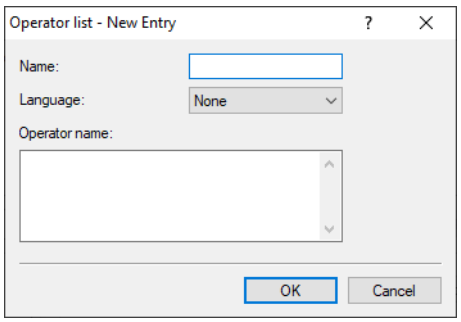
This item sets the language for the selected icon.

Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the ***File management*** feature. We recommend PNG as the file format.

Operator list

Using this table you manage the cleartext name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.



Name

Assign a name for the entry, such as an index number or combination of operator name and language.

Language

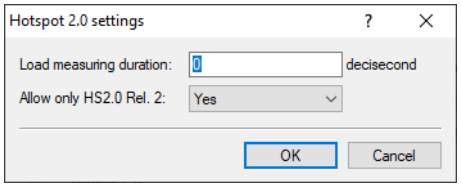
Select a language for the hotspot operator from the list.

Operator name

Enter the cleartext name of the hotspot operator.

Hotspot 2.0 settings

This table is used to configure particular settings for Hotspot 2.0.



Load measuring duration

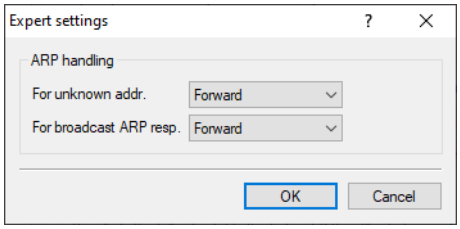
Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

Allow only Hotspot 2.0 Release 2

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

Expert settings

This table is used to configure the expert settings for Hotspot 2.0. The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. An alternative solution would be to suppressing broadcast/multicasts via **Transmit only unicasts, suppress multicasts and broadcasts** in the logical WLAN network settings.



For unknown addresses

In case of an unknown address, the packet is either forwarded or discarded.

For broadcast ARP responses

In case of a broadcast, the packet is either forwarded or discarded.

15.2.4.7 Interface for property management systems

If you use a property management system (PMS), certain device types and series give you the option of connecting your Public Spot module with your PMS database via the PMS interface. If you operate a hotel, this offers you the possibility of automatically providing your guests with access to your Public Spot when they register. This access can optionally be free of charge or fee-based (using prepaid time credits), whereby all fees are charged to the guest's bill for their room. The last name, room number and, optionally, an additional security ID (for example, registration number or departure date) are used as login data.

In contrast to a voucher solution, using the PMS interface gives you the advantage of not requiring any additional administrative steps for the setup and management of a Public Spot user account. The device creates a user account by itself as soon as the user accesses the Public Spot and logs in with his registration data. Any future changes for this guest (room change, departure date change, check-out, etc.), which affect registration, are retrieved autonomously from your PMS.

The following login methods are currently supported:

1. Voucher
2. PMS login
3. PMS login and voucher
4. E-mail
5. SMS

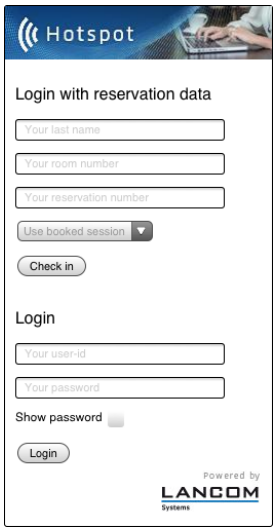
With login method (2), the login, for example, for hotel guests, can be based on the room number and last name, while you sell vouchers to your guests in your restaurant. Of course, even with the PMS interface enabled, you still have the option to issue vouchers, for example, for day guests or visitors.

The login method is configured globally for each device, and is thus the same for all SSIDs or networks.

The PMS interface currently only includes support for hotel property management systems from Micros Fidelio via TCP/IP.

Functional description

If you enable the PMS interface and provide a free or fee-based login page, the Public Spot portal page displays new input fields, which guests can use to authenticate by entering their surname, the room number and, if applicable, a further security identifier. The type of this identifier is set in the Setup menu; options include a registration number or the guest's arrival/departure date. If you have allowed access to your hotspot as a fee-based service, a drop-down menu additionally appears, which guests use to select the prepaid time quota or tariff/rate that they want to buy (e.g. 1 min for EUR 0.20, or 1 hours for EUR 1). The PMS working in the background automatically charges the costs to the room bill.



Every time a guest logs in to the Public Spot, the device initiates a comparison of the entered login data with that in the PMS. The PMS informs the device if it detects a valid match. The device then creates a new session for the guest and makes an entry in the corresponding accounting table (WEBconfig: **Status** > **PMS-Interface** > **Accounting**). The device records all hotel guests, and the corresponding prices, who have logged on via the PMS interface, irrespective of whether the connection is free or charged. The device then activates user access to the Internet.

A user with charged access can purchase additional time while logged on. Users who log off before the time quota expires can resume the session at a later time by selecting the corresponding field on the login page. The device stores the session until it becomes invalid, i.e. when the time quota is used up or when the PMS informs the device that the guest has departed. For a new login and synchronization with the PMS, the device recognizes that there is still a valid user account and continues using it instead of creating a new one.

If there is a change to the registration information (such as the room number), then an existing session initially remains unaffected. Only when the current session is closed an the guest logs on to the Public Spot again is it necessary to authenticate with the modified credentials. An exception occurs when a guest is checked-out of the PMS: In this case, the device immediately terminates an existing session.

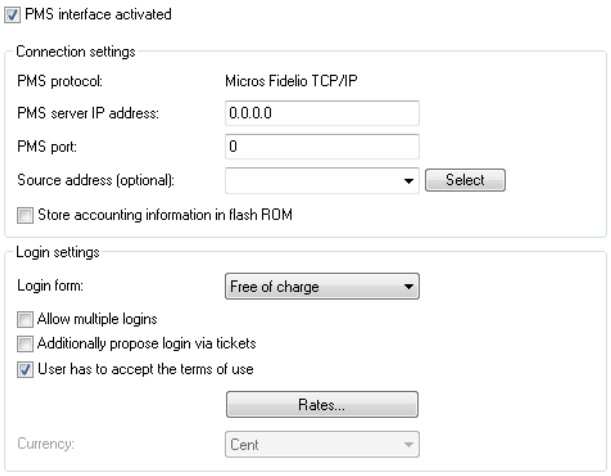
Your users should make sure that they log out properly from the Public Spot. Without a proper logout (caused by closing the browser, disconnecting the network, switching off the device, etc.) the user is considered to be still logged in. This can cause a problem for the user at login if you, as the Public Spot operator, have not allowed multiple logins.

Using *Station monitoring*, you can automatically log off these users after a specified idle time. This feature is off by default. However, for fee-based access, you absolutely should enable this. Otherwise, the device's automatic internal logout will only occur after the user account has expired, i.e., when the purchased time credit has been used up completely.

A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

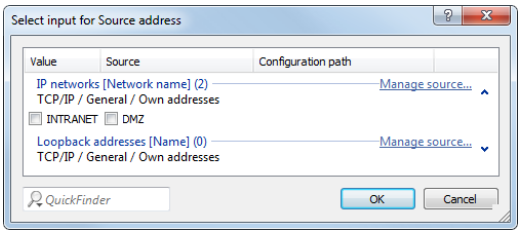
Configuring the PMS interface

Configure the PMS interface of your device in the menu **Public Spot** > **PMS-Interface**.



In this window you have the following options:

- **PMS interface activated**: Enable or disable the PMS interface for the device.
- **PMS protocol**: Identifies the protocol used by your property management system. Currently, the hotel property management systems from Micros Fidelio is supported only via TCP/IP.
- **PMS server IP address**: Enter the IPv4 address of your PMS server.
- **PMS port**: Enter the TCP port where your PMS server is accessible.
- **Source address**: Click on the **Select** button, in order to configure another address where your PMS server sends its reply messages. By default, the PMS server sends its replies back to the IP address of your device without having to enter it here.



Possible formats for entering the address include:

- Name of the IP network (ARF network), whose address should be used.
- `INT` for the address of the first Intranet
- `DMZ` for the address of the first DMZ

  If an interface with the name "DMZ" already exists, the device will select that address instead.

- `LB0`...`LBF` for one of the 16 loopback addresses or its name

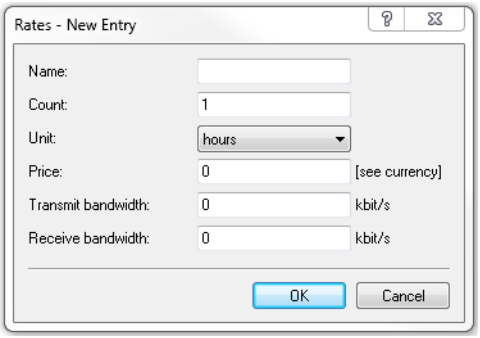
The device always uses **unmasked** loopback addresses, even on masked remote stations!

- Any IPv4 address

- **Store accounting information in flash ROM**: Enable or disable whether your device stores accounting information in regular intervals on the internal flash-ROM. By default this occurs hourly, but you can change the interval using the setup menu. Enable this option in order to prevent a complete loss of accounting information in case of a power outage.

  Please note that frequent writing operations to this memory will reduce the lifetime of your device.

- **Login form**: Choose the login form that will be shown as a portal page for your PMS interface. Possible values are:
  - `free`: Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.
  - `charge` Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate at the hotspot on the portal page with their username and room number, and also to select a rate.
- **Allow multiple logins**: Enable or disable this if you want to allow a hotel guest to use the same credentials to login to the hotspot with multiple devices.
- **Additionally propose login via tickets**: Enable or disable whether you also want to allow login with vouchers in addition to login with the combination of username/room number.
- **User has to accept the terms of use**: Enable this checkbox in order for hotel guests to accept the terms and conditions for the use of your hotspot.
- **Rates**: If you offer fee-based Internet access, this table is used to manage the tariff rates for the accounting.



  - **Name**: Specify a descriptive name for the rate here.
  - **Count**: Enter the rate for the time quota, for example, `1`. Combined with the unit, this is the value shown in the screenshot above, e.g., 1 hour.
  - **Unit**: Select the unit for the time quota from the list. Possible values are: `Minutes`, `Hours`, `Days`
  - **Price** Enter the amount charged for the time quota. In combination with the currency selected in the Login settings, the value amounts to 50 cents, for example.
  - **TX bandwidth**: Here you specify the maximum transmit bandwidth for this rate.
  - **RX bandwidth**: Here you specify the maximum receive bandwidth for this rate.

  A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

- **Currency**: If you offer fee-based Internet access, you set the currency used to bill your time quotas here (time quotas are set up using the Rates table). This unit is also displayed on the portal page. Please note that this currency must match the one on the PMS server. Possible values are:
  - `Cent`
  - `Penny`

Advanced settings

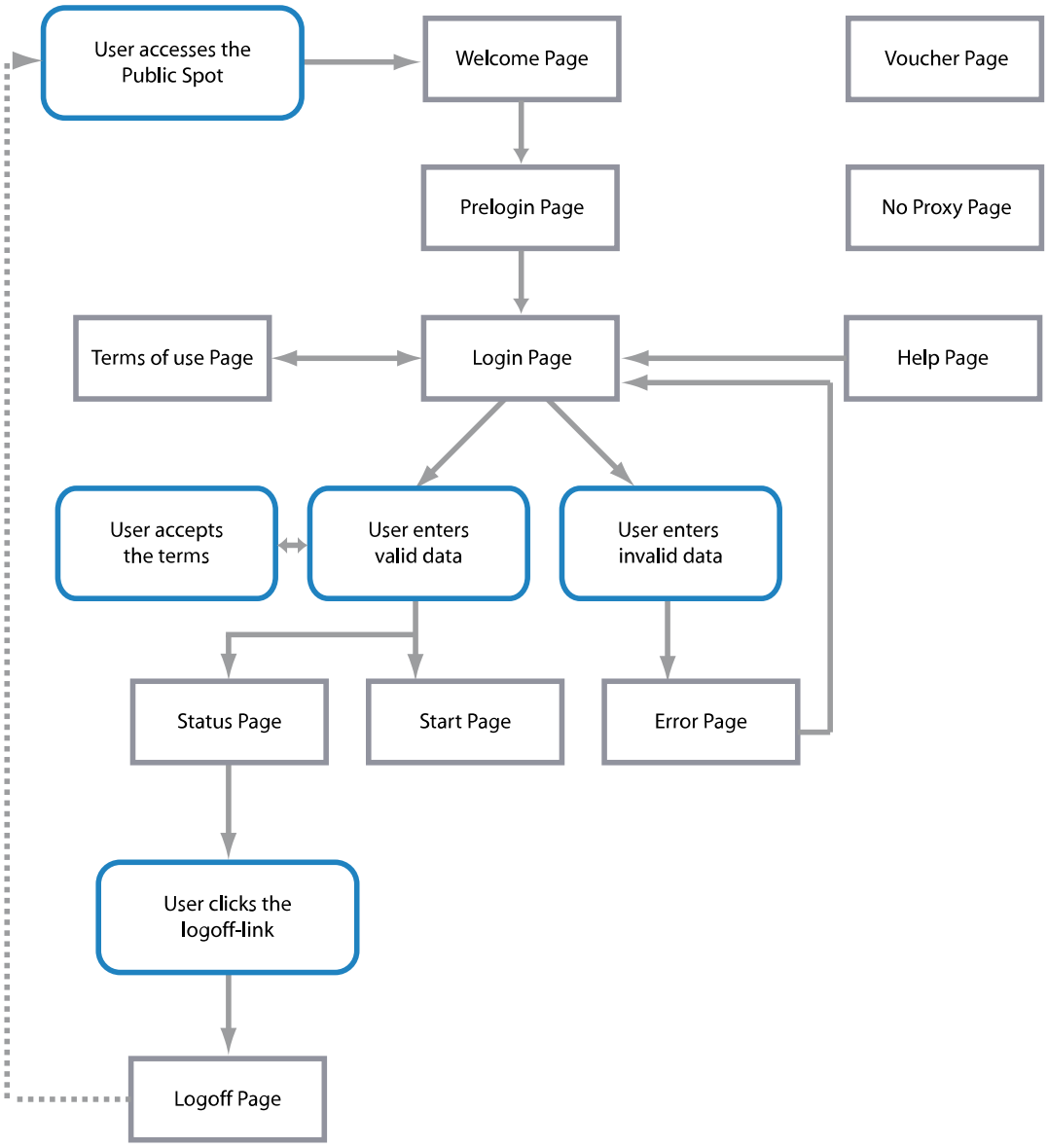
Advanced settings for the PMS interface are made on the console or in the setup menu. An overview of all additional parameters can be found in the *Appendix*.

15.2.5 Internal and customized voucher and authentication pages (templates)

By default, your device uses pre-installed templates for the login page and all other authentication pages that your user sees before, during and after a Public Spot session. However, you do have the option of adapting the individual web pages to your requirements and changing the design. You need basic HTML knowledge of DIV containers and cascading style sheets (CSS), in order to effectively change the structure and layout of the individual pages.

15.2.5.1 Possible authentication pages

The following flow-chart shows an overview and interaction of all authentication pages available with the Public Spot module: The chart takes the example of authentication using access credentials. Depending on the authentication mode and errors that can occur, the interaction may vary slightly:



The **Welcome** or **Login** pages are displayed to users when they access the Internet or the Public Spot for the first time.

- The **Welcome** page precedes the login page and is optional for most authentication modes: You can use this page, for example, to welcome a user, to provide information about the services available, or to provide instructions on how to use the Public Spot before continuing to the Start page with the login form. Only if you have selected the authentication mode "Login via agreement" is it compulsory for a customized Welcome page (containing the agreement) to be displayed, because it takes the place of the login form on the login page.

  The pre-installed default pages on your device do not include a Welcome page. If you set up this type of page without loading a template onto the device or an external server, the user either lands directly to the login page or receives an error message, depending on the login mode.

- **Authentication** includes the login form, assuming that Public Spot authentication requires the use of access credentials and that the latter have to be requested.

- The page with the **Terms of use** is only displayed if you require the confirmation of your terms of use for the selected authentication mode. In this case, a check box is displayed below the login form with an extra link that opens the terms in a pop-up.

The default pages installed on your device only include a placeholder and a generic Terms and Conditions page.

After the user has logged in with his login data (if necessary), the device checks that the information is correct and displays either an **Error** page, which sends the users back to the login page, or shows the **Start** page.

- Here, the **Error** page is only displayed to unauthenticated Public Spot users, which means that it is more or less directly associated with the login process. Typical situations in which a user sees the error page include unauthorized access to the Public Spot, when a user limit is exceeded, failed authentication due to the entry of incorrect credentials, or in case of failure of the authentication server. If you have set up monitoring of a remote site, the page could also appear whenever the Public Spot module registers a WAN link disconnection, as it provides advance notice to potential users about the lack of network availability (see *Error page in case of WAN connection failure* on page 1270).

  Users who are already authenticated will see an appropriate error message from their browser.
- If there are no errors during login, the **Start** page verifies the successful login and after a few seconds redirects the user to the Internet page originally requested by user.

Additionally, a successful login is followed by a popup window with the **Status** page.

- The **Status** page shows the user the current information about his session (e.g., time used so far, sent/received data volumes, and validity period for his account). It also offers a link to close the session and stop the accounting. A user clicking on this link is redirected to the **Logout** page.
- The **Logout** page confirms to the user that the logout from the Public Spot was successful.

The remaining **Fallback error**, **Help** and **No-proxy** pages are isolated pages not related to the login process.

- The **Fallback error** page appears whenever the device cannot deliver a custom template page and the fallback to the LCOS internal default page is missing. Delivery can fail, for example, if you have specified an incorrect file path within the pages table, or if the template page does not exist on the device.
- The **No-proxy** page is displayed whenever a user tries to connect via HTTP on port 8080 instead of port 80. In intranets, port 8080 is typically used for HTTP proxies. Since this proxy is configured with a static IP address in the browser settings, but these cannot be configured via DHCP, the user would not be able to reach this proxy. The purpose of this page is just to instruct the user to disable the proxy before the user can proceed.
- The **Help** page is only a placeholder used to embed and display specific information (e.g., details about the login or where to get vouchers) on the remaining authentication pages (e.g. the Welcome page). The default pages contain neither a help page nor any link pointing to such a page. To use a help page, you must first create a custom template page.

The **Voucher** page is not one of the authentication pages: This is the graphic template for printing the vouchers. By uploading your own template, you can print tickets with the corporate design of your own company.

15.2.5.2 Pre-installed default pages

Ex-factory, your device comes pre-installed with all of the pages you need to setup an operational Public Spot.

The following table gives you a quick overview of the default pages included with LCOS:

Table 35: Overview of installed default pages

Page designation	Pre-installed?
Welcome…	No
Login…	Yes
Error…	Yes
Start…	Yes

Page designation	Pre-installed?
Status…	Yes
Logoff...	Yes
Help...	No
No proxy	No
Voucher…	Yes
Terms of use...	No
Fallback error	Yes
Login (e-mail)...	Yes
Prelogin (e-mail)...	Yes
Login (e-mail to SMS)...	Yes
Prelogin (e-mail to SMS)...	Yes

These pages were deliberately designed to be simple, not to use any fancy features like dynamic HTML or Java Script, and just to present the necessary elements as-is. The use of plain XHTML and CSS to produce the necessary elements only ensures that the pages appear correctly on a variety of browsers and screen sizes.

As the operator of a hotspot you may want to design more sophisticated pages or display a more neutral page without the manufacturer's logo. For that reason, the Public Spot module gives you the option to customize some of the default pages, or if necessary to replace them with your own design. The latter can be done either by using HTTP redirection or templates that you upload to the device and that the device processes like an intelligent HTML pre-processor. These template pages can be stored directly to the flash memory, so you can do without an external HTTP server.

Additional languages for the authentication pages

With LCOS8.84, the Public Spot module authentication pages (i.e. all pre-installed default pages except for the voucher page) support the languages French, Spanish, Italian and Dutch. This allows you to offer Public Spot access to a broader range of international users. The language displayed is determined by the settings in the Web browser used to access the Public Spot.

Multilingual support refers exclusively to the 8.84 internal default pages. You can implement multilingual customized template pages with an external server.

15.2.5.3 Customizing the standard pages

As an alternative to installing complete user-defined Web pages, the device provides the option of customizing the pre-installed default pages to a certain extent. This includes for example the input of a login text that is displayed to your users in the registration form, or replacing the header image (logo). In this way, you can quickly deploy a customized Public Spot without having to deal in-depth with the subject of the Web page authoring.

Customized text or login title for the login page

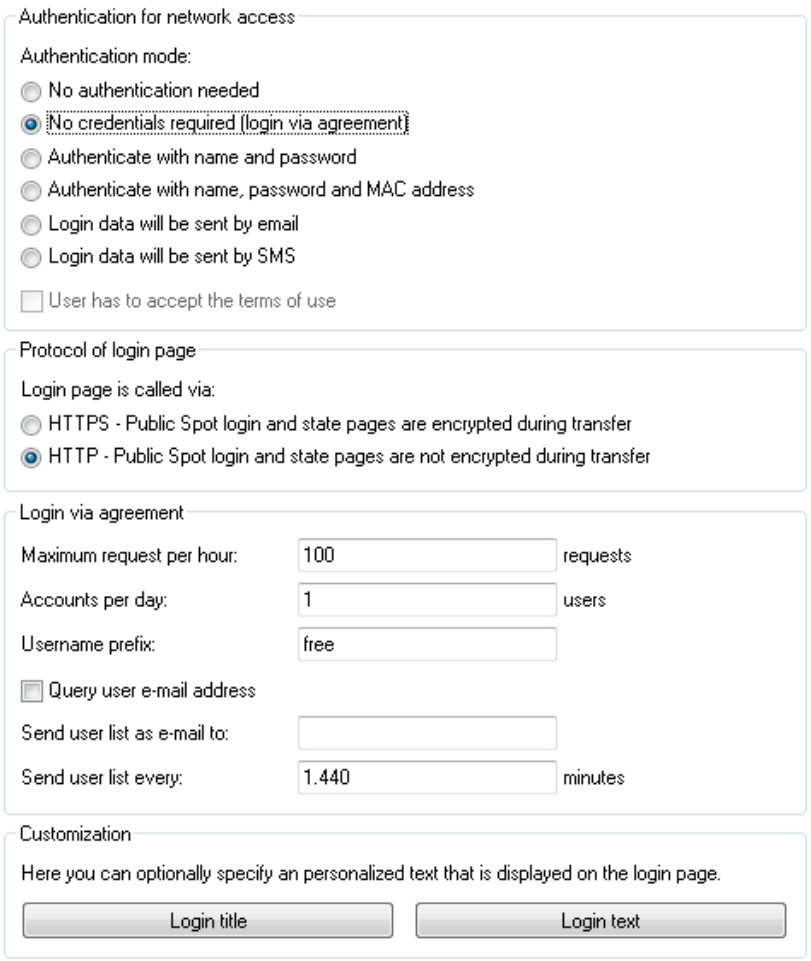
The Public Spot module gives you the option to specify customized **login text** and a **login title**, which appear on the login page in the box of the login form. The title and the text can be entered for a number of languages (English, German, French, Italian, Spanish and Dutch). The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text or title is specified for a language, then the device falls back to the English login text (if available).

Please note that the login text and the login title are separate items.

Carry out the following steps to set up customized text or title on the login page.

1. In LANconfig, open the configuration dialog for the device.

2. Navigate to the dialog **Public Spot** > **Authentication**, click on the button **Login text** or **Login title** and select a language.



3. In the dialog that opens, enter the text that your Public Spot should display to users. You can enter an HTML string with max. 254 characters composed of:

```
[Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&amp;'()+-,/:;&lt;=>?[\]^_.#*
```

LANconfig automatically transforms umlauts into their respective equivalents (`ü` to `ue`; `ß` to `ss`; etc.). To type umlauts, use their HTML equivalents (such as `ü` for `ü`), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

```
Welcome!<br/><i>Please complete this form.</i>)
```

4. Click **OK** to complete your entries and load the configuration back to the device.

Once the configuration has been written successfully, the new login text and login title appears the next time the Public Spot page is called.



Custom header images for variable screen widths

A component of the pre-installed pages in the device is a header image (logo), which is displayed to your users above the login form for the Public Spot. You can change this header image as you please, for example to reflect the application environment or your corporate design. There is no need for an external Web server; you can simply upload the image directly into the device via the file management in WEBconfig or the configuration management in LANconfig.

A special feature of the header image is that it is available in the device as two possible variants: One version is for large screens or browser windows with a horizontal resolution exceeding 800 px (normal monitors, laptops, tablet PCs, etc.), and one is a small picture for screens with a lower horizontal resolution (PDAs, mobile phones, etc.). This allows you to provide header images for different target groups and to provide them a login page that is appropriate for their device.



Figure 24: Login page for large screens

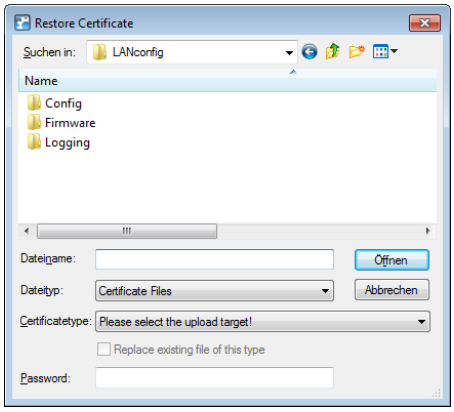


Figure 25: Login page for small screens

The available resolutions are set by the CSS file of the device. The pre-installed default graphics allow for 800x150 px for the large screen and 258x52 px for the small screen. The file type must be either JPG, GIF, or PNG.

To upload a new header image to the device either as a large or small version, follow the steps below.

1. Start LANconfig and highlight the device.
2. In the menu bar, click on **Device** > **Configuration management** > **Upload certificate or file**. The **Upload certificate** dialog opens.



3. Set the **File type** to **All files** and select the **Certificate type** that you want to upload.
   - **Public Spot - Header image of pages**: Certificate type for large screens
   - **Public Spot - Header image box**: Certificate type for small screens
4. Choose your custom header image and click on **Open**. LANconfig then starts the file upload.

After uploading successfully, the new header image appears the next time the Public Spot page is called.

You can check that the large and small header images are displayed by your Public Spot by setting your browser window width to >800 px and then reducing the width of the window. The CSS technology automatically switches between the large and small pictures.

Show/hide the vendor logo and header on the voucher

By default a voucher output by the device contains the header image and logo stored with the Public Spot homepage. The option **Public Spot** > **Wizard** > **Print header and company emblem** allows you to disable these graphics directly on the device without having to upload a customized version of the voucher template. In the case, the device outputs a neutral text voucher.

15.2.5.4 Configuration of user-defined pages

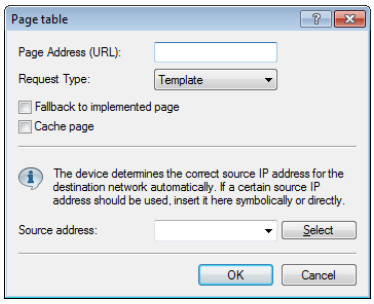
If you would like to replace the pre-installed pages with your own webpages, you can either store them directly on the device or on an external HTTP server. Sophisticated HTML pages may require more storage space than the space available on the device. There are additional advantages when using websites from an external server:

- Changes can be applied centrally. This reduces the effort required to change the login pages when using several devices.
- The server can dynamically provide the pages whose appearance is influenced by the information that the device provides. This information is discussed in more detail in the following chapters.

The storage location for the templates is entered in LANconfig in **Public Spot** > **Server** > **Page table** > **<Name of the template>** > **Page address (URL)**. There are currently three protocols available for the URL:

- `http://`...: Fetch the page via HTTP from an external server. TCP-port overrides and user/password specifications are possible.
- `https://`...: Similar to HTTP, but use HTTP over SSL for an encrypted connection.

› `file://...`: Retrieve the template from the given file in the device's local file system.



You can use any file name. If you decide to store the template pages in the device's local memory, they require the URLs reserved specially for this purpose. An internal standard page will be replaced by a new page loaded into the device by entering the local URL as the **Page address (URL)**.

Table 36: Overview of the reserved file names for template pages

Local URL on your device	Page designation
file://pbspot_template_welcome	Welcome…
file://pbspot_template_login	Login...
file://pbspot_template_error	Error...
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Logoff...
file://pbspot_template_help	Help...
file://pbspot_template_noproxy	No proxy
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Terms of use...
file://pbspot_template_fallback	Fallback error
file://pbspot_template_reg_email	Prelogin (e-mail)...
file://pbspot_template_login_email	Login (e-mail)...
file://pbspot_template_reg_sms	Prelogin (e-mail to SMS)...
file://pbspot_template_login_sms	Login (e-mail to SMS)...

*) Template for printing vouchers, no authentication page

By uploading user-defined webpages, only the webpages that are pre-installed on the device are replaced, but not overwritten. They can be rolled back to the device's proprietary default pages at any time by deleting the local URL.

To provide the highest possible compatibility with earlier display devices and web browsers, you should avoid using frames, if possible. Also, specialized content such as JavaScript or plug-in elements can lead to an erroneous display.

Login pages depending on the login mode

The following table provides an overview of which login page is displayed by the device in the various authentication modes. If a login mode has no customized page template, the Public Spot module takes the default 8.84 page:

Table 37: Overview of login pages of each authentication mode

Authentication mode	Page designation
No authentication required	–
No credentials required (login after agreement)	Welcome…
Authenticate with name and password	Login...
Authenticate with name, password and MAC address	Login...
Login data will be sent by e-mail	› Prelogin (e-mail)... › Login (e-mail)...
Login data will be sent by SMS (text message)	› Prelogin (e-mail to SMS)... › Login (e-mail to SMS)...

Special template pages for Smart Ticket

The Public Spot module in LCOS versions prior to 8.84 used a central login page for all authentication modes. As of LCOS8.84, you can optionally equip the device with separate template pages for the Smart Ticket function (for self-sufficient user registration via e-mail/SMS). Two pages have to be configured for registration via e-mail/SMS: **Registration(...)** and **Login(...)**.

- On the registration page, users enter their personal data (e-mail address or mobile phone number) to register for the Public Spot and to request its login data.
- On the login page, users then enter their credentials in order to authenticate at the Public Spot.

The following table provides an overview of the related dependencies that you need to create your own page templates:

Table 38: Overview of dependencies of the SmartTicket login pages

Authentication mode	Page designation	Local URL on your device	Page template identifiers
Login data will be sent by e-mail	Prelogin (e-mail)...	file://pbspot_template_reg_email	<regemailform>
	Login (e-mail)...	file://pbspot_template_login_email	<loginemailform>
Login data will be sent by SMS (text message)	Prelogin (e-mail to SMS)...	file://pbspot_template_reg_sms	<regsmsform>
	Login (e-mail to SMS)...	file://pbspot_template_login_sms	<loginsmsform>

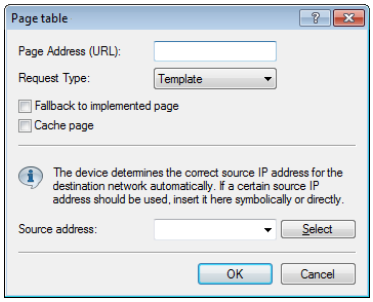
15.2.5.5 Setting up a customized template page

A custom template page allows you to replace the internal LCOS template pages with your own Web pages. This does not overwrite the LCOS templates, but just exchanges them for your own pages. If need be, you can fallback to the standard pages.

The steps below use the example of a **Login** page to show you how to set up a custom template page with the help of LANconfig.

1. You can load your customized error page either onto an external HTTP(S)-server or as the **Public Spot - Login page (* .html, * .htm)** into the memory of the device.
   Further information about uploading your own templates and sample files are available on the Internet in the *LANCOM Support Knowledgebase* under *Implementing your own websites for the LANCOM Public Spot option*.

2. Open the device configuration dialog in LANconfig, navigate to the **Public Spot** > **Server** dialog and select **Page table** > **Login**.



3. Enter the URL of the login page on the external server under **Page address (URL)** or the reference for a file on the local device (`file://pbspot_template_login`).

4. You can make these additional settings if necessary.

   - **Request type**: If you are using an external server, you can change the way in which the page is called. By default (in the setting **Template**) the device loads an externally stored HTM(L) page from the specified URL for further processing by the internal HTTP server. If you change the setting to **Redirect**, the device outsources the processing of the pages to the external server (also see *User-defined pages via HTTP redirect* on page 1317).
   - **Fallback to implemented page**: If you use an external server and chose the template type **Request**, the Public Spot module is able to use the internal LCOS template in case of HTTP(S) errors (e.g. if the server is unavailable). This enables the Public Spot to continue operating (also see *Auto fallback* on page 1318). If you do not activate this setting, the Public Spot displays the fallback error page instead.
   - **Cache page**: On some devices, you can write local and external templates to a cache. Learn more about under *Template caching* on page 1316.
   - **Source address**: This setting allows you to specify the loopback address used by the device to connect to the external HTTP(S) server. By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

5. Close this dialog and also the general configuration dialog each with click on **OK**. LANconfig then writes the new settings back to the device.

That's it!

Embedding graphics in user-created template pages

Images for your vouchers can now be uploaded into the device because a further five images slots (voucher image 1 to voucher image 5) are now available for your pages. These images are permanently stored in the flash memory of the device.

How to transfer the images into the device is described in the section *Custom header images for variable screen widths*. When uploading, set the **Certificate type** to "Public Spot - voucher image 1" to "Public Spot - voucher image 5".

Modify the HTML template of the relevant voucher (e.g. with a text editor such as Notepad++) and reference the uploaded images by including the following in the template: `<img src="/images/voucherimg1">` to `<img src="/images/voucherimg5">`. How to set up a custom template page is described in the section *Setting up a customized template page*.

15.2.5.6 Template caching

When configuring user-defined template pages on devices with sufficient memory (e.g., Public Spot gateways), you have the option to cache templates on the device. Caching improves the performance of the Public Spot module, particularly

in large-scale scenarios where the device internally caches templates and the HTML pages that were generated from them.

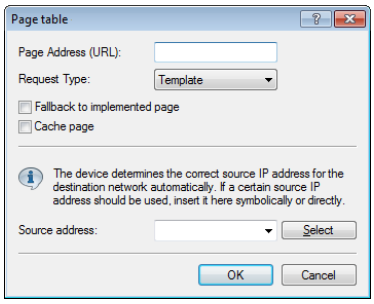
Caching is possible for:

- Templates stored in the local file system
- Templates stored on external HTTP(S) servers with static URLs

Templates on external servers that are referenced with template variables are not cached on the system.

Enable template caching

In LANconfig under **Public Spot** > **Server** > **Page table** > **<Name of the page template>**, caching for a page template is enabled by setting **Cache page**.



The corresponding parameter can be found under **Public Spot Module** > **Page table** > **Template cache**.

Delete template cache

The device automatically deletes or updates the templates stored in the cache once you load a new template file in the file system of your device (for local storage) or when the cache period for an HTTP(S) template runs out (for storage on an external server). The device evaluates the `Cache control` header of an HTTP(S) template in order to determine the maximum cache period.

If no `Cache control` header is set, the website is not cached and is immediately discarded. When setting up an individual template, ensure that you combine any META tag with a reasonable cache period (in seconds), for example, `<meta http-equiv="cache-control" content="max-age=60">`. The duration of the cache period depends on the scenario; there are no specific recommendations.

However, you do have the option of manually deleting the template cache with an action. In the status menu under **Public Spot** you can do this by starting the action **Flush template cache**.

15.2.5.7 User-defined pages via HTTP redirect

If you implement user-defined pages with redirection (request type: redirect), your device transforms it as follows: Whenever your device must send the respective page to a client, it will expand the URL according to the rules given in the previous chapter and will send an HTTP 307 (temporary redirect) response to the device, with this URL as the new location.

Redirects are particularly meaningful if you use a welcome page and all authentications should be performed on one external gateway. In this case, the clients can be immediately redirected to this gateway. This feature is often used with the external device controller.

15.2.5.8 User-defined pages via page templates

The device can alternatively act as a client and use the extended URL to download a user-defined page via an HTTP connection. The internal pre-processor takes of the processing of the page and subsequently sends the result to the Public Spot user. This pre-processor makes it possible to process session-specific data, although the server has a static

page available. The URL syntax understood by the device's built-in HTTP client is the syntax recognized by web browsers. However, only a subset of what is recognized by browsers is supported:

- The user authentication is performed using the form `user:password@host/...`
- The device is incapable of automatically resolving non-fatal HTTP errors such as redirects. Make sure that an access to this page will return the page directly.

Usage of symbolic names for the server's host instead of plain IP addresses is supported, given that DNS is properly configured. In many aspects, this mechanism can be considered like a proxy, which fetches HTML pages and then sends them to the client. The biggest difference is that the URL of the pages is determined by the device and not by the client of the Public Spot user.

Auto fallback

For every entry in the page table, it is possible to individually define whether a fallback should be used or not. This fallback feature is only meaningful if a page is defined as a template (request type: template), and not as a redirect (request type: redirect). While fetching a page via HTTP, various errors can appear:

- The DNS lookup for a host name may fail.
- The TCP/HTTP connection to the server may fail.
- The HTTP server may respond with an error code (e.g. 404 if an invalid URL was given).

By default, the device passes this type of error on to the user so that the user can start a new request or inform the provider of the Public Spot. Alternatively, the configuration of a fallback feature can ensure that the hotspot continues to function by using the default pages instead. You enable the fallback feature in LANconfig using the setting **Fallback to implemented page**.

Passed HTTP attributes

As mentioned above, in some respects the device may be seen as an HTTP proxy that fetches login and status pages for the client. HTTP proxies are obliged to keep certain HTTP attributes intact while forwarding a client request:

- The device forwards cookies between the client and the server. Client cookie values can also be sent transparently to the server and the server can set cookies on the client. Using cookies is necessary if the files that are sent from the server have ASP scripts, since ASP stores the session ID in a cookie.
- The device will forward the `User-Agent` value provided by the client. This allows a server to deliver different pages, based on the browser and system platform on the client side. PDAs and mobile phones for example call for web pages optimised for their small displays.
- The device inserts an `X-Forwarded-For` line into the HTTP request to report the device's IP address.
- WEBconfig generally attempts to use a tag named `Accept-Languages` provided by client browsers to match the request to one of the languages provided by its internal message tables (currently, only German and English). The selected language is communicated to the server via another `Accept-Languages` tag, in the hope that the server will provide a page in the appropriate language. When the server delivers the page, the device will check for a Language tag in the server's response to see if the server was actually capable of delivering a page in the requested language. If not, it will adapt the strings used in template expansion (see next section) to the actual language of the page.

15.2.5.9 URL placeholder (template variables)

The URLs specified in the page table do not need to be absolute strings. You have the option to integrate template variables in the address which are then filled-out with parameters from a Public Spot session when the device requests the pages from the server. Placeholders have a form similar to C format strings, e.g., a percent sign immediately followed by a single, lowercase character. The following placeholders are defined:

%a

Inserts the device's IP address. The placeholder only returns a value if the **Request type** in the **Page table** is set to `Template`.

Note that this placeholder cannot generate a reachable address if the device itself is located behind another router with activated NAT.

%c

Inserts the LAN MAC address of the Public Spot device as a 12-character hexadecimal string. The output is in the format 'aa:bb:cc:dd:ee:ff'.

%d

Enter the URL parameter '%d' as the circuit ID, for example `http://ipaddress/?circuit=%d&nas=%i`. The Public Spot module replaces this variable with the circuit ID that is detected in the client's DHCP request.

This requires "DHCP snooping" to be configured on the AP in such a way that the AP can query the circuit ID in the Public Spot station table of the WLC.

In this way it is possible for the Public Spot welcome page displayed on the clients to be customized by location.

%e

Inserts the device serial number.

%i

Inserts the NAS port ID. In this context, 'NAS' stands for 'Network Access Server'. This variable contains the interface of the device that the client used to login. For a WLC or router without WLAN this corresponds to a physical interface, such as `LAN-1`, or, for a standalone access point, it is the SSID.

%l

Inserts the device host name.

%m

Inserts the MAC address of the client as a 12-character hexadecimal string. The individual bytes are separated by colons.

%n

Inserts the name of the device the way it is configured in the setup menu under **Name**.

%o

Inserts the URL of the Internet page which the user initially requested. After successful authentication, the device forwards the user to this URL.

%p

Adds the IP address of the Public Spot device to the ARF context of the respective client.

Assuming that your device is active in various IP networks, you can use this variable to specify the IP address used by the device in the network where the client is also located.

%r

Adds the IP address of the client (from the perspective of the Public Spot device in the respective ARF context).

%s

If the client is connected to the device via a WLAN interface, this placeholder will insert the WLAN SSID used in the network that the client is connected to. This feature is particularly interesting when MultiSSID is used, since this gives the server the opportunity to display different pages based on the SSID. If the client is connected via another access point that connects to the device via a Point-2-Point connection, the SSID of the first WLAN will be inserted. If the client is connect via Ethernet, the placeholder remains empty.

%t

Inserts the routing tag which is appended to the client's data packets.

%v

If the requesting client is assigned an individual VLAN ID, this variable contains the source VLAN ID.

%0-9

Inserts a single number between 0 and 9.

%%

Inserts a single percent character.

In order to be able to use variables for a template, add the parameters to the **Page address (URL)** in the page table. In the following URLs the variable `%i` is replaced with `LAN-1` as described in the sample above:

Example: `http://192.168.1.1/welcome.php?nas=%i`

Example: `http://192.168.1.1/%i_welcome.html`

15.2.5.10 Tags and syntax of page templates

After the device receives the page from the server, it performs some transformations to the page template before sending it to the client. These transformations replace pre-defined HTML tag placeholders with data belonging to the client's current session (e.g. the current resource consumption in the status page). An HTML page delivered by the server could therefore better be described as a template for an actual HTML page displayed in the client's browser. HTML syntax was chosen for the placeholders to allow editing of page templates without interfering with syntax sensitive HTML editors.

In total, three placeholder tags are defined:

- `<pblink **identifier**>**text**</pblink>`

  Marks **text** as a clickable link to an **identifier**, typically to link to another page. Note that </pblink>is just an alias for , since this symmetrical definition causes less trouble with HTML syntax checkers. For example, the following fragment defines a link to the help page:

  ```
  Please click <pblink helplink>here</pblink>for help.
  ```

- `<pbelem **identifier**>`

  Insert the item specified by **identifier** at this place. For example, the following line inserts the user's time credit:

  ```
  Session will be ended in <pbelem sesstimeout>.
  ```

- `<pbcond **identifier(s)**>**code**</pbcond>`

  Only insert **code** into the page if all the identifiers are TRUE, i.e. numeric values are not equal to zero and string values are not empty. Note that the current implementation does not allow nested conditionals. Continuing from the previous example, the session timeout is only displayed if there is a time limit (a session without timeout internally has a session timeout of zero):

  ```
  <pbcond sesstimeout>Session will be terminated in <pbelem sesstimeout>seconds.</pbcond>
  ```



A set of sample page templates is available from LANCOM Systems. They are not meant to be used in productive systems, but instead to illustrate the use of page templates, and provide a starting point for your own creations.

15.2.5.11 Page template identifiers

The following identifiers can be used when designing customized template pages. The device does not differentiate between upper and lower case.

Please note that not all identifiers are available for all printouts! Not all identifiers are available on all pages.

ACCOUNTEND

Valid for: `<pbelem>`

This identifier supplements the voucher with information about the voucher's validity, i.e. from when and until when the created access account is valid.

APADDR

Valid for: `<pbelem>`

This identifier contains the Public Spot's IP address, as seen from the client's perspective. Can be used for user-defined login forms when the `LOGINFORM` element is not used.

AUTOPRINT

Valid for: `<pbelem>`

This identifier inserts a Java script into the page with the instruction to open the print dialog for printing the displayed page. Please note that in this case you **must** complete the `pbelem` tag with a separate `script`, e.g. `<pbelem autoprint></script>`.

BANDWIDTHPROFNAME

Valid for: `<pbelem>`

This identifier contains the bandwidth profile that the user is associated with.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

COMMENT

Valid for: `<pbelem>`

This identifier adds an optional comment to the voucher, assuming that you have entered an appropriate text into the Setup Wizard.

HELPLINK

Valid for: `<pblink>`

This identifier contains the URL to the help page provided by the device.

LOGINEMAILFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by e-mail.

LOGINERRORMSG

Valid for: `<pbelem>`

This identifier returns the error message from LCOS in the case of a failed authentication or a WAN-connection failure. This identifier is only available on the general error page and the fallback error page.

To retrieve the error message from the RADIUS server in the event of a failed authentication, use the identifier **SERVERMSG**.

LOGINFORM

Valid for: `<pbelem>`

This identifier contains the HTML form for authentication at the Public Spot when authenticating with user name and password (and MAC address, if applicable).

LOGINLINK

Valid for: `<pblink>`

This identifier contains the URL to the login page provided by the device.

LOGINSMSFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by SMS.

LOGOFFLINK

Valid for: `<pblink>`

This identifier contains the URL to the logout page provided by the device.

ORIGLINK

Valid for: `<pbelem>` `<pblink>` `<pbcond>`

This identifier contains the URL originally requested by the user prior to the authentication process. If it is unknown, this value is empty.

PASSWORD

Valid for: `<pbelem>`

On a voucher, this identifier contains the password for Public Spot access.

REDIRURL

Valid for: `<pbelem>` `<pblink>` `<pbcond>`

This identifier holds a possible redirection URL contained in the RADIUS server's authentication response (if there was one). It is only defined for the error and start page.

REGEMAILFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via e-mail (registration).

REGSMSFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via SMS (registration).

RXBANDWIDTH

Valid for: `<pbelem>`

This identifier contains the maximum reception bandwidth of the bandwidth profile.



This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

RXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data so far received by the device from the client in this session, expressed in bytes. It is zero for a station that is not logged in.

RXTXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data received by the device from the client so far, or sent to the client in this session, expressed in bytes. This means that it is the sum of TXBYTES and RXBYTES.

SERVERMSG

Valid for: `<pbelem>` `<pbcond>`

This identifier holds the reply message contained in the RADIUS server's authentication response (if there was one). Only applicable for the error and start pages. In the case of a failed authentication, this identifier contains the error message from the RADIUS server.

To retrieve the error message from the LCOS server in the event of a failed authentication, use the identifier **LOGINERRORMSG**.

SESSIONSTATUS

Valid for: `<pbelem>`

This identifier contains a textual representation of the current status of the client relative to the device (whether authenticated or not).

SESSIONTIME

Valid for: `<pbelem>`

This identifier contains the time that has passed since the login on the Public Spot.

SESSTIMEOUT

Valid for: `<pbelem>` `<pbcond>`

This identifier contains the remaining time for the current session. After this time, the device ends the current session automatically. This identifier is zero for a session with no time limit.

SSID

Valid for: `<pbelem>` `<pbcond>`

This identifier on a voucher contains the SSID to be used for Public Spot access.

STATUSLINK

Valid for: `<pbelem>` `<pblink>`

This identifier contains the URL to the logout page provided by the device. A reference that opens a new browser window is automatically generated within the `<pblink>` element.

TXBANDWIDTH

Valid for: `<pbelem>`

This identifier contains the maximum transmission bandwidth of the bandwidth profile.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

TXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data transmitted by the device to the client so far in this session.

USER NAME

Valid for: `<pbcond>`

This identifier allows you to supplement the voucher page with conditional HTML code, which is only printed for certain users or administrators. `USER` is a prefix and **must** be placed before the user name (`NAME`) and a space. To generate HTML output specifically for the user 'root' when calling the voucher page, use the following syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

When used in larger Public Spot scenarios with central administration, such as with a WLAN controller, this dependency can be used for the purpose of site localization: To do this, you create a Public Spot admin for each of the relevant access points and you specify a conditional voucher text for each administrator.

USERID

Valid for: `<pbelem>`

This identifier contains the user ID (in the form of the username) with which the current session was started. The identifier is not specified if the client is not (yet) logged in.

VOLLIMIT

Valid for: `<pbelem>` `<pbcond>`

This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

VOUCHERIMG

Valid for: `<pbelem>`

This identifier inserts the page banner image (in large size) into the page.

New placeholders from LCOS version 9.20:

These placeholders enable the page templates to be fine tuned. Unlike the placeholders mentioned above, these placeholders do not output any additional descriptive text, but their values only.

${SSID}

Returns the network name / SSID.

${USERID}

Returns the user name.

${PASSWORD}

Returns the user password.

${COMMENT}

Returns the comment.

${BandwidthProfName}

Returns the name of the bandwidth profile.

${TxBandwidth}

Returns the specified maximum bandwidth (transmit direction).

${RxBandwidth}

Returns the specified maximum bandwidth (receive direction).

${ACCOUNTEND}

This identifier returns the end of the ticket (date and time).



To use this placeholder, you need to include the jquery library in the template. To do this, add the following to the template:

```
<script src="/jquery/jquery.js" type="text/javascript"></script>
```

```
<script src="/jquery/jquery.tmpl.min.js" type="text/javascript"></script>
```

You also need to use the new placeholders inside a <script> block:

```
<script id="voucherTemplate" type="text/x-jquery-tmpl">

[... Contents ...]

</script>
```

15.2.5.12 Graphics in user-defined pages

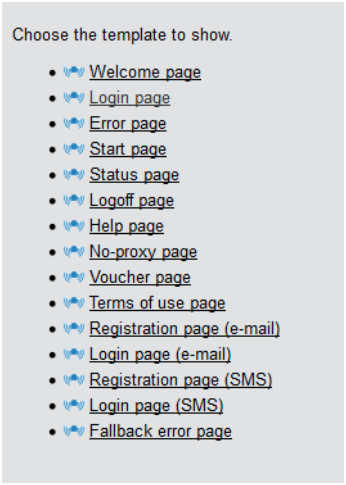
All but the simplest web pages contain images, which are fetched by the client's browser independent of the HTML page itself. The graphic files for the pre-installed page are also stored on the device. The device automatically adapts the necessary permissions so that even unauthorized clients have access to the images without problems. However, every access to the referenced (device-external) images for user-defined pages are treated like a normal Internet access, and would automatically send the user back to the welcome or start page.

In order to avoid this behavior, you should make sure that the servers where the graphics are stored are included in the **free servers**. Free servers are addresses that have unlimited access, and are therefore also accessible by unauthenticated clients, and are not billed by the accounting feature in the same way as the rest of the data traffic.

The chapter *Open access networks (no login)* on page 1253 contains additional information about configuring free servers. Note that if a user-defined page is defined as a redirect, this of course has to be defined as a free IP address.

15.2.5.13 Template preview in WEBconfig

You can view the changes to the Public Spot templates in WEBconfig by switching to the view **Extras** > **Public Spot template preview**.

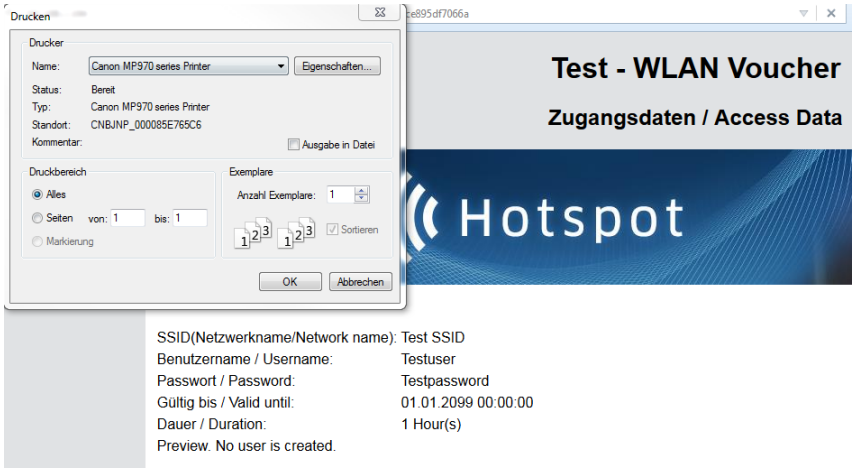


Select a template to display from the list.

The selected template is displayed in the same browser window. Use the "Back" function of your browser to return to WEBconfig.

Some templates contain JavaScript code. This code is executed when the template is invoked. For example, the "Voucher page" template contains code that starts a printout when the page is displayed.

This page contains test data. However, no user is created at this point. This allows you to test the template and print it out.



If a template does not exist or cannot be found, an error message is displayed by WEBconfig.

15.2.5.14 Public Spot Captive Portal API

The Public Spot supports the new Captive Portal API standard according to *RFC 8908*. The standard allows Wi-Fi clients in a hotspot to automatically find a captive portal or login page.

The client receives the URL of the portal page via DHCP and uses an API request to the hotspot to check whether a login is required or whether access is already permitted for the client. This significantly speeds up the user experience in a hotspot and, by defining a standard, now provides better manufacturer interoperability between hotspots and clients.

The following steps are required:

1. The use of TLS certificates in the Public Spot is mandatory. Without an HTTPS login, the client does not send a request to the portal.
2. The DHCP server must provide the Captive Portal DHCP option to the client.

The configuration in LANconfig is located under **Public-Spot** > **Server** > **Captive Portal API (RFC 8908)**.



Captive portal API enabled

Enables or disables the Captive Portal API function in the Public Spot.

User portal URL

(Optional) By default, the Captive Portal API supports TLS only. For this reason the device must have a trusted certificate and a DNS name. By default, the parameter can be left empty and it will be inserted automatically by the system. To do this, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate. If an external hotspot server is used, a URL of this server can be entered here. Another requirement is that the clients in the hotspot must find the captive portal via DHCP option. For this purpose, the corresponding DHCP option according to *RFC 8910* must be configured for the hotspot network.

Venue URL

(Optional) URL (TLS) through which the operator can provide the user with additional information about the location of the hotspot, e.g. the website of the hotel with the hotspot.

Configure DHCPv4 option (according to RFC 8910)

In LANconfig, create a new table entry under **IPv4** > **DHCPv4** > **DHCP options**.

Option number

Number of the option that should be sent to the DHCP client. In this case 114.

Network name

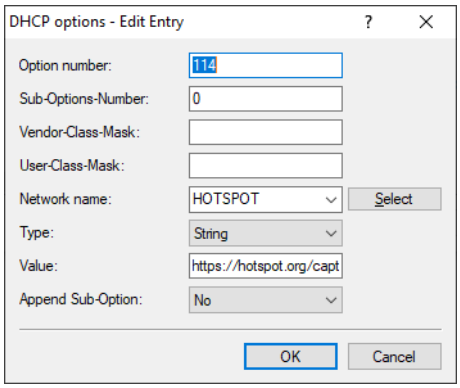
Name of the Public Spot network (see IPv4 networks)

Type

Entry type. In this case String.

Value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name. Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



Configure DHCPv6 option (according to RFC8910)

In LANconfig, create a new table entry under **IPv6** > **DHCPv6** > **DHCPv6 server** > **Additional options**.

Interface name/Relay IP

Name of the Public Spot network (see IPv6 networks)

Option code

103

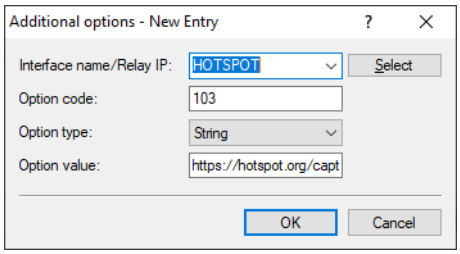
Option type

String

Option value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name.

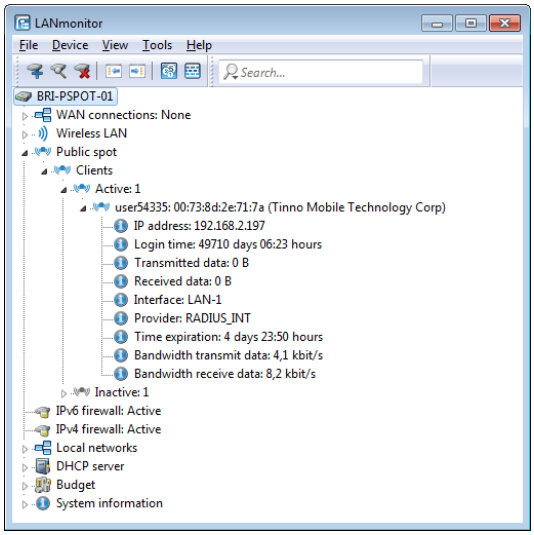
Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



15.2.6 Viewing Public Spot clients

LANmonitor can optionally display detailed information about the clients associated with the Public Spot.

1. Open the menu item **Public Spot** > **Clients**.
2. Double-click on **Active** to display the active clients, or on **Inactive** to display inactive clients.
3. Double-click on a client to retrieve detailed information about it.



15.2.7 Displaying advertising to Public Spot users

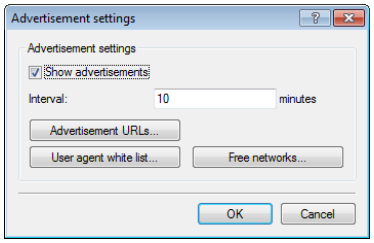
You can optionally display advertising to Public Spot users at configurable time intervals. The Public Spot shows the advertisement in the normal browser window of the user and not using a pop-up, since all modern browsers normally block pop-ups. In the Public Spot station table, a client can have one of three states:

- Authenticated: The client is logged on and can surf in Internet.
- Unauthenticated: The client is not logged on and cannot surf in Internet.
- Advertisement: The next time a client calls a URL, it is redirected to an advertisement URL.

You have the option to exclude certain networks and user agents from the display of advertisements by means of a whitelist.

1. In the device configuration, select the menu branch **Public Spot** > **Server** and click on **Advertisement settings**.

2. Enable the **Show advertisements** checkbox.



   You can now change the interval between advertisement displays, and also other settings.
3. Under **Interval** you specify the time in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of `0` forwarding occurs directly after login.
4. Click on **Advertisement URLs** to add an advertisement URL. If you add multiple URLs, the Public Spot displays them in sequence after the specified interval.
5. Optional: Click on **User agent white list** to add user agents, which the Public Spot excludes from the display of advertisements.
6. Optional: Click on **Free networks** to add networks, which the Public Spot excludes from the display of advertisements. This can be used in various ways, for example to enter the automatic search URLs used by the browser, e.g. `*.google.com`. Typically, a browser sends keyboard input at the address bar to a search engine; by setting the exception, the advertisement page does not responding to this.

   Login-free networks are generally ad-free networks. There is no need to explicitly include these networks into the whitelist.
7. Close all dialog windows by clicking on **OK**.

Public Spot users will be redirected to an advertisement URL after the specified time interval unless they are using a whitelisted user agent or they are located in a free network.

The timing of the advertisements refers to the session time of the active Public Spot clients. If a client stop sending data for a certain time, then the interval before the Public Spot displays advertising again will be delayed by this time.

15.3 Access to the Public Spot

15.3.1 Requirements for logging in

- Device with network adapter
- Operating systems supporting the TCP/IP protocol (automatic IP-address retrieval by DHCP active)
- Web browser (supporting JavaScript and Frames)
- Direct Internet access (use of proxy deactivated)
- WLAN access information (network name, encryption information)
- Valid user data (user identifier and password)

Information for WLAN access

A maximum of two pieces of information are required to access the WLAN:

- **The network name of the WLAN (SSID)**

  If the Public Spot's base stations are configured for operation as a closed network, the user must know the exact name of the wireless LAN, its SSID.
- **WLAN encryption**

Although it is possible to provide guest access via encrypted connections using, for example, WPA, Public Spots are not generally operated with WLAN encryption. Protection is provided in this case using authentication with a username and password. Data security when transmitting data on the Public Spot must be provided by the end user (e.g., using a VPN client).

Information for LAN access

If the IP addresses on your network are automatically assigned (for example, via DHCP), your users only need:

- a LAN socket that connects to the Public Spot.
- a LAN cable to connect their LAN adapter to the LAN socket.

Information for authentication

The user needs to have the following information to hand when logging in:

- User identifier
- Password
- MAC address

If you set the authentication mode for a Public Spot at the base station to "MAC+User+Password", you, as the operator, must know the MAC addresses of the end devices employed by your users. An end device automatically and continuously transmits its MAC address when communicating with a base station. The user does not have to manually enter this information when logging in, but instead it is communicated just once to the operator before attempting to login.

15.3.2 Logging in to the Public Spot

1. Log in to the WLAN of the Public Spot (for WLAN connections) or connect to the network using an Ethernet cable (for LAN connections).
   The different types of mobile devices and WLAN adapters offer various ways of entering the settings required for accessing the WLAN. Many devices require the network name (SSID) of the WLAN to be entered into the configuration program for the WLAN adapter. Some other products also provide an overview of all base stations in the vicinity, from which the user simply chooses the one they want to use.

   Depending on the configuration, the user receives the necessary settings for the LAN-adapter connection either automatically from the network or a connected DHCP server, or from the network administrator.

2. Start your Web browser.

   As soon as the Web browser attempts to access any Internet site, the Public Spot automatically intervenes and presents the login page. The login page, or the login form displayed within it, appear differently depending on which

firmware version you are using and which login mode you have selected. In the following, we assume a login with a voucher (or by user name and password).



Figure 26: Login page for large screens

3. Enter the complete **user ID** and **password** in the corresponding fields and confirm your entries with **Login**.

   To login, you should use a Web browser with JavaScript support enabled to ensure that session status information can be displayed in a popup window.

   If the login to the Public Spot is successful, an additional window pops up with the main information about the current session. This window is also used for the login. This window should be left open throughout the session (e.g., it can be minimized).

   If the login fails, an error page opens with a request to return to the login page and to repeat the authentication. The form takes over a portion of the previously entered data as an aid to the user, e.g. in case of typos.

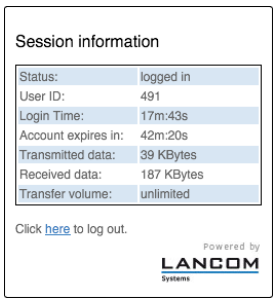
15.3.3 Session information

The window with session information is automatically updated at regular intervals. Along with the status and current user ID, the information displayed includes the connection time and the volume of transferred data.

If the session-information window is not open, you can open it by entering the following in the address line in the browser:

```
http://<IP address of the Public Spot>/authen/status
```

Alternatively, you can open the session page with the short URL `http://logout`.



15.3.4 Logging out of the Public Spot

The session information window can be used to logout from the Public Spot. Click on **here** in the bottom line of text in the window.

If the session-information window is not open, you can enter the following into the address line in the browser:

`http://<IP address of the Public Spot>/authen/logout`

Alternatively, you can open the session page with the short URL `http://logout` to logout from the Public Spot.

The operator can set up the Public Spot to automatically logoff users if they cannot be reached for 60 seconds. In case of doubt, please ask the Public Spot operator if automatic logoff (*Station monitoring*) is activated.

15.3.5 Advice and help

The following sections present solutions to the most common problems that may occur when operating a Public Spot.

15.3.5.1 The Public Spot login page is not displayed

- The Internet access must be set up so that it is directed via the network adapter and not via a dial-up networking connection. To check this, take a look at the connection settings for your Web browser. If you use Microsoft Internet Explorer, you must disable the dial-up configurations in **Tools** > **Internet Options** > **Connections**entered there.
- Internet access must be direct, i.e. without going via a proxy server. In Microsoft Internet Explorer, you can disable the use of a proxy server in the menu **Tools** > **Internet Options** > **Connections** > **LAN-Settings...**.
- If you are making the connection with a WLAN adapter: Ensure that your network adapter can in fact find the Public Spot. Your WLAN adapter gives you the option of searching for an access point.
- If you are making the connection with a WLAN adapter: Check if your network adapter has all of the necessary settings to access the Public Spot network:
  - You probably have to enter the network name for the WLAN.
  - When working with an encrypted Public Spots, you are also required to enter the corresponding WPA or WEP key.
- Check that your network adapter is set up for automatic retrieval of an IP address (DHCP). Your device should not have a fixed IP address.

If your network adapter is set up with a fixed IP address, adjusting it for automatic retrieval by DHCP may cause important configuration information to be lost. Ensure that you note all of the values listed in the network settings (IP address, standard gateway, DNS server, etc.).

15.3.5.2 Login not working

- Ensure that you enter the user data correctly and in full. Ensure that you use the correct capitalization for all entries.
- Is the CAPS-LOCK key activated on your device? This causes the capitalization to be reversed. Deactivate the CAPS-LOCK key and repeat the entry of your login data.
- The Public Spot operator may be checking more than just the user ID and password, but also the MAC address (physical address) of your network adapter as well. In this case, ensure that the Public Spot operator is informed of your correct MAC address.

15.3.5.3 It is no longer possible to login

If the Public Spot breaks off communications after a number of login attempts have failed, you should deactivate your WLAN adapter for at least 60 seconds (or your entire device) or disconnect the LAN adapter from the network, and then try again.

15.3.5.4 The session information window is not being displayed

To display the session-information window, enter the following line into the address line of your Web browser:

`http://<IP address of the Public Spot>/authen/status`

The Public Spot operator can supply you with the `<Public Spot's IP address>` upon request.

15.3.5.5 The Public Spot requests a new login for no reason (WLAN)

When moving into the signal coverage area of another access point (roaming), it is necessary to login again. If you are located in the overlap area between two access points, you may even experience a change of connection between the two access points at regular intervals. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

› LANconfig: **Public Spot** > **Users** > **Roaming Secret**

15.4 Tutorials for setting up and using Public Spots

The following tutorials describe examples of how the Public Spot option can be implemented.

15.4.1 Virtualization and guest access via WLAN controller with VLAN

Many companies wish to offer Internet access to their visitors via WLAN. In larger installations the required settings apply to multiple access points, and these can be programmed centrally in the WLAN controller.

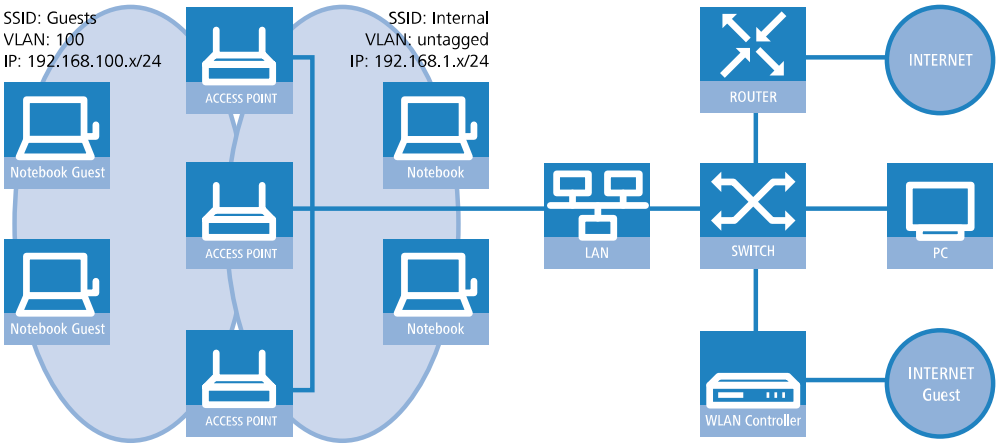
15.4.1.1 Targets

- Wireless LAN infrastructure available to internal employees and guests
- Shared physical components (cables, switches, access points)
- Separation of networks with VLAN and ARF
- Break-out of data streams to certain target networks:
  - Guests: Internet only
  - Internal employees: Internet, all local devices and services
- Guests login to the WLAN with a Web form.
- Internal employees use WLAN encryption for authentication.

15.4.1.2 Establish

- Management of the access points is handled by the WLC.
- The WLC serves as the DHCP server for the WLAN clients in the guest network.
- The guest network is provided with Internet access via the WLC (e.g. separate DSL access or Internet access via the company DMZ).
- The wired infrastructure is based on managed VLAN-capable switches:
  - Access point VLAN management is handled by the WLC.
  - The VLAN management of the switches is handled separately by the switch configuration.

› The access points operate within the internal VLANs.

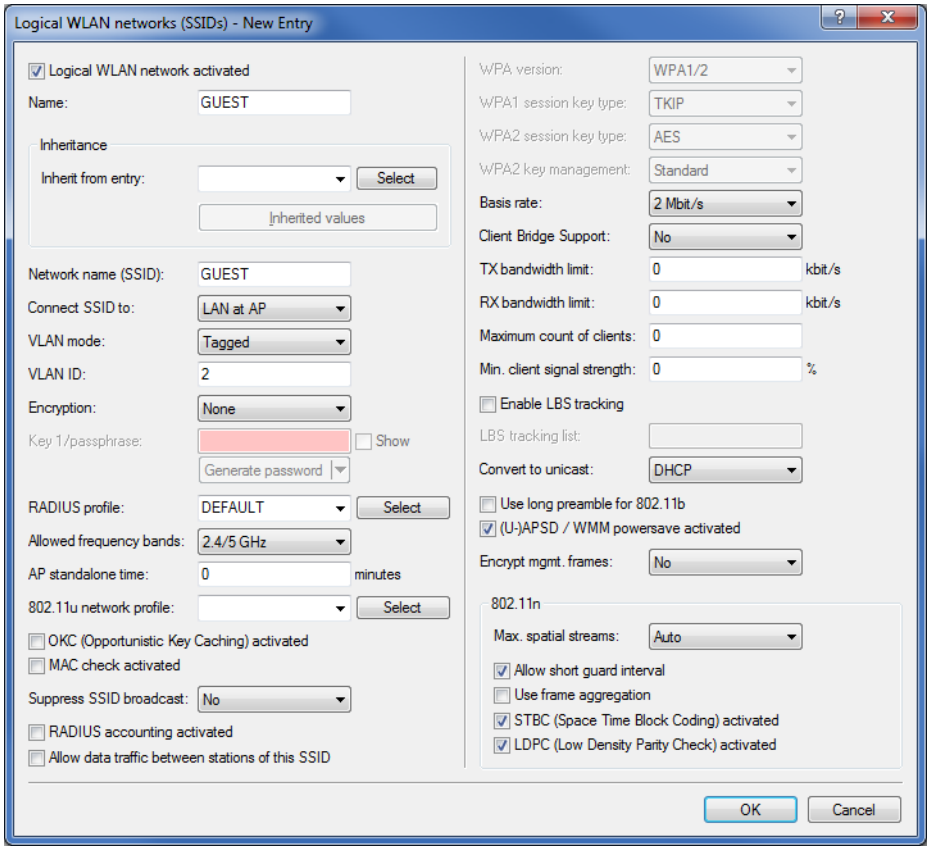


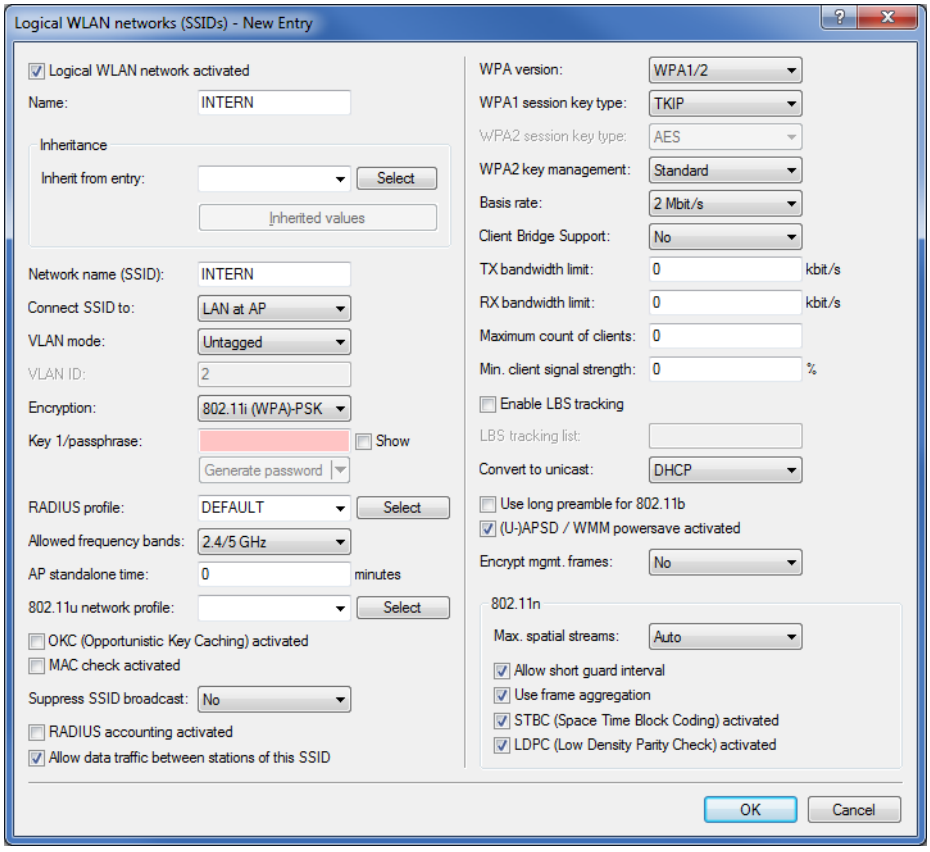
15.4.1.3 Wireless LAN configuration of the WLAN controllers

During the configuration of the WLAN, the necessary WLAN networks are defined and, along with the physical WLAN settings, are assigned to the access points managed by the controller.

1. Create a logical WLAN for guests and one for the internal employees:
   - › The WLAN with the SSID `GUESTS` uses the VLAN ID `100` (VLAN operating mode **Tagged**) and uses **no** encryption.
   - › The WLAN with the SSID `INTERNAL` receives no VLAN ID (VLAN operating mode **untagged**, i.e. packets are transferred in the Ethernet without a VLAN tag) and uses WPA encryption, e.g. **802 11i (WPA)-PSK**.

› LANconfig: **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**

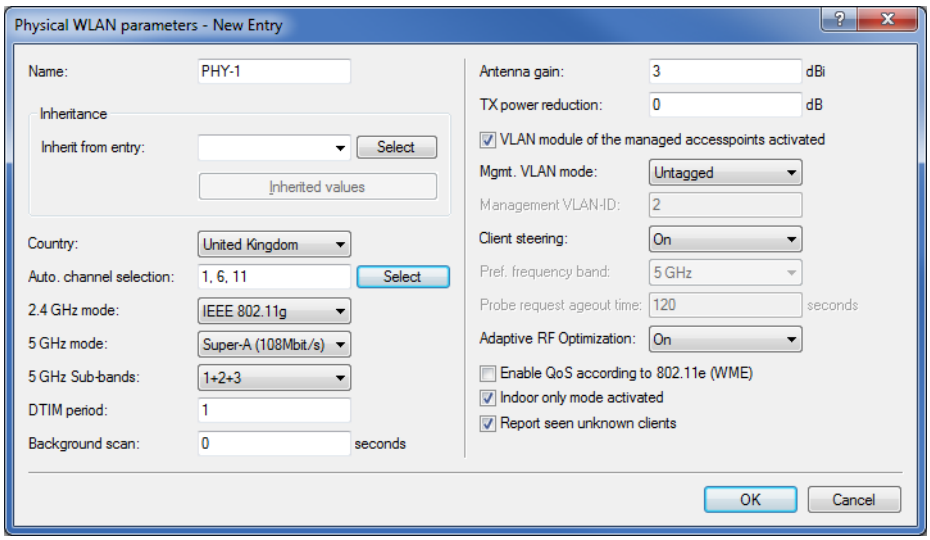




If you set the **VLAN mode** to **untagged**, LANconfig will gray-out the **VLAN ID** input field in the add/edit dialog shown above. However, the corresponding table **Logical WLAN networks (SSIDs)** still displays the assigned VLAN as a value in the grayed-out box. This entry is only of internal significance, as the acceptable range is between 2 and 4094. Ultimately it is the VLAN operating mode which is decisive: If this is set to **untagged**, then a VLAN ID is not transmitted under any circumstances.

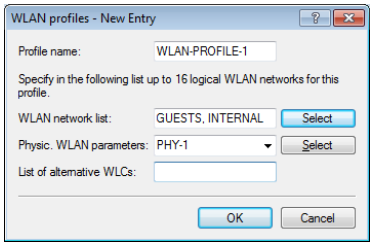
2. Create a set of physical parameters for the access points.
The management VLAN ID is set to `1`, which serves to activate the VLAN function (but without a separate management VLAN for the device; the management data traffic is transmitted untagged).

   › LANconfig: **WLAN-Controller** > **Profiles** > **Physical WLAN parameters**



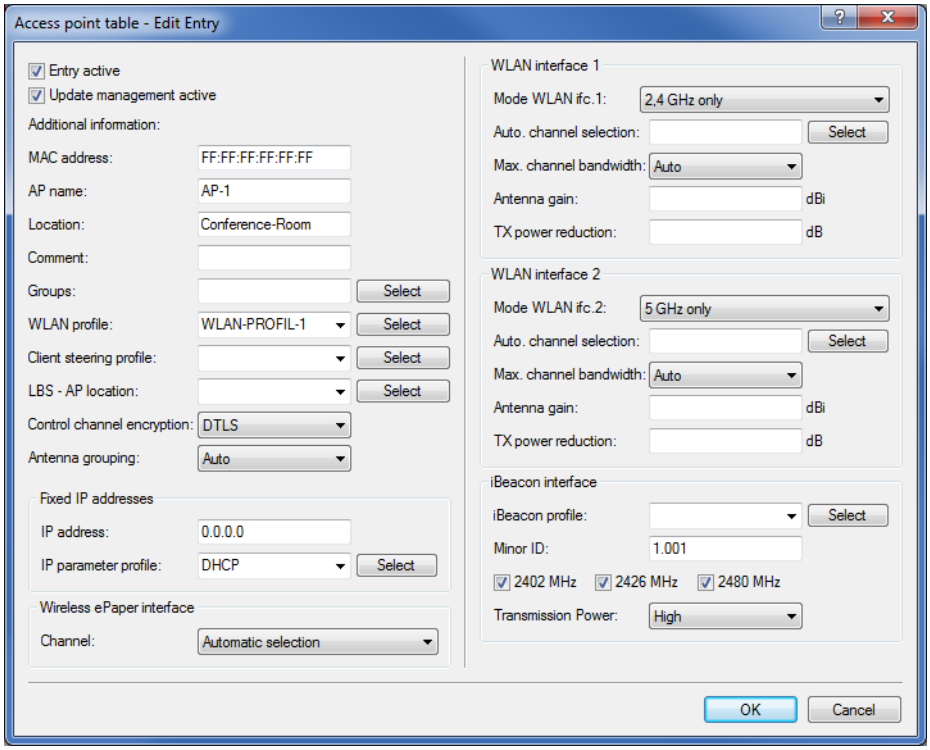
3. Create a WLAN profile that you can assign to the access points.
   The two logical WLAN networks and the set of physical parameters defined earlier are collected into this WLAN profile.

   › LANconfig: **WLAN-Controller** > **Profiles** > **WLAN-Profiles**



4. Assign this WLAN profile to the access points managed by the controller.
   Do this by entering each access point with its MAC address into the access point table. Alternatively you can use the **Default** button to create a default profile, which applies to all access points.

   › LANconfig: **WLAN controller** > **AP configuration** > **Access point table**



15.4.1.4 Configuring the switch (LANCOM GS-2326P)

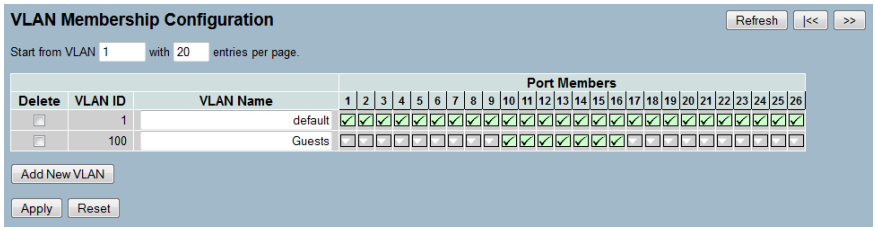
In this section we describe the configuration of the switch using the LANCOM GS-2326P as an example.

1. Under **Configuration** > **VLAN** > **VLAN-Membership**, create an additional VLAN group for the guest network.

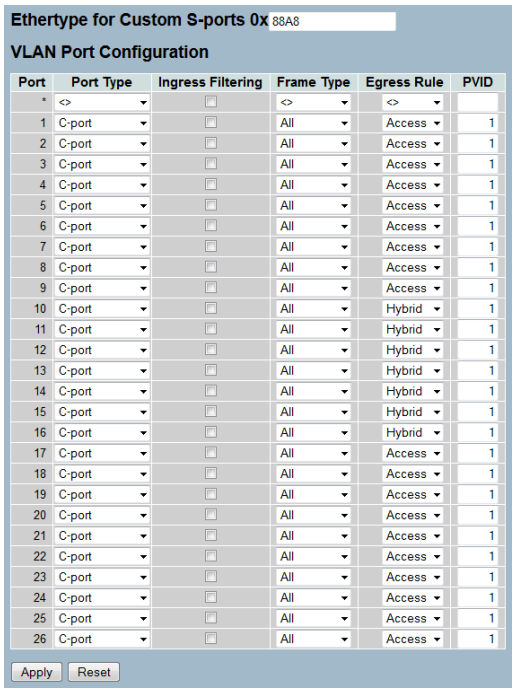
   To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the group `default`, and that for the guests is mapped to the group `guests`.

   › The VLAN group for the internal employees uses the default VLAN ID `1`. This VLAN ID used for internal administration applies on all ports and is operated untagged, i.e. all untagged incoming data packets are given the VLAN ID 1 for internal routing, and this is removed again from outgoing data packets (see also "PVID" in the next step).

› The VLAN group for the guests uses the VLAN ID `100`, which you entered earlier when configuring the WLAN in the controller. This ID applies only to the ports which the WLAN controller and the access points are connected to (in this example: Port 10 to 16, green checkmarks for **Port members**). The switch does not remove tags from outgoing data packets. i.e. all tagged incoming packets with VLAN ID 100 retain this tag and are routed only to the ports that are members of the corresponding group.



2. Under **Configuration** > **VLAN** > **Ports** set the **Port Type** for all ports to **C-port**. See the documentation about your switch for details about this setting.
3. Configure the **Egress rule** for each port.
   › All ports except port 10 to 16 are given the **Access** rule. As a result, these ports forward only tagged packets and all others are dropped.
   › The ports 10 to 16 are given the rule **Hybrid**. As a result, these ports forward both untagged and tagged packets.



Ensure that the **PVID** (port VLAN ID) for each port is set to a value of `1`. The PVID is the VLAN ID that a port assigns to incoming data packets which do not already have a VLAN tag; Therefore, the PVID corresponds to the VLAN ID of the `default` group.

4. OPTIONAL: If you wish to allow access to the guest network via Ethernet, go to **Configuration** > **VLAN** > **Ports** and, for example, set the **PVID** to `100` for ports 17 to 20 and, under **Configuration** > **VLAN** > **VLAN-Membership**, assign these ports to the group `Guests`. All untagged incoming data packets arriving at these ports are given VLAN ID 100.

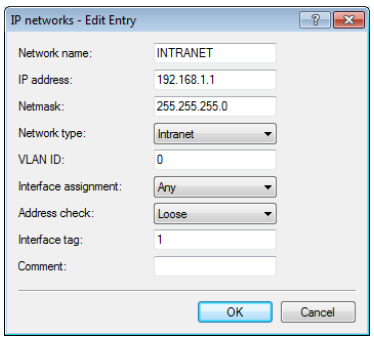
Note that these data packets can only leave the switch via the ports of the guest network.

15.4.1.5 Configuring the IP networks in the WLAN controller

To separate the data streams on layer 3, two different IP networks are employed (ARF – Advanced Routing and Forwarding).

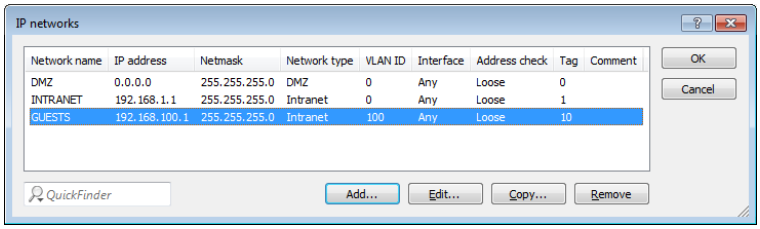
1. For the internal network, set the **INTRANET** to the address `192.168.1.1`.
   This IP network uses the **VLAN ID** `0`. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The **interface tag** `1` is used for the subsequent break-out of data in the virtual router.

   › LANconfig: **TCP/IP** > **General** > **IP networks**



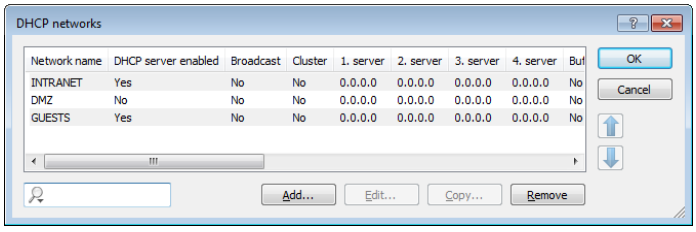
2. For guests, create a new IP network with the address `192.168.100.1`.
   This network uses the **VLAN ID** `100`. In this way, all data packets with this ID are assigned to the guest network. Here, too, the **interface tag** `10` is used later by the virtual router.

   › LANconfig: **TCP/IP** > **General** > **IP networks**

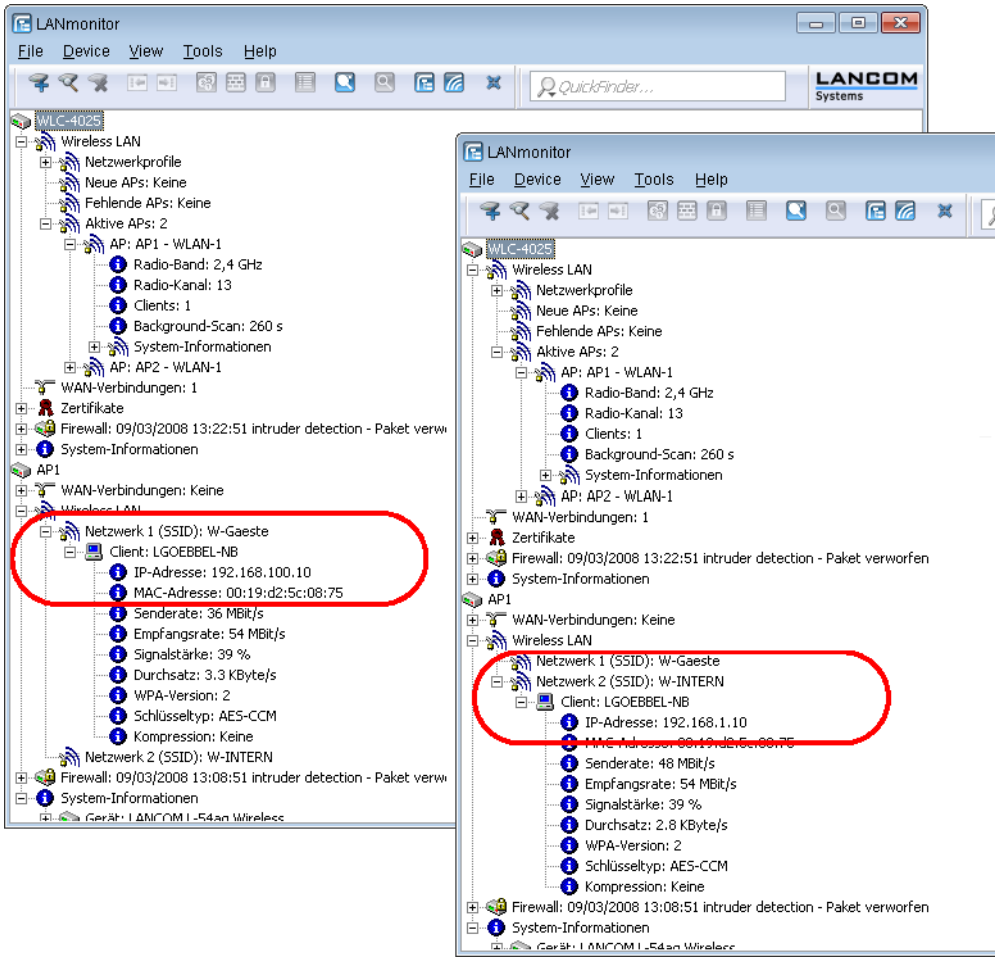


3. Enable the DHCP server for both IP networks.

   › LANconfig: **TCP/IP** > **General** > **IP networks**



With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.

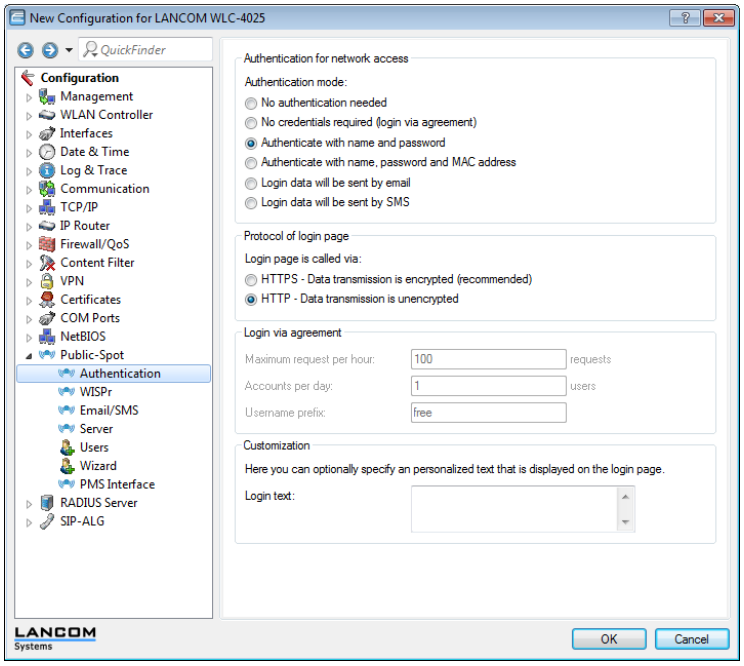


15.4.1.6 Configuring Public Spot access accounts

The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. Authentication is performed by requesting user information via a web interface. If necessary, you can can set a time limit for the access.

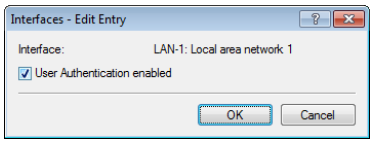
1. You should activate authentication for network access by name and password.

› LANconfig: **Public Spot** > **Authentication** > **Authentication for network access**



2. Activate user authentication for the controller's interface that is connected to the switch.

› LANconfig: **Public Spot** > **Server** > **Operation settings** > **Interfaces**

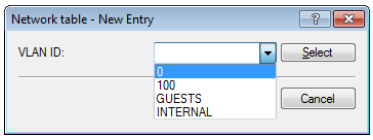


3. Restrict access to the Public Spot.

   You restrict use of the Public Spot to data packets from this virtual LAN by entering the VLAN ID of "100" for the guest network into VLAN table. Other data packets from other VLANs will be forwarded to the Public Spot without a login. Note that access to WEBconfig via the Public Spot interface is restricted to the authentication pages only (see *Limit configuration access*).

   If the interface is not restricted to the VLAN ID, the controller will no longer be reachable at the specified physical Ethernet port!

   › LANconfig: **Public Spot** > **Server** > **VLAN table**



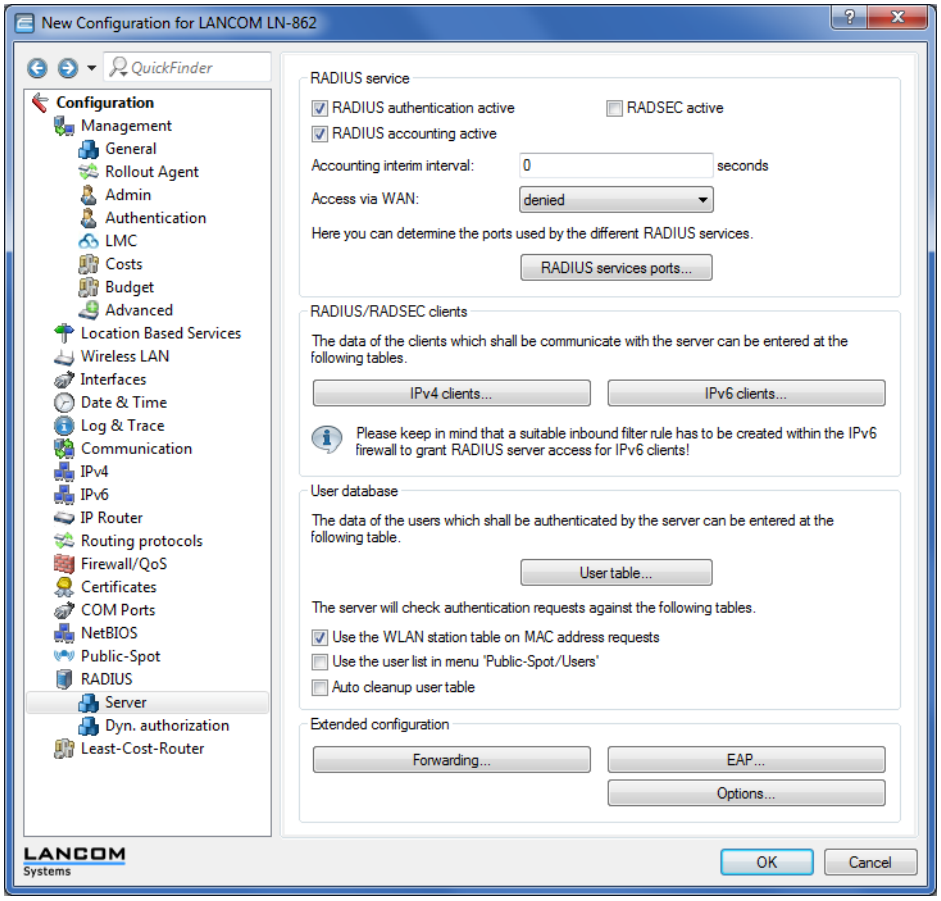
4. Enable the option to clean up the user table so that your device automatically deletes entries that are no longer needed.

   › LANconfig: **RADIUS** > **Server** > **User table** > **Auto cleanup user table**

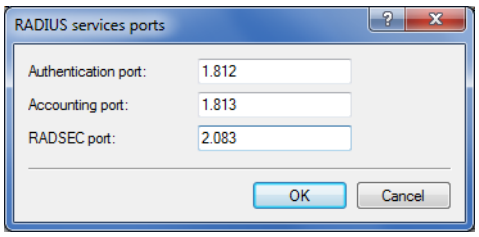
15.4.1.7 Configuring the internal RADIUS server for Public Spot operation

The Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. In order to use these Public Spot access accounts, the internal RADIUS server has been preconfigured with default values. You can inspect this setup in **LANconfig** as follows:

1. Navigate to **RADIUS** > **Server** > **RADIUS service**.
2. Ensure that checkmarks have been set for **RADIUS authentication active** and **RADIUS accounting active**.



3. Click the button **RADIUS services ports**.



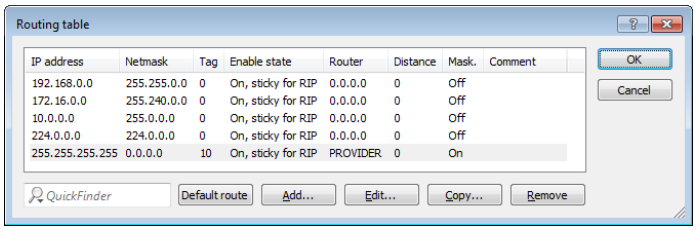
The default settings are available here for inspection.

15.4.1.8 Configuring Internet access for the guest network

1. In order to provide Internet access for guest network users, there is a wizard to set up access to a provider network.
2. Limit access to the provider network.
   In order for this access to be available to users of the guest network only, set the routing tag "10" for the corresponding route. This ensures that only data packets from the IP network "GUEST" with the interface tag "10" are transmitted

to the provider's network. The different routing tag values ensure that data cannot be routed between the guest network and the internal network.

› LANconfig: **IP router** > **Routing** > **Routing table**



3. Optional: If necessary, use **Device** > **Configuration Management** > **Upload certificate or file** in LANconfig to upload an HTML template and an image as a template to the device for output of the voucher.
The image can be a GIF, JPEG or PNG file of max. 64 KB in size.

15.4.2 Virtualization and guest access via WLAN controller without VLAN

15.4.2.1 Overlay network: Separating networks for access points without using VLAN

In many cases, networks in a shared physical infrastructure are separated by using VLANs. However, this method assumes that the switches operated in the network are VLAN-capable and that these are configured for VLAN operations. Consequently, the administrator has to rollout the VLAN configuration for the whole network.

WLCs enable you to separate the networks while minimizing the use of VLANs. The APs use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the WLC, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the WLC and a single, central switch. All of the other switches in this example work without a VLAN configuration.

With this configuration, you reduce the VLAN to the core of the network structure (illustrated with a blue background). What's more, only 3 of the switch ports in use require a VLAN configuration.

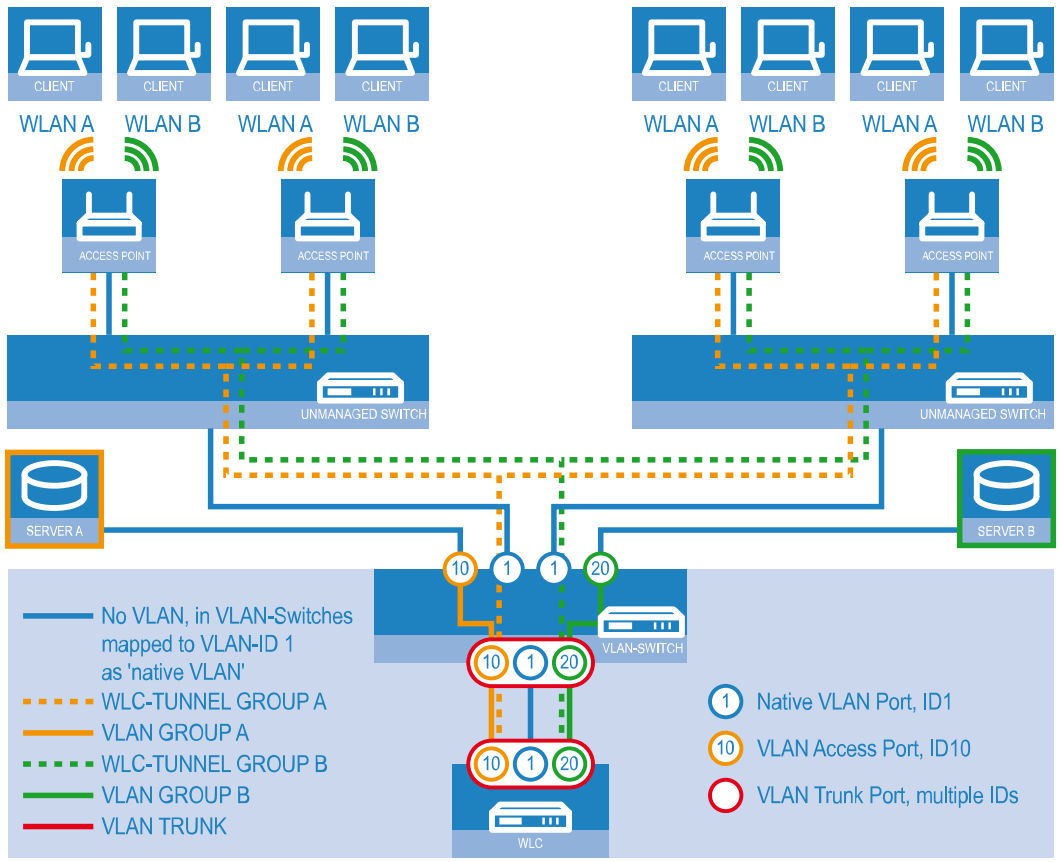


Figure 27: Example application: Overlay network

The diagram shows a sample application with the following components:

- The network consists of two segments, each with its own (not necessarily VLAN-capable) switch.
- Each segment contains several APs, each of which is connected to one of the switches.
- Each AP provides two SSIDs for the WLAN clients in two different user groups, shown in the diagram in green and orange.
- Each user group has access to its own dedicated server that is separated from other user group. The servers can only be accessed via the corresponding VLANs, i.e. through the access ports configured on the switch.
- A single WLC manages all of the APs in the network
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLC.

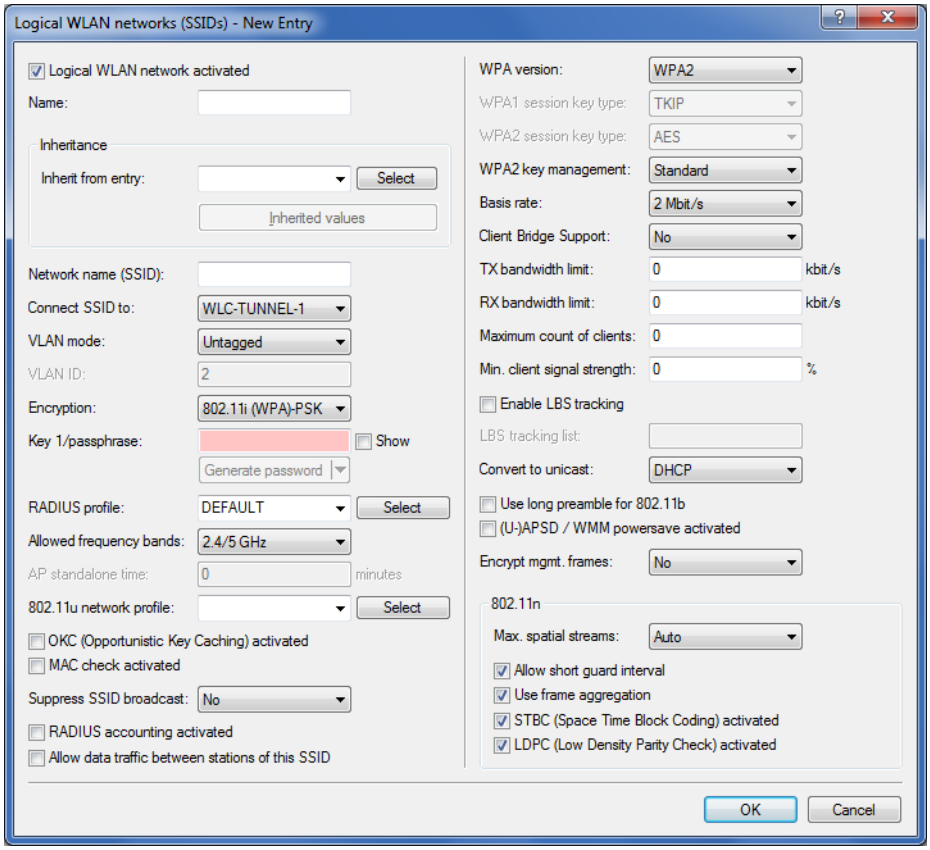
The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which AP is being used and regardless of the segment in which the client is located.

The following description assumes a working basic configuration of the WLC. The configuration of the VLAN switch is not part of this description.

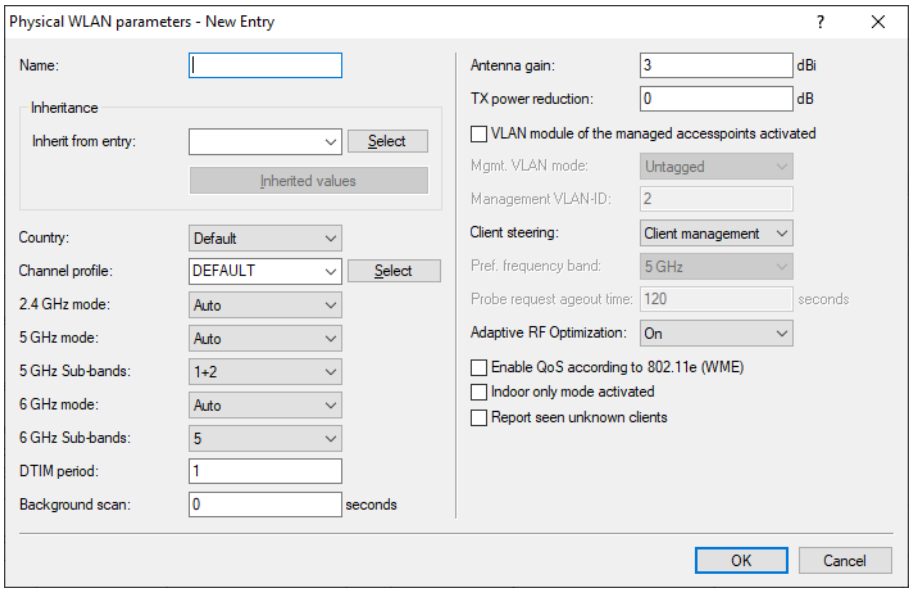
Configuring the WLAN settings

1. For each SSID, create an entry in the list of logical networks, each with a suitable name and the corresponding SSID. Connect the SSID to a WLC tunnel, for example the first SSID to "WLC-TUNNEL-1" and the second to "WLC-TUNNEL-2 '. Set the VLAN mode to 'tagged', set the VLAN ID '10' for the first logical network and the VLAN ID '20' for the

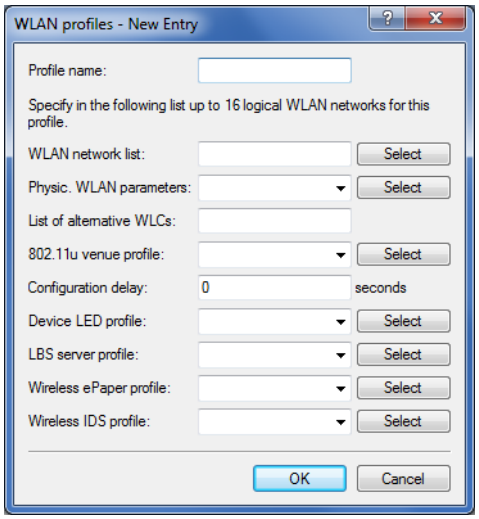
second logical network. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.



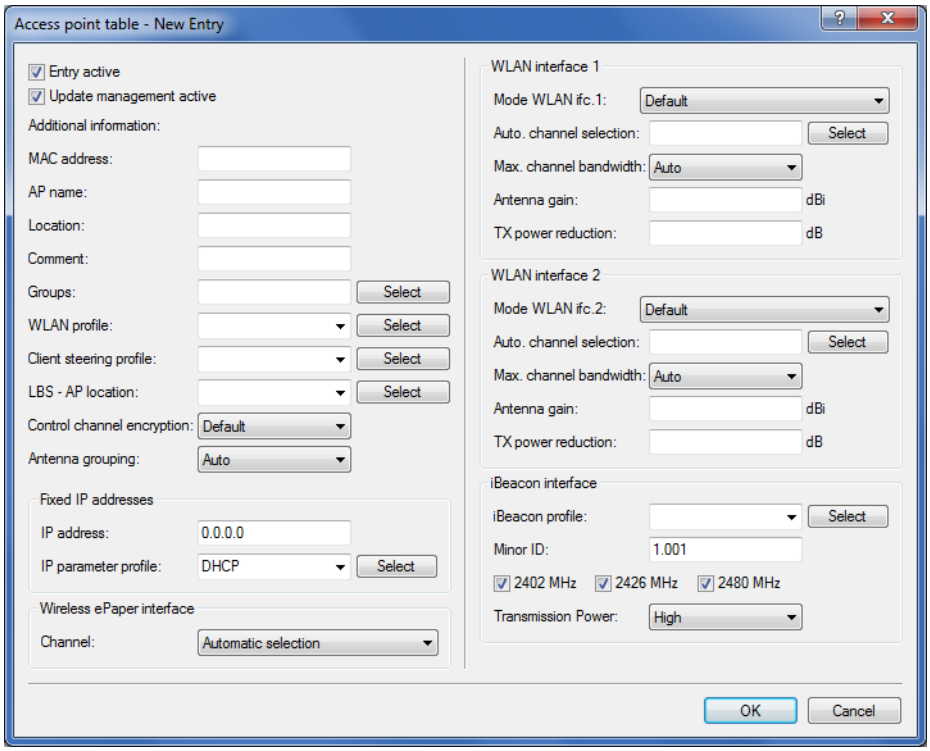
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. For this profile in the physical WLAN parameters, enable the option to turn on the VLAN module on the APs. Set the operating mode for the management VLAN in the APs to 'Untagged'. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.

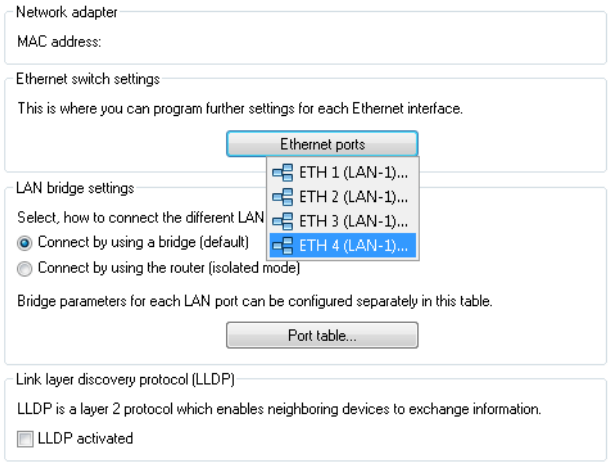


4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.

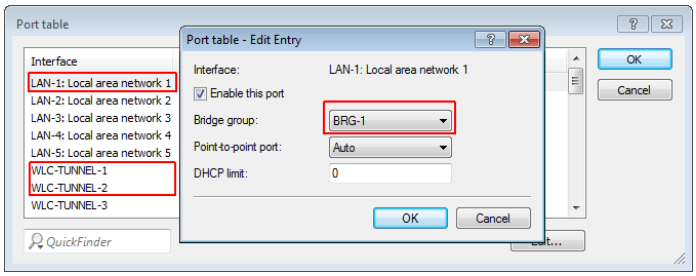


Configuring the interfaces on the WLC

5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Make sure that the other Ethernet ports are not assigned to the same LAN interface. In LANconfig you find these settings under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.

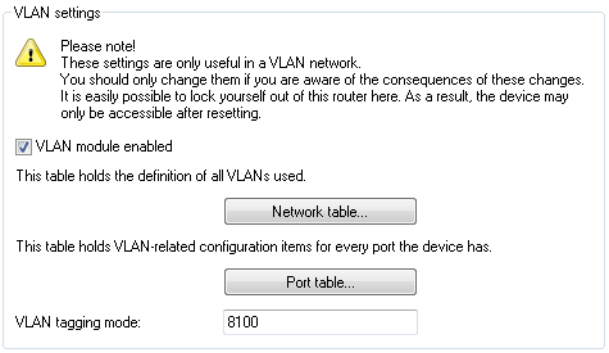


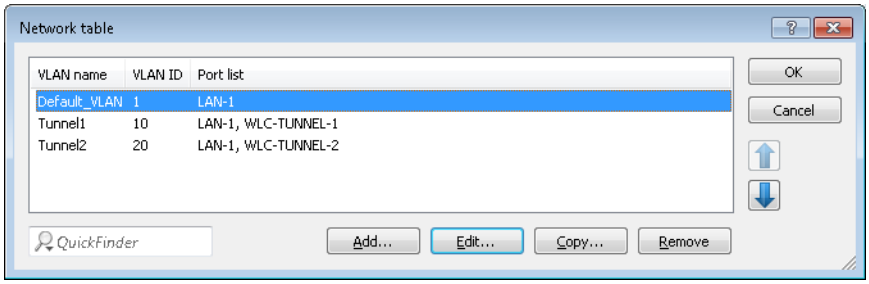
6. Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.



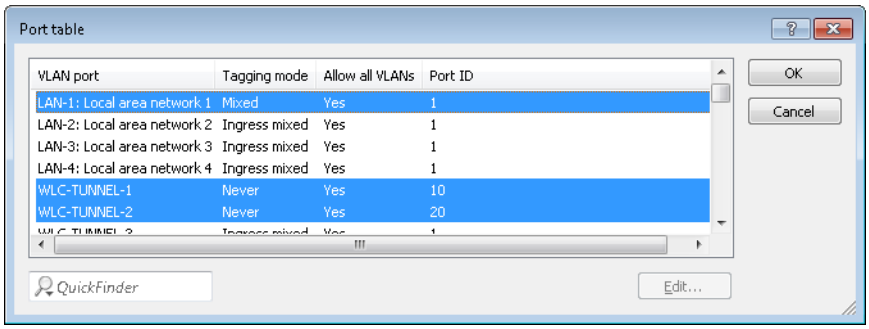
By default, the LAN interfaces and WLC tunnels do not belong to a bridge group. By assigning the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-Tunnel-1' and 'WLC-Tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

7. Activate the VLAN module of the WLC under **Interfaces** > **VLAN** and, under **VLAN table**, assign the LAN port you selected above (LAN 1) and also the corresponding WLC tunnel to the desired VLAN.





8. Under **Interfaces** > **VLAN** > **Port table**, set the Tagging mode of the tunnel interface and the LAN interface, and set the corresponding port VLAN ID.



Depending on how the switch is configured, set the Tagging mode of the LAN interface to 'Mixed' or 'Always'.

In most cases the tunnel interfaces are operated with the mode 'Never', because packets here (from the WLAN) always arrive untagged and the WLC marks them with the port VLAN ID

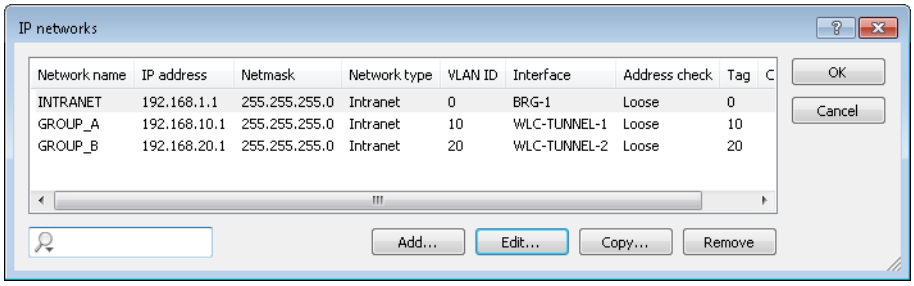
When you activate the VLAN module, please observe that the ARF networks configured on the WLC must be given a VLAN ID. In the VLAN configuration outlined above, you need to set the VLAN ID for the IP network to '1' in order for the WLC to reach the network without a VLAN tag.

A similar configuration is achieved by making the access point set a VLAN tag for packets that are to be sent via the tunnel, in which case the VLAN module of the WLC is not used.

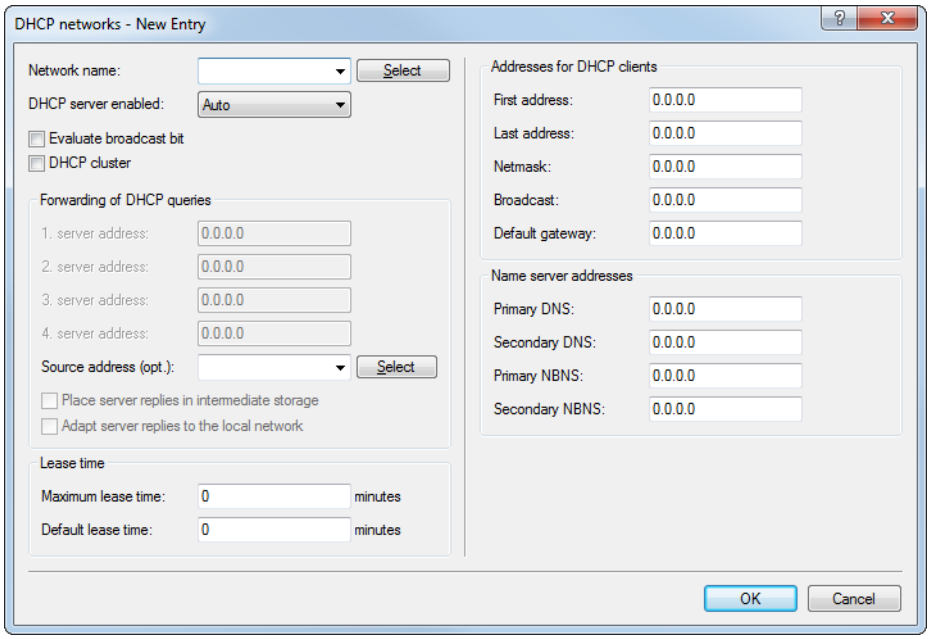
However, this bridging of the various WLC tunnels with one another causes broadcasts to be redirected into all of the tunnels; with a certain number of tunnels/SSIDs and APs, this can lead to load problems on the network and on the WLC. The VLAN module configuration presented here prevents this.

9. In addition you configure the IP settings for the networks that are separated on layer 2 under **IPv4** > **General** > **IP networks**.

To prevent the device from connecting these networks via layer 3, a separation must also be configured on layer 3, for example by using a port tag or by means of the firewall.



10. The WLC optionally acts as a DHCP server for the APs. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **IPv4** > **DHCPv4** > **DHCP networks**.



15.4.2.2 WLAN controller with Public Spot

This scenario is based on the first scenario (overlay network) and enhances it to include specific settings for user authentication.

The configuration of a Public Spot can be greatly simplified if the payload data sent from the WLAN to the WLC is routed through a WLC tunnel. A Public Spot can, for example, provide guests with Internet access in parallel with, but separated from, an internal wireless LAN.

In this example, the employees of a company have access to a private WLAN (SSID), while the guests use a Public Spot to access the Internet. In all areas of the building, the APs provide two SSIDs, 'COMPANY' and 'GUESTS'.

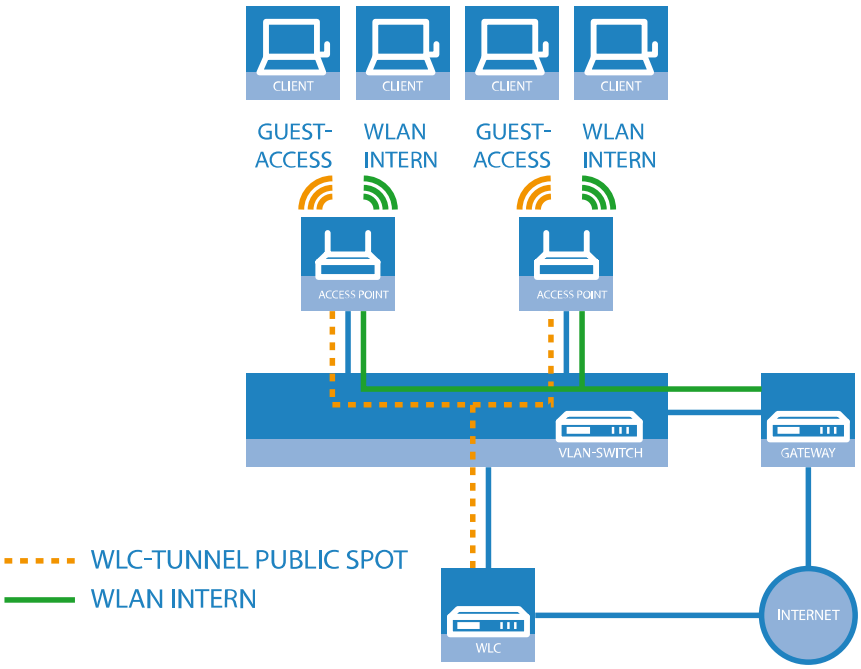
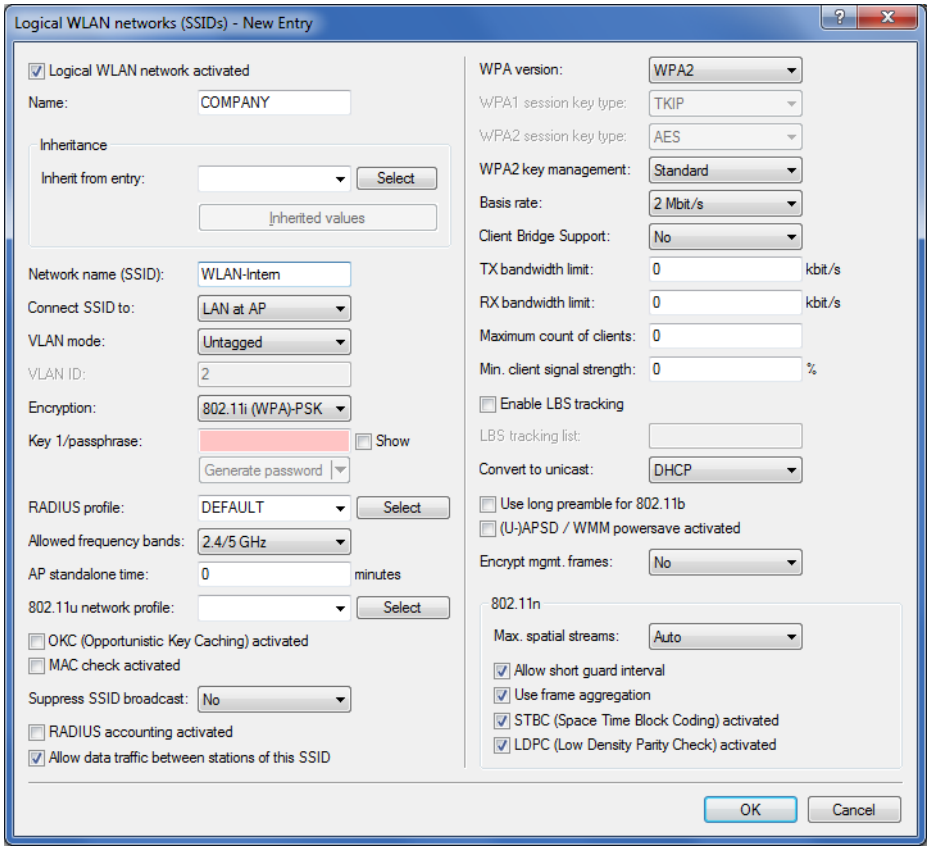


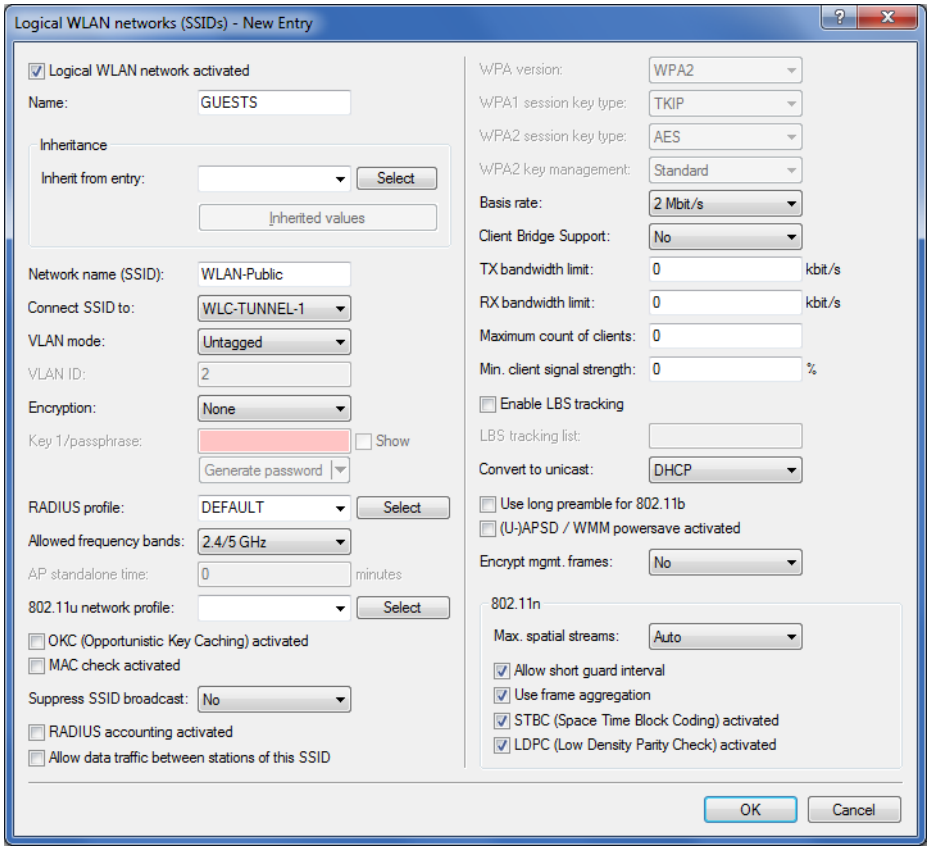
Figure 28: Example application: WLAN controller with Public Spot

The aim of the configuration: A WLAN client that associates with the internal SSID should have access to all internal resources and the Internet via the central gateway. The APs break-out the payload data from the internal clients locally and pass it on directly to the LAN. The guests' WLAN clients associate with the Public Spot. The APs send the payload data from the guest clients through a WLC tunnel directly to the WLC, which uses a separate WAN interface for Internet access.

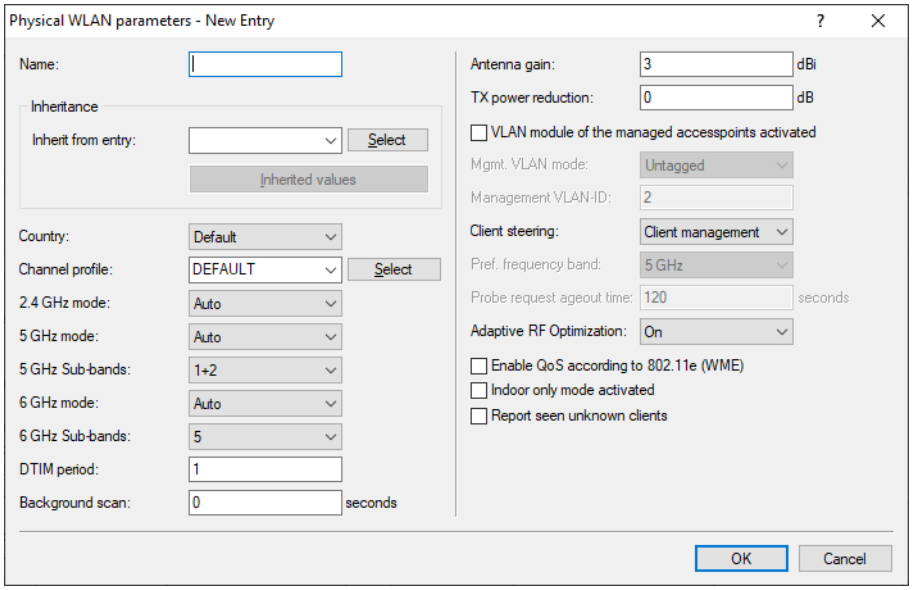
1. The internal WLAN and the guest WLAN each require an entry to be created in the list of logical networks, each with a suitable name and the corresponding SSID. Link the SSID for internal use with the 'LAN at AP', and the SSID for guests with (for example) 'WLC-TUNNEL-1'. Disable encryption for the guest network SSID so that the guests' WLAN

clients can associate with the Public Spot. You should also prevent inter-station traffic for this SSID. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.

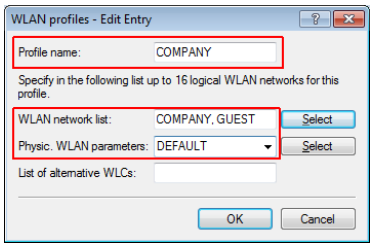




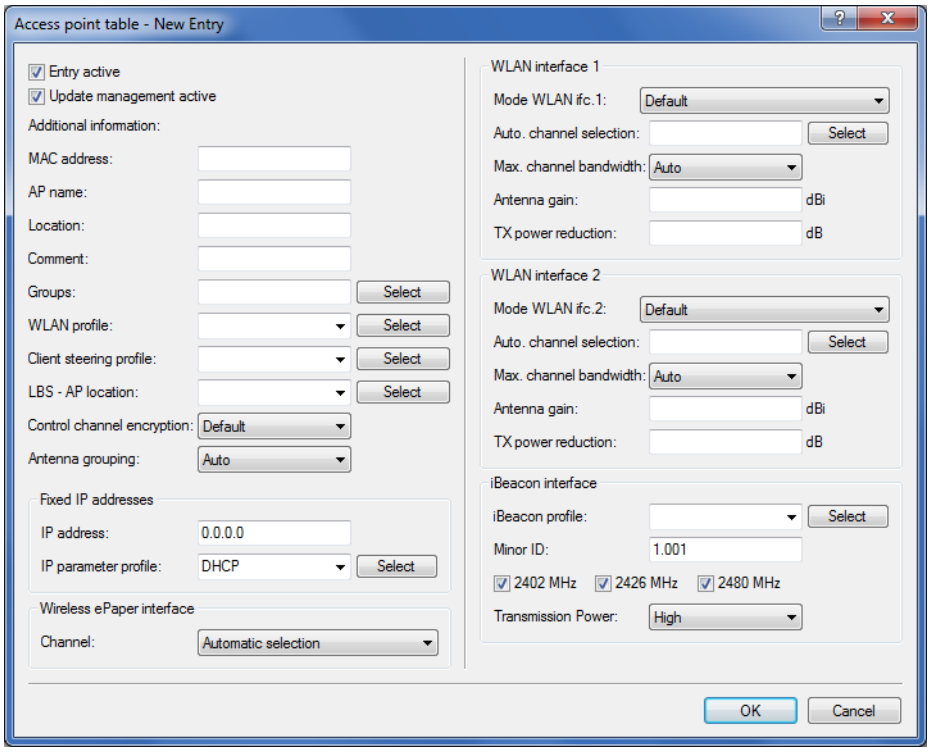
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



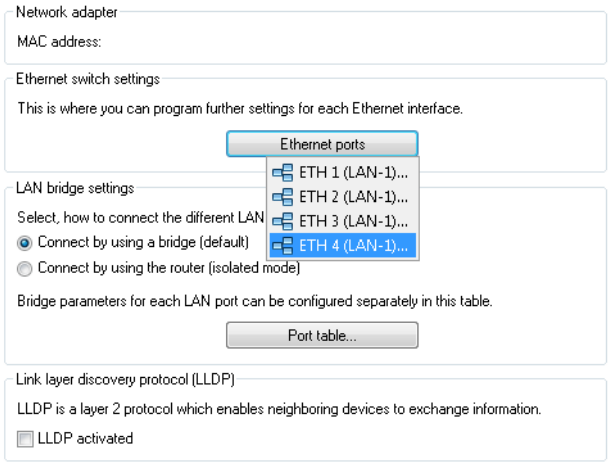
3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.



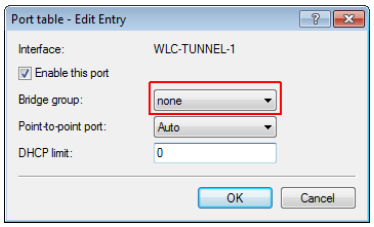
4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.



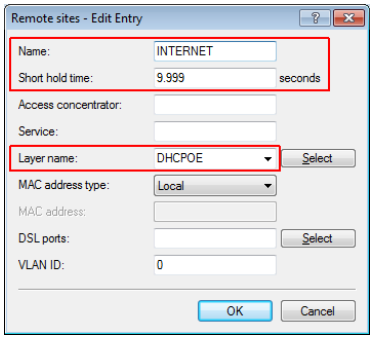
5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical LAN interface 'DSL-1'. The WLC then uses this LAN interface for the guest network Internet access. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.



6. Verify that the logical LAN interface 'WLC-tunnel-1' is not allocated to a bridge group. This ensures that the other LAN interfaces do not transmit any data to the Public Spot. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.

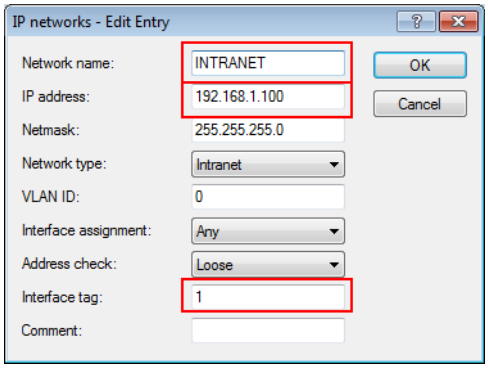


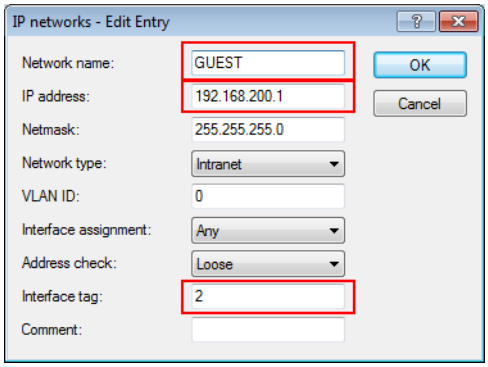
7. For the guest Internet access, create an entry in the list of DSL remote sites with the hold time '9999' and the pre-defined layer 'DHCPOE '. This example assumes that Internet access is provided by a router with DHCP server. In LANconfig you find this setting under **Configuration** > **Communications** > **Remote sites** > **Remote sites**.



8. For internal users, create the IP network 'INTRANET' with (for example) the IP address '192.168.1.100' and the interface tag '1'. For the guest access, create the IP network 'GUEST-ACCESS' with (for example) the IP address of

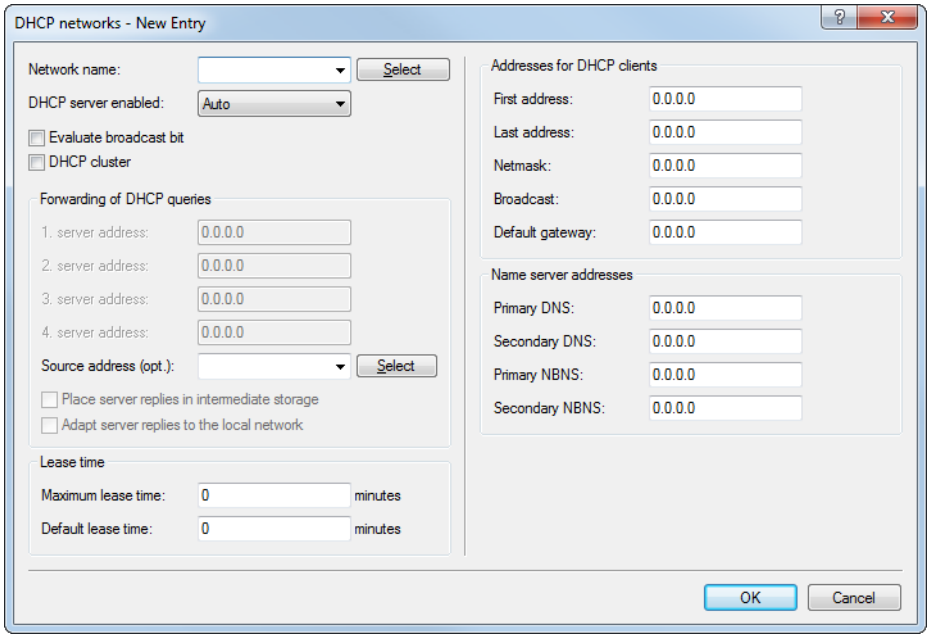
'192.168.200.1' and the interface tag '2'. The virtual router in the WLC uses the interface tags to separate the routes for the two networks. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **General** > **IP networks**.



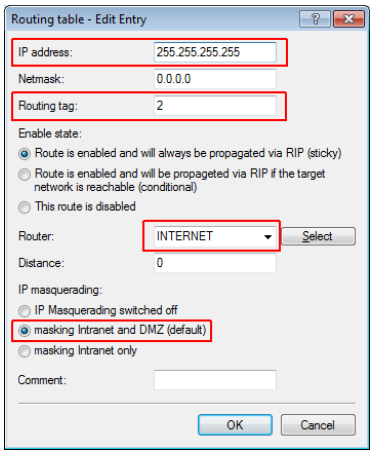


9. The WLC is able to act as a DHCP server for APs and the associated WLAN clients. To set this up, activate the DHCP server for the 'INTRANET' and the 'GUEST-ACCESS'. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **DHCP** > **DHCP networks**.

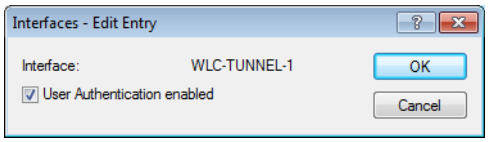
Activation of the DHCP server is obligatory for the guest network and optional for the internal network. There are other ways of realizing a DHCP server for the internal network.



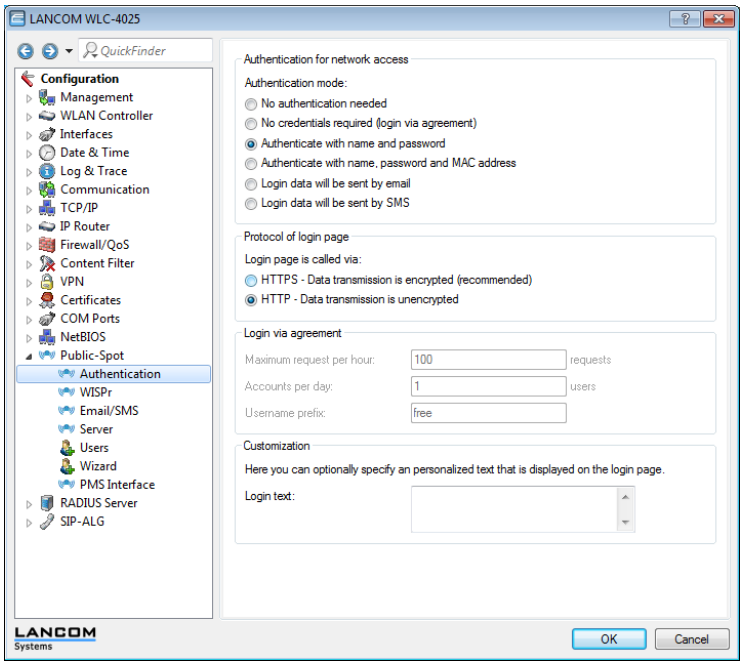
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLC. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under **Configuration** > **IP router** > **Routing** > **Routing table**.



11. Activate the Public Spot user authentication for the logical LAN interface 'WLC-Tunnel-1'. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Server** > **Operational settings** > **Interfaces**.



12. The final step is to enable authentication via the Public Spot for the WLC. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Authentication**.



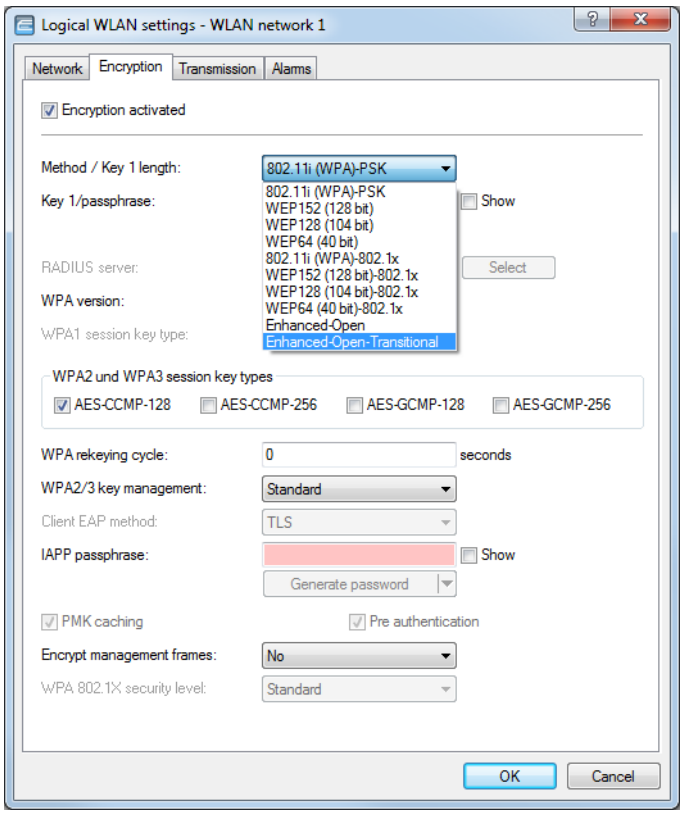
In addition to configuring the WLC, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

15.4.3 Setting up a secure hotspot with Enhanced Open

Enhanced Open for the first time provides a way to offer a secure, yet easy-to-use hotspot.

Enhanced Open has been combined with the LANCOM Public Spot option.

The WLAN to be used for the hotspot is set up in the usual way with the exception that the encryption method is set to **Enhanced Open Transitional**:



Not only is entering a key not required, it is not even possible: A client enabled for Enhanced Open establishes an encrypted connection to the access point without any key having to be entered. To the user, it is just like using an unencrypted, open WLAN: There is no need to enter any previously communicated key as with WPA2-PSK.

The Transitional mode allows an SSID to be used concurrently by clients that support Enhanced Open as well as by clients that do not yet support Enhanced Open. For the latter clients, no encryption is used at all and the SSID works like an open, unencrypted SSID. Once Enhanced Open has become more widespread, you can switch from Transitional mode to regular Enhanced Open mode.

After this, you can proceed as usual with the configuration of the Public Spot module. Since the Public Spot module is independent of the encryption settings of the WLAN interfaces, all of the functions of the Public Spot module can be used without restriction in conjunction with Enhanced Open.

In summary, Enhanced Open is ideal for hotspot operation as it provides a higher level of security than the open hotspots used in the past. The optional Transitional mode ensures that even clients that do not yet support Enhanced Open can be connected in a way that is transparent to the user.

15.4.4 Setting up an external RADIUS server for user administration

Some applications user data is not stored on the device, but on an external, centralized RADIUS server. In this case, the Public Spot must communicate with the external RADIUS server to check the user data.

Please note that specific functions (such as the Public Spot wizards in WEBconfig) are not available to you if you use an external RADIUS server for user administration!

The following instructions assume that you know the IP address of a functional RADIUS server in the network.

The following configuration steps are used to set up a Public Spot that will be used with an external RADIUS server:

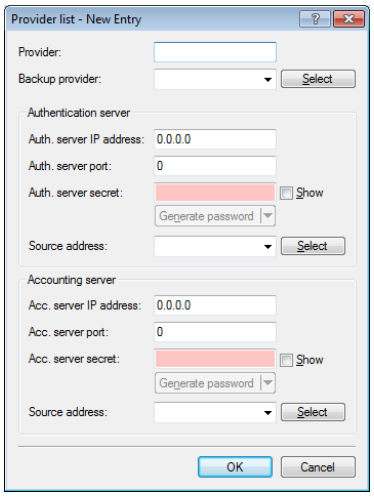
1. Follow the steps in the section *Manual Installation*.

   Among other things, the exact time on the device is necessary for the proper control of time-limited access.

   If authentication with an additional check of the physical address (MAC address) is enabled, the Public Spot transmits the MAC address of the end device to the RADIUS server. In this manner the Public Spot does not see whether the MAC address was actually checked or not. For MAC address checks to work without problem, the RADIUS server must be configured accordingly.

2. Enter the settings for the RADIUS server.

   When configuring a Public Spot, user registration data can be forwarded to one or more RADIUS servers. You configure these servers in LANconfig under **Public Spot** > **Users** > **Users and RADIUS servers** > **RADIUS server**. The registration data that individual RADIUS servers require from the clients is not important to the device that provides the Public Spot, since this data is transparently passed on to the RADIUS server.



   IP addresses specified here must be static. The Public Spot must be able to contact the specified destination addresses. For IP addresses outside of your own network, a router that has contact to the destination network must be specified as a gateway in the DHCP settings for the Public Spot. You have to define this gateway as the default route in the routing table.

   In order for the RADIUS server to record the connection data, the information on the accounting server must be specified in full. As an alternative to using a RADIUS accounting server, the connection information from the Public Spot can also be output by the SYSLOG function.

3. That's it!

   Your Public Spot is now ready for operation. All users with a valid account on the RADIUS server can use the Web interface to login to the Public Spot.

15.4.5 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate users with IEEE801.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. You define how the RADIUS requests are forwarded to the external RADIUS server on the WLAN controller.

The settings described below are only necessary if you are operating an external RADIUS server on your device in addition to the Public Spot in the external RADIUS server.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

15.4.5.1 Realm-tagging for RADIUS forwarding

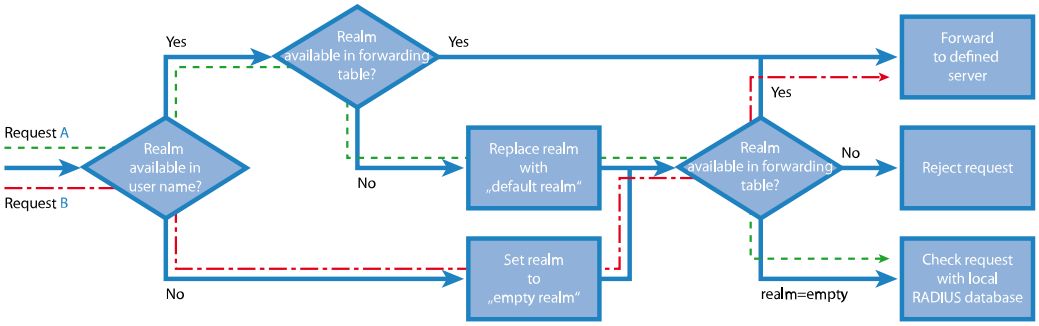
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. The purpose of realms is to address domains within which user accounts are valid. The WLAN controller can transmit the realms with authentication requests to the RADIUS server. Alternatively, the RADIUS server can change the realms in the user names for the purpose of RADIUS forwarding:

- The value defined for "Standard realm" replaces an existing realm of an incoming request if no forwarding is defined for that existing realm.
- The value defined under "Empty realm" is **only** used by the RADIUS server if the incoming user name **still does not** have a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no matching entry exists in the forwarding table, the request is refused.

If the WLAN controller checks the realm and finds that it is empty, it **always** checks the authentication request with the internal RADIUS database.

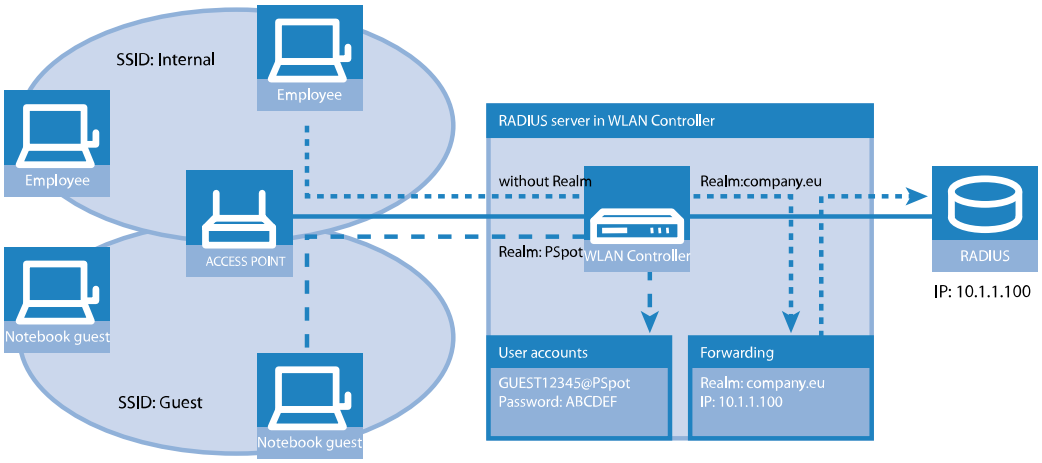
The following flow diagram illustrates the method used by the RADIUS server to process realms:



Using different realm tags allows different RADIUS servers to be targeted with requests. The way in which the device's RADIUS server makes decisions for the two requests is shown in the diagram:

1. Because the user names for guest access accounts are generated automatically, they are suffixed with an appropriate realm, such as "PSpot". Because the forwarding table does not contain this entry and the standard realm is empty, the WLAN controller forwards all authentication requests with this realm to the internal RADIUS server.
2. To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the device can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified

in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.

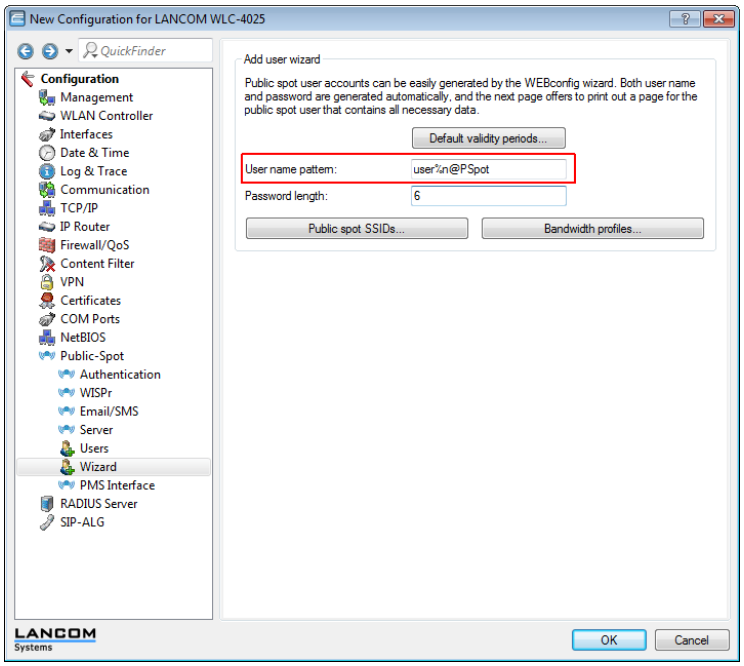


15.4.5.2 Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

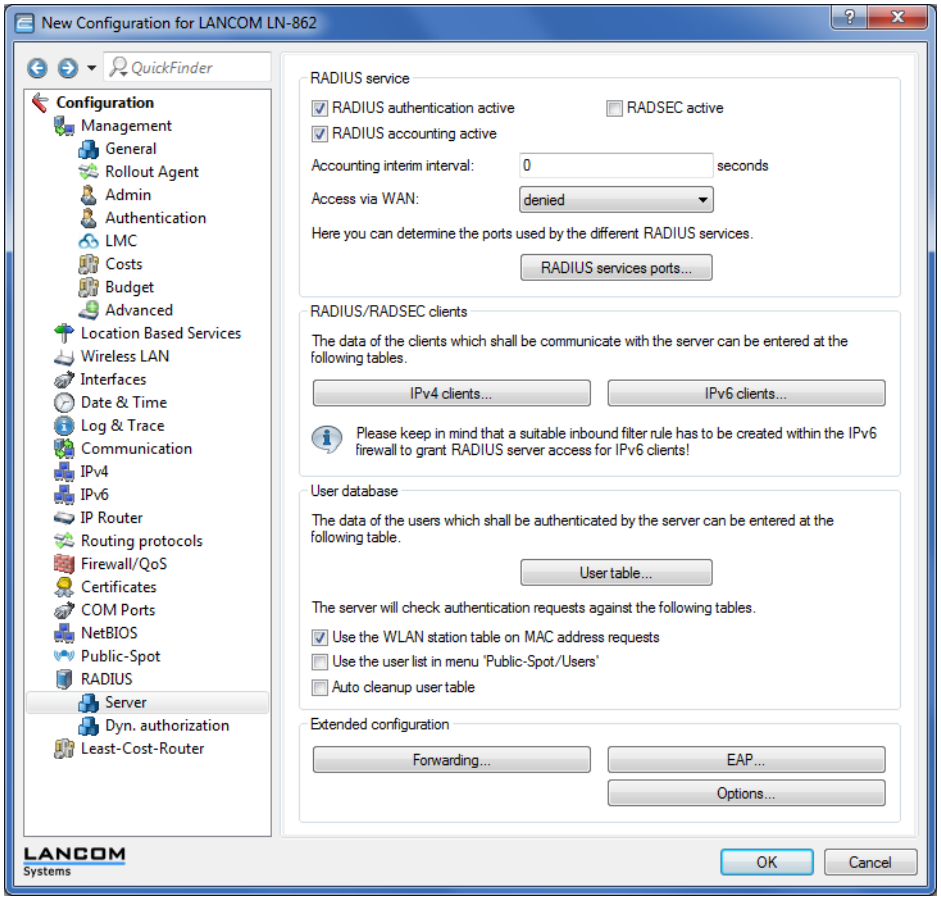
1. In the Public Spot, adapt the pattern of user names such that a unique realm can be suffixed.
   For example, if the pattern is "user%n@PSpot", the Public Spot generates usernames with the format "user12345@PSpot".

   › **LANconfig: Public-Spot** > **Wizard** > **Add user wizard**



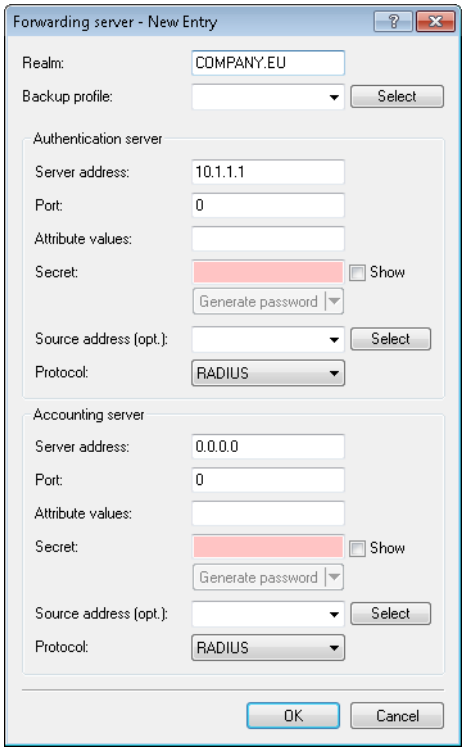
2. In the WLAN controller's RADIUS server, define an "empty realm" (e.g., "COMPANY.EU").
   This realm is attached to all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controller's RADIUS server from attaching a realm, you must leave the "Default realm" field blank.

› **LANconfig: RADIUS > Server > Extended configuration > Forwarding > RADIUS forwarding > Forwarding server**



3. In order for the WLAN controller to forward authentication requests from internal users to the external RADIUS server, suitable entries must be made in the forwarding settings.

All incoming RADIUS requests which have the realm "COMPANY.EU" will be forwarded to the specified IP address.



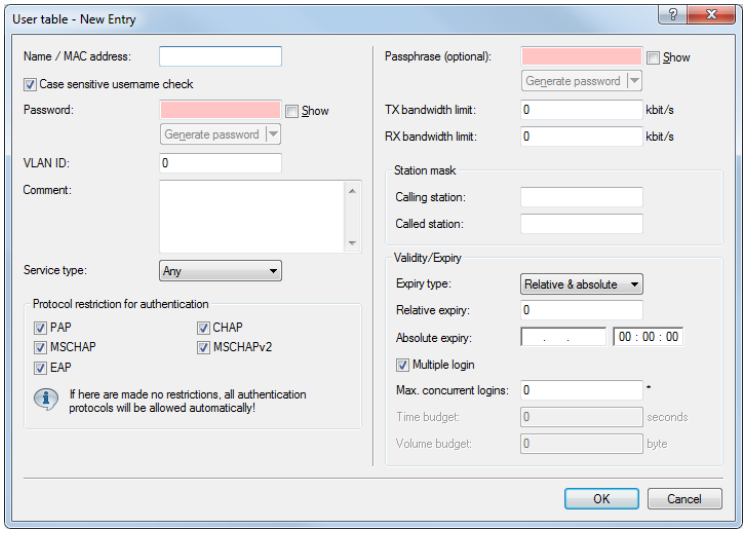
4. Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

15.4.6 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to only authenticate specific WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal RADIUS user database of the WLAN controller.

Enter the MAC addresses in the RADIUS database using LANconfig, and enable all authentication methods. For **Name/MAC address** and **Password** select the corresponding MAC address in the format "AABBCC-DDEEFF".

› LANconfig: **RADIUS** > **server** > **User database** > **User table**



15.4.7 Setting up an external SYSLOG server

Depending on the use case, storage of the usage data is required for the operation of a Public Spot. This data can be stored to a SYSLOG server, for example. Some SYSLOG servers are available as free software.

To save user data from a Public Spot by means of SYSLOG, the external SYSLOG server has to be configured in the respective Public Spot. Once this is done, messages are sent for logging to the SYSLOG server whenever Public Spot user accounts are created or deleted, and at the beginning and end of Public Spot sessions. The message issued at the end of a session—with the source "Login" and the priority "Information"—also includes information on the transferred data volumes and the IP address used.

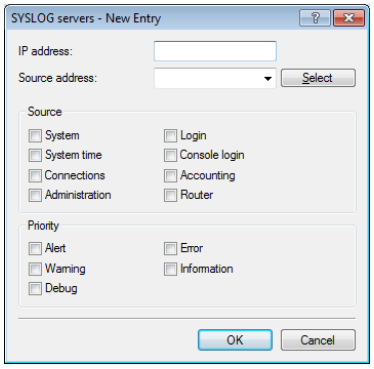
Further information on the configuration of SYSLOG is available in the section *The SYSLOG module*. You can find legal information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

15.4.7.1 Configuring an external SYSLOG server

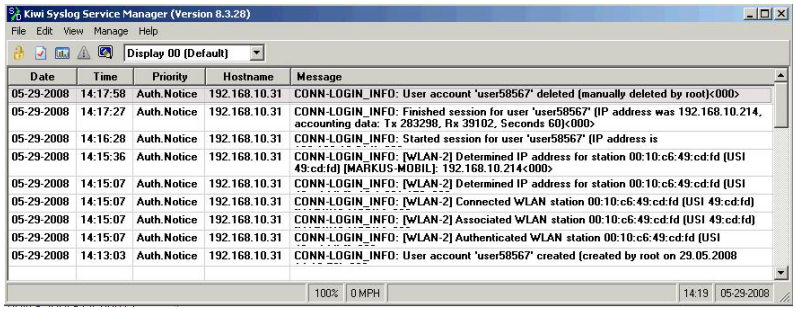
Your device is capable of logging the creation and deletion of Public Spot users, as well as their login and logout activities. You can also transfer this internally stored information to an external SYSLOG server. The following steps show you how you can set up logging with a program installed on an external SYSLOG server (in this example, "Kiwi").

1. Start LANconfig and open the configuration dialog for your device.
2. Change to the dialog **Log & Trace** > **General** and open the table **SYSLOG servers**.

3. Add a new entry. Specify the **IP address** of the computer where the SYSLOG client is installed (e.g., `192.168.10.237`), and enter the **Source** (`Login`, `Accounting`) and the **Priority** (`Information`).



4. Close the dialog and store the configuration on your device.
5. Start the analysis program on your SYSLOG server (e.g., "Kiwi"). As soon as the program has started, it logs the creation and deletion of Public Spot accounts and also the user logins and logouts.



15.5 XML interface

In order to be able to cover a wide range of Public Spot scenarios, the default authentication method of name and password is not sufficient by itself. Access and accounting models based on social media, credit cards and other methods often require additional access data, which the Public Spot in this form would be unable to manage.

The implemented XML interface connects the Public Spot and an external gateway. It directs the user data only to the gateway that handles the authentication and accounting, and it only sends information about the duration and limits of the user access to the Public Spot.

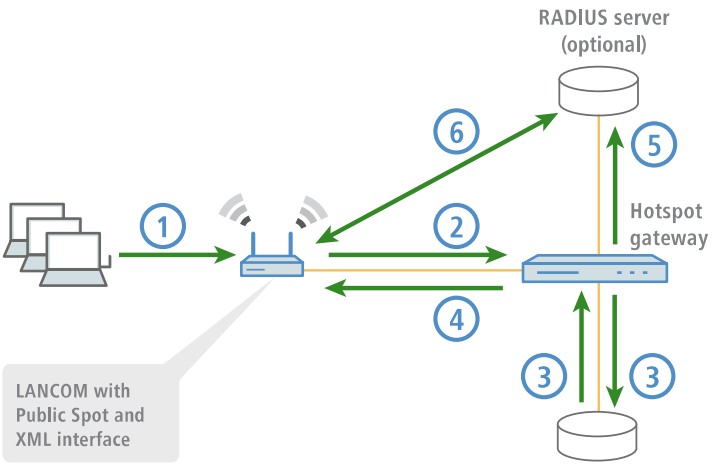
In this case, the Public Spot only performs the following tasks:

- Forward the user requests
- Restrict unauthorized access attempts
- Accept gateway commands to start and stop a session
- Accounting for sessions, if applicable

Since it is not realistic to implement all existing, and at times very specific scenarios with the associated gateway commands on the Public Spot, the XML interface was designed to be flexible and multi-purpose.

15.5.1 Feature

The communication between the XML interface and external gateway is processed as follows:



1. The user connects to the Public Spot's WLAN and sends an HTTP request to the Public Spot.
2. The Public Spot forwards the login procedure's HTTP request to the external hotspot gateway. The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

   The Public Spot forwards the MAC address of the requesting Public Spot client to the external gateway. To implement this, navigate to **Public-Spot-Module** > **Page-Table**, set the **Type** to "Redirect" and suffix the **URL** with the parameter `?myvar=%m`.

   Example: `http://192.168.1.1/?myvar=%m`

   In this case, `myvar` is a freely selectable variable. The variable `%m` is vital here, as the Public Spot replaces this with the client's MAC address when forwarding the request.

Table 39: Variables

Variable	Meaning
%s	SSID name
%v	Source VLAN
%i	Interface (applies to LAN, WLAN, WLC-tunnel)
%t	Routing tag
%m	MAC address of the client
%c	MAC address of the Public Spot gateway
%r	Remote IP (client)
%p	Local IP (Public Spot gateway)
%o	Original URL called by the client
%n	Device name of the Public Spot gateway
%e	Serial number of the Public Spot gateway
%l	Host name of the Public Spot gateway
%0-9	Inserts a single number between 0 and 9
%%	Inserts a single percent character

3. The hotspot gateway checks the user's credentials and, if applicable, it can contact further systems to charging to credit card, for example.
4. The hotspot gateway sends an XML file with the user data to the Public Spot's XML interface. The external hotspot gateway contacts the device with the Public Spot XML interface using the URL `http://<Device-URL>/xmlauth`.

   The Public Spot's XML interface analyses this file and initiates the corresponding actions. In the case of a login request, the XML interface inserts the user and the corresponding MAC address into the list of logged-in Public Spot users. In the case of a logout request, the XML interface removes the user from this list again. At the same time, the XML interface confirms the request by sending a corresponding XML file to the hotspot gateway.

   In order for the Public Spot to be able to process the instructions in the XML file, a special administrator must be set up on the device who has the function right "Public-Spot -XML-interface". This hotspot gateway logs in to the Public Spot with this admin account.

   While the user is logged in to the Public Spot, the XML interface and hotspot gateway can exchange status information about the current session in the form of XML files.

   If the user has exhausted his online quota, the hotspot gateway will send a stop command to the XML interface, and then the Public Spot locks further access for that user. The XML interface also confirms that the login is blocked by sending the corresponding XML file to the hotspot gateway.
5. If the additional use of a RADIUS server is enabled, the hotspot gateway authenticates a user at a RADIUS server.
6. The Public Spot sends relevant data to the RADIUS server throughout the session, for example to facilitate the accounting of the Public Spot usage. By default, the Public Spot uses its internal RADIUS server for this. If necessary, you can configure the device running the Public Spot to use an external RADIUS server.

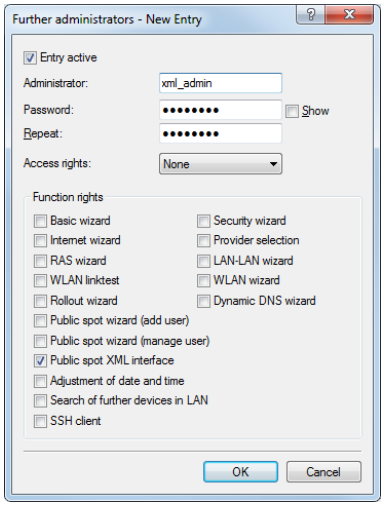
Communications between the Public Spot and a hotspot gateway with the use of XML is not standardized. Configure the hotspot gateway according to the instructions in the *Commands* section in order for the Public Spot and hotspot gateway exchange the XML messages in the required form. XML messages are exchanged invisibly without a graphical user interface. You can use tools such as *cURL* to test the exchange of messages.

15.5.2 Setting up the XML interface

The following section describes how to set up the XML interface.

1. Using **Management** > **Admin** > **Further administrators** you create a new administrator with the function right **Public Spot XML interface**.

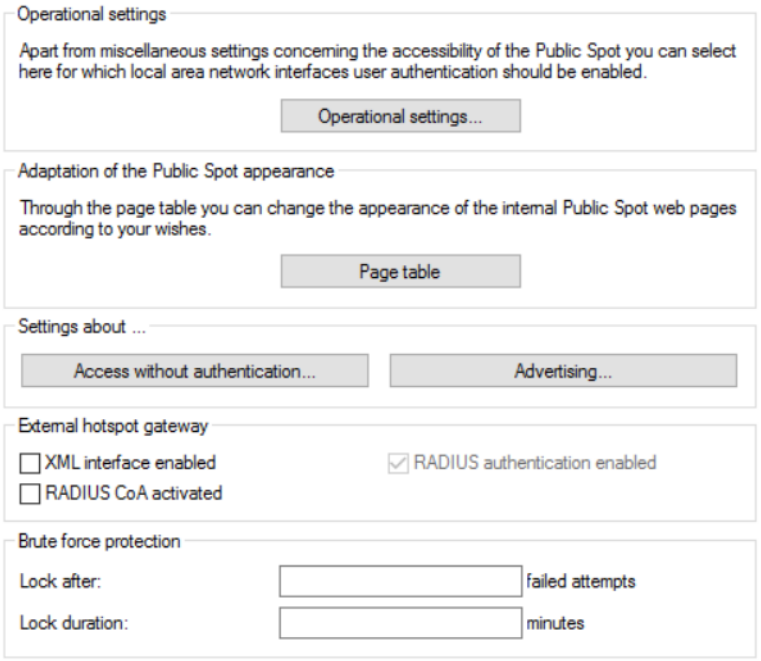
   This is the administrator account that the (external) gateway uses to send its XML requests to the Public Spot XML interface.



The new administrator should not have any further Public Spot function rights, since they represent a potential security risk in combination with the XML interface (e.g., if the communication between XML sender and device is unencrypted).

2. You enable the XML interface in **Public Spot** > **Server** in the section **External hotspot gateway** and RADIUS authentication.

   Incoming XML requests are forwarded by the Public Spot either to the internal RADIUS server or, if an external RADIUS server is used via a realm, to the external RADIUS server



3. In the section **Allow access without authentication** click on the button **Free Networks** and add a new network. Enter the **Name/IP address** of the login page. In **Netmask** enter `255.255.255.255`.

   When defined as a free network, the user has direct access to the login page of the gateway without having to login to the Public Spot first.

4. Configure the gateway so that it sends the user's session data to the Public Spot XML interface as an XML file. For questions about configuring the gateway, please refer to the applicable service provider.

15.5.3 Analyzing the XML interface using cURL

The following section describes the analysis of the XML interface with the open-source software cURL.

Client for URL, or cURL, is a command line application use for transferring files on a network without the use of a Web browser or FTP client. "cURL" is a component of many Linux distributions and is also available for other operating systems.

To analyze the XML interface using cURL, you need an administrator account with the function right "Public Spot XML interface" for the Public Spot.

1. First download cURL and install or unpack it.
2. Start cURL with the console command `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`.

   The parameters have the following meaning:

filename

Path and name of the local XML file, e.g. the login request from the *examples*.

user

Username with the function right titled "Public Spot XML interface". The XML feature does not work without this authentication.

pass

User password.

myhost

IP address or DNS name of the device with the Public Spot XML interface

3. With Telnet you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

15.5.4 Commands

The XML interface can process three types of requests and responses:

- Login
- Logout
- Status

An XML file can contain several requests or answers.

15.5.4.1 Login

If the external gateway sends a "Login" request in an XML file, the Public Spot activates online access for the corresponding user. A "Login" request contains the attribute `COMMAND="RADIUS_LOGIN"`.

If the Public Spot does not use a RADIUS server, a "login" request prompts it to store the user and the associated MAC address directly in the internal Status table. As a result, the user is immediately authenticated in future, and there is no need to display a login page for entering the username and password.

When you operate a RADIUS server, a 'login' request can only be successfully processed if the login data of the corresponding user already exists on the RADIUS server.

The Web API in the Public Spot provides you with a convenient tool for creating new Public Spot users on the device's internal RADIUS server.

The XML interface can process the following XML elements in the **login request**:

`SUB_USER_NAME`

User name

`SUB_PASSWORD`

User password

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

VLAN_ID (optional)

Custom VLAN ID assigned by the device to the Public Spot user upon login. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the XML interface.

The value `0` disables use of a VLAN.

SOURCE_VLAN (optional, only in conjunction with authentication by RADIUS server)

The VLAN ID of the network from which a Public Spot user attempts to login (source VLAN). The Public Spot forwards the source VLAN in its access request to the internal or external RADIUS server. The Public Spot uses the RADIUS attribute 81 (**tunnel-private-group-ID**) together with the RADIUS attributes 64 (**tunnel-type**) and 65 (**tunnel-medium-type**). The RADIUS server uses the source VLAN to decide whether to accept or decline the access request from the Public Spot.

If the RADIUS server accepts the request, it returns the access-accept to the Public Spot along with the above-mentioned RADIUS attributes. The Public Spot then saves the source VLAN for the client and its station list and allows the user to access the Public Spot network.



Use the source VLAN in conjunction with the setup parameter *2.24.47*. This prevents Public Spot users in VLAN-separated Public Spot networks/SSIDs from authenticating once at the RADIUS server and then accessing all of the managed Public Spot networks/SSIDs.



The `SOURCE_VLAN` should not be confused with the `VLAN_ID`. The `VLAN_ID` is not sent to the RADIUS server. However, the Public Spot uses it to assign a VLAN ID provided by the gateway to a successfully authenticated user.

PROVIDER (occasionally required)

Name of the RADIUS server used by the Public Spot for user authentication and accounting. If you do not specify a RADIUS server, the Public Spot uses the server configured globally for the module.

This XML element is mandatory if you

- have configured multiple RADIUS servers for the Public Spot module.
- want to use the XML interface without RADIUS authentication but with RADIUS accounting.

Specifying this XML element is otherwise optional.



The referenced RADIUS server must be present in the configuration.

TXRATELIMIT (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the uplink.

RXRATELIMIT (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the downlink.

SECONDSEXPIRE (optional)

The maximum online time for a user account in seconds. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

The value `0` switches off the monitoring of the time budget.

TRAFFICEXPIRE (optional)

The maximum data volume for a user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

The following entries are allowed:

- `k` or `K`: Specified in kilobytes (kB), e.g. `<TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>`.
- `m` or `M`: Specified in megabytes (MB), e.g. `<TRAFFICEXPIRE>100m</TRAFFICEXPIRE>`.
- `g` or `G`: Specified in gigabytes (GB), e.g. `<TRAFFICEXPIRE>1g</TRAFFICEXPIRE>`.

Without a unit, the specification corresponds to a value in bytes (B).

The value `0` switches off the monitoring of the data volume.

The XML interface then sends the gateway a "Login" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_STATUS

The current user status. The following values are possible:

- `RADIUS_LOGIN_ACCEPT`: Login successful
- `RADIUS_LOGIN_REJECT`: Login rejected

SUB_MAC_ADDR

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

PROVIDER

Name of the RADIUS server to be used for this user.

Some examples of XML files are given below:

Login request

The external gateway sends the data for the start of a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <PROVIDER>DEFAULT</PROVIDER>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

The Public Spot enables 'user2350' in the internal Status table.

Login response:

The XML interface sends a confirmation about the start of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
```

```
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.5.4.2 CoA

If a Public Spot user has to authenticate only and no further changes are required throughout the login, then the parameter `RADIUS_LOGIN` will meet your needs. On the other hand, if you need to change the attributes of an ongoing session for a Public Spot user, you have the option of using `RADIUS_CoA`. To implement a change, your external hotspot gateway sends a `RADIUS-CoA-Request` to the Public Spot, which directly transfers the changes in it to the **Station table** under **Status** > **Public-Spot**.

One application for CoA messages is the automatic throttling of bandwidth: If a Public Spot user has consumed his/her volume budget, an external hotspot gateway is able to throttle the user's bandwidth by evaluating the accounting data and sending a CoA message to the Public Spot.

The XML messages for negotiations between the hotspot gateway and the Public Spot appear as follows:

RADIUS-CoA-Request

The external gateway sends the data with the session change to the Public Spot. The Public Spot then changes the session data in the station table for the authenticated user 'user2350'.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In the example above, the user is assigned a session duration of 3,600 seconds, a transferable data volume of 10,000,000 bytes, and a transmit and receive bandwidth of 100 kbps.

RADIUS-CoA-Response:

The XML interface sens a confirmation to the external hotspot gateway that the session data was changed:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In case of throttling, the change to the user session always affects the quota that is still available to the user. For instance, if the user was logged on for one hour already, then a change of the time quota to six hours means that just five hours remain. If the time quota is less than the time the user is already logged on, the Public Spot logs out the user and sends a logout message to the hotspot gateway.

15.5.4.3 Logout

If the external gateway sends a "Logout" request in an XML file, the Public Spot blocks the corresponding user's online access. A "Logout" request contains the attribute `COMMAND="RADIUS_LOGOUT"`.

The XML interface can process the following XML elements for a request:

`SUB_USER_NAME`

User name

If the device receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then the Public Spot logs out this user.

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`TERMINATION_CAUSE`

Reason for the user to log off

The XML interface then sends the gateway a "Logout" response, which can contain the following XML elements:

`SUB_USER_NAME`

User name

`SUB_STATUS`

The current user status. The following values are possible:

- `RADIUS_LOGOUT_DONE`: Logout successful
- `RADIUS_LOGOUT_REJECT`: Logout rejected

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`TERMINATION_CAUSE`

Reason for blocking access

Some examples of XML files are given below:

Logout request

The external gateway sends the command for ending a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
```

```
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout response:

The XML interface sends a confirmation about the end of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.5.4.4 Status

The external gateway queries the current status of a user from the Public Spot with a "Status" request. A "Status" request contains the attribute `COMMAND="RADIUS_Status"`.

The XML interface can process the following XML elements for a request:

`SUB_USER_NAME`

User name

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Status" response, which can contain the following XML elements:

`SUB_USER_NAME`

User name

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`SUB_STATUS`

The current user status. The following values are possible:

- `RADIUS_STATUS_DONE`: Status request successful
- `RADIUS_STATUS_REJECT`: Status request rejected, e.g. unknown user or MAC address

`SESSION_TXBYTES`

Current sent data volume

SESSION_RXBYTES

Current received data volume

SESSION_TXPACKETS

Number of data packets sent so far

SESSION_RXPACKETS

Number of data packets received so far

SESSION_STATE

Current status of the session

SESSION_ACTUAL_TIME

Current time

Some examples of XML files are given below:

Status request

The external gateway sends the command for a status request to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status response:

The XML interface sends a status message to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <SESSION_ID>2</SESSION_ID>
     <SESSION_TXBYTES>0</SESSION_TXBYTES>
     <SESSION_RXBYTES>0</SESSION_RXBYTES>
     <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
     <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
     <SESSION_STATE>Authenticated</SESSION_STATE>
     <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

15.6 Appendix

15.6.1 Commonly transmitted RADIUS attributes

The RADIUS client module was implemented on the basis of RFCs no. 2865 and no. 2866.

These specifications define various attributes, some of which are an absolute necessity and some of which are optional. The following overview shows which attributes are transmitted/processed in messages between RADIUS servers and base stations.

15.6.1.1 Messages to and from the authentication server

Transferred attributes

As previously mentioned, your device transmits far more than just the username and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with standard attributes. These additional attributes are manufacturer-specific with the manufacturer code 2356 (LANCOM Systems GmbH).

Table 40: Overview of the RADIUS attributes transmitted by the device to the authentication server

ID :	Name	Meaning	Possible values in LCOS
1	User name	The name entered by the user.	
2	User-Password	The password entered by the user.	
4	NAS-IP-Address	IP address of your device	<IPv4 address of the device>
6	Service-Type	Type of service that the user requested. The value "1" stands for Login.	
8	Framed-IP-Address	Specifies the IP address that is assigned to the client.	<IP address of the client>
30	Called-Station-Id	MAC address of your device	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC address of the client The address is given byte-wise in hexadecimal notation with separators.	<nn:nn:nn:nn:nn:nn>
32	NAS identifier	Name of your device, if configured.	<Device-Name>
61	NAS-Port-Type	Type of physical port over which a user had requested authentication.	› **ID 19** denotes clients from WLAN. › **ID 15** denotes clients from Ethernet.
87	NAS-Port-Id	Description of the interface over which the client is connected to your device. This may be a physical and a logical interface. Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.	For example › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27

Processed attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

Table 41: Overview of the supported RADIUS attributes

ID :	Name	Meaning	Possible values in LCOS
18	Reply-Message	An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the `SEVERMSG` element.	

ID :	Name	Meaning	Possible values in LCOS
25	Class	An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.	
26	Vendor 2356, Id 5 LCS-Account-End	Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Specifies a comma-separated list of advertisement URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.	
27	Session-Timeout	Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.	
28	Idle timeout	Defines a time period in seconds after which the device will terminate the session if no packets were received from the client. This value may possibly overwrite the idle timeout that is defined locally under **Public Spot** > **Server** > **Idle timeout**.	
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	

ID :	Name	Meaning	Possible values in LCOS
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	
85	Acct-Interim-Interval	Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an **Accounting update cycle** for the Public Spot module.	

Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session's time limit.

15.6.1.2 Messages to/from the accounting server

Transferred attributes

The set of RADIUS attributes transmitted to a RADIUS server in an accounting request is similar to the set of attributes transmitted in an authentication request. However, additional attributes specific to accounting will be added. The following attributes are present in all RADIUS accounting requests:

Overview of the RADIUS attributes transmitted by the device to the accounting server

1

User name

Name of the account that was used for authentication.

4

NAS-IP-Address

IP address of your device

8

Framed-IP-Address

IP address that was assigned to the client

25

Class

All class attributes that the RADIUS authentication server sent in its authentication response.

30

Called-Station-Id

MAC address of your device

31

Calling-Station-Id

MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).

32

NAS identifier

Name of your device, if configured.

40

Acct-Status-Type

Request type which signals the start or stop of accounting, or an interim update. Please refer to the section *Request types* for further information.

44

Acct-Session-Id

A series of characters that uniquely identify the client. It consists of the MAC address of the network adapter, the login timestamp (measured in seconds since January 1, 1970 0:00:00), and the session counter that your device manages locally.

61

NAS-Port-Type

Type of physical port over which a user had requested authentication.

- **ID 19** denotes clients from WLAN
- **ID 15** denotes clients from Ethernet

87

NAS-Port-Id

Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

In the case of an accounting stop request or an interim update, the request contains the following additional attribute:

42

Acct-Input-Octets

The sum of all data bytes received from the client in this session, modulo 2^{32}.

43

Acct-Output-Octets

The sum of all data bytes sent to the client in this session, modulo 2^{32}.

46

Acct-Session-Time

The total duration of the client's session in seconds.

If the session was ended due to an idle timeout, this value is reduced by the idle time.

47

Acct-Input-Packets

The number of data packets that your device received from the client during the session.

48

Acct-Output-Packets

The number of data packets that your device sent to the client during the session.

49

Acct-Terminate-Cause

The reason for termination or the end of the accounting session. This is sent if **Acct-Status-Type** has the value `Start` or `Stop`.

52

Acct-Input-Gigawords

The upper 32 bits of the sum of all data bytes received from the client during this session.

53

Acct-Output-Gigawords

The upper 32 bits of the sum of all data bytes sent to the client during this session.

55

Event-Timestamp

The elapsed time since this accounting request was submitted by the device, measured in seconds since January 1, 1970 0:00:00. This attribute is only present if your device's real time clock contains a valid value.

Note that the RADIUS accounting only starts accounting after a client successfully logs in, i.e. the time needed for authentication is not recorded. Using *Traffic-Limit-Option* you can limit the data traffic during the authentication phase. The final accounting stop request also contains the termination cause attribute (49). An overview of these attributes can be found in the LANCOM "Public Spot: Implementation Guide", available from *www.lancom-systems.com*.

Processed attributes

Your device currently does not process any attributes in responses sent by a RADIUS accounting server.

15.6.2 RADIUS attributes transmitted via WISPr

If you enable WISPr and you use an external RADIUS server, the Public Spot transmits the attributes (access request):

- **Location ID**
- **Location name**
- **Logoff URL**

These attributes are subset of the values configured in the previous section. The provider or roaming broker can use them to identify the location of the client for accounting purposes. Vendor Specific Attributes (VSA) are used with the IANA Private Enterprise Number (PEN) 14122.

The Public Spot processes the attributes (access accept) from an external RADIUS server:

- **Redirection URL**: URL to which a client should be redirected after login. This function is not supported by all smart clients.
- **Bandwidth max up**: Maximum uplink bandwidth available to the client.
- **Bandwidth max down**: Maximum downlink bandwidth available to the client.
- **Session terminate time**: Time when the client should be automatically de-authenticated. According to ISO 8601, the format is `YYYY-MM-DDThh:mm:ssTZD`. If "TZD" is not entered, the client is de-authenticated according to the local time on the Public Spot.
- **Session terminate end of day**: The value of this attribute can be either 0 or 1. It indicates whether the client is de-authenticated on the Public Spot at the end of the accounting day.

For accounting purposes, the Public Spot uses the following attributes:

- **Location ID**
- **Location name**

16 Voice over IP – VoIP

16.1 Introduction

Voice over IP (VoIP) stands for voice communication in computer networks based on the Internet protocol (IP). The core idea is to provide the functions of traditional telephony via cost-effective and wide-spread networking structures such as the Internet. VoIP itself is not a standard, rather it is a collective term for the various technologies (equipment, protocols, voice encoding, etc.) which make voice communications in IP networks possible.

A variety of terminology is used to describe telephony over a network (LAN or Internet). The terms "Voice over IP" or "IP telephony" are used as synonyms, although in actual fact they have different meanings.

- Strictly speaking, "Voice over IP" is merely a term for the technology of transmitting calls across data networks in real-time using the IP protocol (Internet protocol). The term is also used when the technology is implemented only in the provider's core networks, in what is known as the backbone
- The term "IP telephony" is used when the VoIP technology is also used in the terminal equipment, so that the call subscriber uses the IP network for telephony.
- "Internet telephony" is also used to describe telephony using VoIP over the Internet in general.

In the following, "Voice over IP" is usually used even to refer to IP telephony in accordance with general custom.

There are four basic types of terminal equipment that can be used for VoIP telephony:

- With software running on the PC, known as a "softphone".
- With an IP or VoIP telephone that is connected directly to the local network.
- With a conventional telephone that is connected to the local network by an adapter (analog telephone adapter, ATA).
- Via a VoIP gateway that converts telephone calls from telephones (analog and ISDN) to VoIP and can then communicate between the two "telephone worlds" like a PBX.

There is a basic difference between a VoIP connection being established between two pieces of terminal equipment that are connected directly to the data network (PC or IP telephone) and the situation where a subscriber in the land-line or mobile telephone network requires the translation of the signaling, numbers and voice data. To differentiate the various connection variants, a device in the LAN has become known as a "PC", and a device in the land-line network has become known as a "phone".

PC-to-PC communication

With this application, the terminal equipment has to be integrated directly into the user's LAN. Examples are a PC, an IP telephone or a telephone that is connected to the LAN using an ATA.

Different software solutions are available for the PC, known as "softphones". Note that some of these programs can only communicate with users of the same software and not with softphones from other manufacturers. Communication is usually free of charge within the Internet. A current example is Skype, which uses its own protocol.

PC-to-phone and phone-to-PC communication

In this case, the call data has to be transmitted from the Internet to the landline network, usually using what are known as VoIP gateways. In general, these gateways are provided by providers and are subject to a fee.

So that the subscriber can even be called on a PC, he or she needs a VoIP telephone number that is usually provided by a provider.

VoIP providers usually only provide individual numbers and not complete number ranges with a switchboard number and extension numbers. This is why the numbers that are provided by public providers are not attractive to many business customers. When the LANCOM VoIP router is used with a SIP gateway, previously-used numbers can be maintained; the functions of VoIP telephony can also be used.

16.2 VoIP implementation in LANCOM VoIP routers

The main task of the VoIP implementation in the LANCOM VoIP router is to connect telephone calls from different local interfaces (LAN, WLAN, ISDN) to the WAN connections that can be accessed by the router. This enables switching between the local interfaces (local call) and also the WAN interfaces.

The basis for the implementation and switching is the SIP protocol. The calls over all interfaces are converted into SIP by the interface translator (this mainly concerns the ISDN interfaces).

Furthermore, the bit-transparent connection is usually used for calls between multiple local ISDN interfaces to achieve the highest possible compatibility and quality.

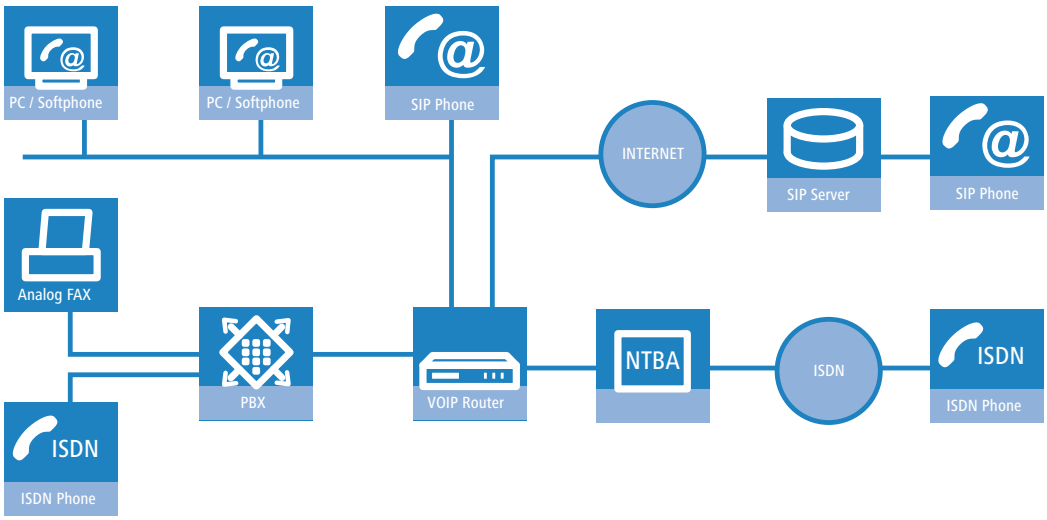
16.2.1 Example applications

Voice over IP solutions offer advantages for a broad spectrum of applications, starting with small companies and extending to large corporations with extensive networks of subsidiaries. In the following section, we will demonstrate a number of examples.

Detailed information about the configuration is available in the chapter 'Configuration of VoIP functions'.

16.2.1.1 Supplementing existing ISDN PBXs

VoIP functions can be conveniently added in to existing telephone structures by using a LANCOM VoIP router. The LANCOM VoIP router is simply connected between the public ISDN connection (e.g. ISDN NTBA) and the ISDN PBX.



Telephone calls over the PBX and its ISDN telephones remain possible just as before; the telephones remain available under the familiar telephone numbers. This application additionally offers the following options:

› In addition to the ISDN telephones, VoIP telephones or VoIP softphones can be included in the telephone infrastructure. VoIP subscribers in the internal LAN are also able to call external ISDN subscribers.

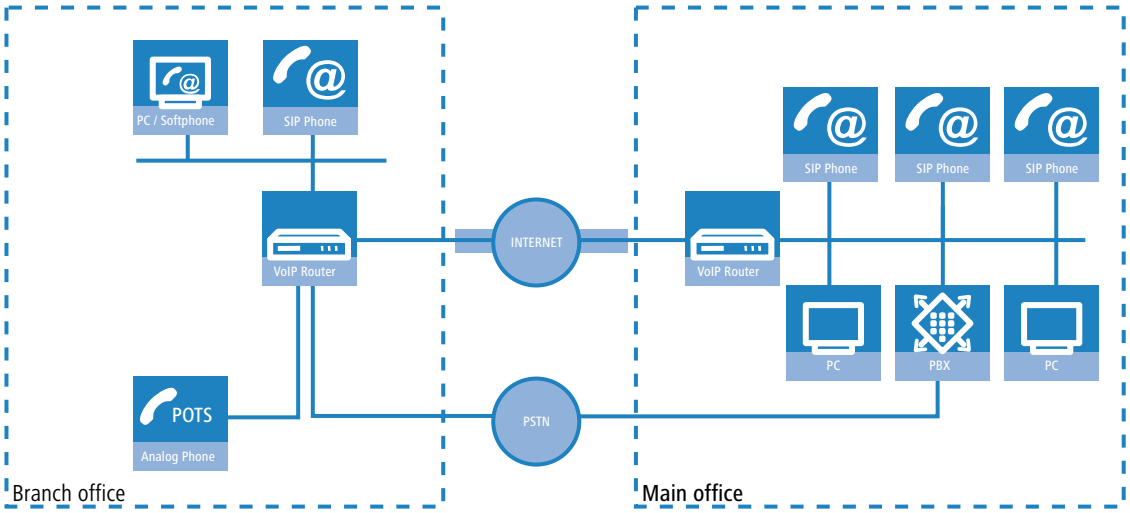
- The ISDN telephones continue to function, and additionally they can call all of the internal VoIP telephones and softphones in the LAN.
- Calls to external SIP subscribers who use the same Internet provider are often available at no cost.
- With the appropriate connection to a public SIP provider, any other SIP subscriber worldwide can be called, irrespective of the provider network. As an alternative to a direct ISDN connection, ISDN network subscribers can also be reached over a diversion via the SIP provider. The costs depend on the provider's particular tariff models. Often, long-distance and overseas calls via a SIP provider are significantly cheaper than the traditional telephone connection.

In this constellation, the LANCOM VoIP router takes over the switching of the calls. The device can be individually configured, for example, to use the access codes to decide upon the switching of a call either via the ISDN interface, or via the Internet as a VoIP call.

16.2.1.2 Connecting subsidiaries or home offices to the headquarters

Many subsidiaries or home offices already have a connection to the network at headquarters over VPN. These connections are normally limited to conventional data transmission. By using VoIP, internal company calls can be made for free over the existing VPN connection and—thanks to the VPN encryption—these calls are secured against eavesdropping.

With a LANCOM VoIP router located in the branch or home office, the two worlds of POTS and VoIP telephony can be united in a single telephone: A VoIP telephone or an existing ISDN telephone can be used for free telephone calls via VPN to the headquarters, or to make standard calls via ISDN.



The advantages of a telephone connection to headquarters:

- The configuration of telephone functions can be carried out centrally in the VoIP PBX at headquarters.
- Subscribers at their branch or home offices connect with the central PBX.
- Calls within the company network are free.
- Outgoing calls are automatically directed to the best line for cost optimization.

16.2.1.3 VoIP for companies through SIP trunking

One of the biggest hurdles for companies that fully migrate to VoIP is to maintain the existing telephone numbers. Normal provider SIP accounts come with a telephone number for the transition to the landline telephone network, but generally these numbers are selected from a pool of numbers available to the provider. However, for companies with a large number of telephone subscribers and numbers, it is of decisive importance that existing telephone and extension numbers are maintained after migrating to VoIP.

With the SIP trunking function, entire ranges of telephone numbers made up of external numbers and their associated extensions can be mapped by LANCOM VoIP routers over a single connection to a SIP provider, assuming that the provider

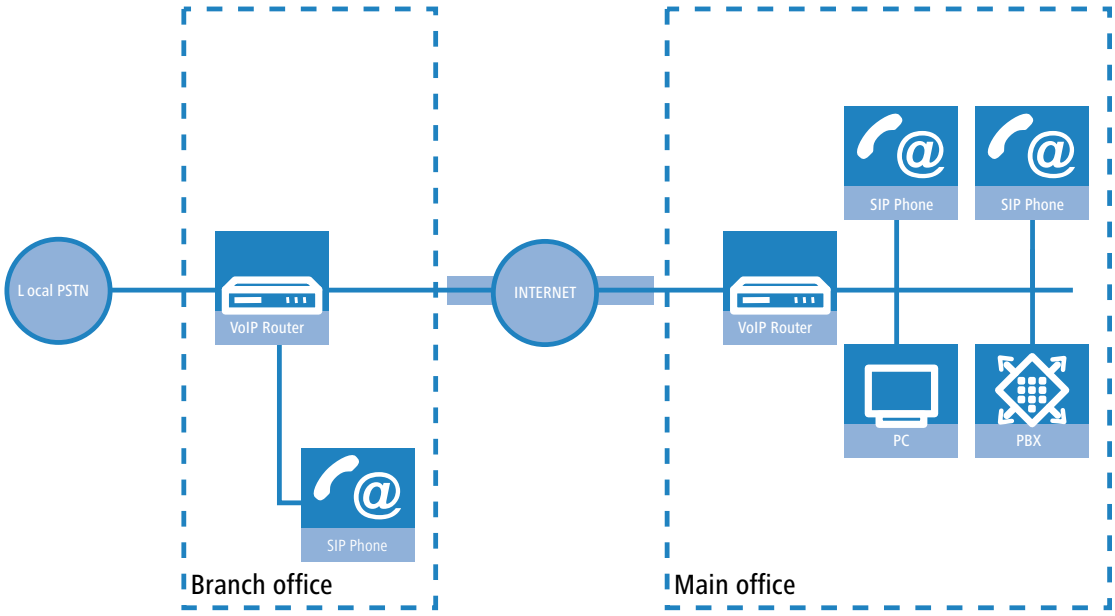
also supports Direct Dialing In (DDI) and can provide multiple connections simultaneously. Generally speaking, SIP providers that offer SIP trunking can acquire the existing telephone numbers from the former telecoms provider.

16.2.1.4 Integrating local ISDN connections with remote SIP gateway

Companies with nation-wide and internationally distributed sites are often interconnected with VPN already. A LANCOM VoIP router can be used not only to connect the SIP and ISDN telephones at a branch office to the SIP-PBX at headquarters; it can also integrate local ISDN networks into corporate communications with help of the "SIP Gateway" function.

The SIP gateway is active for outgoing and incoming calls.

- A company headquarters in New York can, for example, use a LANCOM VoIP router with SIP gateway located at the Los Angeles branch office to telephone with customers and suppliers located in Los Angeles at local rates ("local break-out").
- For improved availability to customers located abroad, the New York headquarters can, for example, use a LANCOM VoIP router with SIP gateway located at their sales office in Italy. Customers can then reach support or service numbers via a standard national telephone number. Calls from the local ISDN network are received and directed within the company network to the appropriate employee. Call routing can be used which identifies the customer's calling number and automatically selects the appropriate connection to be used for forwarding the call.

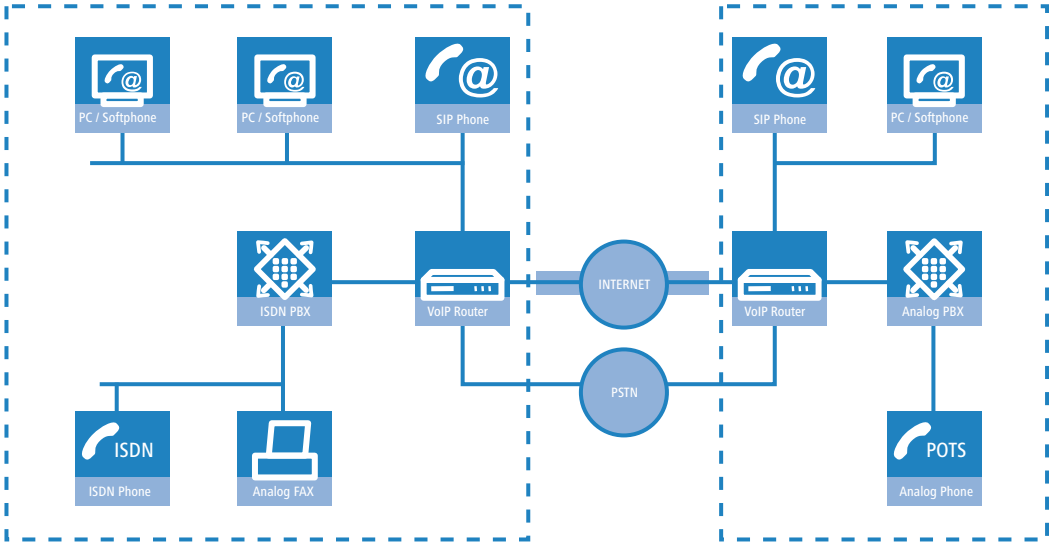


Advantages of the SIP gateway:

- The local ISDN connection at any site is available for use by any of the offices throughout the entire company.
- National and international long-distance calls can be mapped to local or regional calls, so saving costs.
- Automatic routing of incoming calls to the appropriate employee.

16.2.1.5 Connecting sites without a SIP PBX

Companies with widely dispersed offices and without their own SIP PBX can also take advantage of VoIP site-to-site connectivity. In this "Peer-to-Peer" scenario, a LANCOM VoIP router has been implemented at two locations.



Along with data transfer via VPN, it is also possible to use VoIP functions between the two locations.

The advantages of peer-to-peer site connectivity

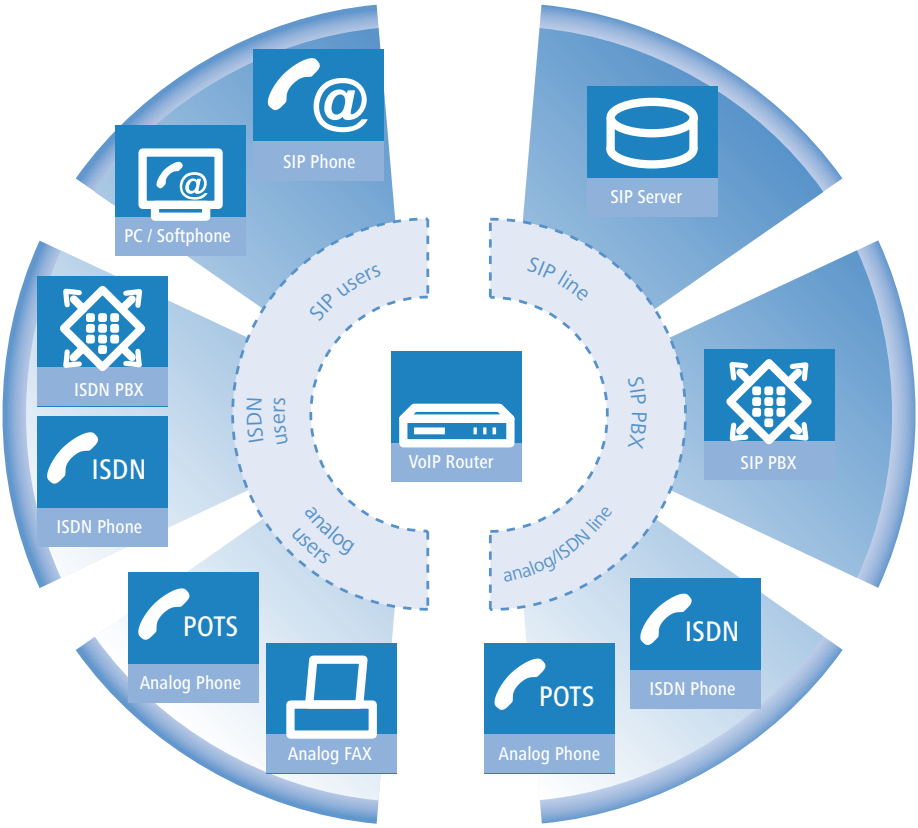
- ISDN PBXs at different locations can form a common internal telephone network.
- A SIP PBX is not necessary.
- Calls within the company network are at no charge.
- Outgoing calls are automatically directed to the best line for cost optimization.
- Incoming calls can be switched directly to the appropriate employee at a different location.

16.2.2 The central position of the LANCOM VoIP router

LANCOM VoIP routers take up a central position in the switching of telephone calls between internal and external subscribers over the different channels of communication. Depending on the model and equipment, the devices interconnect the following communication participants and channels into a common telephone infrastructure.

1. Internal VoIP terminal devices connected to LAN, WLAN and DMZ, such as SIP telephones and SIP softphones
2. The internal ISDN infrastructure with ISDN PBX and ISDN telephones
3. Analog terminal devices, internally connected either into the ISDN network via a PBX with a/b ports, or alternatively into the VoIP network over an ATA (Analog Telephone Adapter).
4. External SIP providers and all of the external subscribers attainable through them
5. Upstream SIP PBXs with all of the internal and external subscribers reachable through them

6. The external ISDN world via ISDN NTBA or upstream ISDN PBX, and all of the external subscribers available via the land-line network



16.2.2.1 Users and lines

Telephony subscribers in internal areas can take part in voice communications and, in the LANCOM VoIP environment, are referred to as "users". The LANCOM differentiates between:

ISDN users

A maximum of 40 terminal devices connected over the ISDN network, including ISDN and analog devices connected to an upstream ISDN PBX.

When connecting downstream PBXs to point-to-point lines, the number of possible ISDN subscribers is determined by the length of the extension number (DDI). In this case, all of the telephones and terminal equipment connected to the PBX can be mapped with a single ISDN user entry.

SIP users

A maximum of 40 (with the LANCOM VoIP +10 option) SIP terminal devices connected over LAN and WLAN and analog devices connected with an ATA.

The external paths of communication available to the users are known as "lines". The LANCOM knows the following lines:

ISDN

A connection to an ISDN NTBA over the TE interface. The NT interface can additionally be used to connect ISDN terminal devices directly or via a downstream ISDN PBX.

SIP lines

A maximum of 55 lines (with VoIP +10 option) are possible. There are three different types of SIP line:

- A "Single account" line acts like a normal SIP account with a single telephone number. The internal users can all make use this account for making SIP calls, although only one call can be conducted at a time.

Depending on the provider services, these lines can be used to reach subscribers in the provider networks, subscribers in other SIP networks (partner networks), or even land-line subscribers. Your own availability at your own telephone number or even solely with a SIP name over the Internet also differs from provider to provider.

- A "trunk" line acts like an extended SIP account with a main external telephone number and multiple extension numbers. Internal users use this account in parallel and several calls can be made simultaneously (until the maximum available bandwidth is exhausted).
- As a "SIP gateway" line, the LANCOM VoIP router provides a remote SIP PBX with a transition to the local ISDN network. The SIP gateway is registered at the SIP PBX with a single number, although several calls can be conducted at once (until the maximum available bandwidth is exhausted). The connection between the SIP PBX and the LANCOM VoIP router is normally established over a VPN connection.

SIP PBX systems

Maximum 4 connections to upstream SIP PBXs. These lines are generally connections to large PBXs in the network at headquarters which can be reached via a VPN connection.

The precise number of users and lines available varies between models and software options.

16.3 Call switching: Call routing

All calls between internal subscribers and subscribers who can be reached over external lines are handled as SIP calls by the LANCOM—even if the connection is between two ISDN subscribers.

The call router in the LANCOM VoIP router handles the switching of the calls. The switching relies mainly on the information in two tables:

- For telephone numbers arriving at the call router, rules in the call-routing table are able to alter these numbers if needed and can decide which line to use for a call.
- The table for the locally registered user provides information about which terminal device is available at which internal telephone number.

The bandwidth reservation, QoS settings and firewall settings that are necessary for reliable transmission of voice data are carried out automatically by the LANCOM.

- When establishing a connection, the LANCOM checks (under consideration of the permitted codecs) the maximum bandwidth that will be required.
  - This bandwidth is then automatically reserved by the QoS module upon initiation of the connection.
  - If negotiation shows that the maximum bandwidth is not available, the connection will not be made.
  - If negotiations between the terminal devices can agree upon a codec with lower bandwidth requirements, then the reserved bandwidth will be reduced accordingly.
- All packets from ISDN users are given a DiffServ marking by the LANCOM (with SIP users, the QoS marking is usually handled by the telephones or softphones):
  - SIP packets for signaling are marked as CS1.
  - RTP packets are marked as EF.
- The ports required for the transmissions are activated automatically.

16.3.1 SIP proxy and SIP gateway

The tasks involved in switching calls between the different lines of SIP and ISDN subscribers are handled by two functions in the LANCOM VoIP router.

SIP proxy

A SIP proxy handles the switching between callers.

SIP gateway

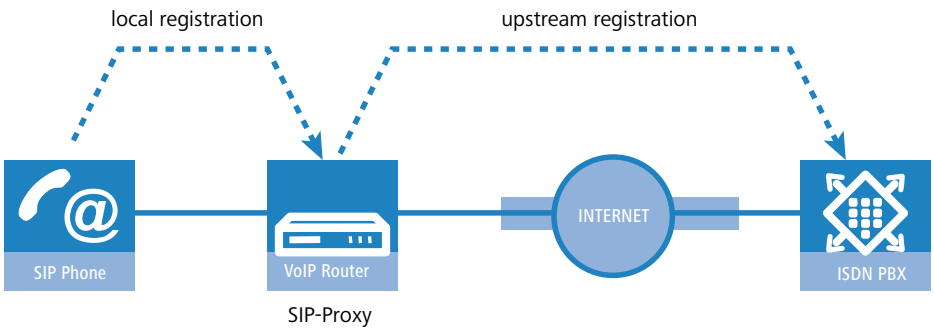
The SIP gateway handles the conversion between IP-based telephony that uses the SIP protocol and other (telephone) networks, for example the ISDN network.

16.3.2 User registration at the SIP proxy

A LANCOM VoIP router represents the central exchange for SIP calls between different subscribers wanting to communicate over different types of line. The tasks of switching in the LANCOM are handled by the SIP proxy. A telephone signals the SIP proxy that it needs to establish a connection, and the SIP proxy uses certain rules to decide which line is to be used for the connection. Conversely, incoming calls are assigned to a certain terminal device by the SIP proxy according to its rules.

For terminal devices to be able to take part in this switching, they must be registered with the SIP proxy. Where the registration is limited to call switching by the LANCOM, we refer to "local registration".

If other exchanges are involved, e.g. an SIP PBX at another location, then we refer to an upstream registration. In this case, the LANCOM accepts the request for registration and forwards it upstream. In this instance, the LANCOM is described as "transparent proxy".



The great advantage with this two-stage registration comes to bear in the backup event: If the connection to an upstream SIP PBX is not available, the SIP proxy can handle the user who is registered upstream as a local user and can then direct the calls over alternative lines.

16.3.2.1 Registering at the LANCOM VoIP router (local registration)

For local registration at the LANCOM, the user just has to send a valid VoIP domain to the SIP proxy and has to be registered as a SIP user. Valid domains include the internal VoIP domains of the LANCOM VoIP router and all of the domains entered for a SIP line.

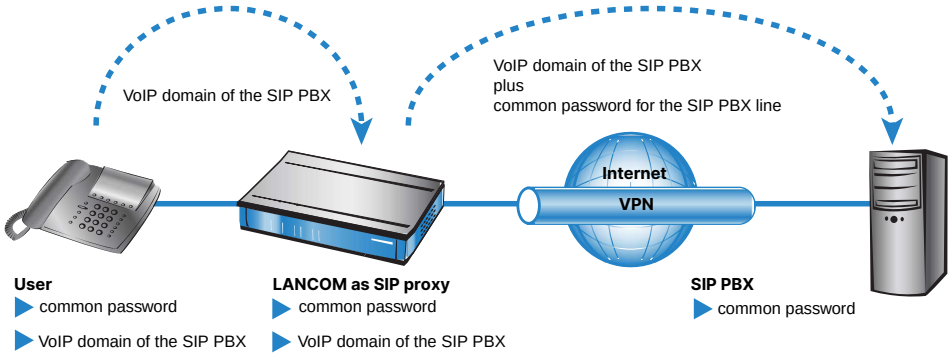
- For SIP terminal devices in the LAN (SIP telephone or SIP softphone), the domain is entered in the configuration.
- The domain cannot be entered into ISDN terminal equipment; instead, ISDN users have to be registered in the LANCOM configuration with a corresponding entry as an ISDN user.
- To prevent unknown subscribers from registering, authentication at the SIP proxy can be set as a prerequisite to local registration (local authentication). In this case, an entry as a SIP or ISDN user with corresponding password in the LANCOM VoIP router configuration is essential.

Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users in the WAN require an appropriate user entry and authentication by password.

16.3.2.2 Registration at an upstream SIP PBX (upstream registration)

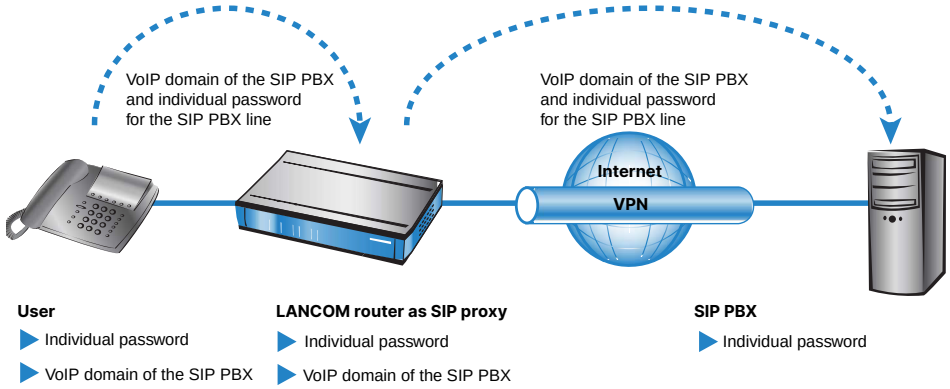
Generally, authentication by user and password is always required for registration at a SIP PBX. There are two possible ways of transmitting the authentication data to the SIP PBX:

- All SIP and ISDN users at the LANCOM VoIP router end use the same shared access information. In this case, only the VoIP domain for the SIP PBX and the appropriate user ID are entered into the SIP terminal device. For ISDN users, the VoIP domain of the SIP PBX is entered into the LANCOM as an ISDN user. The SIP proxy recognizes the request for registration at the upstream SIP PBX if the domain communicated from the client agrees with a domain entered for the SIP PBX line. The proxy then forwards the registration data together with the shared password to the SIP PBX.



- If SIP or ISDN users at the LANCOM VoIP router are entered into the SIP PBX with different passwords, then the users have to enter their individual passwords upon registration. Consequently, each SIP or ISDN user has an entry in the

LANCOM with the individual passwords, which are also entered into the SIP terminal devices. Users with shared and individual passwords can be managed in parallel.



16.3.2.3 Particular aspects for ISDN users

Integrating ISDN terminal equipment into the LANCOM VoIP environment and the necessary steps for configuration depend upon the application at hand and, if applicable, upon the options available with a PBX. The main questions to be answered by the user are as follows:

- Can ISDN terminal devices telephone internally with SIP users?
- Are ISDN terminal devices available externally over SIP lines?
- Can ISDN terminal devices telephone externally over SIP lines?

If ISDN terminal equipment can be reached over an ISDN TE interface on the LANCOM, it is described as "upstream". From the perspective of the LANCOM, the ISDN terminal devices are on an external line. This ISDN terminal equipment is normally not classified as being for local users, and so no entries for ISDN users are necessary.

ISDN terminal equipment at an upstream ISDN PBX...

- can make internal calls to SIP users if the corresponding telephone numbers are configured as internal MSNs in the ISDN PBX.
- can receive internal calls from SIP users if the internal MSNs of the ISDN equipment are output to the ISDN line by the call-routing table, for example over a standard route.
- can only make calls over SIP lines if the PBX is able to output certain call numbers over its internal ISDN bus. Otherwise, all calls not matching with its internal MSNs would be forwarded by the ISDN PBX to the public telephone network.
- can only receive calls from an upstream SIP PBX if entered into the LANCOM as an ISDN user and registered as such with the SIP PBX.

If ISDN terminal equipment can be reached over an ISDN NT interface on the LANCOM, it is described as "downstream". For the LANCOM, this is then a local subscriber that can be reached via the list of registered users. As ISDN terminal devices cannot send domain information to register at the LANCOM, this must be entered as an ISDN user so that it can be made known to the VoIP system.

ISDN terminal equipment at a downstream ISDN PBX...

- can make internal calls to SIP users by entering the character for an outside line as required by the PBX and then dialing the SIP user's internal number. The PBX then forwards the call to the SIP user's internal number—without the outside-line access code—over its external ISDN bus to the LANCOM.
- can receive internal calls from SIP users as long as the entry for the ISDN user contains the correct assignment of the internal number to the appropriate MSN. The LANCOM takes a call to the ISDN user's internal number, translates it to the MSN, and outputs it to the allocated ISDN bus. The PBX receives the MSN as if it were an external call and forwards it to the corresponding ISDN terminal equipment.
- can conduct incoming and outgoing calls over SIP and ISDN just like SIP users. Again, the outside-line code may be necessary for outgoing calls.

Dynamic ISDN users at point-to-point connections

When connecting downstream PBXs to a point-to-point interface of the LANCOM VoIP router, the number of possible ISDN terminal devices is only limited by the length of the extension number. With three-figure extension numbers, almost 1000 terminal devices can be connected, all of which can be managed as ISDN users in the LANCOM VoIP router. Through an ISDN user entry with a # character as a placeholder for the telephone numbers, all ISDN terminal devices with their respective extension numbers can be set up as dynamic ISDN users.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

16.3.3 Number translation at network transitions

LANCOM VoIP routers switch calls between different telephone networks, e.g. the ISDN network, various SIP provider networks, and the internal telephone network. These networks generally have different ranges of numbers or even completely different conventions for addressing subscribers. Whereas the traditional land-line network uses numerical characters with country code and area access codes, the world of SIP allows alphanumerical names along with domain information.

The transition between these zones must guarantee the correct translation of "telephone numbers" so that the intended subscriber can be reached.

Depending on the application at hand, both the called and the calling numbers have to be modified in such a way that a call can be returned to the original caller.

Call number translation at the transition to outside lines is primarily implemented by mapping entries in the ISDN and SIP lines and by rules in the call-routing table.

16.3.4 The Call Manager

The Call Manager has the central task of allocating the calls waiting to be switched to a certain line or to a certain user. The Call Manager makes this allocation by using the call-routing table and the list of registered users. The calls are switched in the following steps:

- Processing of called numbers (Called Party ID)

  First of all there is a check to see whether a numeric or alphanumeric number is available. Typical dialing separators such as "()-/" and <blank> are removed. A leading "+" is left in place. In this case, the number is still treated as a numeric number. If the check reveals any other alphanumerical character, the number is treated as alphanumeric and remains unchanged.

- Resolving the call in the call routing table

  After processing the Called Party ID, the call is passed over to the call-routing table. Entries in the call-routing table consist of sets of conditions and instructions. The entries—with the exception of the default routes—are searched through and the first one that satisfies **all** of the conditions is executed.

- Resolution of the call with tables of local subscribers

  If no entry is found in the call-routing table, then the Call Manager searches through the list of local subscribers. Call routing considers all of the users known to the call router (registered SIP users, configured ISDN users). If an entry is found that agrees with the called number and that has the matching destination domain, then the call is delivered to the corresponding subscriber.

  If there is no local subscriber with matching number and destination domain, then the following cycle searches for an agreement between the number of the local subscriber and the called number; the destination domain is ignored.

- Resolution of the call with default entries in the call-routing table

  If the preceding cycles referring to the call-routing table and lists of local subscribers remain unsuccessful, then the waiting call is checked once again with the call-routing table. This pass only takes the default routes into account, however. The numbers and destination domains entered into the default routes are ignored. Only the source filters are processed, assuming that the default route has these filters.

Specific examples of call-routing procedures can be found in the configuration examples described.

16.3.5 Telephony with LANCOM VoIP routers

Using the LANCOM VoIP router opens up a variety of new possibilities for making telephone calls. Depending on the constellation of terminal equipment implemented (e.g. SIP or ISDN telephones, SIP or ISDN PBX systems) and depending on the configuration for call routing in the LANCOM VoIP router, certain information is critical for understanding the establishment of connections.

16.3.5.1 Automatic outside line access

Using the LANCOM VoIP router and the enhancement with VoIP functionality within your telephone structure is designed to support the users' telephone behavior with the greatest possible convenience. One of the core aspects of this is the use of "spontaneous" or "automatic" outside line access, a feature that is familiar to users of standard PBX systems.

- Most PBX systems are configured in such a way that the telephone subscribers must dial a "0" before the desired telephone number in order to gain access to an outside line - that is, to carry out a telephone conversation via a public telephone network.

  Without the "0" prefix, the number dialed is considered to be an internal number from another extension line on the private PBX.

- If "automatic outside line access" is set up, all numbers dialed are directed over the public telephone network. In this case, internal telephone calls to other extensions are not possible or only possible when a special symbol is dialed before the number.

When the telephone structure is extended with a LANCOM VoIP router, a variety of new possibilities become available for connecting telephone terminal equipment. This includes the existing analog or ISDN telephones (where necessary, connected to the respective PBX) or VoIP terminal equipment such as SIP telephones or PCs with VoIP software.

As a new and central building block in the telephone structure, the LANCOM VoIP router assumes many of the PBX tasks for the terminal equipment connected to it. As such, you can also set up the automatic outside line access for the terminal equipment connected to the LANCOM VoIP router directly for the ISDN or SIP subscriber groups, thereby adapting it to existing telephone behavior.

- When automatic outside line access is turned off, subscribers must dial a "0" before the desired number in order to carry out a telephone conversation via a public telephone network.

  All calls without a "0" preceding the number will be treated as calls to internal extensions within the private telephone network.

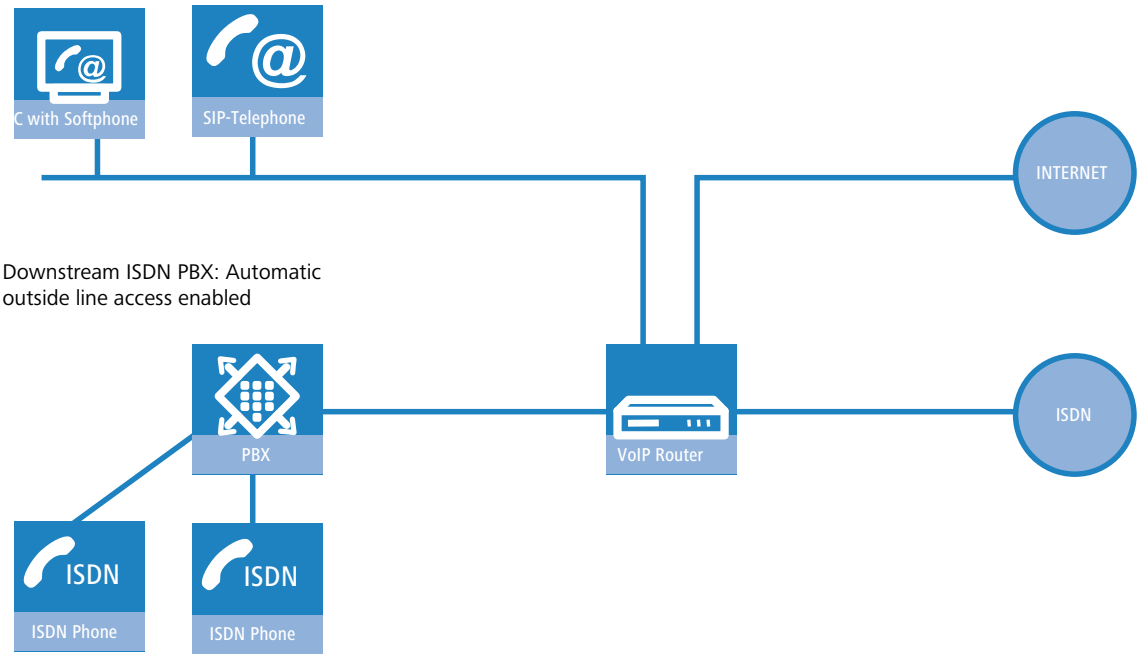
- If automatic outside line access is turned on, all numbers dialed will be directed over a public telephone network.

  For telephone calls to internal extensions, a special symbol or a specific number combination must be dialed before the number. With the default settings, when automatic outside line access is enabled, a star * is activated as the identification symbol for an internal number. This setting can be adjusted to match the character that you are familiar with.

If you operate the LANCOM VoIP router on the extension line of a PBX, we recommend that you configure outside line access for the router in the same way as for the PBX so that the behavior remains unchanged from the user's perspective.

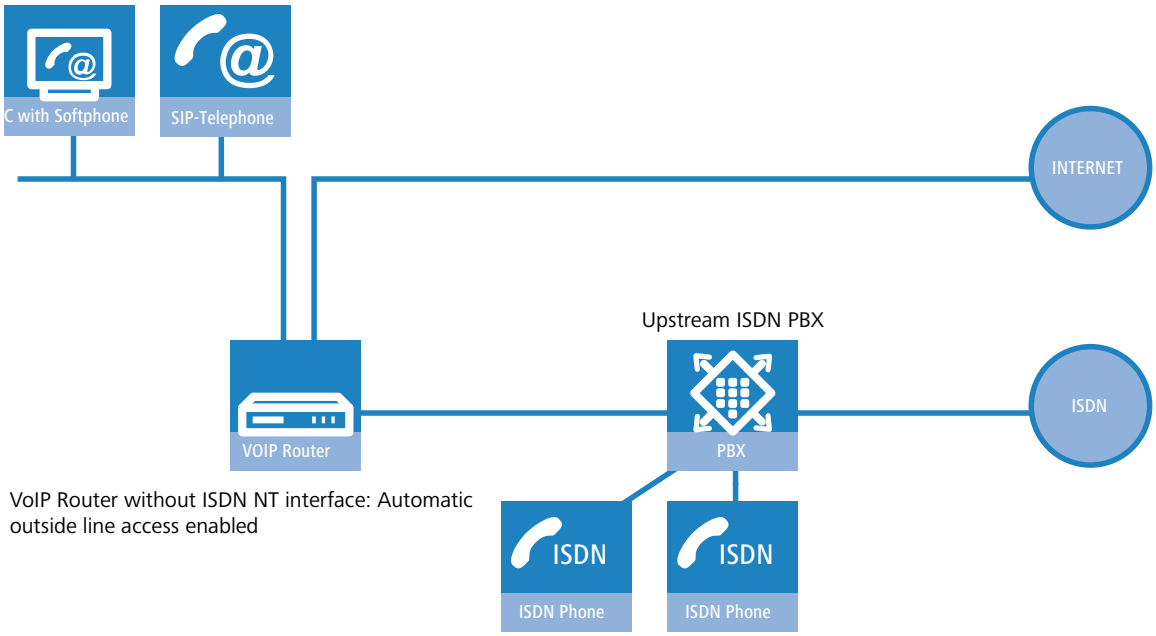
Example of a downstream PBX

A LANCOM VoIP router is switched between the ISDN outside line and the existing ISDN PBX. In the PBX, automatic outside line access is enabled, the call router settings for the LANCOM VoIP router decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.



Example of an upstream PBX

A LANCOM VoIP router is connected to an ISDN PBX extension line. In the LANCOM VoIP router, automatic outside line access is enabled, and the settings for the upstream PBX decide whether or not a "0" must be dialed for outside line access for the connected ISDN and SIP subscribers.



16.3.5.2 Dialing different number ranges

When dialing other parties, the following number ranges are available for use:

- Internal numbers are comparable to the extension numbers for traditional PBX systems. Subscribers can reach one another directly using these internal numbers without having to go through a public telephone network.

  The internal numbers must be unique for all subscribers within the private telephone network, this also includes any other PBX systems that may be connected!

  The internal subscribers can be reached by simply dialing the internal number without a "0" preceding it.

  Depending on the settings for automatic outside line access, a special preceding dialing signal may be required.

- Via **local telephone numbers** you can reach external parties who are in the same local telephone network as the LANCOM VoIP router, i.e. users with the same area code as the public line for the LANCOM VoIP router.

  In decentralized locations that extend beyond city or state boundaries, the physical location of the device is decisive, even if a central PBX is located at a different location. Therefore, for a LANCOM VoIP router in London, all telephone subscribers in the local telephone network for London can be reached using local numbers, even if a SIP PBX connected via VPN can be reached in Manchester.

  Depending on the settings for automatic outside line access, a "0" prefix may be required.

- The **national and international numbers** behave in the same way as local numbers; here, the physical location of the devices is decisive for the assignment of corresponding access codes. Therefore, a LANCOM VoIP router in Austria belongs to the national telephone network in Austria, even if there is a VPN connection to the SIP PBX at the headquarters in Germany.

Depending on the settings for automatic outside line access, a "0" prefix may be required.

16.3.5.3 Service numbers

Certain service numbers (emergency numbers, toll-free or expensive premium lines) can be subjected to special treatment by the call router.

- For example, this ensures that emergency numbers for the police or fire department are always reached, even if the subscribers do not dial the correct preceding dialing signal for outside line access.

  With the default settings, the emergency numbers "110" and "112" are configured in such a way that they can be dialed correctly with or without the preceding "0".

- For toll-free numbers such as "0800", a direct connection via ISDN is usually selected in order to use the toll-free land-line to land-line connection.

16.3.5.4 Dialing via specific lines

The LANCOM VoIP router allows additional phone lines to be used for voice communication as a supplement to your existing ISDN exchange lines. These new lines may be to a SIP PBX connected via VPN, or to a public SIP provider on the Internet. Each time a connection is established, the call router uses pre-determined rules to decide which of the existing lines is to be used for the call.

As an alternative to the automatic selection by the call router, you can direct individual calls to a certain line, for example when you want to call a party purposely via ISDN and not via the SIP PBX at the headquarters. For this purpose, the call router assigns specific code numbers to existing lines, such as "98" for ISDN or "97" for a SIP provider. The targeted call via this line is then initiated with the corresponding identifier:

- The call with "020 123456" is assigned to a corresponding line by the call router, e.g. via the SIP PBX at the headquarters.
- However, the call with "98 020 123456" is made directly via the ISDN connection by the call router.

16.3.6 Hold call, swap call, transfer call

LANCOM VoIP routers support various services which are familiar to users of the ISDN network:

- With **call hold** the user can place an active call into a wait state. In this state the user can make a call to another person, for example.
- With **swap call**, the user can switch to and fro between two connections. The user is only connected with one caller at a time, while the other caller is put on hold.
- With **transfer call** the user switches an active call over to another call which is on hold. The two callers are then connected and the user is no longer involved in the call.

The services call hold, swap call and transfer call are available to all local SIP, ISDN and analog users, and also to subscribers at an upstream SIP PBX; however, they can only be initiated by a SIP user.

16.3.7 Transmission of DTMF tones

ISDN telephone networks introduced the possibility of transmitting information about which button was pushed on the telephone using DTMF tones (Dual Tone Multiple Frequency). With the help of DTMF tones, the telephone user can communicate with voice mailboxes and computer telephony systems, for example.

In VoIP applications, special mechanisms are required to assume the DTMF tone function. If, for example, during a telephone call, a button is pressed on a VoIP telephone or a VoIP softphone, this should trigger the same action as a call with an ISDN telephone.

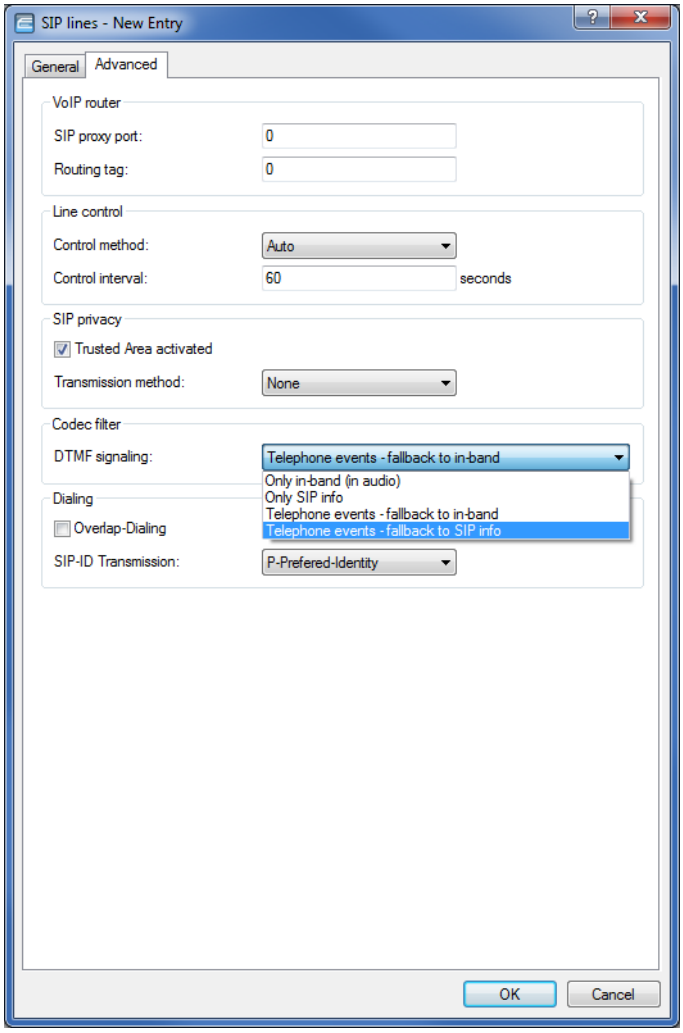
Generally, DTMF tones are transmitted in VoIP applications in one of two ways:

- In-band describes the transmission of the DTMF tones in the same data stream in which the voice data are transferred. However, this procedure is relatively unreliable because the DTMF tones in the IP datastream can easily be mistaken for voice data, particularly when using compression codecs.
- Out-of-band describes the transmission of the DTMF tones in a stream that runs parallel to the actual voice data. Two standards are generally used for out-of-band transmission:
  - SIP INFO (RFC 2976)
  - RFC 2833 (RTP Payload for DTMF Digits)

  Both variants can encapsulate information into the signaling data stream depending, for example, on the buttons pressed, their tone frequency, and the length of time the button was pressed. In addition, events that should be transmitted with DTMF tones can also be transmitted in cleartext in the SIP data.

16.3.7.1 Configuring DTMF signaling

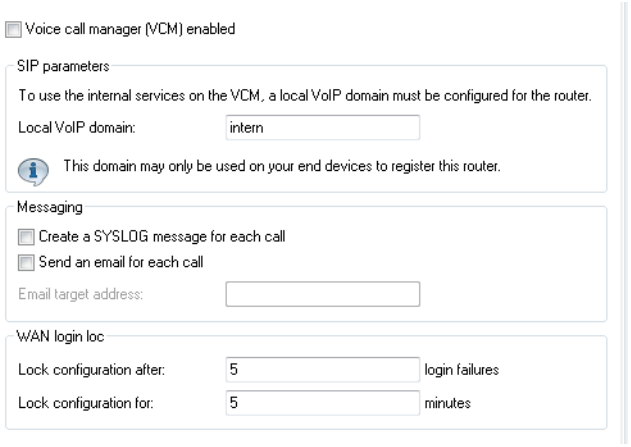
When configuring the DTMF signaling, you specify which variant is used for the transmission of the DTMF tones under **Voice Call Manager** > **Lines** > **SIP lines**:



16.4 Configuring the VoIP parameters

16.4.1 General settings

To configure the settings for the general VoIP parameters, navigate to **Voice Call Manager** > **General**.



Voice Call Manager (VCM) enabled

Enables or disables the Voice Call Manager.

Local VoIP domain

Name of the domain in which the connected telephones and the LANCOM Wireless router are operated.

- Terminal devices working in the same domain register as local subscribers at the LANCOM Wireless router and make use of the SIP proxy.
- Terminal devices working with the other domain of an active SIP PBX line register themselves as subscribers at an upstream PBX.

Create a SYSLOG message for each call

Each time a call is made with the LANCOM VoIP router a SYSLOG message is created.

Please consider that you can only use this feature with the proper SYSLOG settings.

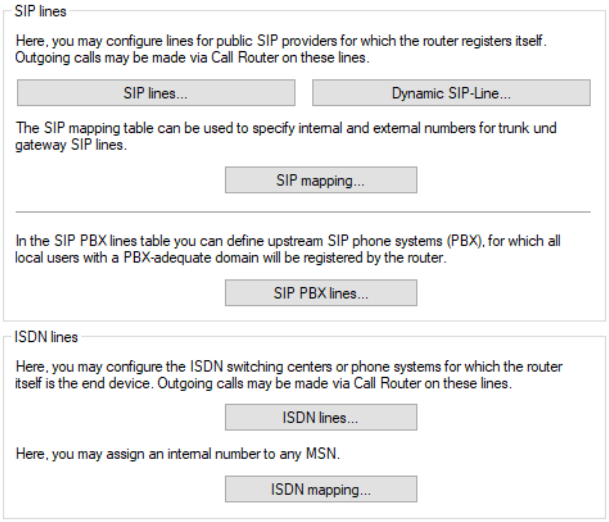
Send an e-mail for each call

Each time a call is made with the LANCOM VoIP router an e-mail is sent to the defined address.

Please consider that you can only use this feature if you have set up the appropriate SMTP account.

16.4.2 Line configuration

The parameters for the lines are configured under **Voice Call Manager** > **Lines**.

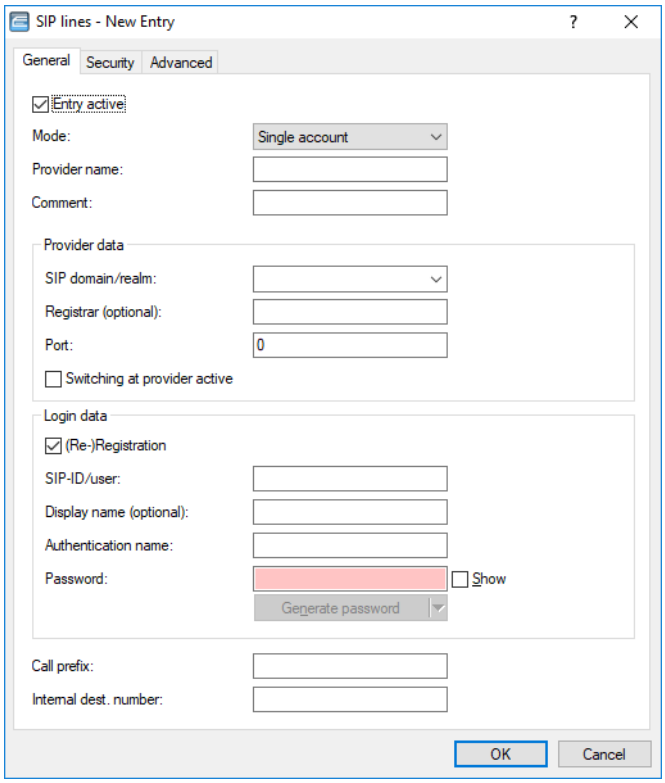


16.4.2.1 SIP lines

The device uses these lines to register with other SIP remote stations (usually SIP providers or remote gateways at SIP PBXs). The connection is made either over the Internet or a VPN tunnel.

The settings are configured under **Voice Call Manager** > **Lines** by clicking the button **SIP lines**.

The **General** tab contains the following configuration options:



Entry active

Activates or deactivates this entry.

Mode

This selection specifies the operating mode of the SIP line. Possible values are:

Single account

Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal destination number. The maximum number of simultaneous connections is either set by the provider or it depends on the available bandwidth and the codecs being used.

Trunk

Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main switchboard number with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: “From:”). For incoming calls, the prefix is removed from the destination number (SIP: “To:”). The remaining digits are used as the internal extension number. In case of error (prefix not found, destination equals prefix) the call is forwarded to the internal destination number as configured. The maximum number of connections at any one time is limited only by the available bandwidth and possibly by the provider.

Gateway

Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: “From:”) and sent in a separate field (SIP: “Contact:”). For incoming calls the dialed number (destination) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth and possibly by the provider.

Link

Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP: "From:") is not modified. For incoming calls, the dialed number (destination; SIP: "To:") is not modified. The maximum number of connections at any one time is limited only by the available bandwidth and possibly by the provider.

Flex

- To the outside the line behaves like a commercially available SIP account with a single public number.
- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

Table for number translation:

Single account	SIP number incoming to the line	SIP number sent from the line
Outgoing call	“From:”	The number registered at the provider (User ID)
Incoming call	“To:”	User ID

Trunk	SIP number incoming to the line	SIP number sent from the line
Outgoing call	“From:”	Switchboard number (User-ID) + “From:”
Incoming call	Switchboard number (User-ID) + “To:”	"To:" as internal extension

Gateway	SIP number incoming to the line	SIP number sent from the line
Outgoing call	“From:”	The number registered at the provider (User ID)
	“From:”	“Contact:”
Incoming call	“To:”	“To:”

Link	SIP number incoming to the line	SIP number sent from the line
Outgoing call	“From:”	“From:”
Incoming call	“To:”	“To:”

Name

The name of the line: This may not be the same as another line (SIP provider, ISDN or SIP PBX) configured on the device.

Comment

Comment on this entry.

SIP domain/realm

SIP domain/realm of the upstream device. Provided the remote device supports DNS service records for SIP, this setting is sufficient to determine the proxy, outbound proxy, port and registrar automatically. This is generally the case for typical SIP provider services.

Registrar

The SIP registrar is the point at the SIP provider that accepts the login with the authentication data for this account.

This field can remain empty unless the SIP provider specifies otherwise. The registrar is then determined by sending DNS SRV requests to the configured SIP domain/realm (this is often not the case for SIP services in a corporate network/VPN, i.e. the value must be explicitly set).

To force SIP registration via IPv4 or IPv6 the SIP domain can be entered in the field **Registrar** followed by the suffix **?4** or **?6** (e.g. **SIP-Domain.com?4**). See also *Configuration option for IPv4/IPv6 resolution with DNS resolutions* on page 171.

Outbound proxy

The SIP provider's outbound proxy accepts all SIP-call signaling that originates from the device for the duration of the connection.

This field can remain empty unless the SIP provider specifies otherwise. In this case, the outbound proxy is identical to the registrar. This is a typical configuration for SIP-provider offerings.

Port

This is the remote port used to communicate with the provider.

Switching at provider active

Call switching (transfer call) between two remote subscribers can be handled by the device itself (media proxy) or it can be passed on to the exchange at the provider if both subscribers can be reached on this SIP provider

line. The advantage of this is that the LANCOM VoIP router no longer requires the bandwidth. Otherwise, the media proxy in the device switches the media flows, such as when connecting two SIP provider lines.

Switching at the provider will only work if both connections are routed via the same provider line.

An overview of the main SIP providers supporting this function is available in the Support area of our Internet site.

(Re-) registration

This activates the (repeated) registration of the SIP provider line. Registration can also be used for line monitoring.

To use (re-) registration, set the line monitoring method on the **Advanced** tab to "Register" or "Automatic". The device renews its registration after the monitoring interval expires. If the provider's SIP registrar suggests a different interval, the devices uses this value automatically.

SIP-ID/user

Telephone number of the SIP account or name of the user (SIP URI).

For a SIP trunking account, the switchboard number is entered here. For incoming calls, any numerals after the switchboard number are interpreted as extension numbers (DDI) and these are passed to the call router. For outgoing calls, DDI numbers received from the call router are combined with the switchboard number. This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored either there or on the terminal device, then a SIP-PBX line should be set up.

Display name

Name for display on the telephone being called.

Normally this value should not be set as incoming calls have a display name set by the SIP provider, and outgoing calls are set with the local client or call source (which may be overwritten by the user settings for display name, if applicable). This settings is often used to transmit additional information (such as the original calling number when calls are forwarded) that may be useful for the person called. In the case of single-line SIP accounts, some providers require an entry that is identical to the display name defined in the registration details, or the SIP ID (e.g. T-Online). This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored either there or on the terminal device, then a SIP-PBX line should be set up.

Authentication name

Name for authentication to the upstream SIP device (provider/SIP PBX).

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to register with an upstream device using the data stored either there or on the terminal device, then a SIP-PBX line should be set up.

Password

The password for authentication at the SIP registrar and SIP proxy at the provider. For lines without (re-)registration, the password may be omitted under certain circumstances.

This access data is used to register the line (single account, trunk, link, gateway), but not the individual local users with their individual registration details. If individual users (SIP, ISDN, analog) are to

register with an upstream device using the data stored either there or on the terminal device, then a SIP-PBX line should be set up.

Call prefix

The device places a call-prefix number in front of the caller number (CLI; SIP "From:") for all incoming calls on this SIP line. This generates unique telephone numbers for return calls.

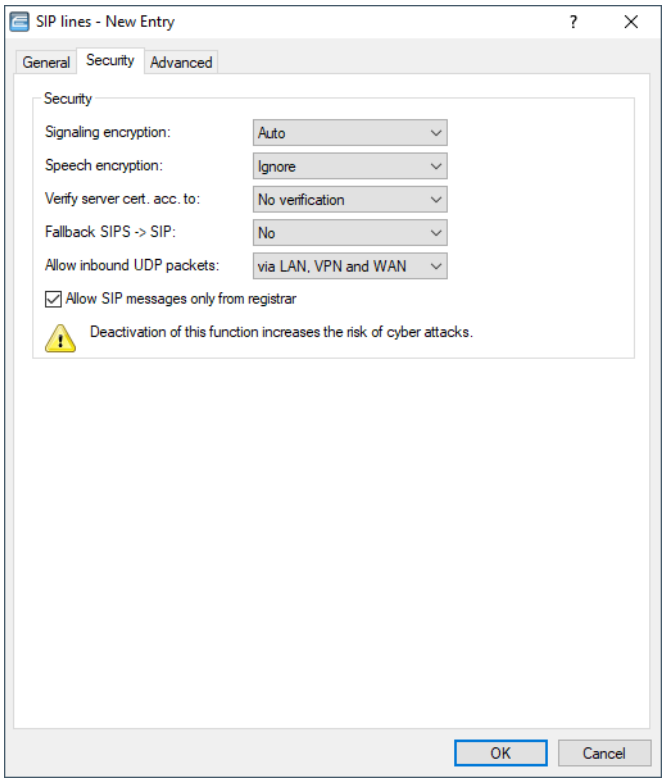
For example; you add a number here, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Internal destination number

The effect of this field depends upon the mode set for the line:

- If the line is set to "Single account" mode, all incoming calls on this line with this number as the destination (SIP: "To:") are transferred to the call router.
- If the mode is set to "Trunk", the destination number is determined by removing the trunk's switchboard number. If an error occurs, the call will be supplemented with the number entered in this field (SIP: "To:") are transferred to the call router.
- If mode is set to "Gateway" or "Link" the value entered in this field has no effect.

The **Security** tab contains the following configuration options:



Signaling encryption

This setting determines the protocol used for signaling encryption (SIP/SIPS) for communications with the provider.

Automatic

NAPTR (Naming Address Pointer) records are used for DNS resolution. In the DNS data, the provider specifies the use of transport protocols such as UDP, TCP or TLS. The provider can also specify weights or priorities.

If TLS is specified as the transport protocol for signaling encryption by NAPTR, voice encryption is also used automatically, regardless of the explicit configuration setting of voice encryption.

No (UDP)

All SIP packets are transmitted connectionless. Most providers support this setting.

No (TCP)

All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.

TLS

Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider. The TLS version selected in the configuration is taken as the minimum requirement for TLS encryption.

Speech encryption

This setting determines if and how the speech data (RTP/SRTP) is encrypted when communicating with the provider.

Speech encryption	
Reject	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are rejected. The speech channel is not encrypted.
Ignore	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are accepted. The speech channel is not encrypted.
Prefer	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are accepted. The speech channel is only encrypted if the remote peer also supports encryption.
Force	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are rejected. The speech channel is either encrypted or is not established.

If you require the encrypted transmission of speech data, the signaling must also use an encrypted channel. Please note that the use of SRTP is no guarantee of end-to-end encryption.

Verify server cert. acc. to:

With this setting, you specify whether the certificate of the SIP server is verified against certain Certificate Authorities (CAs). CA certificates from globally recognized certificate chains are updated with LCOS updates. They can also be manually updated by truststore updates.

Server certificate	
No verification	The server certificate is not verified. All valid server certificates are accepted, whichever CA they were signed by. This setting is useful for accepting self-signed certificates.

Server certificate

All trusted CAs	The server certificate is verified against all CAs known to the device. These include all CAs that LCOS "knows" to be trusted and also those from the VoIP server certificate slots 1 to 3. The encrypted connection is only established if one of these certificates is validated successfully.
VoIP cert. slot 1	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 1 of the VoIP certificates.
VoIP cert. slot 2	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 2 of the VoIP certificates.
VoIP cert. slot 3	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 3 of the VoIP certificates.
Telekom-Shared-Business-CA4	With this setting, the device only accepts server certificates signed by the Telekom Shared Business CA4 CA. Use this setting for SIP trunk connections from Deutsche Telekom.

Fallback SIPS > SIP

No

No fallback to an unencrypted connection is performed. If it is not possible to establish an encrypted connection to the VoIP provider, the line remains unregistered.

UDP

As a rule, encrypted SIP connections are made with the TCP protocol and unencrypted connections are made with the UDP protocol. This setting switches directly to an unencrypted UDP connection if the encrypted TCP connection cannot be established.

Complete

If an encrypted TCP connection with the configured TLS version cannot be established, then attempts are made to establish an unencrypted TCP connection, and finally a UDP connection in order to register the VoIP line.

This setting provides the best compatibility, but may lead to a longer registration time.

Allow inbound UDP packets

If the provider line uses UDP to communicate with the registrar, it receives UDP packets on the desired local port. With this setting you specify the network context in which a UDP packet is accepted. The device only accepts a packet from the WAN / VPN / LAN if you have activated the corresponding setting. Otherwise the packet is dropped.

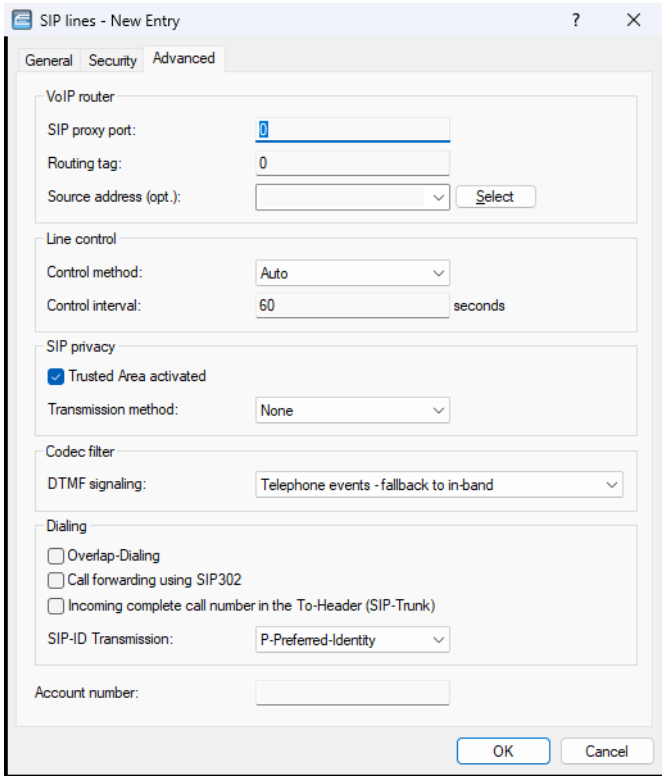
Allow SIP messages only from registrar (strict mode)

If this mode is activated, incoming SIP messages are only accepted from IP addresses that were reported by the provider when the domain / registrar was resolved.

If the VoIP provider signals a call from an IP address that was not included in the DNS resolution of the domain / registrar, the incoming call is not signaled to the internal subscriber.

Deactivating this function increases the risk of cyber attacks. SIP messages sent by an attacker can lead to calls being established and unwanted costs. SIP messages that are forwarded to internal clients can potentially exploit security vulnerabilities in the terminal devices.

On the tab **Advanced** you configure the SIP proxy, the line monitoring, and the calling line identification restriction.



SIP proxy port

This is the local port used by the SIP-proxy device to communicate with the remote station.

By default "0" is set here. The port is dynamically selected from the pool of available port numbers. You can also specify of a port in the range of "1" to "65535".

Routing tag

This routing tag selects a certain route in the routing table for connections to this SIP server.

Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

Control method

Specifies the line monitoring method. Line monitoring checks if a SIP provider line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked. Possible values are:

Automatic

The method is set automatically (default).

Deactivated

No monitoring. The line is reported as available when the option (re)registration is disabled. Otherwise it will be considered to be available only after a successful registration. This setting does not allow the actual line availability to be monitored.

Register

Monitoring by means of register requests during the registration process. This setting also requires **(Re-)registration** to be activated for this line.

Options

Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited, for example, for lines without registration.

Monitoring interval

The monitoring interval in seconds. This value affects the line monitoring with option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again.

Trusted area activated

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.



Please note that not all providers support this function.

Transmission method

Specifies the method used for transmitting the caller ID in the separate SIP-header field. Possible values are:

None

The default setting, so no transmission takes place.

RFC3325

Transmission according to "P-Preferred-Id/P-Asserted-Id".

IETF-Draft-Sip-Privacy-04

Transmission according to "IETF-Draft-Sip-Privacy-04" by means of RPID (Remote Party ID).

DTMF signaling

Depending on the requirements, it may not be sufficient to transmit “inband” DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Only in-band (in audio)

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

Only SIP info

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

Telephone events – fallback to in-band (default)

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

Telephone events – fallback to SIP info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

Overlap dialing

Overlap dialing significantly reduces the waiting time between the number being dialed and the call being established.

With overlap dialing disabled, your LANCOM device uses an overlap timer. The factory setting for this is 6 seconds. If the timer expires without you dialing any further numbers, the number entered so far is considered to be complete and the call is established.

With overlap dialing enabled on the line, portions of the dialed number are immediately sent to the All-IP provider.

If the All-IP provider responds with "484 number incomplete", the Voice Call Manager collects any additional dialed digits and sends them to the exchange again.

In this way, calls are established as quickly as possible without the 6 second delay, as you are accustomed to from your ISDN connection.



However, since this functionality is not supported by all SIP providers, overlap dialing has to be configured for each individual SIP line.

Call forwarding using SIP 302

Activates call forwarding via SIP 302 at the SIP provider. See also *Call forwarding (call deflection / partial rerouting) at the SIP trunk (SIP 302)* on page 1445.

SIP-ID transmission

This field sets the way in which the SIP ID is transmitted for outgoing calls when operating a SIP trunk. Depending on the provider, it may be necessary to transmit the SIP ID via a different field, as otherwise the call might be rejected by the provider.

The following values can be selected:

- P-Preferred-Identity (default value)
- FROM
- None
- P-Preferred-Identity without DDI
- PPI-PPI
- None – PPI (P-Preferred-Identity)
- None – PAI (P-Asserted-Identity)

Selecting the option **P-Preferred-Identity** (PAI- PPI) transmits the SIP ID including the DDI via the PPI/ PAI. The source telephone number is transmitted via the FROM field.

Selecting the option **FROM** transmits the SIP ID via the FROM field. The source telephone number is transmitted via the PPI / PAI field.

With the setting **None**, the SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI / PAI.

In contrast to the P-Preferred-Identity, the setting **P-Preferred-Identity without DDI** does not transmit an extension number (DDI) in the SIP ID via the PPI.

Selecting the option **PPI- PPI** (PPI) transmits the SIP ID including the DDI via the PPI. The source telephone number is transmitted via the FROM field.

With the setting **None – PPI (P-Preferred-Identity**, the SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI.

With the setting **None – PAI (P-Asserted-Identity**, the SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PAI.

With a single account, outgoing calls always signal the SIP ID in the **FROM** field.

Account number

Enter here a phone number that belongs to this SIP connection.

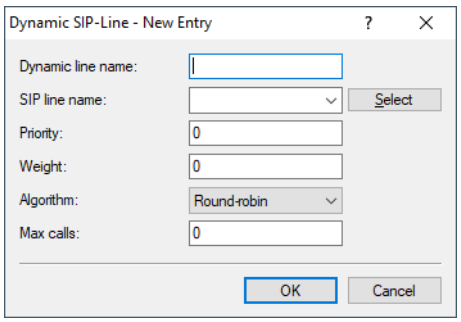
For SIP lines of the type "Flex", this source number is transmitted in the PPI for account verification.

If the FROM number is modified by call routing or if the SIP phone sends a number that does not match the connection, this will not cause the call to be rejected by the provider.

This allows CLIP no screening calls to be made directly via the VCM, provided the feature is supported by the SIP provider.

16.4.2.2 Dynamic SIP lines

The settings are configured under **Voice Call Manager** > **Lines** by clicking the button **Dynamic SIP line**.



Dynamic line name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

SIP line name

Here you select one of the already configured physical SIP connections.

Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line. The following algorithms can be used:

Weight

This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin

With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority

The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

Max. calls

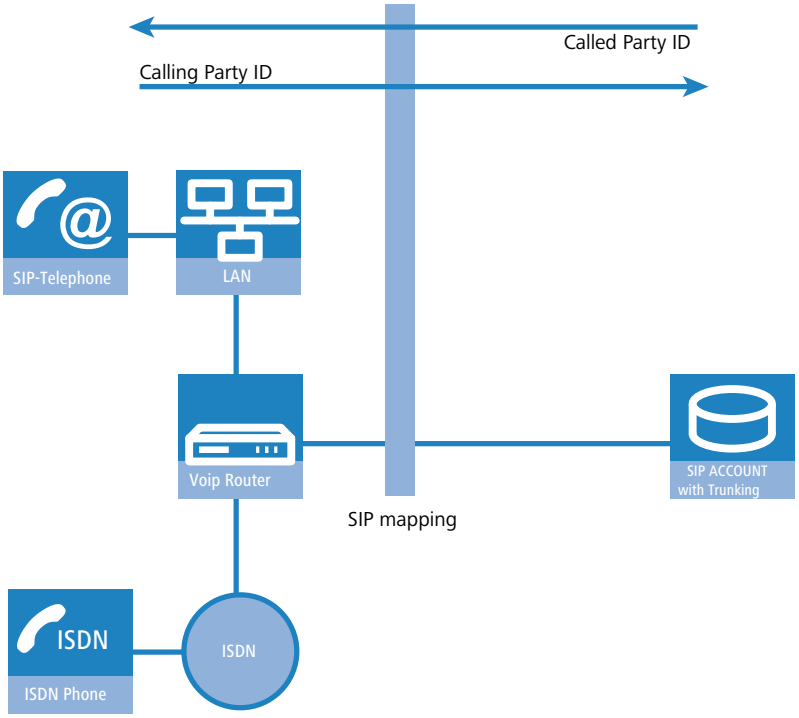
Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

16.4.2.3 SIP mapping

The entries made under SIP mapping establish a series of rules for number translation to SIP lines in the trunk or gateway mode.

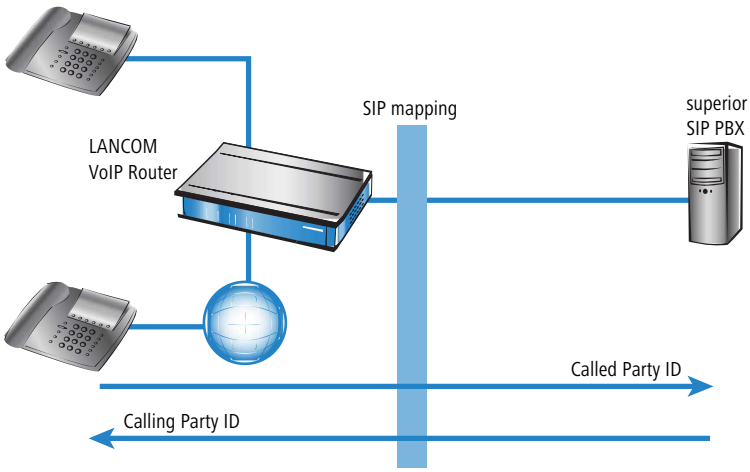
- A SIP line in trunk mode is used for mediating between internal numbers and the range of telephone numbers offered by a SIP account.
  - For incoming calls, the destination number (called party ID) is modified. The internal number is used if the called party ID matches with the external telephone number.
  - For outgoing calls, the calling party ID is modified. The external number is used if the calling party ID matches with the internal telephone number.

For SIP mapping on trunk lines, only the extension (DDI) is mapped. The extension is interpreted as those numerals which follow the switchboard number (SIP ID or SIP line).

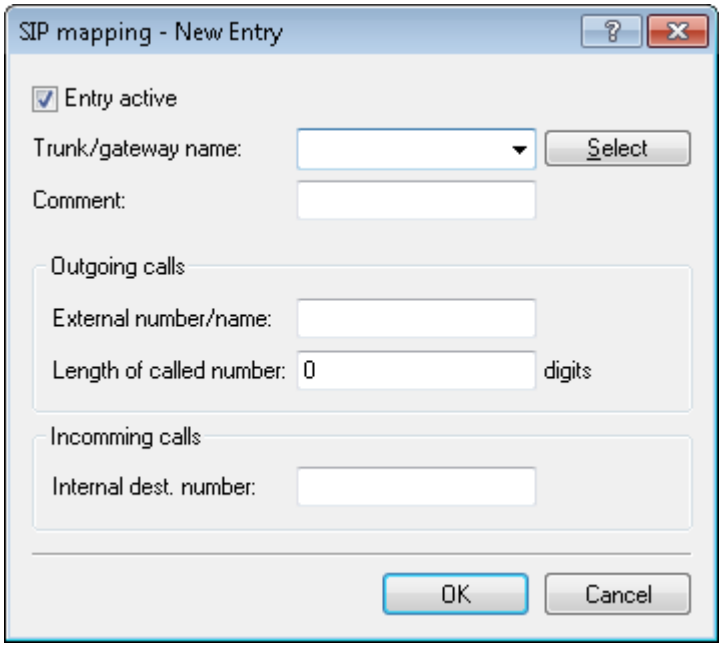


- For a SIP line in gateway mode, the telephone number plan of the upstream SIP PBX is adapted to the internal numbers in the call router.
  - For incoming calls (from the SIP line), the calling party ID is modified. The internal number is used if the calling party ID matches with the external telephone number.
  - For outgoing calls (to the upstream PBX), the destination number (called party ID) is modified. The external number is used if the called party ID matches with the internal telephone number.

For SIP mapping to gateway lines, the full telephone number is mapped. Depending on the configuration, the call number arriving at the ISDN interface can be subjected to further mapping (ISDN mapping).



SIP mapping is configured under **Voice Call Manager** > **Lines** by clicking the button **SIP mapping**.



Entry active

Activates or deactivates this entry.

Trunk/gateway name

Name of the line which is the destination of the call number mapping.

Comment

Comment about this rule.

External number / name

Call number within the range of those used by the SIP trunk account or upstream SIP PBX.

Length of called number

This value defines the number of numerals required for a called number to be regarded as complete. It only applies to SIP gateway lines with entries that end in a # symbol.

For an outgoing call, the external called number generated from this entry is automatically regarded as complete according to the defined number of numerals, and then forwarded. This process speeds up the dialing process. Alternatively, the called number is regarded as complete when:

- The user concludes the dialed number with a # symbol, or
- a precisely matching entry was found in the SIP mapping table without a # symbol, or
- the wait time expires.

By setting the length of called number to '0' you deactivate the premature dialing of the called number based on its length.

Internal destination number

Telephone number in the range of the VoIP router.

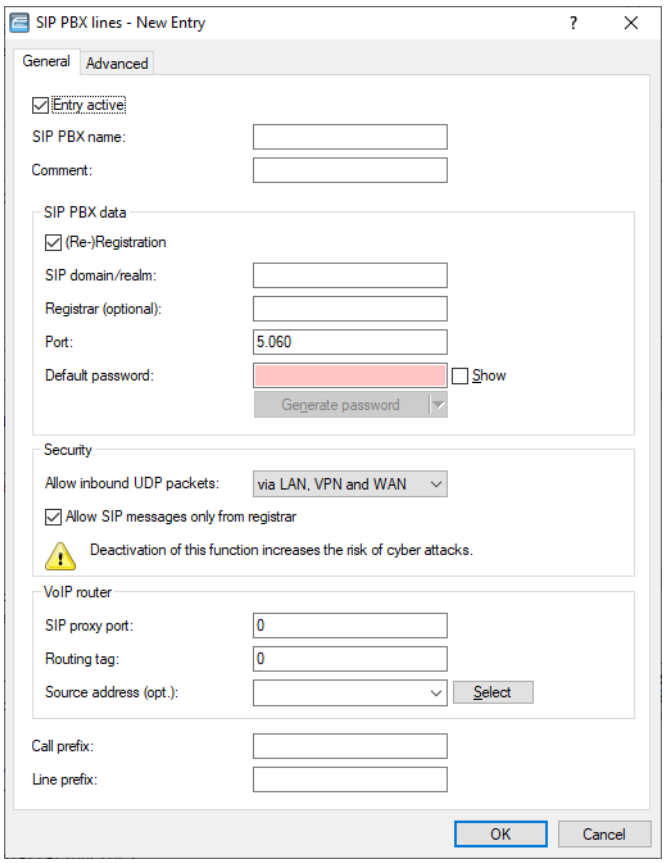
Using the # symbol as a placeholder allows blocks of numbers to be captured by one rule.

16.4.2.4 SIP PBX lines

These lines are used by the device to connect to upstream SIP PBXs. Connections are usually directed via VPN.

The settings are configured under **Voice Call Manager** > **Lines** by clicking the button **SIP PBX lines**.

The **General** tab contains the following configuration options:



Entry active

Activates or deactivates this entry.

SIP PBX name

Name of the line. This may not be the same as any other line (ISDN or SIP provider, or SIP PBX) configured on the device.

Comment

Comment on this entry.

(Re-) registration

This activates the (repeated) registration of the SIP PBX line. With (re-)registration activated, it is also possible to operate line monitoring.

To use (re-) registration, set the line monitoring method on the **Advanced** tab to "Register". The device renews its registration after the monitoring interval expires. If the SIP registrar of the SIP PBX suggests a different interval, the devices uses this value automatically.

SIP domain/realm

SIP domain/realm of the upstream SIP PBX.

Registrar (optional):

The SIP registrar is the point that accepts the login with the configured authentication data for this account in the SIP PBX.

Outbound proxy (optional)

Port

Port of the upstream SIP PBX to which the device sends the SIP packets.

Make sure that you activate this port in the firewall in order for the connection to work.

Default password

Shared password for registering with the SIP PBX. This password is required under the following circumstances:

- When SIP subscribers should be able to register at the PBX even without their own SIP credentials in the SIP user table of the device;
- When SIP users are able to register at the device without a password (no local authentication) but have access to the upstream SIP PBX by means of the shared password. In this case, the domain of SIP users must match the domain of SIP PBX line.

Allow inbound UDP packets

If the provider line uses UDP to communicate with the registrar, it receives UDP packets on the desired local port. With this setting you specify the network context in which a UDP packet is accepted. The device only accepts a packet from the WAN / VPN / LAN if you have activated the corresponding setting. Otherwise the packet is dropped.

Allow SIP messages only from registrar

Enable this checkbox if you want to receive SIP messages only through the registrar.

SIP proxy port

This is the local port used by the device proxy to communicate with the upstream SIP PBX. If this is set to "0", the device expects packets from the SIP PBX to arrive at the local SIP UDP server port (5060).

Packet assignment is made faster by configuring a fixed, unique local port and entering this as the destination port in the SIP PBX.

Routing tag

Routing tag for selecting a certain route in the routing table for connections to this SIP PBX.

Source address

The device automatically determines the correct source IP address for the destination network. If you want to use a fixed source IP address instead, enter it symbolically or directly here.

Call prefix

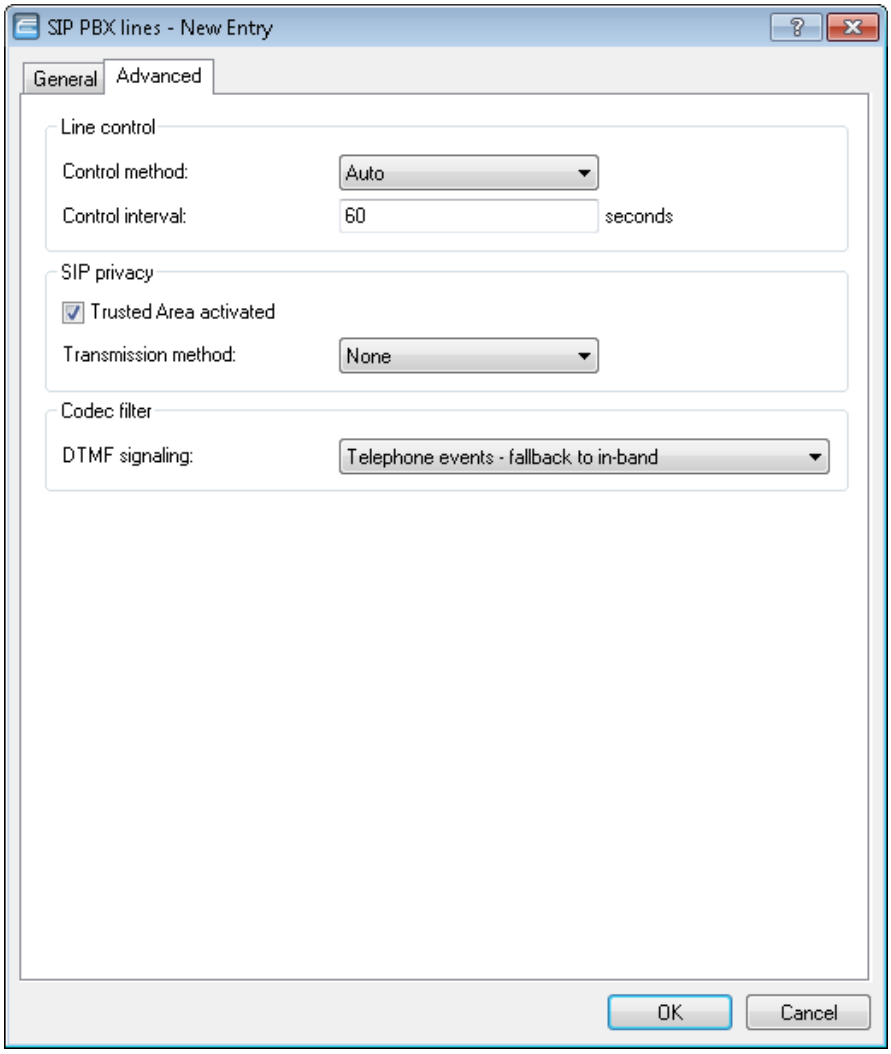
The device places a call-prefix number in front of the caller number (CLI; SIP "From:") for all incoming calls on this SIP PBX line. This generates unique telephone numbers for return calls.

For example; you add a number here, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

Line prefix

For outgoing calls on this line, the device inserts this prefix in front of the calling number in order to create a complete telephone number that is valid for this line. For incoming calls, the device removes this prefix, if applicable.

On the tab **Advanced** you configure the line monitoring, as well as the calling line identification restriction.



Control method

Specifies the line monitoring method. Line monitoring checks if a SIP PBX line is available. The Call Router can make use of the monitoring status to initiate a change to a backup line. The monitoring method sets the way in which the status is checked. Possible values are:

Automatic

The method is set automatically.

Deactivated

No monitoring. The line is always reported as being available. This setting does not allow the actual line availability to be monitored.

Register

Monitoring by means of register requests during the registration process. This setting also requires **(Re-)registration** to be activated for this line.

Options

Monitoring via Options Requests. This involves regular polling of the remote station. Depending on the response the line is considered to be available or unavailable. This setting is well suited for e.g. lines without registration.

Monitoring interval

The monitoring interval in seconds. This value affects the line monitoring with option request. The monitoring interval must be set to at least 60 seconds. This defines the time period that passes before the monitoring method is used again.

Trusted area activated

Specifies the remote station on this line (provider) as "Trusted Area". In this trusted area, the caller ID is not concealed from the caller, even if this is requested by the settings on the line (CLIR) or in the device. In the event of a connection over a trusted line, the Caller ID is first transmitted in accordance with the selected privacy policy and is only removed in the final exchange before the remote subscriber. This means, for example, that Caller ID can be used for billing purposes within the trusted area. This function is interesting for providers using a VoIP router to extend their own managed networks all the way to the connection for the VoIP equipment.



Please note that not all providers support this function.

Transmission method

Specifies the method used for transmitting the caller ID in the separate SIP-header field. Possible values are:

None

The default setting, so no transmission takes place.

RFC3325

Transmission according to "P-Preferred-Id/P-Asserted-Id".

IETF-Draft-Sip-Privacy-04

Transmission according to "IETF-Draft-Sip-Privacy-04" by means of RPID (Remote Party ID).

DTMF signaling

Depending on the requirements, it may not be sufficient to transmit “inband” DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Only in-band (in audio)

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

Only SIP info

The DTMF tones are transmitted “out-of-band” as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

Telephone events - fallback to in-band (default)

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

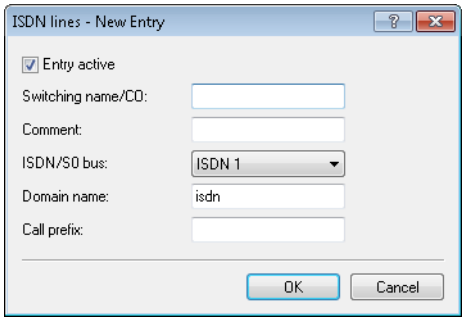
Telephone events - fallback to SIP info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

16.4.2.5 ISDN lines

The ISDN lines are configured under **Voice Call Manager** > **Lines** by clicking the button **ISDN lines**.



Entry active

Enables or disables the ISDN line.

Switching name/CO

Name of the line. May not be identical to another line that is configured in the device.

Comment

Comment on the line

ISDN/S0 bus

ISDN interface(s) with which the device is connected to the ISDN network. The line entered here are usually configured as ISDN-TE.

Domain name

Domain of the "SIP world" used by the device to manage calls from and to the ISDN line.

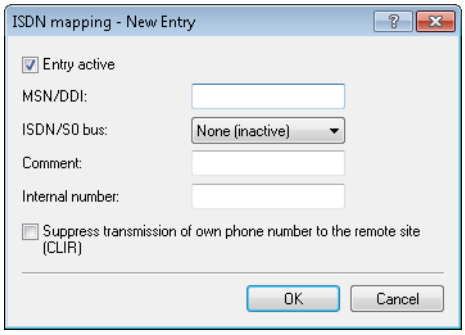
Call prefix

The device places a call-prefix number in front of the caller number (CLI; SIP "From:") for all incoming calls on this ISDN line. This generates unique telephone numbers for return calls.

For example; you add a number here, which the call router analyzes (and subsequently removes) to select the line to be used for the return call.

16.4.2.6 ISDN mapping

With ISDN mapping, you assign external ISDN telephone numbers (MSN or DDI) to the telephone numbers that are used internally. To do this navigate to **Voice Call Manager** > **Lines** and click the button **ISDN mapping**.



Entry active

Enables or disables the external telephone number.

MSN/DDI

This line's external telephone number in the ISDN network.

The device forwards incoming calls for this MSN to the internal number configured below. For outgoing calls, the device replaces its own number with the MSN configured here.

- MSN: Number of the telephone line
- DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, you can use a single entry to address entire groups of numbers, e.g. when using extension numbers

ISDN/S0 bus

ISDN interface(s) used for connecting terminal devices to the device. These line have to be configured as ISDN-NT.

Comment

Comment on the external telephone number.

Internal Number

Internal telephone number of the ISDN telephone or name of the user (SIP URL).

For incoming calls, this is the SIP name or internal telephone number of the telephone to which the call from this interface is switched with the corresponding MSN/DDI. For outgoing calls, the SIP name is replaced by the MSN/DDI of the corresponding entry.

By using the # character as a placeholder, you can use a single entry to address entire groups of numbers, e.g. when using extension numbers.

Hide your telephone number from the person being called (CLIR)

When enabled, the device does not reveal your telephone number to the called party.

16.4.3 Configuration of users

Local users are the terminal devices that are connected to the VoIP device. Users are categorized as follows:

SIP users

Users who are connected to the LAN by means of SIP. For the configuration of the user, it is unimportant if the LAN is accessed locally or via VPN (via the Internet). Along with SIP phones, you have also the option of setting up a SIP PBX as a user (internal SIP trunk connection).

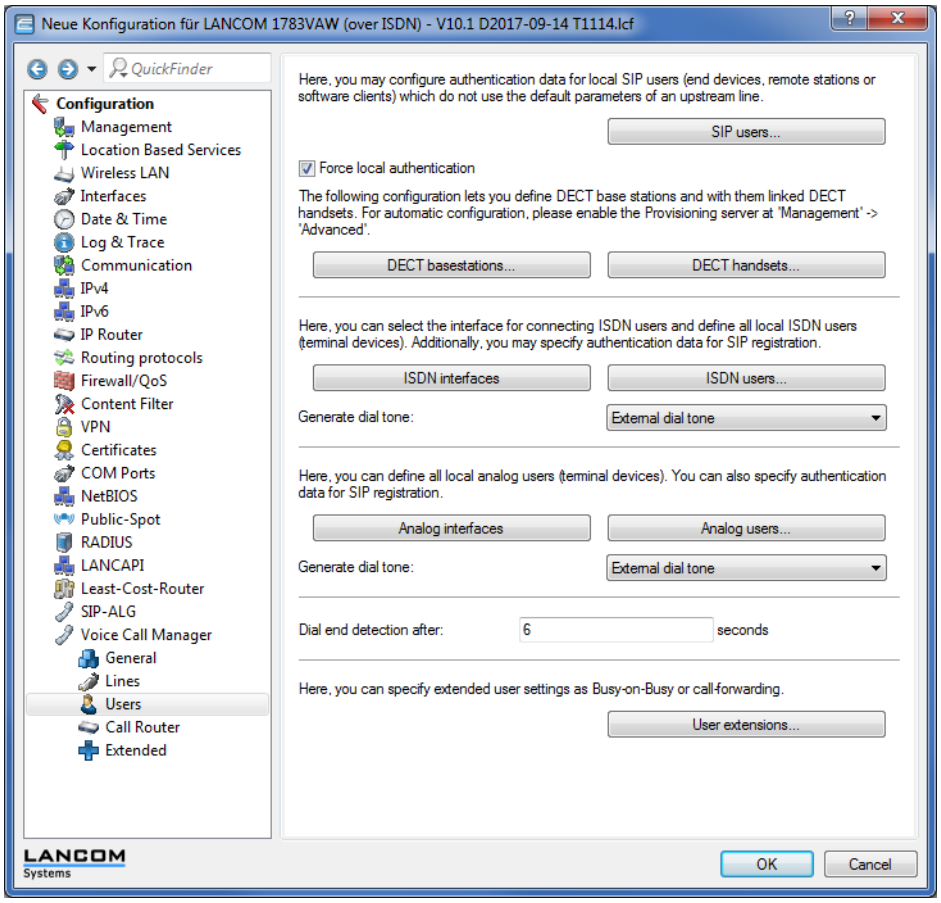
ISDN users

Users who are connected by ISDN. These users use the SIP gateway to telephone using the VoIP function.

Analog users

Users who are connected via analog interfaces. These users use the SIP gateway to telephone using the VoIP function.

Users are configured with LANconfig under **Voice Call Manager** > **Users**.



16.4.3.1 SIP users

The SIP proxy usually accepts a registration from all SIP users who register themselves with a valid domain and are known to the system as a SIP user. If under **Voice Call Manager** > **Users** in the section **SIP users** you enable the option **Force local authentication**, the only subscribers who can register at the SIP proxy are those stored in a user table with the appropriate access data.

Automatic registration without entering a password is restricted to the SIP users in the LAN. SIP users from the WAN, as well as ISDN and analog users, are required to authenticate themselves by using the password in their corresponding user entry.

The button **SIP users** opens the dialog for configuring the authentication data of the SIP users (terminal equipment, remote stations or software clients) that do not use the default parameters of an upstream SIP PBX line.

Depending on the model you can create different numbers of SIP users, whereby identical names or identical numbers are not permitted.

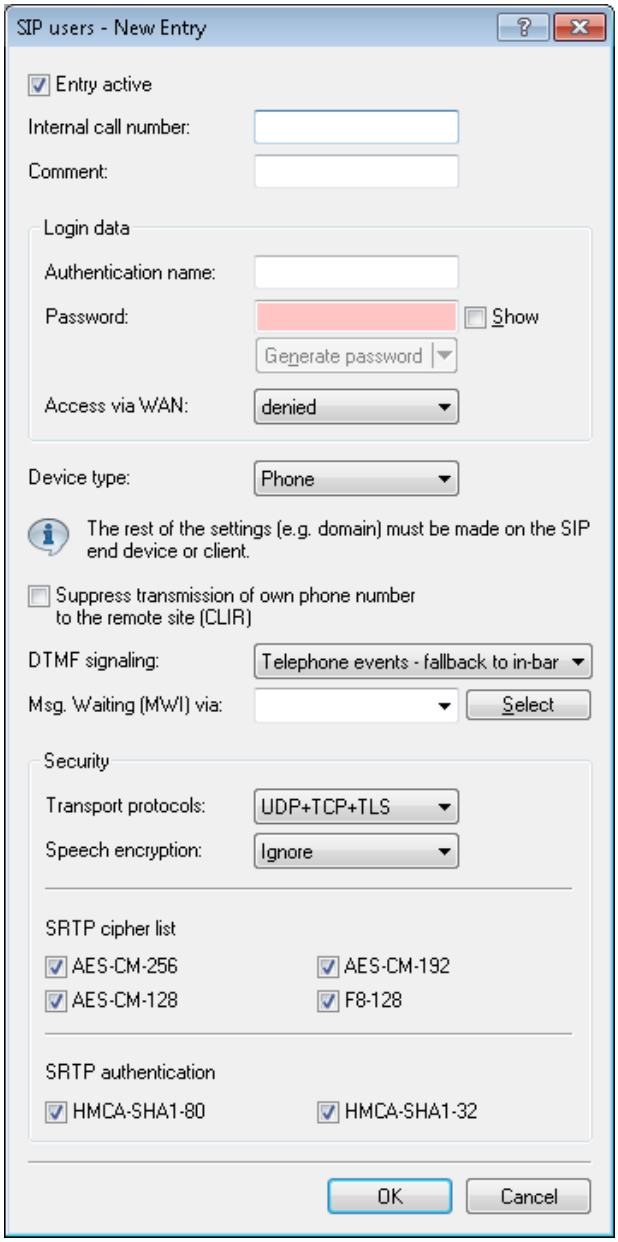


Figure 29: Adding a new entry to the SIP user table

The domain that is used by the SIP subscriber is usually configured in the terminal equipment itself.

Entry active

Activates or deactivates this entry.

Internal telephone number

- Telephone number of the SIP phone
- Name of the user (SIP URI)

- Switchboard number of the SIP PBX, followed by a `#`. Your SIP PBX must be in the same network as your device, either locally or connected via VPN (internal SIP trunk connection).

Comment

Comment about this SIP user.

Authentication name

Name for authentication at the SIP proxy, and also to any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. This name is required if registration is mandatory (e.g. when logging in to an upstream SIP PBX or when **Force local authentication** is set for local users).

Password

Password for authentication to the SIP proxy, and also to any upstream SIP PBX, when the user's domain is the same as the domain of a SIP PBX line. It is possible for users to log in to the local SIP proxy without authentication (**Force local authentication** is deactivated for SIP users) and where applicable to an upstream SIP PBX using a shared password (**Standard password** on the SIP PBX line).

Access from WAN

Permission for SIP users to authenticate via a WAN connection. Possible values are:

- Denied (default)
- Only via VPN

Device type

Specify what type of device is used by the SIP user.

Hide your telephone number from the person being called

Switches the transmission of the calling-line identifier on/off.

DTMF signaling

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

Only in-band (in audio)

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

Only SIP info

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters `Signal` and `Duration` (as per RFC 2976). There is no parallel transmission of G.711 tones.

Telephone events - fallback to in-band (default)

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to inband transfer as per G.711.

Telephone events - fallback to SIP info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include `telephone-event` signaling, negotiations fallback to transfer as per SIP-Info message.

Msg. Waiting (MWI) via

The presence of voice messages left on your provider's online mailbox are signaled by notifications on the device. Signaling occurs in different ways depending on the terminal type. Select the line for which this function should be enabled from the list of configured SIP lines under **Voice Call Manager** > **Lines** > **SIP users**.

Notification only occurs if the provider supports this function.

Transport protocols

Select a protocol used by this user to communicate with the local SIP server. If the appropriate protocol is not selected, SIP requests from this user will be rejected with a SIP error response (SIP/406). This ensures that no users are able to register with a protocol that has not been allowed here.

UDP

All SIP packets to this SIP user are transmitted via connectionless UDP. Most SIP users support this setting.

TCP

All SIP packets to this SIP user are transmitted via connection-oriented TCP. The TCP connection is maintained for the duration of the registration.

TLS

All SIP packets to this SIP user are transmitted connection-oriented. Also, all SIP packets are encrypted.

Speech encryption

Use this entry to specify the protocol used to transmit the voice data (RTP/SRTP) of a call to the local SIP server.

Reject

There is no encryption proposal for calls by this user. Calls by this user with an encryption proposal are rejected. The voice channel is never encrypted.

Ignore

There is no encryption proposal for calls by this user. However, calls from this user with an encryption proposal are accepted. However, the voice channel is never encrypted.

Prefer

Calls by this user cause an encryption proposal. Calls from this user without an encryption proposal are also accepted. The voice channel is only encrypted if the user supports encryption.

Force

Calls by this user cause an encryption proposal. Calls by this user without a corresponding encryption proposal are ignored. The speech channel is either encrypted or is not established.

If you require the encrypted transmission of voice data, the signaling must also use an encrypted channel. Otherwise an attack on the unsecured signaling could potentially expose the key for the voice data. Please be aware that your provider may decrypt your voice data and re-transmit it newly encrypted or even unencrypted. The use of SRTP is no guarantee of end-to-end encryption.

SRTP cipher list

Here you specify the encryption method used for communication with the user. Select one or more of the following methods:

AES-CM-256

Encryption is performed using AES256. The key length is 256 bits.

AES-CM-128

Encryption is performed using AES128. The key length is 128 bits.

AES-CM-192

Encryption is performed using AES192. The key length is 192 bits.

F8-128

Encryption is performed using F8-128. The key length is 128 bits.

SRTP authentication

With this setting you restrict the amount of (proposed or accepted) SRTP suites that are negotiated with the corresponding user. If you do not select one or more of the ciphers shown below for encrypting the SRTP packets, the device will never propose the corresponding SRTP suite(s) and they are never selected. In this way you can force the best possible encryption.

HMAC-SHA1-80

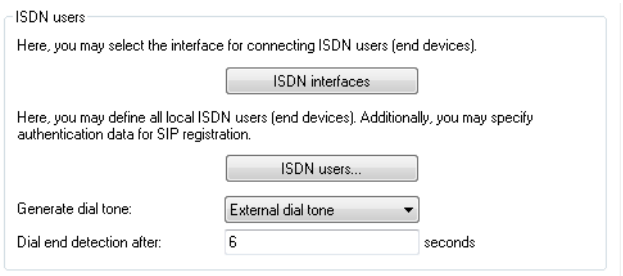
SIP-user authentication is performed with the hash algorithm HMAC-SHA1-80. The hash length is 80 bits.

HMAC-SHA1-32

SIP-user authentication is performed with the hash algorithm HMAC-SHA1-32. The hash length is 32 bits.

16.4.3.2 General settings for all ISDN users

Under **Voice Call Manager** > **Users** you configure the general settings for all ISDN users in the section **ISDN users**.



Generate dial tone

The dial tone determines the noise an ISDN user hears after lifting up the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone for the users with spontaneous outside-line access to simulate the behavior of a standard outside line.

End dial detection after

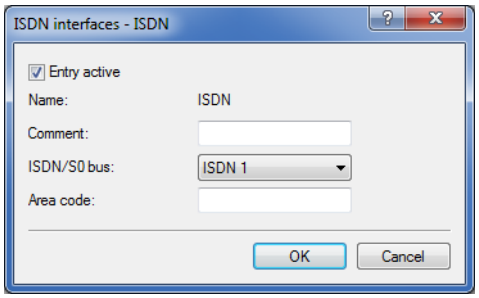
During dialing, this is the time in seconds taken by the device to wait for further digits, after which it takes a number to be complete and sends it to SIP.

If the entry is '0', ISDN users need to suffix the number with the '#' character.

The '#' sign also services to shorten the delay configured here.

16.4.3.3 ISDN interfaces

Click on the **ISDN interfaces** button to adjust the global settings for the interfaces used by the ISDN users. An ISDN T interface (external) or even an ISDN TE interface (internal) can be configured. The latter is the case if users of an upstream PBX are to be managed as local users.



Entry active

Activates or deactivates this entry.

Name

Interface to which the ISDN subscribers are connected.

Comment

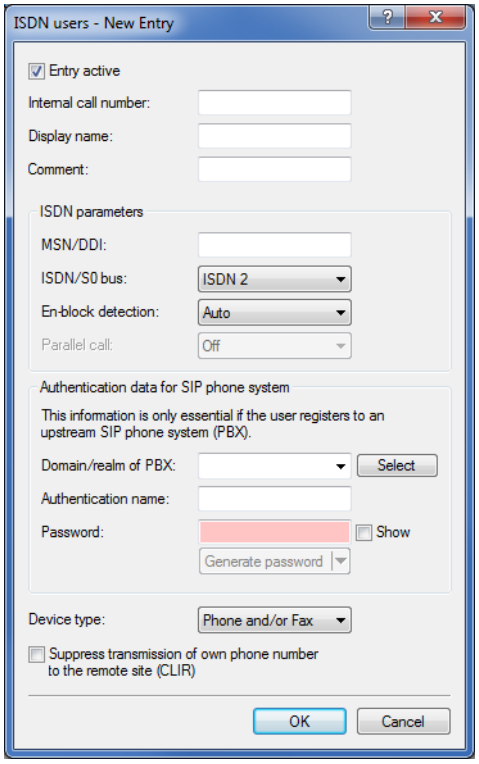
Comment on this entry.

ISDN/S0 bus

Interfaces for the ISDN users to establish a connection.

16.4.3.4 ISDN users

The ISDN user settings are configured by clicking on the button **ISDN users**.



Entry active

Activates or deactivates this entry.

Internal telephone number

Internal number of the ISDN telephone or name of the user (SIP URI).

By using the # character as a placeholder, you can use a single entry to address entire groups of numbers, e.g. when using extension numbers at a point-to-point connection.

User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

Display name

Name for display on the telephone being called.

Comment

Comment on this entry.

MSN/DDI

Internal MSN that is used for this user on the internal ISDN bus.

- MSN: Number of the telephone connection if it is a point-to-multipoint connection.
- DDI (Direct Dialing in): Telephone extension number if the connection is configured as a point-to-point line.

By using the # character as a placeholder, you can use a single entry to address entire groups of numbers, e.g. when using extension numbers at a point-to-point connection.



User entries that use # characters to map user groups cannot be used for registration at an upstream PBX. This registration always demands a specific entry for the individual ISDN user.

ISDN/S0 bus

ISDN interface for the users to establish a connection.

En-bloc detection

With en-bloc dialing the device automatically detects that the dialed number is complete. A result of this is that the device places a call if it recognizes a group of digits as a contiguous block (e.g. for speed dialing). However, redialing is not an option.

Parallel call

If you use this feature, signaling occurs on all selected both ISDN lines. The call is accepted at the first telephone to pick up the call.

Domain/realm of PBX

Domain of an upstream SIP PBX when the ISDN user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

Authentication name

Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

Password

Password for authentication as a SIP user at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password (**Standard password** on the SIP PBX line).

Device type

Type of device connected.

Hide your telephone number from the person being called (CLIR)

Switches the transmission of the calling-line identifier on/off.

16.4.3.5 General settings for all analog users

LANconfig: **Voice Call Manager** > **Users**

Generate dial tone

The dial tone determines the noise an analog user hears after lifting up the receiver. The "internal dial tone" is the same as the tone that a user hears at a PBX without spontaneous outside-line access (three short tones followed by a pause). The "external dial tone" is thus the same as the tone that indicates an external line when the receiver is lifted (constant tone without any interruptions). If necessary, adapt the dial tone for the users with spontaneous outside-line access to simulate the behavior of a standard outside line.

Analog interfaces

The internal analog interfaces (a/b ports) require configuration if they are to be used by local users (connection of terminal equipment).

LANconfig: **Voice Call Manager** > **Users** > **Analog interfaces**

Interface

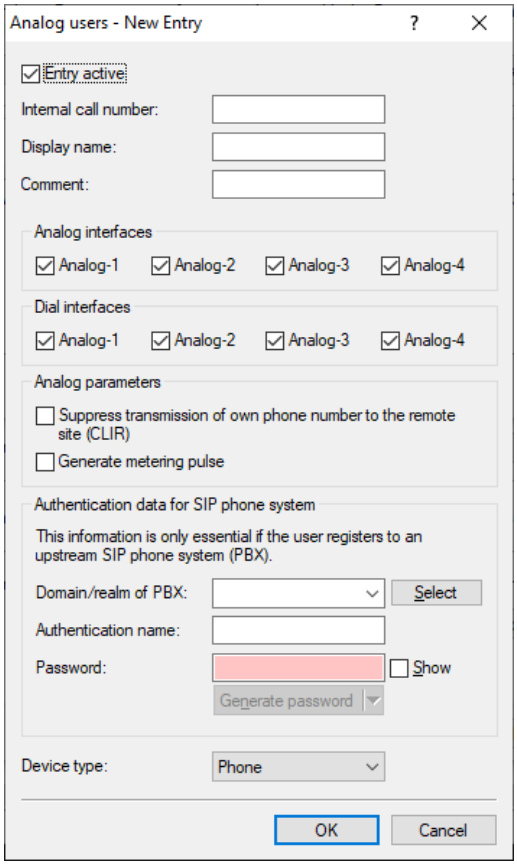
An internal interface to which the analog subscribers are connected.

Entry active

Interface is active / not active.

Analog users

LANconfig: **Voice Call Manager** > **Users** > **Analog Users**



Entry active

Activates or deactivates the entry.

Internal call number

Internal number of the analog telephone or name of the user (SIP URI).

Display name

Name for display on the telephone being called.

Comment

Comment on this entry.

Analog interfaces

Select the Analog interfaces which should be alerted when a call is made to the **Internal call number**.

Dial interfaces

Select an Analog interface. A telephone connected to this interface uses the **Internal call number** as a source number when it makes a call.

Suppress transmission of own phone number to the remote site (CLIR)

Switches the transmission of the calling-line identifier on/off.

Generate metering pulse

The metering pulse is used in analog telephone networks to inform callers of the costs of their calls. With appropriate terminal equipment (e.g. telephone with charge display), the metering pulse is filtered out from the overall signal and this information is converted to display the call charge.

This option allows the metering pulse to be passed on to the analog user/equipment. It is possible for charge information from the ISDN telephone network to be transferred to an ISDN line and converted into an analog metering pulse.

Domain/realm of PBX

Domain of an upstream SIP PBX when the analog user is to be logged in as a SIP user. The domain must be configured for a SIP PBX line in order for upstream login to be performed.

Authentication name

Name for authentication at any upstream SIP PBX when the user's domain is the same as the domain of a SIP PBX line.

Password

Password for authentication as a SIP user to any upstream SIP PBX when the analog user's domain is the same as the domain of a SIP PBX line. It is possible for ISDN users to log in to an upstream SIP PBX using a shared password ("Standard password" on the SIP PBX line).

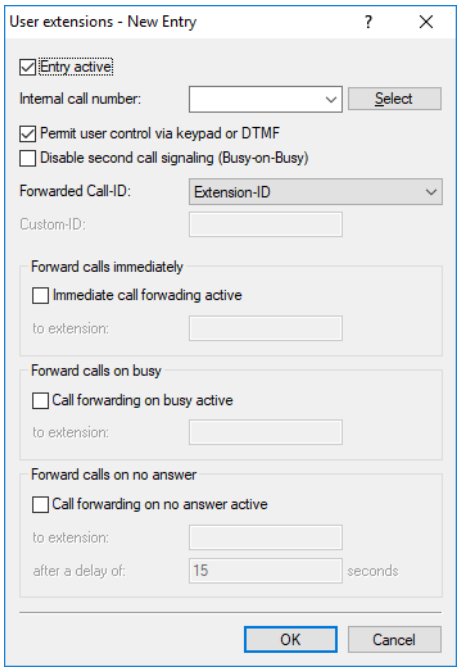
Device type

Type of device connected.

The type determines whether an analog connection should be converted into SIP T.38, where applicable. Selecting "Fax" or "Telephone/Fax" activates fax signal recognition that could result in an impairment of the connection quality for telephones. Therefore please select the corresponding type of device connected in order to ensure optimum quality.

16.4.3.6 Extended user settings

Advanced user settings such as call waiting or call forwarding are configured here by clicking on the button **User extensions**.



Entry active

Activates or deactivates this entry.

Internal telephone number

The call forwarding applies to this telephone number or SIP-ID.

Call forwarding can be set up for all local users (SIP, ISDN or analog).

Permit user control via keypad or DTMF

This activates or deactivates the option for users to configure their settings via the telephone.

Double second call signaling (Busy on busy)

Prevents a second call from being connected to a terminal device, irrespective of whether "CW" (call-waiting indication) is active on the device or not; i.e. there is no "call waiting" signal. The second caller hears an engaged tone. This also applies where an internal telephone number supports multiple logins and just one of the possible terminal devices is already in use.

Forwarded Call ID

Setting the signalled phone number. Possible values:

Extension ID

Signals the phone number that is forwarding the call.

Calling ID

Signals the incoming phone number. When forwarding to a mobile phone, a subscriber can recognize the original phone number of the calling subscriber.

Custom ID

Signals the phone number entered in the field **Custom ID**.

Call-forwarding unconditional (CFU)

Activates or deactivates the immediate forwarding of calls (CFU).

to extension

Destination for immediate unconditional call forwarding.

Forward calls on busy

Activates or deactivates call forwarding on "busy".

to extension

Destination for call forwarding on "busy".

Forward calls on no reply

Activates or deactivates the delayed forwarding of call (after waiting for no reply).

to number

Destination for call forwarding no reply.

After a delay of

Wait time for call forwarding on no reply. After this time period the call is forwarded to the destination number if the subscriber does not pick up the phone.

16.5 Call Manager Configuration

The Call Manager manages and connects the various subscribers and lines described above with one another. The Call Manager's main task is to determine the correct target subscriber for each call and to select a suitable line for this subscriber. To fulfill this task, the Call Manager mainly uses two table areas:

- The Call Routing table
- The tables of local subscribers

As the Call Manager usually switches between internal and external telephone networks with different number ranges, the Call Manager often has to modify the numbers that are dialed. This is known as number translation.

In the world of VoIP telephony it is possible to call numbers and names, such as "anyone@company.com". Although the following description refers to telephone numbers, this also includes telephone names unless specified otherwise.

The procedure known from internal extension lines is used, whereby connections to external subscribers start with a preceding '0'. The Call Manager processes calls to and from all registered subscribers and lines.

16.5.1 Process of call routing

The calls are switched in the following steps:

- Processing the calling number (Calling Party ID)

  First of all there is a check to see whether a numeric or alphanumeric number is available. Typical dialing separators such as "()-/" and <blank> are removed. A leading "+" is left in place. In this case, the number is still treated as a numeric number. If the check reveals any other alphanumerical character, the number is treated as alphanumeric and remains unchanged.

- Resolving the call in the call routing table

  After processing the Called Party ID, the call is passed over to the call-routing table. Entries in the call-routing table consist of sets of conditions and instructions. The entries are searched through and the first one that satisfies **all** of the conditions is executed.

- Resolution of the call with tables of local subscribers

  If no entry is found in the call-routing table, then the Call Manager searches through the list of local subscribers. If an entry is found here matching the number that is called, and that also has the appropriate destination domain, then the call is delivered to the corresponding subscriber.

  If no local subscriber is found for whom the number and destination domain match, another pass is made where it suffices for the telephone number of the local subscriber to match the called number; the destination domain is not considered.

- Resolution of the call with default entries in the call-routing table

  If the previous passes through the call routing table and the lists with the local subscribers were unsuccessful, the call is checked again in the call routing table. This pass only takes the default routes into account, however. It does not include the numbers and destination domains that were entered in the default routes. Only the source filters are processed, assuming that the default route has these filters.

  The procedure described here only considers the call numbers as processed by the Call Router. Mapping to the ISDN or SIP line can also alter the number.

16.5.2 Handling the calling party ID

The configuration options for the call router offer numerous options for manipulating the telephone numbers that are used to establish the connection. The call router usually connects different "telephone worlds" (internal and external,

SIP and ISDN) that use completely different telephone number ranges. In order for the subscribers to communicate successfully with one another, the telephone numbers at the interfaces need to be configured in such a way that, on the one hand, the required subscriber is reached via the correct line and, on the other hand, a return call can be placed successfully (automatically upon "busy", if need be). To enable this return call, the calling number (calling party ID) has to be modified **after** processing by the Call Manager and directly before it is delivered to the relevant subscriber.

16.5.2.1 Handling outgoing calls

The telephone numbers of outgoing calls are translated depending on the line that is used:

SIP lines

The treatment of the calling-party ID on SIP lines depends upon the line's operating mode:

- Individual account: In the case of an outgoing call over a SIP line, the calling party ID is converted to the number that was entered for the SIP line (SIP ID).
- Trunk and gateway: Please observe the information in section SIP mapping.

SIP PBX lines

In the case of an outgoing call over a SIP PBX line, the subscriber is registered at the upstream SIP PBX and is part of the telephone number range there. This is why the calling party ID—which represents the internal telephone number or "extension" of the subscriber in this case—is passed unchanged to the SIP PBX line.

ISDN lines

In the case of an outgoing call over an ISDN point-to-multipoint connection, the calling party ID is converted to the MSN that is entered for the subscriber (or the internal telephone number) in the ISDN mapping table.

If this does not contain an entry for the number that is currently calling, no calling party ID is sent. Similarly, no calling party ID is sent if CLIR (Calling Line Identifier Restriction) is activated.

16.5.2.2 Handling incoming calls

The telephone numbers of incoming calls are translated differently depending on the SIP or ISDN subscriber criteria and whether automatic outside line access is active or not.

The calling party ID is changed depending on the following parameters:

- The prefix ("call prefix" or "Cln-Prefix") that is stored for the **line** (default: <blank>).
- The prefix for internal connections with destination ISDN users ("internal ISDN prefix" or "Intern-Cln-Prefix" - default: '99').
- The prefix for internal connections with destination SIP users ("internal SIP prefix" or "Intern-Cln-Prefix" - default: '99').
- The prefix for external connections with destination ISDN users ("external ISDN prefix" or "Extern-Cln-Prefix" - default: <blank>).
- The prefix for external connections with destination SIP users ("external SIP prefix" or "Extern-Cln-Prefix" - default: <blank>).

The activation of automatic outside line access is taken into account by configuring the prefixes appropriately:

- If automatic outside line access is activated, the internal prefixes are typically set to the dial character that is used to reach the internal subscriber, usually '99' or '*'.
- Without automatic outside line access, the external prefixes are typically set to '0'.

The calling party ID is only supplemented if the incoming call has a calling party ID. If the calling party ID is blank, no prefix is attached.

It is modified as follows:

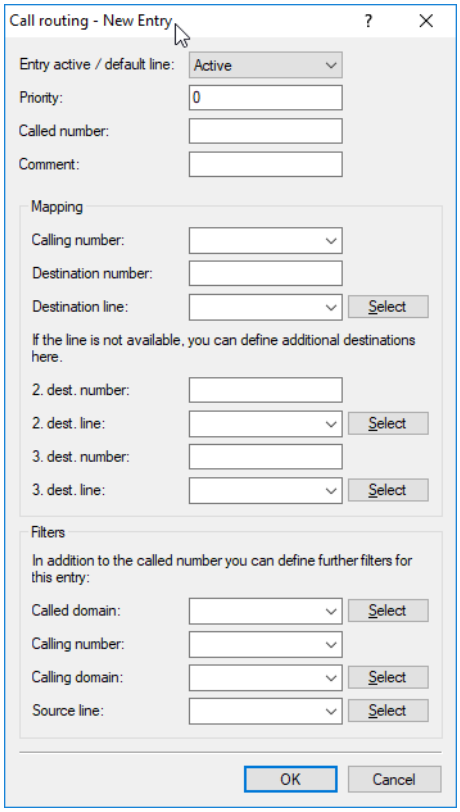
- With internal connections, the internal subscriber prefix (SIP or ISDN) is placed in front of the calling party ID.
- With external connections, depending on the (line) call prefix, the following decision is made:

- (Line) call prefix blank: The external subscriber prefix (SIP or ISDN) is placed in front of the calling party ID.
- (Line) call prefix not blank: The internal subscriber prefix (SIP or ISDN) and the (line) call prefix is placed in front the calling party ID.

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a '0'.

16.5.3 Call-routing table parameters

You configure the call-routing table entries in the LANconfig under **Voice Call Manager** > **Call router** by clicking on the button **Call routing**.



An entry in the call routing table consists of:

- Conditions that have to be met so that the entry is "considered" appropriate. These include:
  - Information about which subscriber is to be called; called number/name (Called Party ID), called domain (if applicable).
  - Information about the calling subscriber; calling number/name, calling domain, source line through which the call reaches the LANCOM VoIP router.
- Instructions regarding the procedure for the call:
  - How is the telephone number translated and modified for further processing?
  - Which line should be used to place the call (destination line)?
  - Which backup lines should be used if the destination line is not available?

The entries are searched row by row; the first suitable entry is performed. For this reason the special entries should be configured first of all, followed by the general entries.

If an entry is found in the call routing table with the destination line "RESTART", then the entire pass starts again with the new, translated called party ID. The entry for the source line (calling line) is deleted for the next pass.

Both the call routing table and the local subscriber table may contain and process alphanumeric names where this makes sense.

Active entry/default line

The routing entry can be activated, deactivated, or marked as a default entry. All calls that can be resolved using the first passes but not using the call routing table or local subscriber table are then automatically resolved using these default entries. You can use any destination name and destination domain; only any source filters that you have set will be processed.

Priority

The Call Manager sorts all entries with the same priority automatically, so that the table can be processed through logically from top to bottom. With some entries, however, the sequence of the entries has to be specified (for the telephone number translation, for example). The entries with the highest priority are automatically sorted to the top.

Called number

The called party name or destination telephone number (without domain information) that is called.

The # character is used as a placeholder for any character strings. All characters in front of the '#' are removed, the remaining characters are used in the "Number/name" field instead of the # character to further establish the connection.

Example: The call routing table contains entry '00049#' as the called number/name and '00#' as the number/name. For all calls with a preceding '0' for outside-line access and the complete dialing code for Germany, only the leading '0' for the outside-line access and the leading '0' for the local area dialing code are retained as the number/name; the country ID is removed. So '00049 2405 123456' becomes '0 02405 123456'.

Independently of this, an alphanumeric number can also be specified.

Comment

Comment on the current routing entry

Calling number

If the calling number is to be replaced by another number in the call route, the desired number must be entered in this field. If the special value "EMPTY" is selected and the filter field **Calling number** is filled with any character (e.g. wildcard #) at the same time, a number suppression for outgoing calls can be configured for the call route.

Destination number

This telephone number is used to continue with establishing the connection. If no connection can be established using this telephone number and the corresponding line, then the backup telephone numbers with their associated lines are used

At least one of the fields **Destination number**, **2nd dest. number** or **3rd dest. number** must have content. They are evaluated in this sequence. A blank field is skipped.

Destination line

The connection is established using the destination line. Normal destination lines can be:

- ISDN
- All defined SIP lines.

The following special functions can be entered as a destination line:

- REJECT highlights a blocked telephone number.

This value also allows you to *prohibit control characters on SIP lines*.

- USER forwards the call to local SIP or ISDN subscribers.
- RESTART begins a new pass through the call-routing table with the previously formed **Destination number**. The former **Source line** is deleted.

This field has to be completed, otherwise the entry is not used.

2nd Destination number, 3rd Destination number

This telephone number is called if nothing is entered in **Destination number** or the corresponding "line" is not available. If the 2nd destination number and the corresponding 2nd destination line are not available, then the 3rd destination number and the corresponding 3rd destination line will be used instead.

Called domain

This entry filters the called domain, the "Called Party Domain". The call router entry is only considered to match if the Called Party Domain for the call matches the domain that is entered here. If nothing is specified, any destination domain is accepted.

The following can be entered as called domains:

- ISDN
- The internal VoIP domains of the LANCOM VoIP router.
- All domains entered for the SIP and SIP-PBX lines.

Calling number

This entry filters the calling number/name, the "calling party ID". It is specified as an internal number or as a national or international telephone number. The domain is not specified. No '0' or other character for a line ID is prefixed; the ID is used as if it comes from the line or from internal telephone calls.

The call router entry is only evaluated as matching if the Calling Party ID for the call matches the number that is entered here. After '#', any characters can be accepted. If nothing is specified here, any Calling Party ID is accepted.

The following special functions can be entered as a calling number:

- EMPTY can be used for Calling Party IDs that are not specified.

Calling domain

This entry filters the "calling domain". The call router entry is only considered to match if the Calling Domain for the call matches the domain that is entered here. If nothing is specified, each calling domain is accepted.

The following can be entered as calling domains:

- ISDN
- The internal VoIP domains of the LANCOM VoIP router.
- All domains entered for the SIP and SIP-PBX lines.

SIP telephones usually have several line keys, for which different domains can be configured. With this filter, telephone calls are handled depending on the selection that is made using different line keys.

Source line

This entry filters the source line. The call router entry is only considered to match if the source line for the call matches the line that is entered here. If nothing is specified, any calling line is accepted.

The following can be entered as the source line:

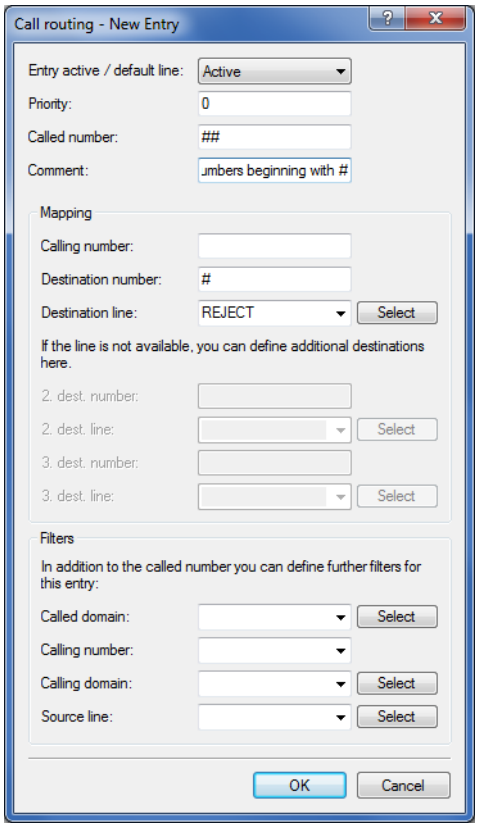
- USER.ISDN for calls from a local ISDN subscriber

- USER.SIP for calls from a local SIP subscriber
- USER # for calls from a local subscriber in general
- All ISDN, SIP and SIP-PBX lines that are entered.

16.5.3.1 Prohibit control characters on SIP lines

This prevents the dialing of control characters. Control codes can, for example, be used to configure call forwarding. You can prevent this for any particular lines or persons. For example, proceed as follows to reject the character '#':

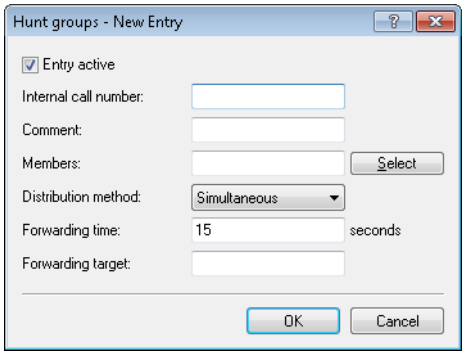
1. Under **Called number:** enter ##.
2. Under **Destination number:** enter #.
3. For the **Destination line** select REJECT.
4. Enter a **Comment:**, e.g. "No numbers beginning with #".



5. Confirm your settings by clicking the **OK** button.

16.5.3.2 Group call functions

You configure the call-routing table entries in LANconfig under **Voice Call Manager** > **Call router** by clicking on the button **Call routing**.



Entry active

Activates or deactivates the entry.

Internal telephone number

The hunt group is available under this telephone number or SIP-ID (max. 64 alphanumerical characters).

The names of hunt groups may not coincide with the names of users (SIP, ISDN, analog).

Comment

Comment about this entry (64 characters)

Members

Comma-separated list of the members of the hunt group. Members can be users, hunt groups or external telephone numbers, and so there is no limit on scaling.

- Possible members: Users, hunt groups, external telephone numbers
- Possible values: Maximum 128 alphanumerical characters.

A hunt group may not contain itself or any parents in the hierarchical system—recursion through member entries is not possible. However, loops to parents in the structure may result from the "forwarding target".

Call distribution

Sets the type of call distribution:

- Simultaneous: The call is signaled to all group members at once. If a member picks up the call within the call-forwarding time, the call is no longer signaled to other group members. If nobody accepts the call within the forwarding time, then the call is switched to its forwarding destination.
- Sequential: The call is directed to one member of the group after the other. If a group member does not accept the call within the forwarding time, then the call is switched to the next member of the group. If nobody in the group accepts the call within the forwarding time, then the call is switched to its forwarding destination.

Forwarding time

If an incoming call is not picked up by a group member within the forwarding time, then the call is forwarded according to the distribution method selected:

- In the case of simultaneous call distribution, the call is forwarded to the forwarding destination.

- In case of sequential call distribution, the call is forwarded to the next group member in line. If the group member is the last one in the sequence, then the call is redirected to its forwarding destination.
- Possible values: Max. 255 seconds.
- Default: 0 seconds
- Significant values: 0 seconds. The call is forwarded immediately to the forwarding destination (temporarily jumps a hunt group in a hierarchy).

If all members of the group are busy or unavailable, then the call is redirected to the forwarding destination without waiting for the forwarding-time to expire.

Forwarding destination

If none of the group members accepts the call within the forwarding time, then the call is switched to the forwarding destination entered here. Forwarding destinations can be users, hunt groups or external telephone numbers. Only one forwarding destination can be entered.

- Possible destinations: Users, hunt groups, external telephone numbers
- Possible values: Maximum 64 alphanumerical characters.

If no forwarding destination is defined, then the call is rejected as soon as the member list has been worked through, or if all members are busy or unavailable.

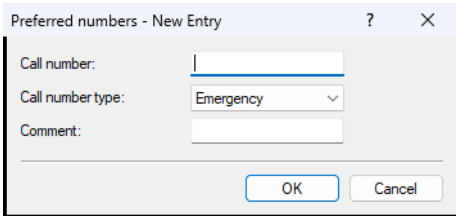
The forwarding destination only becomes active once the group's forwarding time has expired or if no members are available. Here, too, redirection to a higher level of the hunt-group structure is possible, unlike with the "Members" entry.

16.5.3.3 Preferred numbers

Enter emergency phone numbers in this table. If a call to an emergency number cannot be established due to an error message from the SIP provider, an existing call that is using this line (line type Trunk/Flex) or the associated line group (line type Single Account/Provider) will be terminated. This ensures that a voice channel is available for the emergency call.

A line group is defined in the “Dynamic SIP Lines” table. SIP lines with the same “Dynamic-Line-Name” belong to the same group. Typically, these are multiple individual numbers that together provide a certain number of voice channels.

You configure the entries in the table for preferred numbers in LANconfig under **Voice Call Manager** > **Call Router** by clicking the **Preferred numbers** button.



Call number

Enter your call number here.

Call number type

Enter the call number type here.

Emergency

This is an emergency call number.

Private

These call numbers suppress the overlap dialing wait time for this destination.

Comment

Enter a comment for the selected call number here.

16.5.4 Signaling parallel calls in the ISDN

LANCOM business VoIP routers are able to make parallel calls. If you use this feature, signaling occurs on both ISDN lines (ISDN 1 & ISDN 2). The call is accepted at the first telephone to pick up the call.

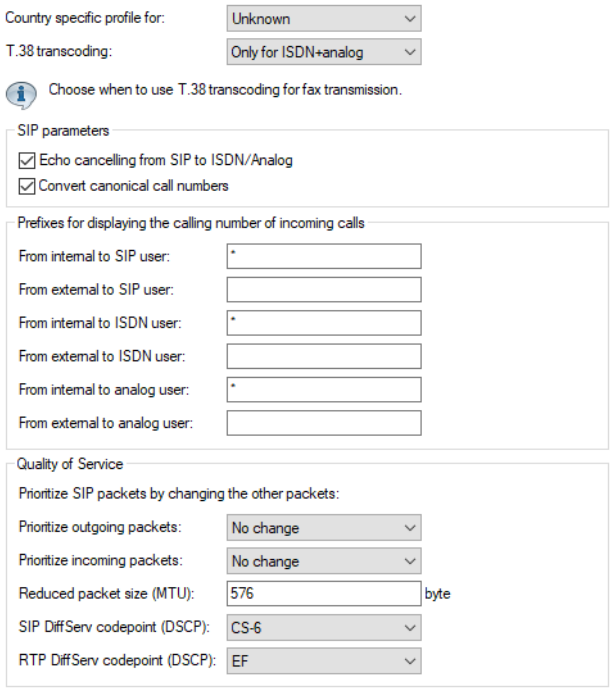
To enable parallel calls, navigate to **Voice call Manager** > **Users** > **ISDN users**.



In the **ISDN parameters** section and under **ISDN/S0 bus**, select the option “ISDN 1 & ISDN 2” and then set the item **Parallel call** to “On”.

16.5.5 Extended settings

To configure the advanced settings for the VoIP Call Manager, navigate to **Voice Call Manager** > **Extended**.



Country specific profile for

This allows you to select a profile for a specific country, which provides the default input values.

Echo canceling from SIP to ISDN

Activates the echo canceling of remote echoes. With an echo that is too strong, subscribers can hear their own voices after a short delay. Activating this option reduces the ISDN echo at the SIP ISDN gateway.

Prefix from internal to SIP user

If an incoming **internal** call is directed to a SIP user, this prefix is added to the calling party ID, if available.

A call is regarded as external if it comes from a "line". If this line is a SIP PBX line, then the call is only external if the incoming calling party ID is preceded by a '0'. All other calls are regarded as internal.

Prefix from external to SIP user

If an incoming **external** call is directed to a SIP user, this prefix is added to the calling party ID, if available.

Prefix from internal to ISDN user

If an incoming **internal** call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Prefix from external to ISDN user

If an incoming **external** call is directed to an ISDN user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Prefix from internal to analog user

This prefix is added to the calling party ID, if available, for an incoming, **internal** call if the call is directed to a analog user. If a line prefix is defined, this is placed in front of the whole of the called number.

Prefix from external to analog user

If an incoming **external** call is directed to an analog user, this prefix is added to the calling party ID, if available. If a line prefix is defined, this is placed in front of the whole of the called number.

Prefer outgoing packets

For all SIP calls, sufficient bandwidth through the firewall is reserved as required by the audio codec being used (provided sufficient bandwidth is available). To control the firewall, you can configure how the remaining data packets that do not belong to the SIP data stream are handled. The following values are possible:

- PMTU reduction

  The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).

- Fragmentation

  The LANCOM wireless router reduces the data packets by fragmenting them to the required length.

- No change (Default)

  The length of the data packets is not changed by the VoIP operation.

For more information, see the description of PMTU and fragmenting with regard to quality of service.

Prefer incoming packets

Similar to the outgoing data packets, you configure how non-VoIP data packets are handled when bandwidth is reserved for SIP data. The following values are possible:

- PMTU reduction

  The subscribers of the data connection are informed that they should only send data packets up to a certain length (Path Maximum Transmission Unit, PMTU).

- No change

  The length of the data packets is not changed by the VoIP operation.

Reduced packet size

This parameter specifies the packet size that should be used for PMTU adjustment or fragmentation while the SIP data have priority.

SIP-DiffServ-CodePoint (DSCP), RTP-DiffServ-CodePoint (DSCP)

The Voice Call Manager marks SIP and RTP packets with DiffServ CodePoints (DSCP), which enables other hardware to recognize and prioritize these packets.

By default, SIP packets (call signaling) are marked with 'CS-1' and RTP packets (voice data stream) are marked with 'EF'. Here you have option to change this behavior. With the setting 'DSCP BE' or 'CS-0' the packets are sent unmarked. Further information on the DiffServ-CodePoints is available in the section *Quality of Service*.



The option 'CS-1' for SIP DSCP is actually outdated now, but it is the default value to ensure backwards compatibility. Common values for modern VoIP installations are 'CS-3', 'AF-31' or 'AF-41'. We recommend using 'CS-3', one of the most widespread settings on the market for use with SIP DSCP.

16.6 Telephony (PBX) functions in LANCOM VoIP routers

A LANCOM VoIP router provides telephony functions for small companies and company branch offices:

- Telephony functions such as call hold, swap, transfer or redirect

- Hunt group function with flexible call distribution and cascading of hunt groups
- Multiple logins to use various telephones under one telephone number

Please note that the extent to which features such as connect call and automatic call forwarding (redirection) are supported by SIP providers can differ greatly. It is impossible to guarantee that this function will work properly with all combinations of SIP devices and SIP providers.

16.6.1 Transfer and forward call

The integration of SIP telephones and VoIP routers into existing telephone structures means that we have to take a fresh look at familiar functions such as forwarding calls. Call forwarding means that a call that has already been placed (routed) is redirected to a new destination either spontaneously by the user (connect call) or by automatic call forwarding set up in advance. SIP-based VoIP telephony uses processes which are fundamentally different to previous technologies. For example, ISDN and analog terminal devices require a telephone exchange that usually has to continue to manage the connection after forwarding. SIP telephones can forward calls without any need of a telephone exchange: The devices make a connection over the shortest possible route and the call router stops its management function immediately after the connection has been established. The SIP exchange is also able to handle signaling over SIP and the actual data transfer over RTP in different ways.

Due to the differences arising from the various types of terminal device, the easiest way to understand call forwarding in a LANCOM VoIP router is to consider different scenarios and to explain the terminology.

16.6.1.1 Active and passive forwarding

When looking at the technical details, it is important to consider the end from which call forwarding is initiated. "Local" users are all SIP, ISDN or analog users who can be reached by the LANCOM VoIP router in their own LAN. "External" users are those accessible via a line (SIP account, SIP trunk, SIP PBX, ISDN or analog).

- Active: A local subscriber initiates call forwarding.
- Passive: An external subscriber initiates call forwarding

16.6.1.2 Call forwarding with and without consulting

A subscriber forwarding a call can either directly hand over an active call to a third subscriber (unattended call forwarding), or a separate call can be made to the third subscriber to communicate the call and then hand it over (attended call forwarding).

LANCOM VoIP routers support unattended call transfer only via the SIP protocol.

16.6.1.3 Charges for calls when forwarding to external users

The forwarding of a call from an external caller to a third party who is also external carries the risk that charges will arise for the ongoing call, even though the initiating subscriber has ended the call.

16.6.1.4 How the LANCOM VoIP router handles call forwarding

Irrespective of which terminal devices are involved in the call forwarding, a LANCOM VoIP router can handle a variety of tasks:

Passthrough

Both subscribers in the call forwarding are at the same end of the connection, e.g. transfer from a local to a local subscriber.

Delegate

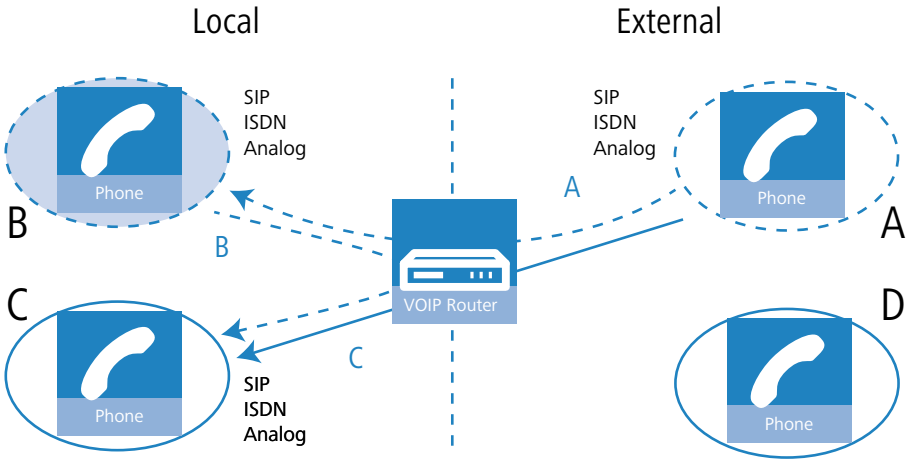
The call forwarding is not handled by the LANCOM VoIP router itself but by an upstream exchange, e.g. in a VoIP PBX that is accessible via a PBX line.

Switching

The LANCOM VoIP router handles the signaling and the data transfer between subscribers.

16.6.1.5 Active forwarding to local users

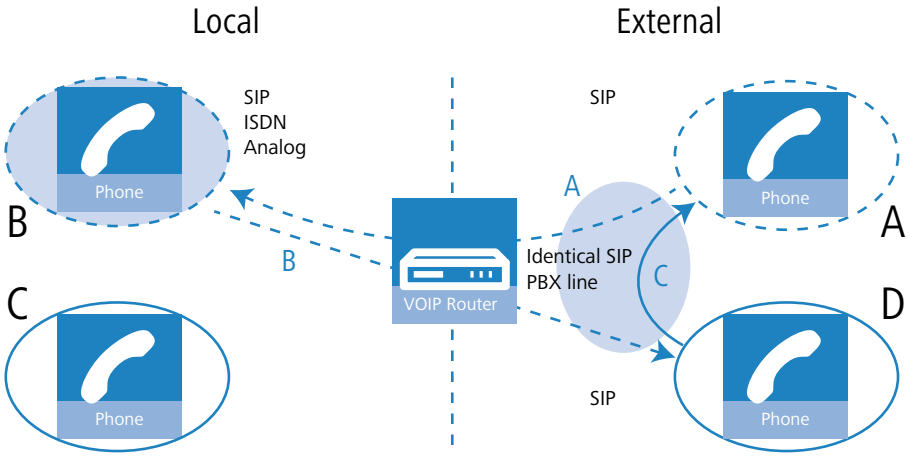
1. An external user **A** makes a call to an internal user **B** (SIP, ISDN or analog).
2. **B** makes a further call to local user **C**. These two users can reach each other directly, so the LANCOM VoIP router only handles the signaling by means of SIP; the data transfer via RTP takes the shortest possible route.
3. Local user **B** initiates the call forwarding (attended/with flash) to **C**.
4. The LANCOM VoIP router manages the call forwarding.



In case of SIP at the external subscriber, this requires that Transfer in SIP (re-invites) is fully supported.

16.6.1.6 Active forwarding to external SIP users

1. An external SIP user **A** makes a call to an internal user **B** (SIP, ISDN or analog).
2. **B** makes an additional call to an external user **D**.
3. If both external users **A** and **D** can be reached via the same SIP line, the LANCOM VoIP router delegates the administration of the call forwarding to the upstream provider.

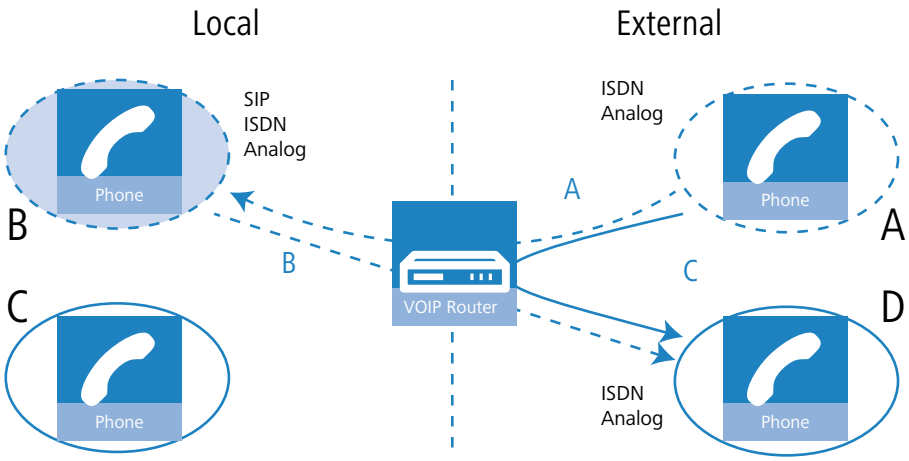


Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

16.6.1.7 Active forwarding to external ISDN users

In some cases upstream exchanges do not support the delegation of call forwarding to external ISDN users, often due to the unclear situation about who carries the call charges. For this reason, call forwarding between external subscribers is always handled by the LANCOM VoIP router.

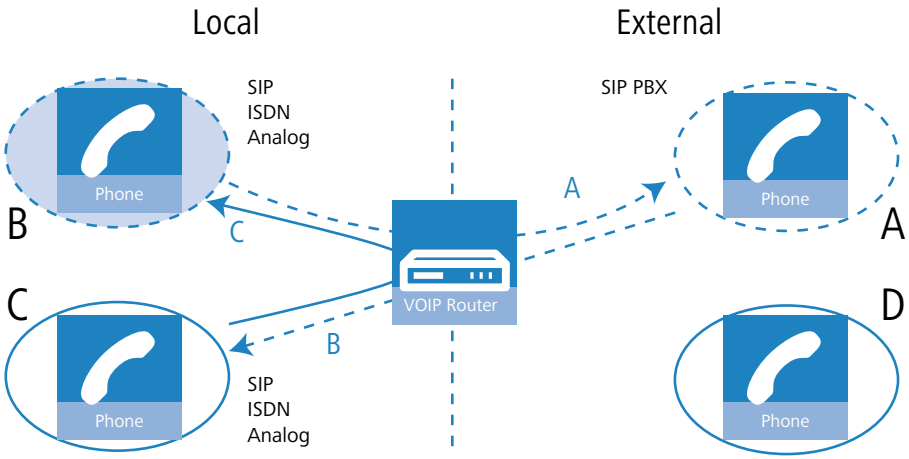
1. An external subscriber **A** (external SIP, ISDN) makes a call to an internal user **B** (SIP, ISDN).
2. **B** makes a further call to an external subscriber **D** (ISDN or analog).
3. The local user **B** then forwards the call (with consultation) to **A**.
4. If both external users **A** and **D** use different protocols (SIP, ISDN), the LANCOM VoIP router assumes responsibility for managing and converting the data.
5. If both external users **A** and **D** use SIP, the LANCOM VoIP router is unable to forward the call.



Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

16.6.1.8 Passive forwarding between local users

1. An internal user **B** (SIP, ISDN or analog) calls an external user **A** (at a SIP PBX line).
2. **A** makes an additional call to a local user **C**.
3. The external user **A** then forwards the call to **C**.
4. The LANCOM VoIP router manages the call forwarding. If the connected subscribers **B** and **C** are internal users, the LANCOM VoIP router only checks the SIP data for signaling and enables the RTP data transfer over the shortest direct path between the SIP users.

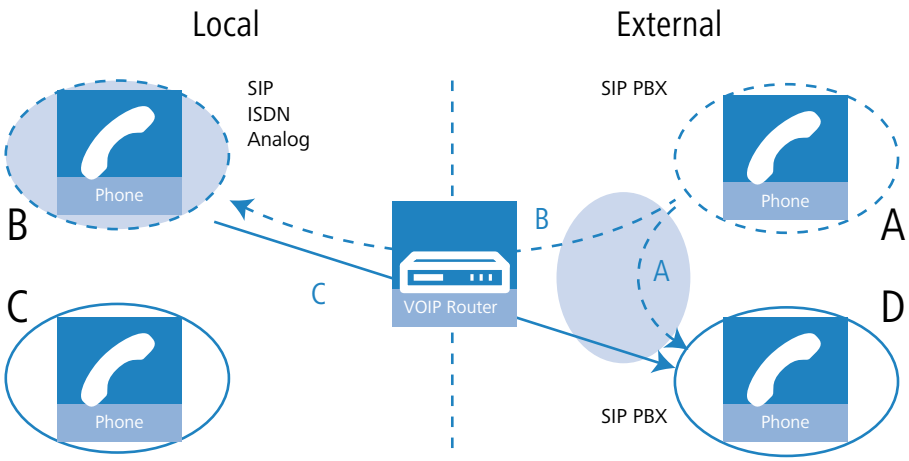


Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

16.6.1.9 Passive forwarding from local to external users

1. An external user **A** (at a SIP PBX line) makes a call to an internal user **B** (SIP, ISDN or analog).
2. **A** makes an additional call to an external user **D** (who is also a subscriber to the same SIP PBX line as **A**).
3. The external user **A** then initiates a connect from **B** to **D**. The LANCOM VoIP router needs to establish a connection to **D** for this.

The LANCOM VoIP router can only establish this connection if **D** can be reached via the same SIP-PBX line as **A**, i.e. if external call forwarding is permitted.



Requires that the VoIP PBX fully supports Transfers in SIP (re-invites).

16.6.2 Spontaneous call management by the user

16.6.2.1 Functions for spontaneous call management

Calls can be managed on an individual basis and the LANCOM VoIP router supports the services known from the ISDN network:

- With call hold the user can place an active call into a wait state. In this state the user can make a call to another person, for example.
- Establishing an additional call while a call is on hold is referred to as consulting. This call can be ended again and the conversation with the call on hold continued.
- With swap call, the user can switch to and fro between two connections. The user is only connected with one caller at a time, while the other caller is put on hold.
- With call swap the user switches an active call over to another call which is on hold. The two callers are then connected and the user is no longer involved in the call. A subscriber forwarding a call can either directly hand over an active call to a third subscriber (unattended call transfer), or a separate call can be made to a third subscriber to communicate the call and then forward it (attended call transfer).

16.6.2.2 Using spontaneous call management with various telephones

SIP telephones and SIP softphones generally feature special keys or menu entries to manage calls. Different terms may be used depending on the model or software program, but the functions are as follows:

- CALL HOLD: Places an active call into a wait mode or swaps between two active calls. On ISDN and analog telephones this function is often referred to as the F-key/Flash/Call hold function (F key).

- HANG UP: End the current call.
- SWAP: Swap between two active calls (depending on the ISDN telephone, this may be initiated by a display-menu entry, a special key, or the "F" key).
- TRANSFER: Initiates the call forwarding (can be triggered by "hanging-up" with an active call and a call on hold)[1].

These functions can be used to manage calls as follows:

Holding/consulting and continuing with calls	SIP	ISDN	Analog
To place a call on hold, press the Flash/Call hold key (or "F" on analog phones).	CALL HOLD	HOLD or F	R
The caller can no longer hear you and you can initiate a second call by dialing a telephone number (consulting).			
To continue with a call which is on hold, press the Flash/Call hold key again (or "F 2").	CALL HOLD	HOLD or F	F 2
If the consultation call has not yet been picked up, you can stop the consulting by hanging up the handset on a SIP or ISDN telephone.[1]	HANG UP (1st call rings)	HANG UP (1st call rings)	R 1 (back to 1st call)
You can stop the consultation call with the appropriate menu function of the telephone (e.g. "Cancel") or "F 1" (analog).[1]			

Swap	SIP	ISDN	Analog
To open a second line during a call, first press the Flash/Call hold key (or "F" on analog phones).	CALL HOLD	HOLD or F	R
The other caller can no longer hear you.			
Dial the number for the second caller while the first call is on hold.	123456789	123456789	123456789
If you cannot reach the second caller, you can return to the call which is on hold by pressing the hold key (or "F" on analog telephones).			
As soon as two simultaneous connections are open, you can use the hold key (or swap key for ISDN phones, "R" and "2" for analog phones) to swap to-and-fro between the two connections.	CALL HOLD	CALL HOLD / SWAP	F 2
You will be connected to one of the other callers; the other caller is placed on hold.			
To end an active call, hang up the handset on SIP or ISDN telephones, and on analog phones press "R 1".	CANCEL or HANG UP[1]	CANCEL or HANG UP[1]	F 1
The call which is on hold is not automatically reactivated, but it will be signaled (ringing phone) for a period of 15 seconds.			

Call forwarding, consult	SIP	ISDN	Analog
To open a second line during a call, first press the Flash/Call hold key (or "F" on analog phones).	CALL HOLD	HOLD or F	R
The other caller can no longer hear you.			
Dial the number for the second caller while the first call is on hold.	123456789	123456789	123456789
If you cannot reach the second caller, you can return to the call which is on hold by pressing the hold key.			
As soon as you have established two simultaneous connections you can connect the two callers with the connect key (or "F" and "4" on analog phones) or by hanging up the handset.[1]	TRANSFER or HANG UP[1]	TRANSFER or HANG UP[1]	R 4 or HANG UP
Optionally you can switch between the two lines as often as you like before transferring the call. Call transfer always connects the active call and the call on hold.			

Call transfer, blind	SIP
To open a second line during a call, first press the Flash/Call hold key.	CALL HOLD

Call transfer, blind	SIP
The other caller can no longer hear you.	
Dial the number for the second caller while the first call is on hold.	123456789
Press the connect key or hang-up the handset before the second connection has been established.[1]	TRANSFER or HANG UP[1]
The two callers will now be connected “in the background”.	

16.6.3 Configure permanent call forwarding

Along with spontaneous call transfers as controlled by a subscriber during a call, it is often useful to set up a permanent call forwarding ("redirect calls"). For example, a call should be forwarded when a line is busy, if there is no answer within a certain period, or in case of absence (e.g. vacation).

There are two possibilities for configuring permanent call forwarding.

- Via the telephone or terminal device itself with the aid of control characters
- In the configuration of the LANCOM VoIP router by means of the management tools (LANconfig, WEBconfig or telnet)

If permanent call forwarding is activated by both methods, then the behavior of the call forwarding follows the last respective action.

16.6.3.1 Triggering call forwarding

The following events can be used as a trigger or condition of the permanently configured call transfers:

- CFU, call-forwarding unconditional
- CFB, call forwarding on busy
- Delayed call forwarding, CFNR (call forwarding no reply); CFNA (call forwarding no answer)
- No call transfer

All types of call forwarding can be used in parallel with your own destination telephone numbers. If multiple call-forwarding conditions are active, the following priority applies:

1. CFU
2. CFB
3. CFNR

If call forwarding on busy is activated and a corresponding destination number has been defined, for example, then the call will be forwarded to this number before using the number set for call forwarding on no reply.

If the incoming call has already been forwarded from another telephone number, then forwarding will not take place again, so as to avoid endless call-forwarding loops.

16.6.3.2 Configuring user settings with the telephone with character strings

For the configuration of user settings with the telephone, the various technologies (SIP, ISDN, analog) each offer specific possibilities. With ISDN telephones, call forwarding can be controlled by the functional protocol in the ISDN signaling or via so-called keypads (character stings). For analog telephones the same character strings are transferred by DTMF. The SIP protocol provides another option with its REFER method that is supported by most SIP phones and SIP softphones. However, call forwarding can only be controlled by the terminal device. To enable a uniform behavior for users in mixed infrastructures, the LANCOM VoIP router offers an further variant of call forwarding for SIP phones. This is presented here in comparison with ISDN and analog telephones.

1

In some cases, SIP or ISDN telephones can be configured so that hanging-up the handset either causes the consultation or active call to terminate, or a call forwarding is triggered (“Transfer”).

Immediate call forwarding	SIP	ISDN	Analog
Switch on and define destination for call forwarding	*21*TargetNo#	*21*TargetNo#	*21*TargetNo#
Switch off	#21#	#21#	#21#
Switch off temporarily, maintain call-forwarding destination	#22#	#22#	#22#
Switch on again, maintain defined call-forwarding destination	*22#	*22#	*22#

Call forwarding on busy	SIP	ISDN	Analog
Switch on and define destination for call forwarding	*67*TargetNo#	*67*TargetNo#	*67*TargetNo#
Switch off	#67#	#67#	#67#

Call-forwarding on no reply	SIP	ISDN	Analog
Switch on and define destination for call forwarding	*61*TargetNo#	*61*TargetNo#	*61*TargetNo#
Switch off	#61#	#61#	#61#

Please note the following when using character stings to configure call forwarding:

Some ISDN telephones feature special keys or menu entries to configure call forwarding, and these can be used as an alternative to the listed character strings. Refer to the documentation from the corresponding manufacturers.

16.6.4 Call forwarding (call deflection / partial rerouting) at the SIP trunk (SIP 302)

LANCOM routers operating the Voice Call Manager can initiate call forwarding on SIP trunk connections by forwarding the information sent by the PBX to the SIP trunk provider. If this is an ISDN terminal, the partial rerouting (PR) is converted into a “SIP 302 Moved Temporarily” before being transmitted to the provider.

In the SIP lines table, the external call forwarding is configured for each individual SIP trunk line under **Voice Call Manager** > **Lines** > **SIP lines** > **Advanced** by enabling the option **Call forwarding using SIP 302**. With call forwarding enabled, a call-forwarding option initiated from a telephone (ISDN / SIP) is switched directly at the exchange, unless the telephone is part of a call number group or the user is registered multiple times on the LANCOM router.

If the telephone is an ISDN terminal, the partial rerouting is converted by means of the service feature SIP 302 before being transmitted to the provider. The number to which an incoming call should be forwarded is transmitted by the terminal and must be reachable via call routes. The phone number must therefore match the dialing plan in the Voice Call Manager in order for the latter to select the correct line. For this reason, line prefixes have to be specified even though they are removed by the Voice Call Manager once the correct line has been selected.

If the forwarding destination set on the terminal is an internal telephone number, the call forwarding is performed by the Voice Call Manager directly, in which case you have to use the prefix used for internal calls (e.g. **).

16.6.5 Fax via T.38 – Fax over IP (FoIP)

The migration of telephone infrastructure towards VoIP has also increased the demand for fax devices to communicate over VoIP. Even in the age of e-mail, fax transmissions continue to be highly important in legal respects as legally binding documents such as contracts and invoices can be far more easily handled by fax than with the alternative of e-mails with digital signature. The integration of fax devices into VoIP infrastructure can be implemented in two ways:

- Fax messages are transmitted via landline just like a conventional fax.
- The transmission takes place over an Internet connection. Options for this are as follows:
  - The fax signals are transmitted like voice data over a VoIP connection, referred to as "fax over VoIP". Fax transmission should only make use of the G.711 codec, as other codecs are inferior at converting the fax tones

designed for analog networks into digital VoIP data. Due to the highly sensitive nature of fax connections, this method can only be used with high-quality connections, whereby the transmission speed is sub-optimal.

- For example, with the "store-and-forward" principle (ITU-T.37), fax messages are passed from the fax machine to a gateway that stores and converts the fax document. In a second step the fax is transmitted to the destination for conversion back into a fax format. Alternatively fax messages can be sent by e-mail (fax-to-mail and mail-to-fax). Solutions of this type may not meet the legal requirements mentioned above, due to the fact that there is no direct connection between transmitter and receiver.
- With "real-time routing" of fax messages, on the other hand, a direct connection is established between the two fax machines and all data is transferred in real time. The fax machines are connected virtually over the Internet. Communication between the two fax machines follows the ITU-T.38 standard for converting standard fax signals. This variant is also known as Fax over IP (FoIP). The fax messages are not transferred as acoustic signals via VoIP, but rather in a special protocol, that embeds the signals in UDP/TCP packets.

To enable fax transmissions with T.38, the fax machines themselves either have to support the T.38 standard or they must be interconnected over the Internet via fax gateways. LANCOM VoIP routers support the T.38 standard and are thus suitable for operation as fax gateways in VoIP infrastructure.

The fax machines are connected to the LANCOM VoIP routers by means of a suitable interface. The fax gateway in the LANCOM VoIP router handles the conversion of the signals for transmission and reception of fax messages:

- Conversion of T.38 fax data to G.711/T.30
- Conversion of G.711/T.30 fax data to T.38
- Passthrough of G.711/T.30 fax data
- Passthrough of T.38 fax data

If the device type "fax" or "telephone/fax" is selected in the user settings of the ISDN or analog user, the LANCOM Business VoIP router automatically recognizes a fax for transmission and it attempts to transmit via F.38/FoIP. If the remote site does not support this method, the LANCOM VoIP router automatically uses the fax over VoIP-version using G.711 compression.

Successful transmission of fax via FoIP requires that the VoIP infrastructure also supports the T.38 standard. For example, where a public SIP provider is involved, this provider also has to offer T.38 support.

16.6.6 Hunt groups with call distribution

16.6.6.1 Introduction

Calls are normally intended for an individual or their telephone number. Occasionally it is not important to speak to a particular individual, but to anybody in a certain department or with a certain function. In this case, telephone infrastructure collects multiple users into hunt groups where they can all be reached under a single shared telephone number. The group call function can then follow certain rules to distribute or forward incoming calls to the call group.

16.6.6.2 Call distribution

A hunt group consists of two or more users, or even other hunt groups, as potential destinations for an incoming call. Hunt groups are comparable to local users and have their own number and, as such, they can be used as a destination number in the call router.

Incoming calls can be distributed by a variety of methods, allowing different scenarios to be realized.

- Calls are signaled to all group members at the same time (simultaneous)
- Calls are signaled to one member of the group after the other, in a set order (sequential)

Along with the members of the hunt group and distribution method, also to be defined are a call-forwarding time and and call-forwarding destination, all of which control the call-distribution procedure. The forwarding time determines the time period during which the dialed user can answer a signaled call. The forwarding destination defines where the call is to be forwarded to (user, group, internal or external call number) for the case that none of the group members picks up the call within the forwarding time—if no forwarding destination is defined, then the call is rejected.

16.6.6.3 Cascading of hunt groups

The defined hunt groups can themselves be members of a higher-level hunt group, just as hunt groups can be entered as the forwarding destination for a higher-level hunt group. These options enable the establishment of a cascaded hunt-group structure which can form highly complex scenarios by using a multitude of branches. These branches represent the hunt groups and the end points are the users themselves. The following rules apply to structures of this type:

- If a hunt group is used as a member, then this lower-level hunting group causes a new "branch" in the structure to open up when that member receives a call.
- When a lower-level hunt group opens, certain parameters that have been defined, e.g. forwarding time, etc., apply.
- This branch from the lower-level group only remains open for as long as the member in the upper-level hunt group is being signaled according to the settings. If the next member in the upper-level hunt group is reached, then the entire branch along with all of its other sub-branches is closed. The system does not wait until all possible combinations along the branch have been tried out. It is thus possible that there are members defined in a lower-level hunt group who cannot be reached because of settings in the upper-level groups.
- If a member of a hunt group picks up the call, all open branches are closed and all attempts to reach forwarding destinations are stopped.
- If a call remains unanswered after signaling all of the members of an (upper or lower-level) hunt group, then the call is passed on the the call-forwarding destination. This means that any call-forwarding times which may be running in the upper-level hunt groups are ended. In this case the call "jumps" out of the hunt-group structure and is given a new destination.

Example: The following hunt groups have been defined:

Group call number	Comment	Members	Forwarding method	Forwarding time	Forwarding destination
100	Entire company	200, 300, 400	Simultaneous	10	Ext. Dialup remote
200	Service Dept.	201 to 209	Simultaneous	10	100
300	Marketing Dept.	301 to 309	Sequential	10	200
400	Sales Dept.	409	Sequential	15	100
410	Sales Europe group	411, 412, 413, 414, 415	Sequential	10	400
420	Sales America group	421, 422, 410	Sequential	30	400
430	Sales Asia group	431, 432, 410	Sequential	30	400

Each department or group has users who use the final digits in the telephone number, i.e. 411 to 419 for the Sales Europe staff and 409 for the Sales team secretary. Only the group call numbers are communicated externally because all staff members tend to travel frequently on business. The purpose of the hunt-group structure is to connect each customer with a competent staff member in the shortest possible time.

An incoming call directed to the telephone number 420 for a Sales America team member is handled as follows:

1. The call is signaled to the users 421 and 422 in this group for 30 seconds each. If there is no answer, then the hunt group 410 is activated for 30 seconds—a member of the Sales Europe team should take care of the customer if no Sales America team members are available.
2. In the Sales Europe team, calls are distributed to each number for 10 seconds. The hunt group has five members, but with a forwarding time of just 10 seconds, not all of the users can be signaled: The branch is only opened for a maximum of 30 seconds by the upper-level group, in this case 420. This is a way of limiting the maximum waiting time for a customer. If the first three signaled members of the lower-level group 410 do not answer, then the call jumps back to the upper-level hunt group 420.
3. There is still nobody available in the upper-level hunt group 420, and so the call is directed to the call-forwarding destination 400.
4. Hunt group 400 directs the call to the team secretary 409. If here nobody answers for 15 seconds then the call-forwarding destination 100 is used, which addresses the entire company.

5. Hunt group 100 calls all of the numbers in the hunt groups 200, 300 and 400 simultaneously. If even then nobody answers within 10 seconds, then the hunt group forwards the call to an external telephone number, for example a 24/7 call center.

16.6.7 Multiple logins (multi login)

For subscribers using multiple terminal devices, e.g. a softphone on PC and a "normal" telephone on the desktop, multiple SIP, ISDN or analog phones all using the same internal telephone number can log on to the LANCOM VoIP router. Multi-login telephones behave like a single user in a hunt group with 'simultaneous' call distribution:

1. Incoming calls are signaled **simultaneously at all** telephones with this internal number.
2. As soon as a call is picked up at one of the telephones, signaling at the other devices stops.
3. Further incoming calls are signaled to all telephones. If one of the telephones reports that it is “busy”, the entire multi-login group is considered “busy” if this has been configured under *Extended user settings* on page 1426.
4. Outgoing calls can be made from every telephone without limitation.
5. For a multi-login group only one call forwarding setting (call redirection) can be configured. This applies to all telephones and can be set from any telephone.

To use multi-login, multiple telephones can be set to have the same internal telephone number.

16.7 VoIP media proxy – Optimized management for SIP connections

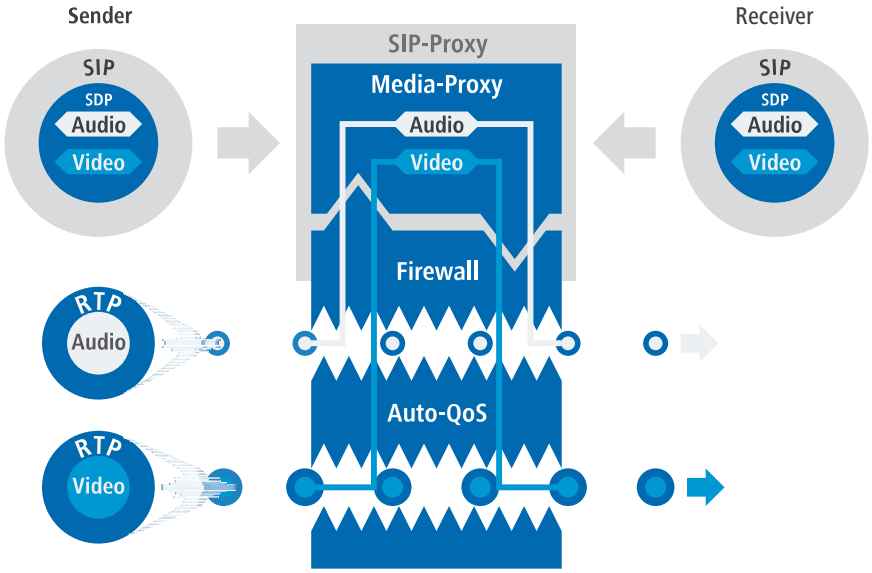
When transferring or forwarding calls between remote subscribers over different SIP lines, the SIP proxy in the LANCOM VoIP router attempts to connect the two callers by means of a REFER or a Re-INVITE. The two external subscribers are not always able to reach one another directly and so the connection may fail. This is because the SIP providers do not make the necessary adaptations, e.g. translation of the destination IP addresses. To improve performance in these situations, the SIP proxy in the LANCOM VoIP routers has been additionally equipped with a media proxy.

The media proxy helps to transfer and forward calls between subscribers who are reachable over different types of telephone line (e.g. SIP PBX line and SIP provider line). The media streams, generally RTP connections, remain unchanged. The media proxy changes the ports and IP addresses in the data packets and it adapts special media end points to the corresponding destination networks (ARF networks, interface and IP address).

Multiple media streams in one SIP connection

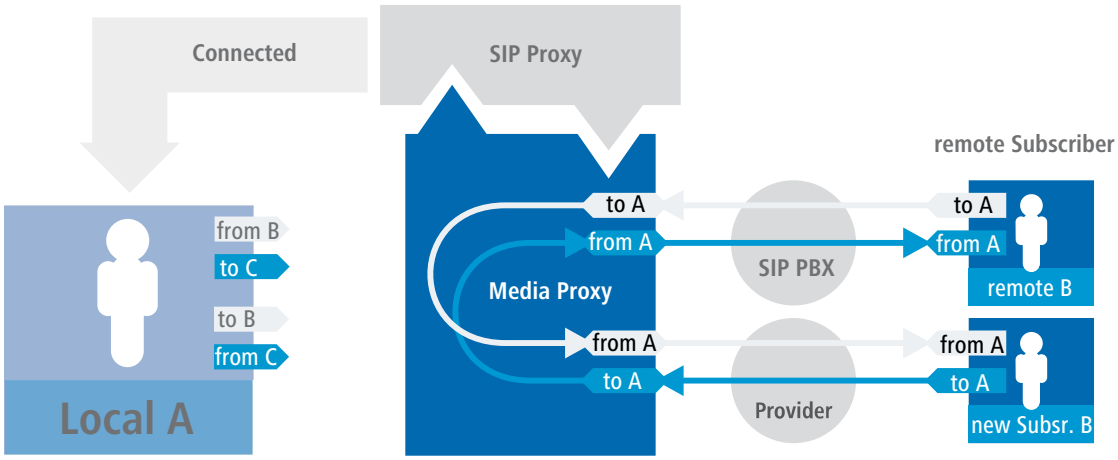
The SIP protocol can negotiate multiple data streams in a session, e.g.separate media streams for audio and video. Each stream is handled separately. A data stream initially terminates at the media proxy and continues from the "other side". This provides the data stream with end points at the LAN and WAN sides of the media proxy.

All of the connection information in the direction of the SIP provider can be maintained and all of the necessary changes to IP addresses, ports, etc., are handled by the media proxy.



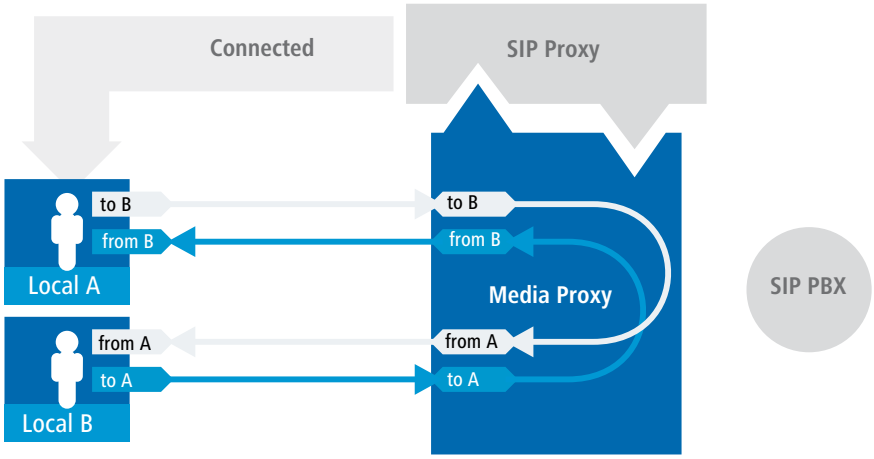
The data streams are all fed through the firewall individually, which enables a differentiated control of the QoS settings, among other things.

Connection management by the media proxy enables all subscribers to be connected to one another, whatever type of line they are using. This makes it possible to connect between SIP, ISDN and analog subscribers, something that a pure SIP connection is not capable of. Furthermore, the monitoring of individual media streams in the firewall allows certain types of application to be permitted or prevented depending on the connection's end point.



Management of media streams in case of an upstream SIP PBX

Even for two subscribers in the same network behind the LANCOM VoIP router, when connected to an upstream SIP PBX the media proxy generates data streams with separate media end points on the LAN side and on the WAN side (towards the SIP PBX).



In this case it is not necessary to pass the media streams through the upstream PBX, so the SIP signaling helps the LANCOM VoIP router to make a new decision about the path to be taken by the connection data. Using the end points in the media proxy the data streams can be connected directly, making a diversion via the SIP PBX unnecessary.

This decision is also made again in the media proxy if a local and an external subscriber are connected in such a way that, ultimately, two local subscribers are connected to one another. The media proxy re-assigns the end points when making the connection, so enabling the direct transmission of the data streams between the local participants.

Managing the media streams in the firewall

The media streams are monitored in the firewall as a matter of principle. A firewall rule is generated for each media stream (audio, video). This rule opens a connection for the corresponding IP addresses and ports for each side (LAN-WAN) and carries out a translation according to the IP-port relationships as specified by the media proxy.

Automatic QoS rules for media streams

The QoS mechanism in the firewall reserves the maximum possible amount of connection bandwidth as agreed during the SDP negotiation (SDP, Session Description Protocol) and the packets are prioritized accordingly.

Handling subscribers using different codecs

When connecting different subscribers, the situation can arise where the codecs available to the subscribers do not match together—there are no common codecs due to the SDP negotiation.

The following situations are to be observed here:

- Connections with different media streams, e.g. a video-telephone call (audio + video) and a traditional telephone call (audio only): This connection will be rejected with the message "Codec mismatch".
- Similar media types (audio-audio, video-video) with codecs that do not match: This connection will be rejected with the message "Codec mismatch".

The media proxy can only connect different subscribers if the media type and the codec type match.

16.8 SIP-ID as switchboard number with trunk lines

Until now, SIP trunk lines were given the SIP ID as the switchboard number and modified to suit the telephone number. However, this method is not supported by all trunk-line providers. For this reason you use the SIP mapping table—just like the ISDN mapping—to explicitly define the way that telephone numbers are processed.

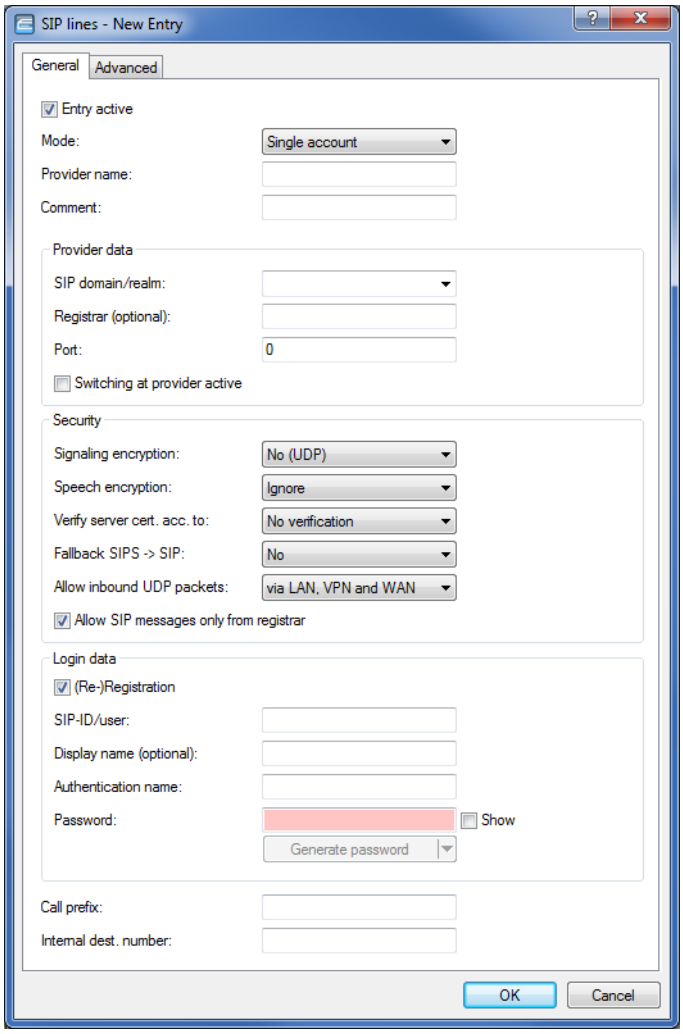
Example: With `0123456789# -> #` the extension numbers of the trunk are mapped 1:1 to the internal telephone numbers.

16.9 Switching at the SIP provider

When switching external SIP connections, the Call Router in the LANCOM VoIP router generally manages the connection for the full duration of the call. This means that the Call Router retains control over a call even when two external subscribers have been connected to one another and the local subscriber on the LANCOM VoIP router side has ended the call. In this case, the LANCOM VoIP router continues to take up bandwidth for connecting the two external subscribers.

If the connections to the two external subscribers both run via the same SIP provider, an alternative is to transfer the call switching to the provider so that the LANCOM VoIP router stops taking up the bandwidth.

You enable the switching at the SIP provider in the LANconfig under **Voice Call Manager** > **Lines** by clicking on **SIP lines** and enabling the option **Switching at provider active** on the **General** tab.



Switching at provider active

Call switching (transfer call) between two remote subscribers can be handled by the device itself (media proxy) or it can be passed on to the exchange at the provider if both subscribers can be reached on this SIP provider

line. The advantage of this is that the LANCOM VoIP router no longer requires the bandwidth. Otherwise, the media proxy in the LANCOM switches the media flows, such as when connecting two SIP provider lines.

Switching at the provider will only work if both connections are routed via the same provider line.

An overview of the main SIP providers supporting this function is available in the Support area of our Internet site.

16.10 SIP Application Layer Gateway (SIP ALG)

SIP is increasingly becoming established as the basis for modern real-time communication in IP networks. Unified Communications (UC) and collaboration, IP telephony, video streaming, camera surveillance, intercoms, paging systems, and audio recordings increasingly rely upon SIP and RTP for switching and transmission.

The NAT (Network Address Translation) typically carried out by the access router at the edge of the LAN presents a barrier to SIP communications. This is because of the addresses transmitted during SIP signaling and also because of the dynamically negotiated media sessions and the UDP-based RTP connections that depend upon them.

Restrictive firewall configurations prevent communications even where client/server-side mechanisms such as STUN, ICE and TURN are used to overcome NAT.

The SIP ALG for LCOS detects SIP connections and the RTP-based media streams that they depend upon and transforms these in line with the NAT rules in the access router.

Also, the SIP ALG monitors the bandwidths of the SIP connections and so provides QoS.

16.10.1 Properties

The SIP ALG for LCOS has the following features:

- **No local registration**

  The SIP proxy does not provide registration for SIP endpoints. Instead, it mediates the registrations directly to the approved SIP domains.

  This means that it is impossible to set up a line backup over alternative voice lines (analog, ISDN).

- **Transparency for SIP extensions**

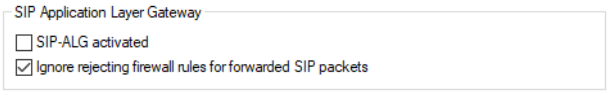
  The SIP ALG also transmits unknown, non-standard header elements to enable the SIP messages to be communicated between terminal devices and SIP PBXs.

  The SIP ALG determines an unambiguous destination for every SIP message. Forking (communication between multiple devices of the same identity) is handled upstream. The SIP ALG merely provides transparent forwarding of these data packets.

16.10.2 Configuration

Activate and configure the SIP Application Layer Gateway (SIP ALG) in LANconfig under **Miscellaneous Services** > **Services** > **SIP Application Layer Gateway**.

The SIP ALG is disabled in the default settings.



SIP-ALG activated

Activate the SIP Application Layer Gateway here.

Ignore rejecting firewall rules for forwarded SIP packets

Here you determine whether the firewall for SIP packets respects Reject rules or whether the packets are forwarded by the SIP ALG in any case.

16.11 Restricting or preventing SIP registration over WAN

To restrict or prevent the SIP registration at the Voice Call Manager over a WAN connection, navigate to **Voice Call Manager** > **Users** and click the button **SIP users**. The SIP users configuration dialog features a parameter that controls this. You can enable access via VPN, or prohibit it completely.



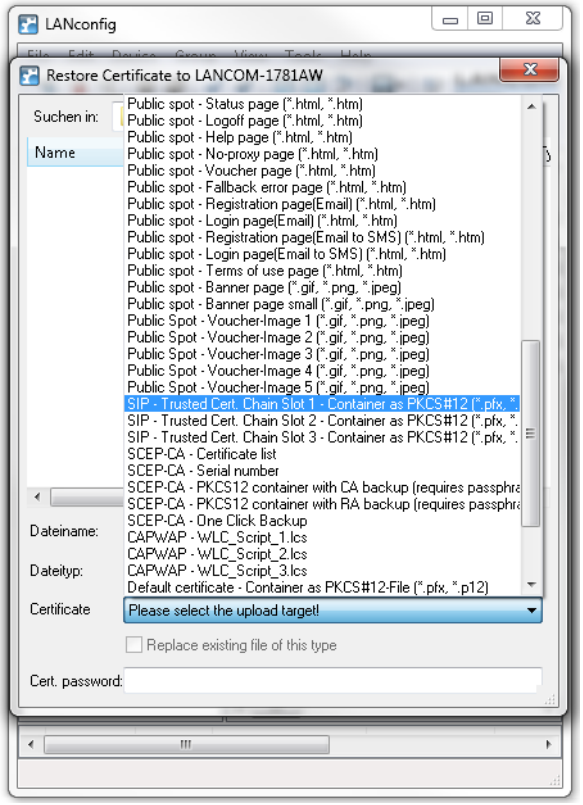
Additional security for the registration is provided by a count of the number of times that a SIP user authenticates incorrectly. Once the counter reaches a threshold value, the device locks the SIP user's account for a certain time. During this period the SIP user cannot log on to the Voice Call Manager. You set the threshold value and the locking time under **Voice Call Manager** > **General** in the section **WAN login lock**.



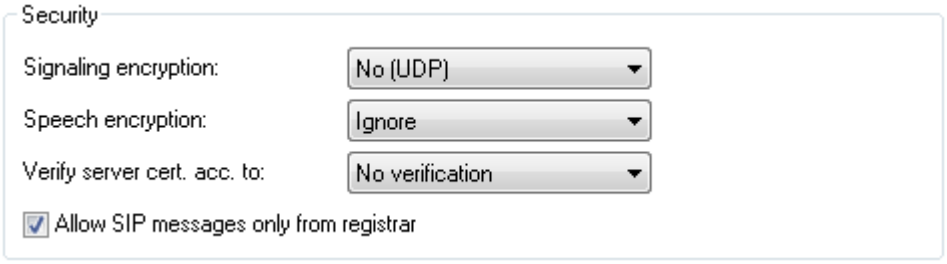
16.12 Certificates for encrypted telephony

You have the option to download certificates for encrypted telephony onto your device and to check whether the existing certificate used by the SIP server to establish a TLS connection should be classified as trustworthy and accepted.

Download the required SIP certificate to your device with LANconfig by navigating to **Configuration management** > **Upload certificate or file** .



In the LANconfig dialog under **Voice Call Manager** > **Lines** > **SIP lines**, select how the SIP certificate is to be checked in the "Security" section:



Verify server cert. acc. to:

With this setting, you specify whether the certificate of the SIP server is verified against certain Certificate Authorities (CAs). CA certificates from globally recognized certificate chains are updated with LCOS updates. They can also be manually updated by truststore updates.

Server certificate	
No verification	The server certificate is not verified. All valid server certificates are accepted, whichever CA they were signed by. This setting is useful for accepting self-signed certificates.

Server certificate

All trusted CAs	The server certificate is verified against all CAs known to the device. These include all CAs that LCOS "knows" to be trusted and also those from the VoIP server certificate slots 1 to 3. The encrypted connection is only established if one of these certificates is validated successfully.
VoIP cert. slot 1	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 1 of the VoIP certificates.
VoIP cert. slot 2	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 2 of the VoIP certificates.
VoIP cert. slot 3	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 3 of the VoIP certificates.
Telekom-Shared-Business-CA4	With this setting, the device only accepts server certificates signed by the Telekom Shared Business CA4 CA. Use this setting for SIP trunk connections from Deutsche Telekom.

16.13 Handling canonical telephone numbers

Canonical telephone numbers (familiar from mobile phones and starting with +) were formerly automatically reformatted into standard telephone numbers. + was converted to `00`.

In WEBconfig under **Extras** > **LCOS menu tree** > **Setup** > **Voice-Call-Manager** > **Convert-Canonicals** you can deactivate automatic conversion by setting **no**, in which case the canonical numbers are processed by the call-routing table. This allows you to specify your own lines for canonical numbers, for example.

16.14 Processing Destination Domains

As the VoIP implementation in the LANCOM VoIP router handles all calls as SIP calls, telephone numbers and SIP subscribers contain domain information. Furthermore, SIP numbers can also contain alphanumeric characters.

The SIP domains are used in LCOS as follows:

- When SIP subscribers register at upstream PBXs or at the LANCOM VoIP router itself.
- When SIP subscribers establish a connection.

LCOS supports the following defined domains:

- ISDN for the ISDN interfaces
- All domains that are entered for the lines

16.14.1 Registration at upstream exchanges

Local SIP subscribers can only register using the domains that are known. The subscribers authenticate themselves at the local LANCOM VoIP router with their user name and password. This excludes domains that correspond to an upstream SIP PBX. These registrations are authenticated at the upstream SIP PBX.

If a subscriber tries to register with an unknown domain, then this may be accepted as a local registration.

16.14.2 Switching internal calls

For internal connections, internal numbers are generally assigned unambiguously. However, SIP telephones, for example, can register with several "lines", such as '1011@provider.com' and '1011@isdn.com', so that a line can be assigned specifically to the required connection.

With internal switching, an attempt is made to find a subscriber whose number and domain match. Only if this was not successful is the call placed using the destination number only. The domain remains unchanged.

For example, calls that are incoming via ISDN (from calling pty id@isdn) are switched to subscriber 1011 (to 1011@isdn). The call to the SIP telephone is displayed on the ISDN line key. If there is no such subscriber with such a domain, then the call is delivered to the first known subscriber '1011'.

16.15 Configuring the ISDN interfaces

LANCOM VoIP routers are equipped with multiple ISDN interfaces, which can be used either to connect the device to an ISDN exchange line or to ISDN terminal equipment.

ISDN-TE interface ("external ISDN line")

An ISDN interface in TE mode for connection to the ISDN bus of an upstream ISDN PBX or to an ISDN NTBA. This ISDN interface can be used for backup connections over ISDN or as a dial-in interface for remote sites.

ISDN-NT interface ("internal ISDN line")

With its ISDN interface in NT mode, the LANCOM VoIP router itself provides an internal ISDN bus. This ISDN interface can be used to connect ISDN PBXs or ISDN telephones.

Ex-factory each ISDN interface is set to TE mode. A cross-over adapter (shipped with the All-IP option) converts it to an NT port. With LANCOM business VoIP routers, this function is controlled via LCOS.

- Multiple TE interfaces provide, for example, up to four B channels as a backup or for dial-in.
- With multiple NT interfaces, for example, a downstream ISDN PBX provides up to eight B channels.

Depending on the combination of ISDN interfaces in TE and NT mode, you need to set up the bus termination, and the appropriate protocol needs to be set in the software. The setting for the protocol allows for the type of ISDN connection to be used (point-to-multipoint or point-to-point).

16.15.1 Point-to-multipoint and point-to-point connections

LANCOM VoIP routers support point-to-multipoint and point-to-point connections:

- Point-to-multipoint connection (point-to-multipoint): Up to 8 ISDN terminal devices can be connected to this type of connection. Terminal equipment can include ISDN telephones and ISDN PBXs, which can be used for connecting yet more equipment. As an alternative, a LANCOM VoIP router can be connected to a point-to-multipoint connection.
- Point-to-multipoint connection (point-to-multipoint): This type of device is suitable for the connection of one ISDN device only, generally an ISDN PBX. As an alternative, a LANCOM VoIP router can be connected to a point-to-point connection.

To connect a LANCOM VoIP router, the interface is set up for the type of line at hand.

Equipment connected to an ISDN connection can be addressed in two ways:

- The devices are addressed with a multiple subscriber number (MSN) that is linked to the ISDN connection and cannot be influenced.

- Terminal devices are addressed via a Direct Dialing In-Number (DDI). However, only the switchboard number is associated with the telephone line; the extension numbers that address the individual terminal devices can be chosen at will and are merely suffixes to the switchboard number. The switchboard number, extension and area selection code (not including the leading zero) can be at the most 11 characters long.

The terms "point-to-multipoint connection" and "point-to-point connection" are used in many countries to describe the technical implementation of point-to-multipoint with MSN and point-to-point with DDI. Other countries may use different types of connection and other combinations of protocol and call-number type, or even different names. Please refer to your telephone network operator for the technical specifications of your ISDN connection.

16.15.2 Bus termination

The configuration of the bus termination is either done in the software or, as is the case with the All-IP option, by using the supplied cross-over adapter.

Bus termination is obligatory with an ISDN interface in NT mode.

Bus termination is generally deactivated for ISDN interfaces in TE mode. If the LANCOM VoIP router is the last device at a longer ISDN bus and this itself is not terminated, it may be advantageous to activate the bus termination for an ISDN interface in TE mode.

16.15.3 Protocol settings

In LANconfig, parameters for the ISDN interfaces are entered in the configuration section 'Interfaces' under 'WAN'. In WEBconfig, Telnet or an SSH client you find the settings for the ISDN interface parameters under `Setup/Interfaces/WAN`.

Select the protocol for each ISDN interface according to its application and the ISDN connection type: Point-to-multipoint and point-to-point connections can be used in various combinations with a LANCOM VoIP router. The following options are available:

- **Automatic** for automatic selection of the operating mode (only in TE mode)
- **DSS1 TE (Euro ISDN)** for connection to a point-to-multipoint ISDN bus.
- **DSS1 TE point-to-point** for connection to a point-to-point ISDN bus.
- **1TR6 TE (German ISDN)** for connection an ISDN bus which uses this protocol (in Germany only).
- **DSS1 NT (Euro ISDN)** to provide point-to-multipoint ISDN interfaces
- **DSS1 NT reverse** to provide point-to-multipoint interfaces while maintaining the ISDN timing of the connected ISDN line.
- **DSS1 NT (point-to-point)** to provide point-to-point ISDN interfaces
- **DSS1 NT point-to-point reverse** to provide point-to-point interfaces while maintaining the ISDN timing of the connected ISDN line.
- **DSS1 timing** to maintain the ISDN timing of the connected ISDN line.
- **Off**

If an ISDN device is attached to an ISDN interface that is set to auto and is not recognized properly, set the required protocol manually.

16.15.4 ISDN connection timing

To ensure trouble-free transmission, all of the components in the ISDN system (LANCOM VoIP routers, upstream and downstream ISDN PBXs and ISDN terminal devices) have to use the same ISDN timing. In the LANCOM VoIP router, an ISDN interface in TE mode can take on the timing of the ISDN line. The TE interface enables the device itself to behave like a terminal device. In NT mode, the LANCOM VoIP router can pass on the on this timing over the ISDN interfaces to

any connected terminal equipment or downstream ISDN PBXs. The NT interface enables the device itself to behave like an exchange.

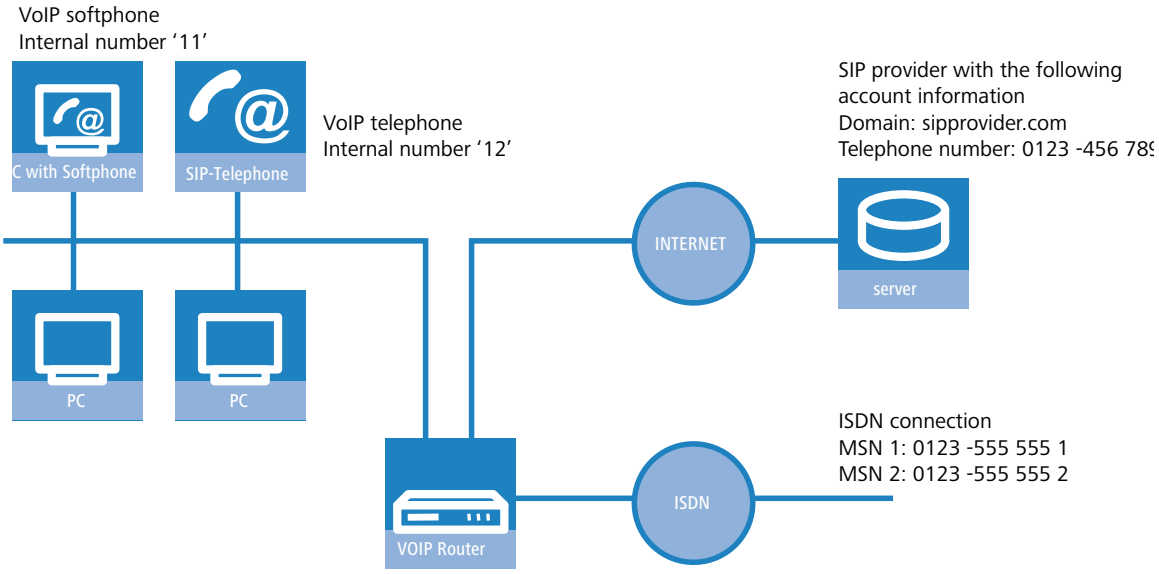
A number of ISDN interface settings are available for specifying the ISDN interface which is to supply the ISDN timing to the LANCOM VoIP router, which in turn passes on the timing to the devices at the NT interfaces.

- **Automatic**: If no interface has been manually selected for the timing, the device automatically searches for a TE interface to supply the timing. To ensure that the timing is synchronous, the TE connectors constantly try to keep the connection activated. This ensures that the timing continues to be supplied even if one of multiple TE lines should be shut off. If none of the TE connectors supply a timing, then the timing system runs "freely" and uses the internal timing of the LANCOM VoIP router.
- **DSS1 timing**: This setting takes on the ISDN timing from this connection, and this is used by the LANCOM VoIP router and further devices connected over the NT interface. In this way, the timing can be switched through in parallel to an existing ISDN PBX at a point-to-point connection. Apart from passing on the ISDN timing, the interface is not active.
- **DSS1 NT reverse** or **DSS1 NT point-to-point reverse**: When all ISDN interfaces are operated in NT mode, the timing system runs "freely" because there is no TE interface to take on the ISDN timing. If in this case the ISDN connections are connected, for example, to an ISDN PBX which is being supplied with ISDN timing from another source, then interference to the transmission may arise because the timing of the LANCOM VoIP router is not synchronous to that of the PBX. In such cases, the reverse setting allows the ISDN timing to be taken from an NT-mode interface, so ensuring that the LANCOM VoIP router runs synchronously with the overall system.

16.16 Configuration examples

16.16.1 VoIP telephony in stand-alone operation

This example shows how to configure a LANCOM which is used as a central device for Internet connectivity and VoIP telephony at a new site.



16.16.1.1 Objective

- Internal telephony with SIP telephones and SIP softphones.
- Access to internal terminal equipment via the MSNs.
- External telephony via the SIP provider with backup over ISDN.

› Calls to emergency and service numbers via ISDN.

16.16.1.2 Requirements

› LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA. The Internet connection has been set up.
› A dialing plan with a unique internal telephone number for all terminal equipment to be connected, here, for example, the number `11` for the VoIP softphone and the number `12` for the VoIP telephone.
› A SIP provider account.

16.16.1.3 Using the information during configuration

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	✔	✔		
Internal numbers	✔	✔	✔	✔
External SIP telephone number	✔			
SIP account access data	✔			
External ISDN telephone numbers (MSNs)			✔	
Country and local area code	✔			

16.16.1.4 Configuring the device

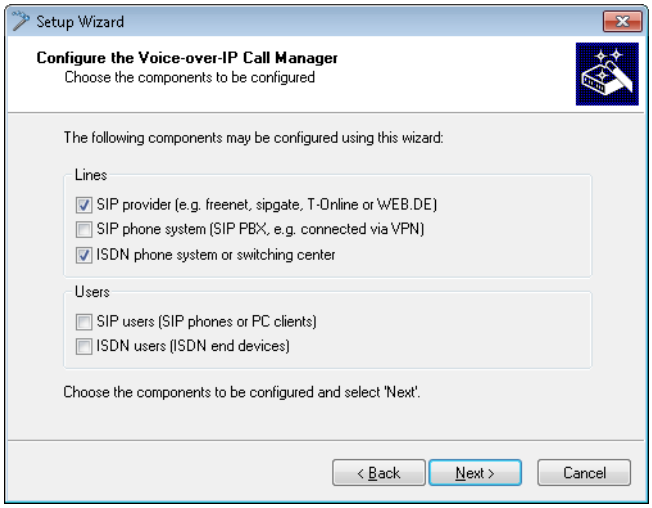
The following steps are required to configure the device:

› Set up the line to the SIP provider
› Enable the ISDN interface, and assign MSNs to the internal numbers

In this example, it is not necessary to configure SIP users: The SIP users are authenticated at the LANCOM with the settings created in the terminal equipment (softphone and VoIP telephone).

Configuring the device in detail:

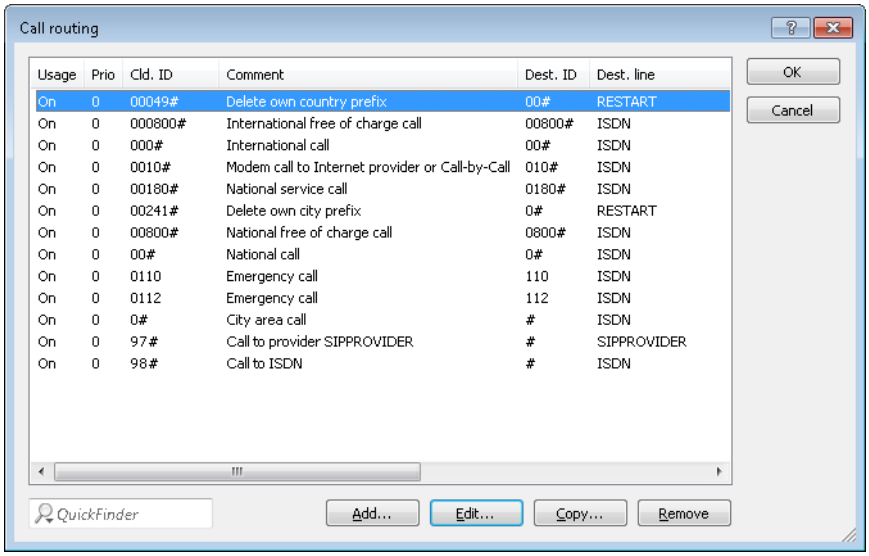
1. Under LANconfig, start the setup wizard for configuring the Voice Call Manager. Enable the options **SIP provider** and **ISDN phone system**.



2. Enter a unique domain for the local VoIP domain which describes the local VoIP area for the site (e.g. `mycompany.internal`.)
3. Configure the line to the SIP provider, for example with the name `SIPPROVIDER` with the following values:
   - Internal default number: All calls arriving from the SIP provider are forwarded to this internal number. Enter an internal number from your dialing plan here, e.g. `11`.
   - SIP domain/realm: You received this domain from your SIP provider; it is usually entered in the format `sipdomain.tld` without the part that designates any specific server.
   - Registrar (FQDN / IP) (optional):
   - Outbound proxy (optional):
   - SIP-ID / user: Enter the SIP number with local area code here, providing that the SIP provider does not require any other information.
   - Display name (optional): The display name is only required if the SIP provider verifies this during registration. If you enter a display name here, then this name will be displayed at the remote site. If the field remains empty, then the display name for the corresponding internal user is transmitted.
   - Authentication name (optional): Special authentication names are not supported by all SIP providers. In many cases, the authentication name is the same as the SIP ID or the user name. Complete this field only if your SIP provider has issued you a special authentication name.
   - Password: Enter the password for SIP access here.

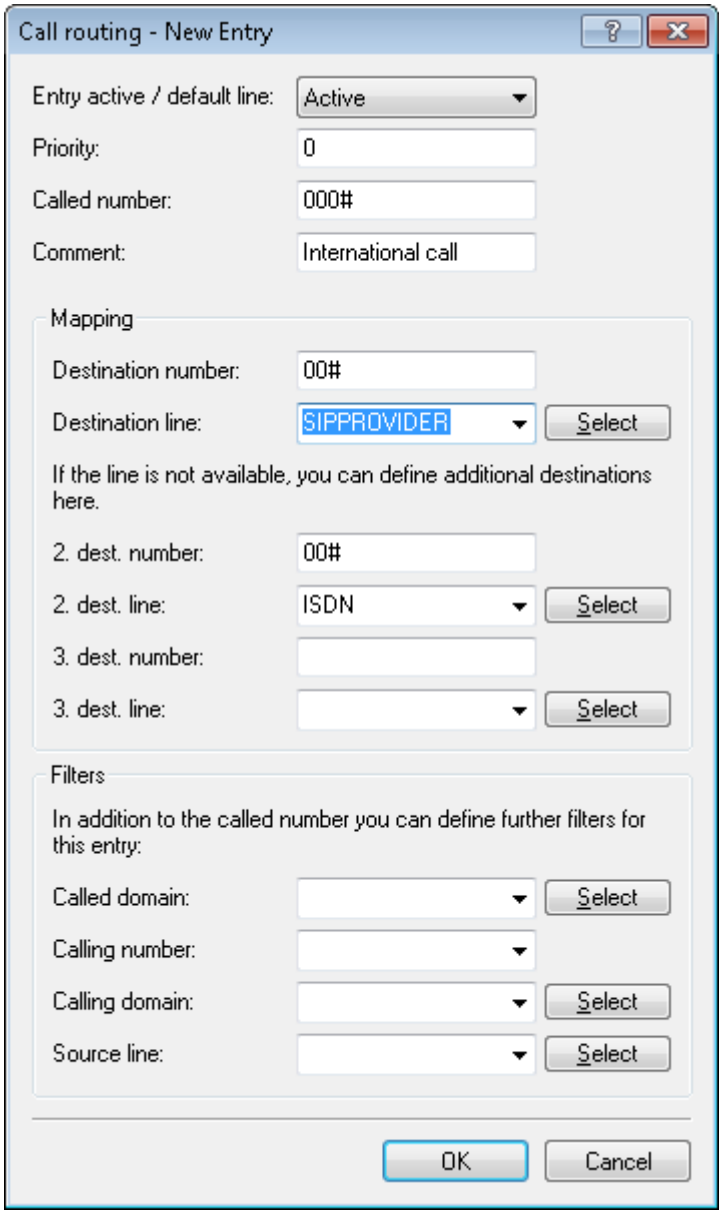
   This description applies to a "user-defined configuration". If you select a special SIP provider from the list, then some of the parameters will be preconfigured automatically.
4. Configure an ISDN line for VoIP telephony use. For every MSN on your ISDN connection, make an assignment to an internal number within your telephone number plan during ISDN mapping.
   - MSN 1 `555 555 1` / internal phone number `11`
   - MSN 2 `555 555 2` / internal phone number `12`
5. Enter the local and national area code for the device's location. Using this information, the Voice Call Manager can decide whether or not outgoing calls are local calls, national or international long distance calls.

6. Based upon the entries made so far, LANconfig creates a suggestion for the call routing table which you can adapt to fit your requirements as follows:



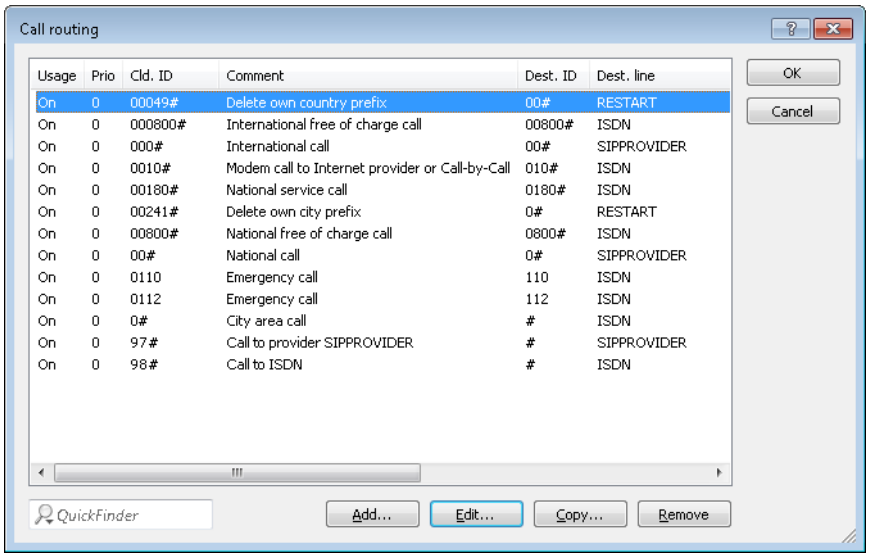
The # sign is a placeholder for any character string. The entry `0#` is therefore suitable for all numbers dialed that have at least one `0` preceding them.

This suggested call routing table would place all external calls over the ISDN line. The SIP line is set up as a backup for international and national long distance calls and local calls that are not in the list of special or emergency numbers.



In order to channel calls to special destinations, such as international and national long distance calls, over the SIP provider, double-click on the corresponding entry in the table and switch the line used from `ISDN` to `SIPPROVIDER`.

Don't forget to switch the backup line from `SIP` to `ISDN`, if necessary! After being adapted for international and national long distance, the call routing table should appear as follows:



16.16.1.5 Configuring the VoIP terminal equipment

Enter the registration information for the first SIP user in the softphone.

16.16.1.6 Call routing procedure for outgoing calls

On outgoing calls, the Call Manager first searches the call routing table from top to bottom. If the Call Router cannot find a matching entry there, it uses the list of registered users:

	User	Dials	Correct call route	Correct user	Mapping, number in use	Destination line
1	VoIP telephone	`11`	None	VoIP softphone	`11`	Internal
2	VoIP telephone	`0 555 555`	**3** `0#`		`0241#: 0241 555 555`	ISDN
3	VoIP telephone	`0 0123 666 666`	**3** `00#`		`0#: 0123 666 666`	SIP provider

1. The Call Manager cannot find an entry that corresponds to `11` in the call routing table. Now it searches the list of registered users and finds the internal SIP user there.

   Call routing uses not just the users configured in the LANCOM, but all of the users that are actually authorized with the call router. This allows SIP users to authenticate with the call router even if they are not entered in the LANCOM. The entry of the internal VoIP domain on the LANCOM is sufficient for authentication, assuming that local authentication is not required.

2. The entry **3** in the call routing table shown above matches the dialed number. The call router removes the `0` outside-line access prefix, adds the area code for the local telephone network and makes the call to `0241 555 555` via the ISDN line.

   The area code for the local telephone network is added on because calls via SIP providers usually require the area code to be dialed.

3. The entry in the call routing table is suitable in this case. The call router removes the `0` prefix for access to the outside line and completes the call to `0123 555 555` via the SIP line. If the SIP line is not available, then the call is made over the ISDN line.

16.16.1.7 Call routing procedure for incoming calls

For incoming calls, the telephone network exchange removes the prefix from the number dialed (destination number). Therefore, the LANCOM only receives the number itself, which may be treated differently depending on the source:

- Numbers from the ISDN network are translated with the ISDN mapping table to the internal number which is entered for the receiving MSN.
- Calls from a SIP network are mapped to the internal destination number entered for the corresponding SIP line.

With the altered number, the Call Manager begins to search the call routing table from top to bottom. If the Call Router cannot find a matching entry there, the call is forwarded directly to the internal number:

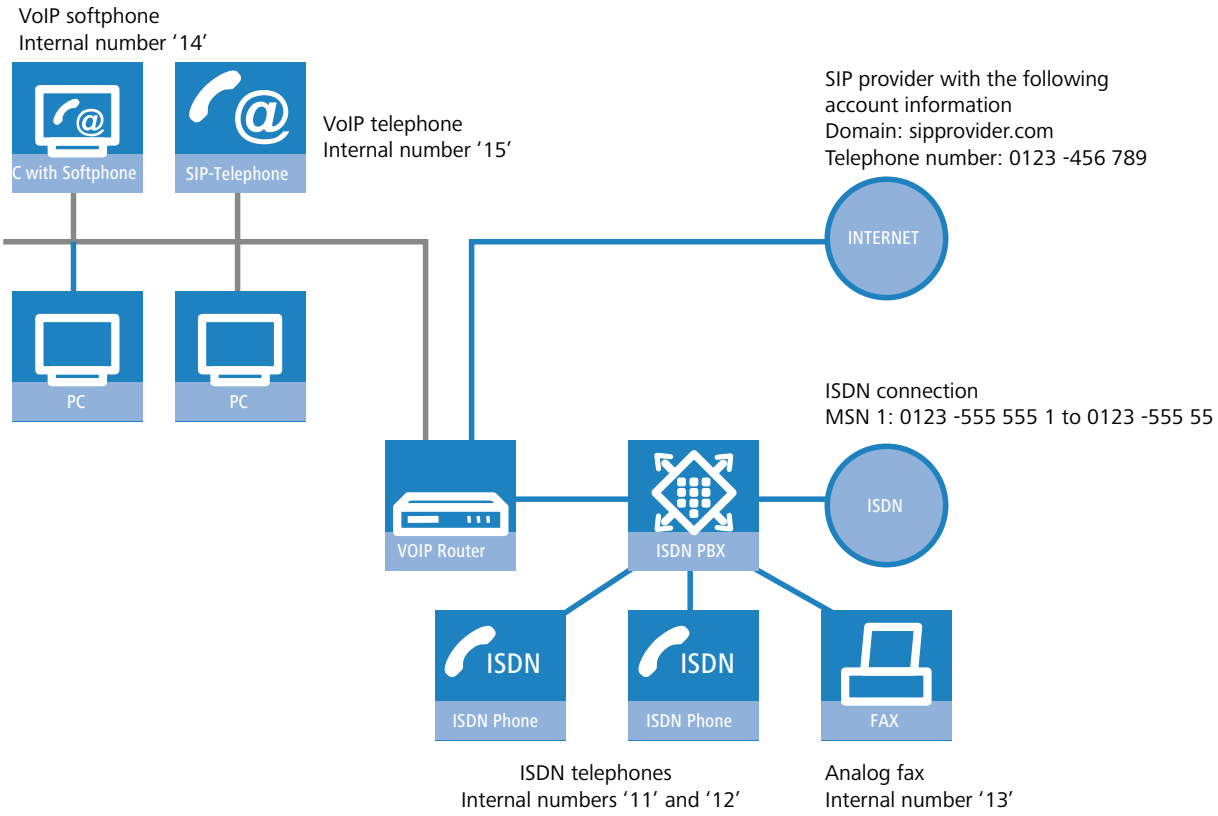
	Remote site dials	Call router receives	Assigned via	Number in use	Correct call route	Destination line
1	`0 123 456 789`	`456 789`	internal destination number for SIP line	`11`	None	Internal
2	`0 123 555 555 1 1`	`555 555 1 1`	ISDN mapping	`11`	None	Internal
3	`0 123 555 555 2 2`	`555 555 2 2`	ISDN mapping	`12`	None	Internal

16.16.2 Using VoIP telephony to enhance the upstream ISDN PBX

This example shows how to configure a LANCOM when an upstream ISDN PBX is enhanced with the VoIP telephony capability. Until now, the MSNs `11` to `13` for the ISDN connection have been used for two ISDN telephones and one analog fax.

The PBX is configured so that subscribers dial `0` to access an outside line.

The LANCOM is operated on an ISDN PBX extension line.



16.16.2.1 Objective

- Internal telephony with ISDN and SIP telephones and SIP softphones.
- External telephony with VoIP terminal equipment via the SIP provider with backup over ISDN.
- External telephony with ISDN terminal equipment in the PBX. Depending on the functionality of the ISDN PBX, ISDN terminal equipment can also use the SIP lines in the LANCOM VoIP router.
- Accessing internal terminal equipment (ISDN and SIP) via the MSNs.
- Calls to emergency and service numbers via ISDN.

16.16.2.2 Requirements

- LANCOM connected to the LAN and WAN; an ISDN TE interface is linked to the extension interface on the ISDN PBX. The Internet connection has been set up.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected. In general, the numbers used are predetermined by the PBX, which often only allows certain number ranges.
- A SIP provider account.

16.16.2.3 Using the information during configuration

Dialing plans with ISDN PBX systems: When crossing from the ISDN network to the internal subscribers, the ISDN PBX converts the external MSNs to internal MSNs. When operating a LANCOM VoIP router at the extension interface of the ISDN PBX, the internal MSNs of the PBX are translated to the internal numbers of the VoIP range. For reasons of clarity, we recommend using congruent internal MSNs/numbers for terminal equipment for all connections.

The following table provides a summary of the information required for configuration and where it can be entered. SIP terminal equipment parameters can be entered using the SIP telephone keypad, the corresponding configuration software, or the softphone configuration menu.

	LANCOM	SIP terminal equipment	ISDN PBX	ISDN terminal equipment
Internal VoIP domain	✔	✔		
Internal numbers	✔	✔	✔	✔
External SIP telephone number	✔			
SIP account access data	✔			
External ISDN telephone numbers (MSNs)			✔	
Country and local area code	✔			

16.16.2.4 Configuring the device

The following steps are required to configure the LANCOM:

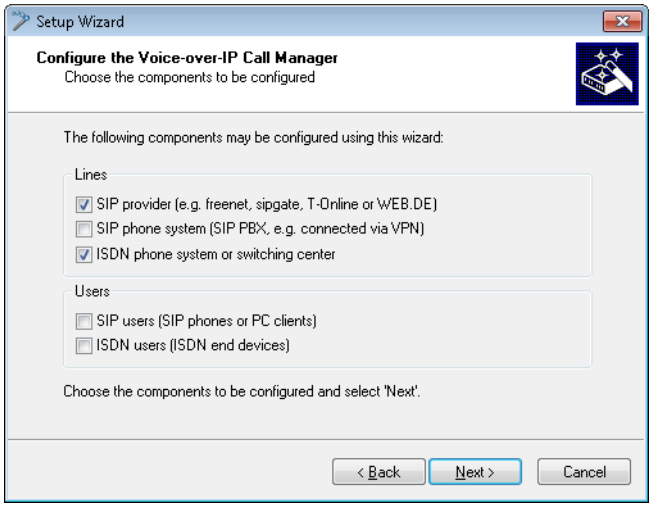
- Set up the line to the SIP provider
- Enable the ISDN interface and the mapping of internal MSNs in the PBX to the internal numbers of the LANCOM VoIP router
- Adapt the call-routing table

In this example, it is not necessary to configure SIP or ISDN users:

- The SIP users are registered at the LANCOM with the settings in the terminal equipment (softphone and VoIP telephone).
  - The ISDN devices can be reached via a corresponding entry in the call routing table.

Configuring the LANCOM in detail:

1. Under LANconfig, start the setup wizard for configuring the Voice Call Manager. Enable the options **SIP provider** and **ISDN phone system or switching center**.



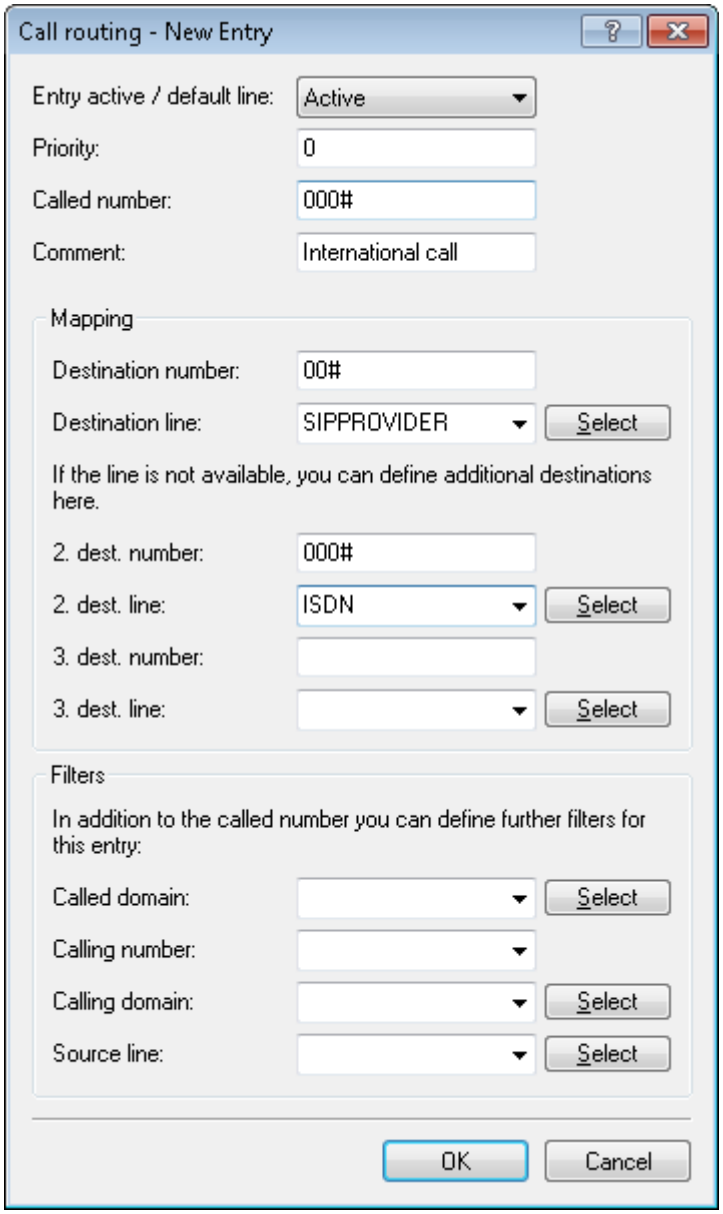
2. Configure the device as described in the preceding examples:

   Unique local VoIP domains

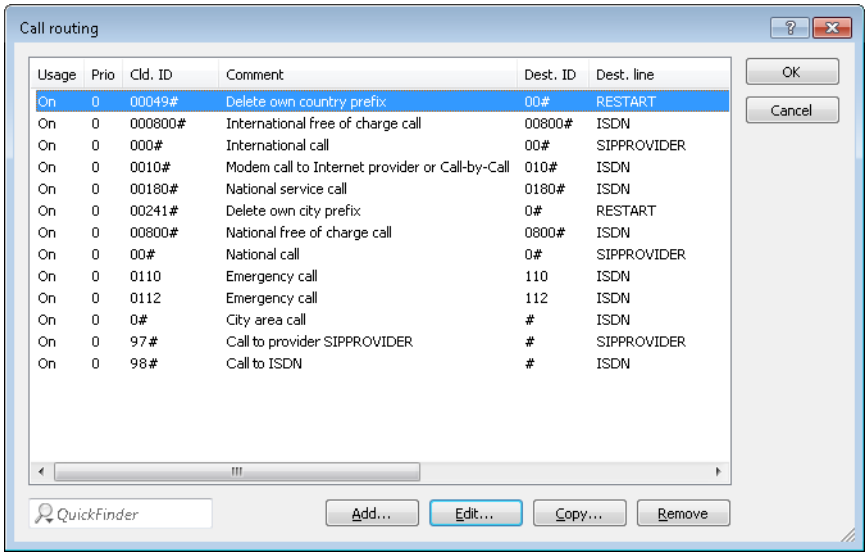
   A line to a SIP provider

   ISDN line

3. Adapt the suggested call routing table in order to direct calls to service numbers automatically over the SIP provider's line. The following example shows the entry for international calls.



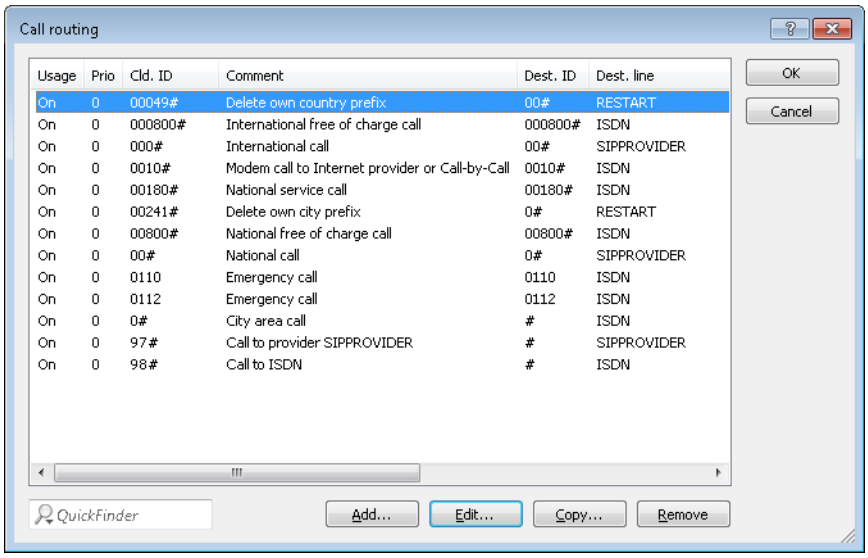
1. After adaptation, the call routing table appears as follows:



The leading `0` is removed from the number for long distance calls, and the call is made via the SIP provider.

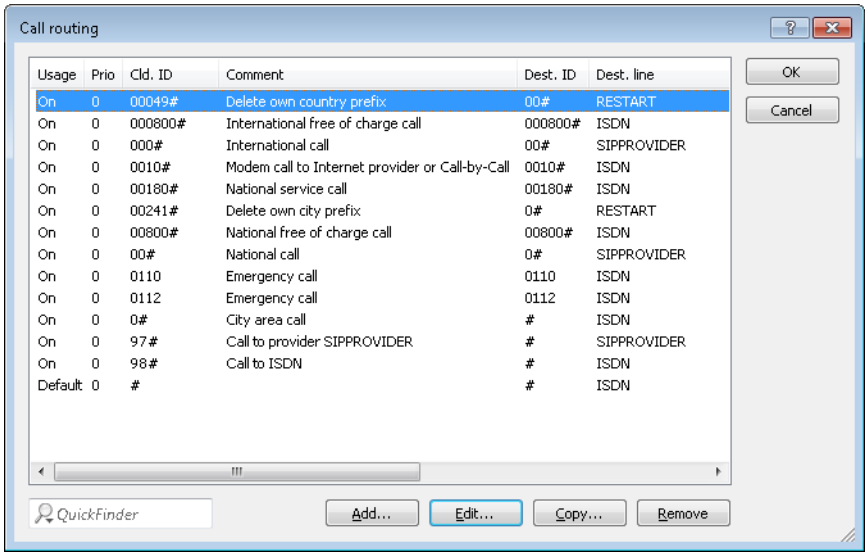
2. For ISDN calls, however, the `0` should not be removed from the destination number because the upstream ISDN PBX requires the `0` to access an outside line. Therefore, adapt the destination number for all entries with the destination line 'ISDN'.

After adaptation, the call routing table appears as follows:



3. In order to allow the ISDN subscribers to be contacted internally by the VoIP users, a default route is also set up which directs all calls that have not yet been resolved to the ISDN line without changing the numbers.

After adaptation, the call routing table appears as follows:



This call routing table is only valid for PBX systems where the subscribers dial `0` to access an outside line. If the PBX uses another mechanism for accessing an outside line, then the table must be adapted accordingly.

16.16.2.5 Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

16.16.2.6 Configuring the ISDN PBX

When configuring the PBX, external MSNs are assigned to internal MSNs. For every VoIP terminal device, a free internal MSN is linked to an external MSN.

External and internal calls from ISDN terminal devices into VoIP telephony

First, the ISDN terminal devices forward the desired destination number to the ISDN PBX when the call is being established. If the number is an internal number/MSN, then the PBX directs the call to the internal ISDN bus. The SIP terminal equipment connected to the LANCOM can only be reached by an internal call if the PBX knows the internal number for the VoIP user.

If your PBX is able to direct external numbers to the internal ISDN bus, then the ISDN terminal devices can also use the lines configured in the LANCOM, such as the SIP provider line, for outgoing external calls.

16.16.2.7 Configuring the ISDN terminal equipment

Configuring the ISDN terminal equipment is generally limited to entering the internal MSN used in the PBX.

16.16.2.8 Call routing procedure for outgoing calls

	User	Dials	Correct call route	Correct user	Mapping, number in use	Destination line
1	VoIP telephone	`14`	None	VoIP softphone	`14`	Internal
2	VoIP telephone	`11`	**3** # (default)		`#: 11`	ISDN
3	ISDN telephone	`14`	**1.** PBX	VoIP softphone	`14`	Internal

	User	Dials	Correct call route	Correct user	Mapping, number in use	Destination line
4	VoIP telephone	0 555 555	**2** 0#		00241#: 0 555 555	ISDN
5	ISDN telephone	0 555 555	**1.** PBX		555 555	ISDN exchange
6	VoIP telephone	0 0123 666 666	**1** 00#		0#: 0123 666 666	SIP provider

1. Internal call between two VoIP terminal devices.
2. Internal call from VoIP to ISDN. In the first pass (without the default routes) the number 11 does not match any of the routes. Similarly, no matching entry is found in the list of authenticated users. In the second pass, the default route finds # (entry **3** in the call routing table shown above) and directs the call **unchanged** to the ISDN line. The PBX receives the call on its internal ISDN bus, recognizes the called number as an internal MSN, and again forwards the call to the internal ISDN bus that the respective ISDN terminal device is connected to.
3. Internal call from ISDN to VoIP. The ISDN PBX recognizes the destination number 14 as an internal MSN and directs the call to the corresponding internal ISDN bus. The Call Router receives the call to 14, does not find a matching entry in the call routing table but does find an entry in the list of authenticated users.
4. External call from the VoIP into the local telephone network. The entry **2** in the call routing table shown above matches the dialed number. The Call Router completes the area code for the local telephone network and sends the call out to the ISDN line. Only now does the SIP PBX removes the 0 outside-line access prefix and makes the call to 0241 555 555 via the ISDN exchange line.
5. External call from ISDN into the local telephone network. The ISDN PBX recognizes the destination number as an external destination, removes the 0 outside-line access prefix and completes the call to 555 555 via the ISDN exchange line.
6. External call from VoIP into the national telephone network. The entry **2** in the call routing table is suitable in this case. The call router removes the 0 prefix for access to the outside line and completes the call to 0123 555 555 via the SIP line. If the SIP line is not available, then the call is made over the ISDN line. In this case, the 0 is retained in the destination number in order to gain access to an outside line through the PBX.

16.16.2.9 Call routing procedure for incoming calls

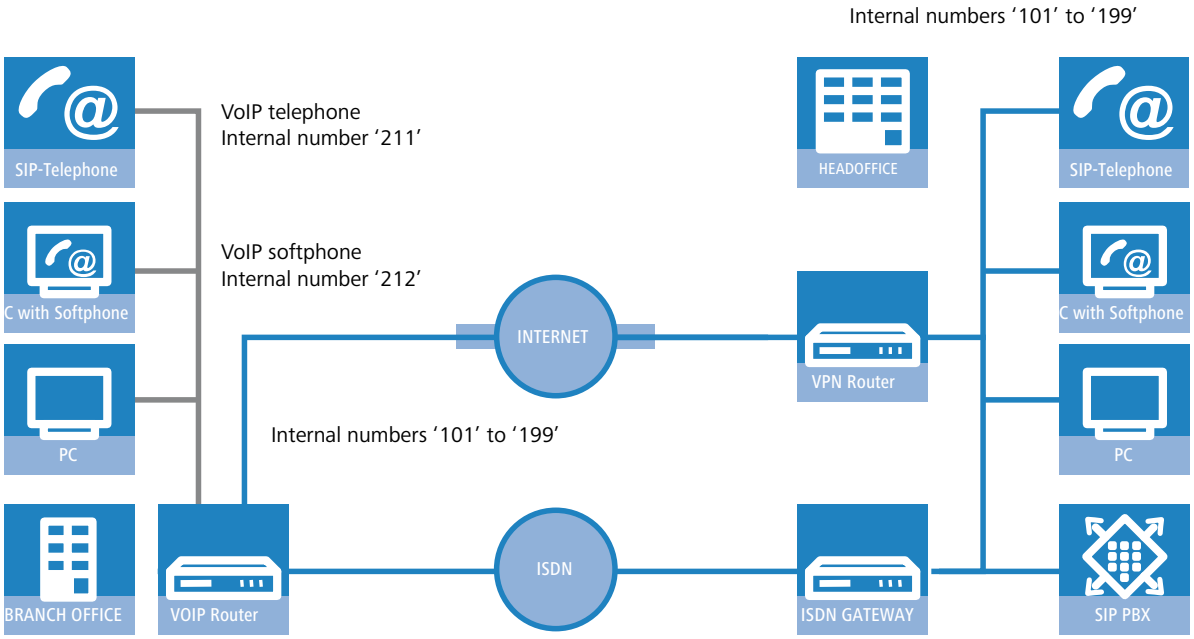
	Remote site dials	Call router receives	Assigned via	Number in use	Correct call route	Destination line
1	0 123 456 789	456 789	internal destination number for SIP line	11	None	ISDN
2	0 123 555 555 1		ISDN PBX	11		Internal
3	0 123 555 555 14 4		**1.** ISDN PBX **2.** List of local users	14	None	Internal

1. The incoming call for the SIP line number is directed to the Call Router along with the internal destination number that has been configured. The Call Router cannot find a matching entry in the call routing table, but it can find a registered user with the matching internal number. Since the user is an ISDN user, the Call Router directs the call to the ISDN line. The PBX receives the number 11 and can determine this call to be an internal call for the connected ISDN telephone.
2. The incoming calls to the MSNs for the connected ISDN terminal equipment can be assigned directly by the PBX itself, the Call Router is not involved here.

3. The PBX directs incoming calls to the MSNs for the connected VoIP terminal equipment to the internal ISDN bus with the internal MSN. The Call Router receives these calls as if they were internal calls and forwards them to the appropriate user since no corresponding entry can be found in the call routing table here either.

16.16.3 Connecting to an upstream SIP PBX

In this example, a branch office network will be connected to the headquarters network over VPN. In addition to data transfer, the telephone structure in the branch office is also connected to the central SIP PBX. A LANCOM VoIP router is used in the branch office network and a LANCOM VPN router acts as the VPN end point at the headquarters. The telephony subscribers at the headquarters receive internal extensions in the number range `101` to `199`; for each of the branch offices, a 10-digit block from the 200 range is reserved - in this example, `211` to `219`.



16.16.3.1 Objective

- Internal telephony between all locations.
- External telephony from the branch office via the SIP PBX at the headquarters with backup over ISDN.
- Calls from the branch office into the local telephone network via ISDN.
- Calls to emergency and service numbers via ISDN.

16.16.3.2 Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact one another with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.
- A SIP provider account.

16.16.3.3 Configuring the device

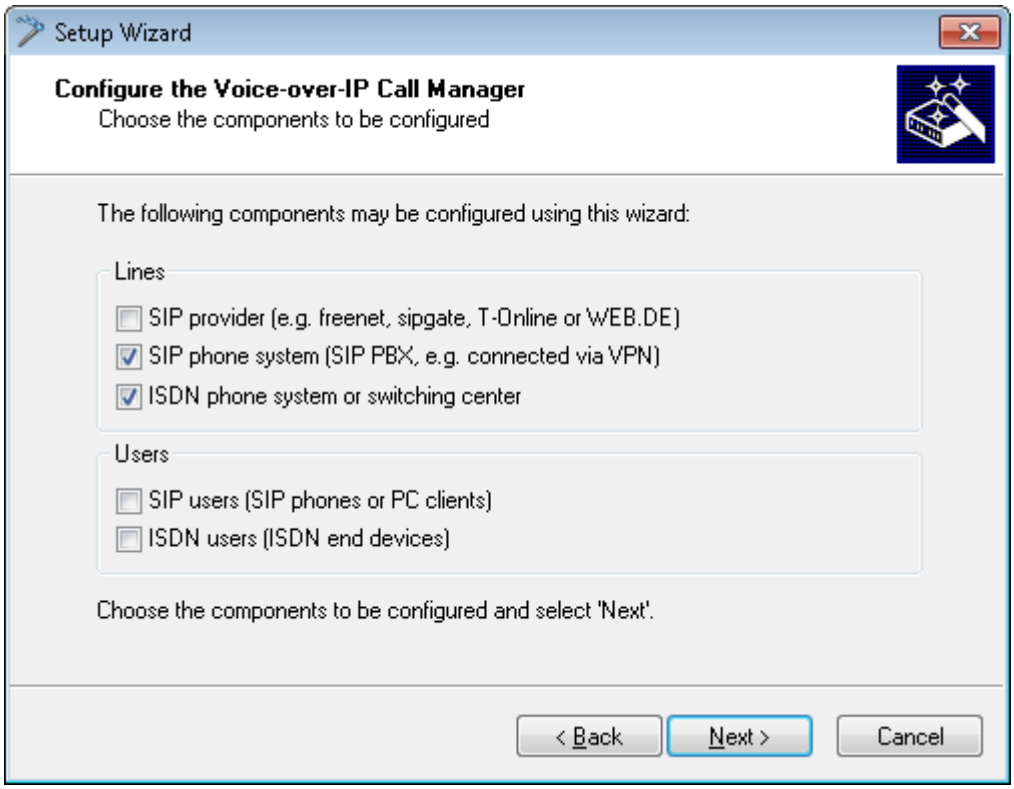
The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

	LANCOM, branch	SIP phone, branch	SIP PBX, headquarters
Internal VoIP domain	`mycompany.BRANCH01`	`mycompany.HQ`	`mycompany.HQ`

	LANCOM, branch	SIP phone, branch	SIP PBX, headquarters
Internal SIP subscriber numbers at the branch office		✔	✔
External ISDN telephone numbers (MSNs)	✔		
Country and local area code	✔		
SIP PBX line	HQ		
SIP PBX domain	`mycompany.HQ`		
SIP PBX registration password	✔		✔
Call route	1. Called number `2#` 2. Destination line `LOCATION_B` 3. Destination number `2#`		

Configuring the LANCOM in detail:

1. Under LANconfig, start the setup wizard for configuring the Voice Call Manager. Enable the options **SIP provider** and **ISDN phone system**.



2. Configure the device as described in the preceding examples:
   - ISDN line with MSN mapping
   - Area and country code for each location
3. Enter a unique domain for the local VoIP domain which describes the local VoIP area for the branch office, e.g. `mycompany.BRANCH01` for the first branch.

4. Configure the line to the SIP PBX with the following values:

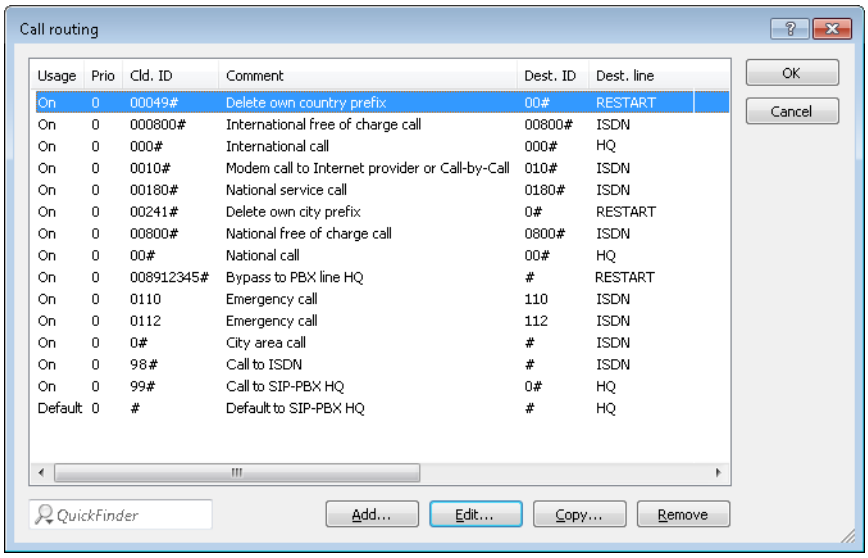
   - SIP PBX line name: A unique name for the line to the SIP PBX, for example `HQ` for "Headquarters".
   - PBX SIP domain/realm: Internal VoIP domain of the SIP PBX, e.g. `mycompany.HQ`.
   - Registrar (FQDN or IP) (optional): SIP PBX address in the headquarters network, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

     Use the IP address of the SIP PBX from the private IP address range at the headquarters as accessed via VPN.
   - Outbound proxy (optional): It is generally not necessary to designate the outbound proxy. You only need to enter a server designation here if the SIP PBX requires the corresponding addresses.
   - Shared PBX password: This password is used by all SIP users when registering at the SIP PBX. If registration with a shared password is not desired, then an individual password can be used for each SIP user. In this case, each of the SIP users are configured with their own password in the LANCOM.
   - Public PBX number: Here, enter the phone number where the SIP PBX can be reached from the public telephone network, e.g. from where the LANCOM is located. The number is entered with the **necessary** prefixes, but without an extension number. For example, if the SIP PBX is located in London and the LANCOM is in Birmingham, then the public PBX number is `020 12345`.

5. The call routing table suggested by the setup wizard automatically allows international and national long distance calls to be made via the SIP PBX at the headquarters.

   In addition, a **default route** is used to direct calls from the LANCOM VoIP users to internal SIP PBX numbers via the corresponding SIP PBX line.

   This special entry is only used during the second pass in the call routing table, after the first pass found no corresponding entry for "normal" routes and if no matching internal number was found in the list of local users.



16.16.3.4 Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples, although in this case the SIP PBX VoIP domain and the internal numbers configured in the SIP PBX are used.

Automatic SIP user authentication at the LANCOM and the SIP PBX.

Using the SIP PBX domain with VoIP terminal equipment registers the user in two ways:

- Since authentication uses a valid domain defined in the LANCOM, terminal devices are registered as "local users".
- Since this domain does not correspond to the LANCOM's own VoIP domain, a simultaneous attempt is made to authenticate at the upstream SIP PBX. If the password used corresponds to the password stored in the SIP PBX for this user, then the registration on the SIP PBX will be successful.

16.16.3.5 Configuring the SIP PBX

In the SIP PBX, all users from the branch office network are entered with their own internal number. For this purpose, either the shared password is entered or a separate password is assigned for each user.

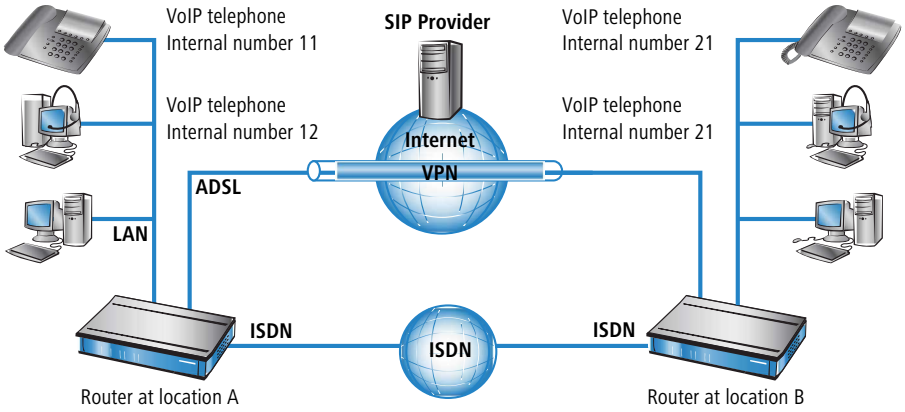
16.16.3.6 Call routing procedure for outgoing calls

	User	Dials	Correct call route	Correct user	Mapping, number in use	Destination line
1	VoIP phone, branch	`212`	None	VoIP softphone	`212`	Internal
2	VoIP phone, branch	`199`	**4** `#`	SIP subscribers at the headquarters	`#: 199`	SIP-PBX
3	VoIP phone, branch	`0 555 555`	**3** `0#`		`0241#: 0241 555 555`	ISDN
4	VoIP phone, branch	`0 0123 666 666`	**2** `00#`		`00#: 0123 666 666`	SIP-PBX

1. Internal call between two VoIP terminal devices at the branch office. The dialed number `212` does not match any of the routes listed in the call routing table. Therefore, the call router searches the local user list, finds the correct entry there and can forward the call internally.
2. Internal call between a VoIP terminal device at the branch office and the internal subscriber `199` at the headquarters. The dialed number `199` does not match any of the routes listed in the call routing table during the first pass. Similarly, no matching entry can be found in the local user list. In the second pass through the call routing table, the default routes are considered too. The route with the called number `#` (**4**) corresponds to all calls which could not be assigned earlier. The call to `199` is therefore conducted over the SIP PBX line.
3. External call from the branch office into the local telephone network. The dialed number `0 555 555` matches the route `0#` (**3**) in the call routing table. The call router removes the `0` outside-line access prefix, adds the area code for the local telephone network and makes the call to `0241 555 555` via the ISDN line.
4. External call from the branch office into a national telephone network. The dialed number `0 555 555` matches the route `00#` (**2**) in the call routing table. The call router directs the call to the SIP PBX line **unchanged**. Only now does the SIP PBX remove the `0` outside-line access prefix and directs the call to `0123 555 555` via the ISDN exchange line.

16.16.4 VoIP connectivity between sites without a SIP PBX

Companies with widely dispersed offices and without their own SIP PBX can also take advantage of VoIP site-to-site connectivity. In this "Peer-to-Peer" scenario, a LANCOM VoIP router has been implemented at two locations.



16.16.4.1 Objective

- Internal telephony at and between both locations.
- External telephony via the SIP provider with backup over ISDN.
- Calls to emergency and service numbers via ISDN.

16.16.4.2 Requirements

- LANCOM connected to the LAN and WAN, an ISDN TE interface is linked to the ISDN NTBA.
- The Internet connection has been set up by means of a VPN tunnel, as has the network connection between the two locations. All terminal devices can contact one another with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected. For each site, a separate number range is used; in this example, the internal numbers for location A begin with a `1` and the internal numbers for location B begin with a `2`.
- Each site has a SIP provider account.

16.16.4.3 Configuring the device

The following table provides a summary of the information required for configuration and where it can be entered. Basically, all that is needed is a SIP PBX line for each location that is correspondingly setup at the remote location

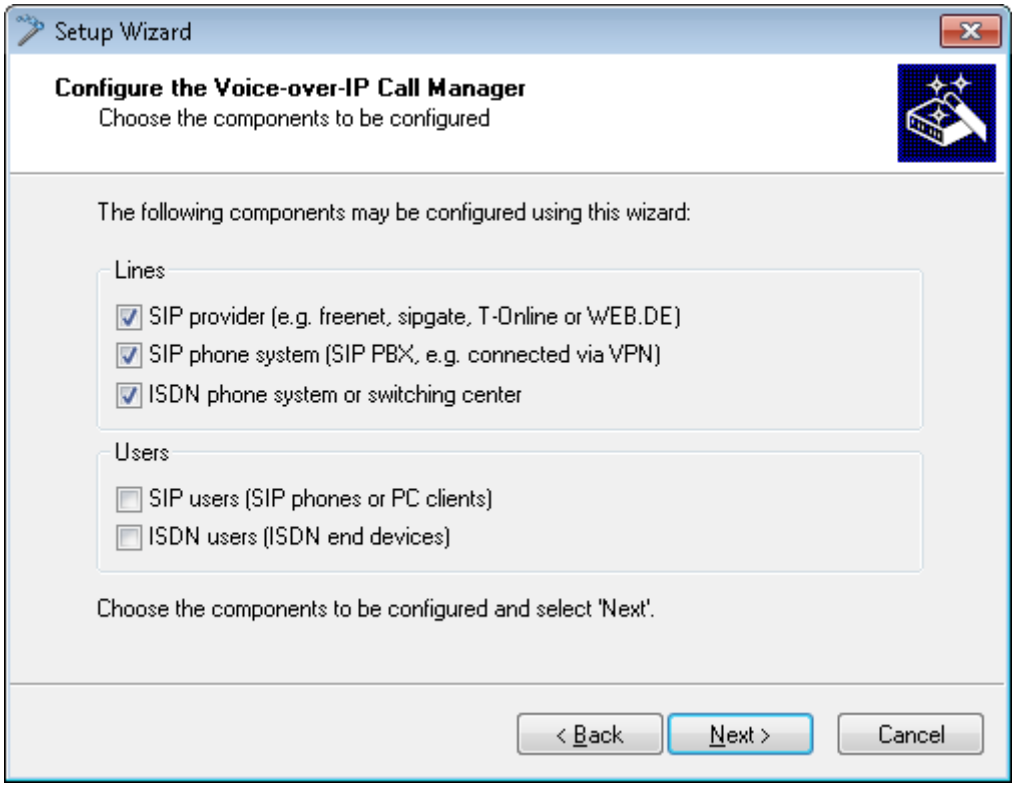
	LANCOM, site A	SIP phones, site A	LANCOM, site B	SIP phones, site B
Internal VoIP domain	`location_A.internal`	`location_A.internal`	`location_B.internal`	`location_B.internal`
Internal numbers		`10` to `19`		`20` to `29`
External SIP telephone number	✔		✔	
SIP account access data	✔		✔	
External ISDN telephone numbers (MSNs)	✔		✔	
Country and local area code	✔		✔	
SIP PBX line	`LOCATION_B`		`LOCATION_A`	

	LANCOM, site A	SIP phones, site A	LANCOM, site B	SIP phones, site B
SIP PBX domain	`location_B.internal`		`location_A.internal`	
Call route	1. Called number `2#` 2. Destination line `LOCATION_B` 3. Destination number `2#`		1. Called number `1#` 2. Destination line `LOCATION_A` 3. Destination number `1#`	

Although SIP PBX lines are the subject of the configuration presented here, you can still use this function even without a PBX.

Configuring the LANCOM in detail:

1. Under LANconfig, start the setup wizard for configuring the Voice Call Manager. Enable the options **SIP provider**, **SIP phone system** and **ISDN phone system**.



2. Configure the device as described in the preceding examples:
   - A line to a SIP provider
   - ISDN line with MSN mapping
   - Area and country code for each location
3. Enter a unique domain for the local VoIP domain which describes the local VoIP area for the site. Both sites use **different** VoIP domains, e.g. `location_A.internal` and `location_B.internal`.
4. Configure the line to the SIP PBX with the following values:
   - SIP PBX line name: Unique name for the line to the remote site.
   - PBX SIP domain/realm: Internal VoIP domain of the remote site.

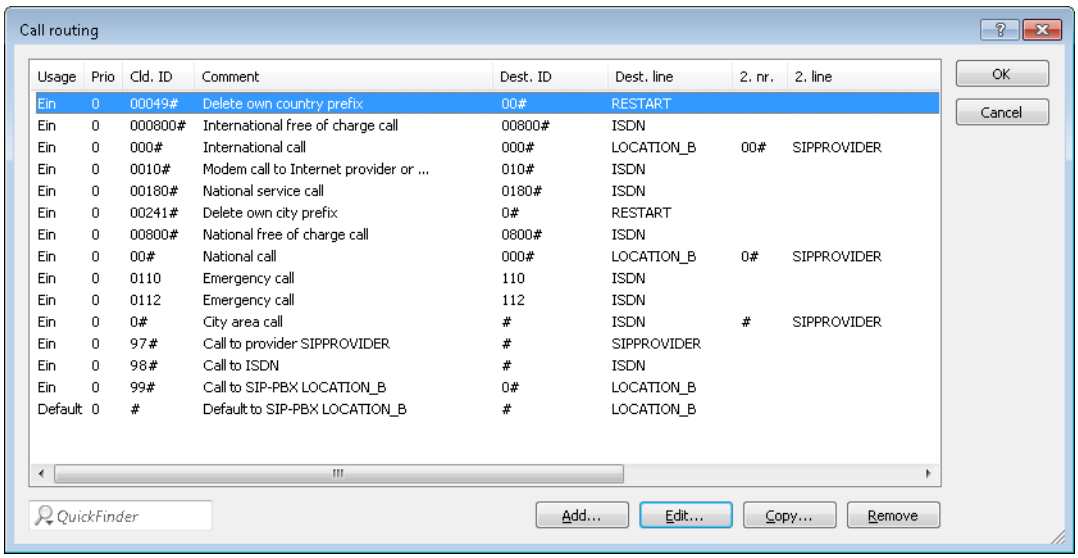
- Registrar (FQDN or IP): Address for the LANCOM at the remote site, in the event that the device cannot be identified via DNS resolution of the VoIP domain (PBX SIP domain/realm).

  Use the private IP address that can be reached via VPN for the LANCOM here, not the public IP.

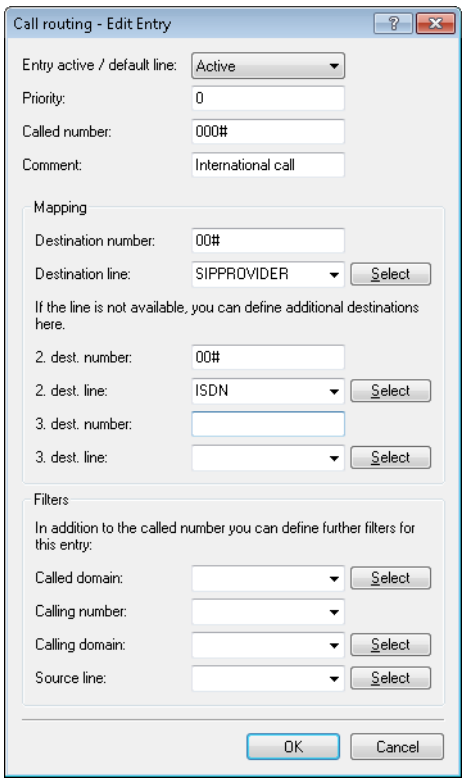
- Leave the field for the shared password empty when registering to the SIP PBX.
- Leave the field for the public PBX number empty.

5. The call routing table suggested by the setup wizard automatically allows international and national long distance calls to be made via the remote site's line, local calls are routed via ISDN.

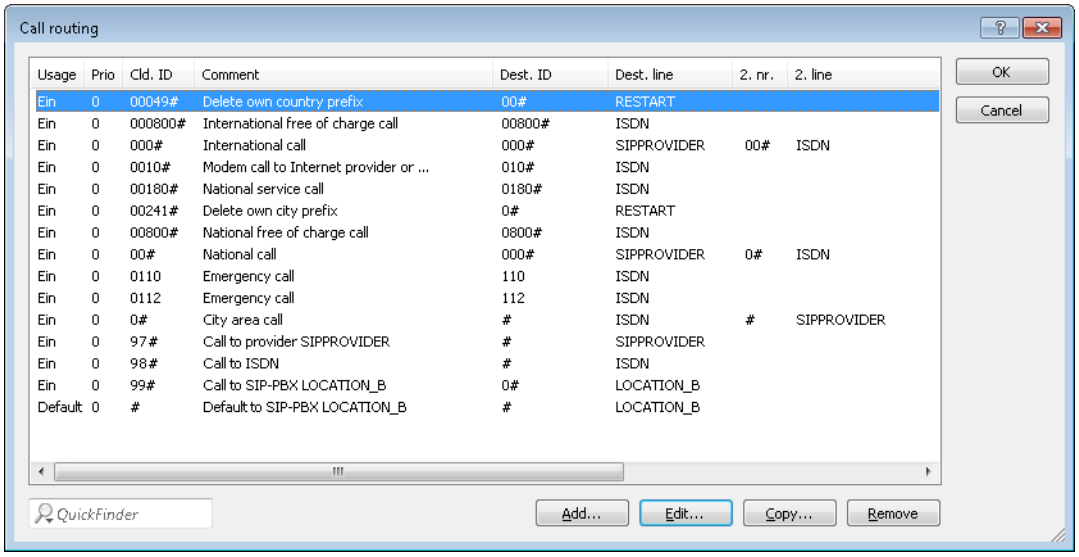
   In addition, a **default route** directs all numbers which cannot be resolved to the remote site's line.



6. Adapt the suggested call routing table in order to make international and national long distance calls via the SIP provider line with backup over ISDN. When doing so, please observe that the `0` preceding the number needs to be removed.



After adaptation for international and national long distance calls, the call routing table appears as follows:



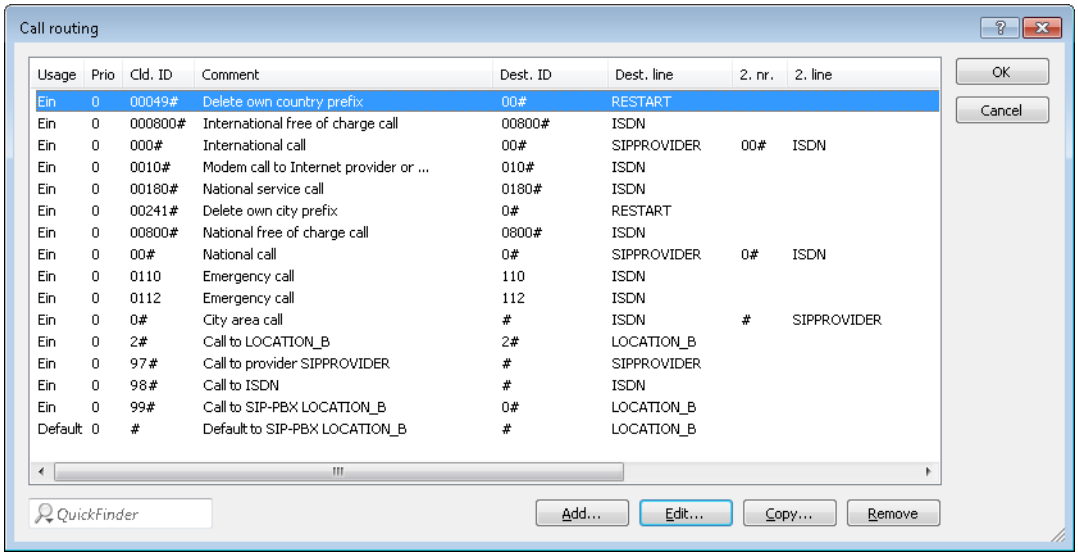
7. In this state, all calls that cannot be resolved by the call routing table and which do not have a corresponding entry in the local user list are automatically forwarded to the remote site.

   If this is not desired, for example where more than two sites are connected in this way, an additional entry can be used to detect the internal calls to a particular site. To achieve this, make a new entry (for the number range `20` to `29` at site B) in the call routing table with the following values:

- Called number / name: e.g. `2#` for all numbers that begin with a 2.
- Number / name: The called number is used unchanged as a destination number, e.g. in this case `2#`.
- Line: Enter the SIP PBX line for the remote location here, i.e. `LOCATION_B`.

In doing so, the default route is adjusted so that all numbers which cannot be resolved are transmitted via ISDN.

After adaptation, the call routing table appears as follows:



This entry for `LOCATION_B` is placed well down toward the end of the call routing table so as not to affect the more general rules. However, for interaction with the other routes, verify that only the internal numbers for the remote site are directed to the respective line.

16.16.4.4 Configuring the VoIP terminal equipment

The VoIP terminal equipment is configured as described in the preceding examples with internal VoIP domains and internal numbers for the local site.

16.16.4.5 Call routing procedure for outgoing calls

For this application, most calls take place as described in the preceding examples. Internal calls between locations are resolved as follows:

	User	Dials	Correct call route	Correct user	Mapping, number in use	Destination line
1	VoIP telephone location A	`21`	`2#`	none	`21`	`LOCATION_B`

1. Internal call between two VoIP terminal devices at locations A and B. The dialed number `21` matches the route **5** `2#` in the call routing table. The call router sends the call out over the line to the remote SIP PBX without changing the number.

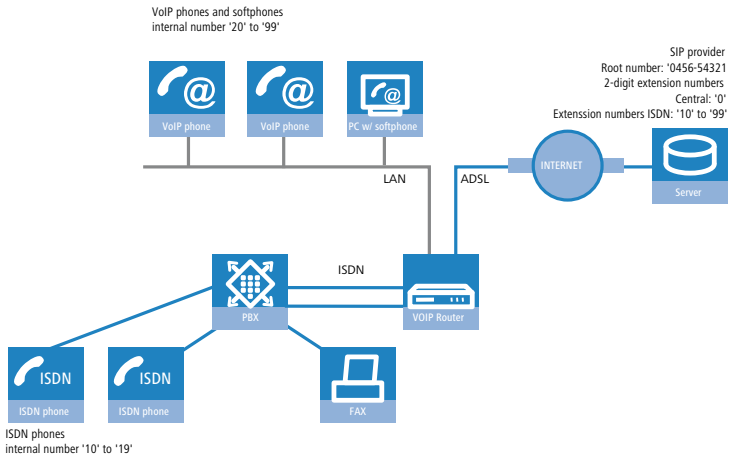
16.16.5 SIP trunking

In telecommunications jargon, trunking is the process by which several lines or connections are combined into one shared line. In the world of VoIP, SIP providers are increasingly offering products which provide the ability to make several calls simultaneously using a single account. Together with the possibility of being able to contact SIP participants via a shared

switchboard number with individual extensions (DDIs), these types of accounts are also becoming attractive for business customers.

There are two possible options when using a SIP account with trunking:

- The customer retains his previous ISDN connection, along with any corresponding telephone numbers from the telephone company, and sets up an additional account having a separate number range with a SIP provider.
- The customer ports the numbers used thus far from the telephone company to the SIP provider and from then on uses the same numbers using SIP.



In this example we will take a look at a company planning to add a SIP trunking account with up to 10 extension numbers. The ISDN terminal devices with point-to-point line extensions used thus far can be retained. All new employees are to be issued with a SIP telephone with an extension via the SIP account.

Unique extensions are used since staff members have to be able to call one another internally. In order to migrate smoothly towards SIP, all ISDN terminal devices are to be contactable using their extension number in **parallel** with the switchboard number of the SIP account. An ISDN telephone should respond to calls to `0456-54321 12`.

Outgoing calls should be directed via the SIP account.

16.16.5.1 Objectives in implementing the LANCOM VoIP router

- Connection of additional SIP terminal devices
- Internal calls between ISDN and SIP terminal devices.
- Low-cost calls by using a shared SIP account.

16.16.5.2 Requirements

- LANCOM connected to the LAN and WAN (via DSL/ADSL), ISDN NT interface(s) are connected to an ISDN PBX.
- The Internet connection has been set up. All terminal devices can contact one another with the IP addresses used.
- A dialing plan with a unique internal telephone number for each piece of terminal equipment to be connected.

16.16.5.3 Configuring the device

This is how the LANCOM is configured for operation at a point-to-point line:

1. When configuring SIP clients, all you need to enter are the internal VoIP domain of the LANCOM VoIP router and the associated internal phone number. The extension numbers previously used for the ISDN terminal devices remain unallocated.
2. A SIP provider line is created for the SIP account. The 'Trunk' option is selected as the mode for this line.
3. Routing of calls is governed by the call routing table. When using the Wizards available with LANconfig, the call routing table is preconfigured such that all out-going calls from ISDN and SIP devices are made using the SIP trunk account.

16.16.5.4 Process of call routing

In this example, call routing benefits from the unique internal telephone numbers.

- For incoming calls, the only information passed to the LANCOM VoIP router is the DDI. Since the DDI and internal numbers are the same in this example, an extension number can be used to put through calls to locally registered SIP users or to dynamic ISDN users.

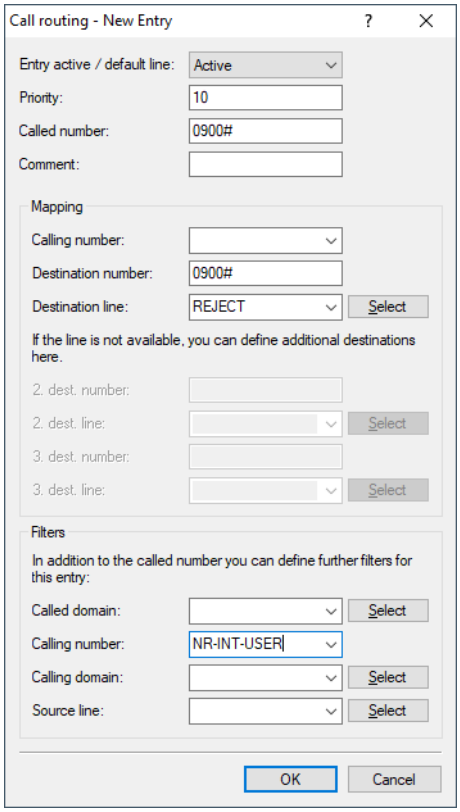
  If the reported DDIs cannot or should not be used directly as internal numbers, the ISDN and SIP mapping tables are used to set up the necessary telephone number translations.

- In the default setting after using the Wizards, SIP is taken to be the normal destination line (with the exception of local calls and special numbers). Local calls, for example, may be switched to SIP by changing an entry in the call routing table.

In this case, the SIP number is displayed at the subscribers on the other side of the connection, even if the call originates from an ISDN terminal device.

16.16.6 Block outgoing calls to service numbers

You have the option to block certain call numbers (e.g. charged hotlines such as 0900) with the following call route:

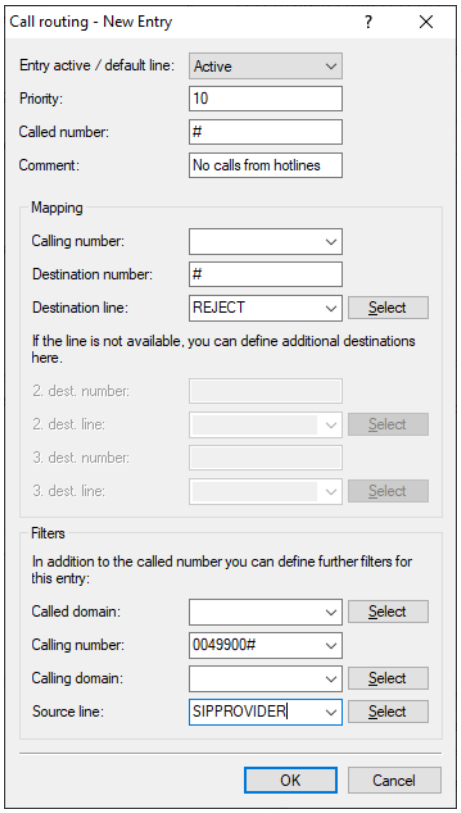


For the calling number, specify a registered client to restrict the rule to those calls made by the corresponding user.

By setting the source line to "User.#", "User.ISDN", "User.SIP" or "User.Analog", you have the option of restricting the rule to the corresponding subscriber, irrespective of the telephone number they are using.

16.16.7 Rejecting incoming calls

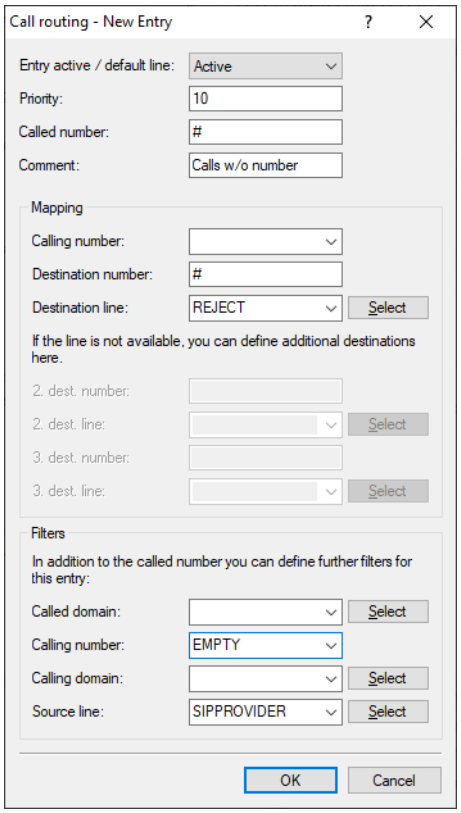
Incoming calls from charged hotlines (0900), for example, can be rejected with the following call route:



Select a source line, e.g. a registered SIP line, to restrict the rule to calls that are signaled via this line.

16.16.8 Reject calls without a calling number

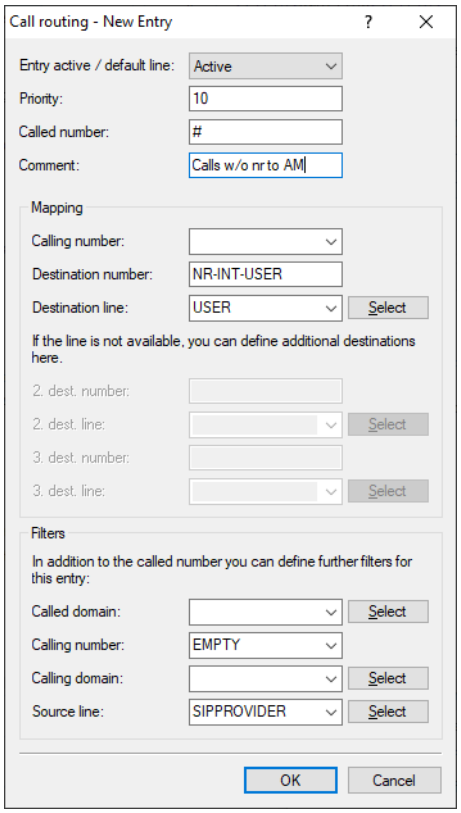
Set the following call route to reject incoming calls that do not contain a calling number:



Select a source line, e.g. a registered SIP line, to restrict the rule to calls that are signaled via this line.

16.16.9 Forwarding calls without a calling number

Set the following call route to redirect incoming calls that do not contain a calling number, e.g. to an answering machine:



Select a source line, e.g. a registered SIP line, to restrict the rule to calls that are signaled via this line.

16.17 Diagnosis of VoiP connections

16.17.1 SIP traces

Trace output can be used to check the internal processes in LANCOM devices during or after configuration. With a SIP trace, all of the SIP information is displayed that is exchanged between a LANCOM VoIP router and a SIP provider or a upstream SIP telephone system The SIP trace is activated with the following command:

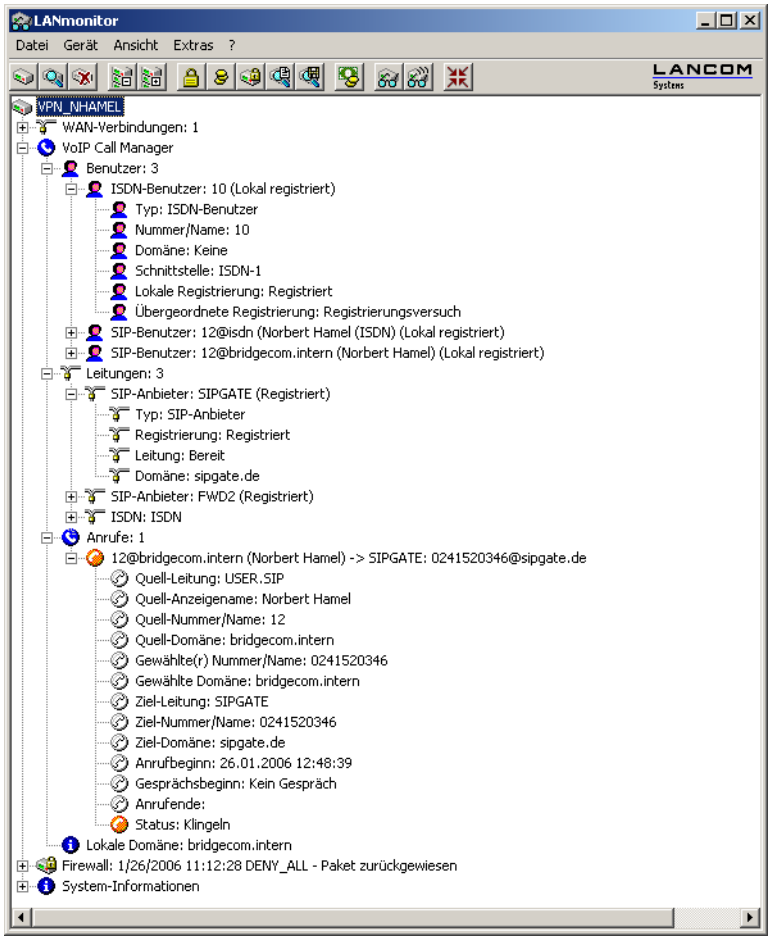
```
trace + sip-packet
```

16.17.2 Connection diagnosis with LANmonitor

LANmonitor displays a wealth of information about calls switched in the LANCOM:

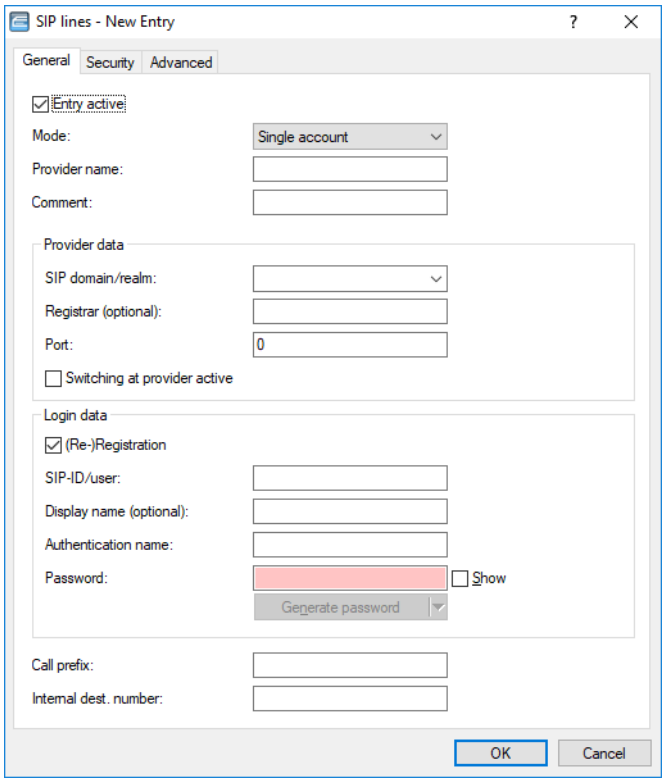
- Information about the registered users.
- Information about the lines available.
- Information about current calls, including the translation of telephone numbers and domains by the Call Manager.

› Information about the fixed and automatic QoS bandwidth reservations and settings.



16.18 VoSIP support in the Voice Call Manager

LCOS supports Voice over Secure IP (VoSIP). This function enables you to encrypt the signaling and voice data. From LCOS version 9.20, you can use VoSIP on all LANCOM business VoIP routers.



Signaling encryption

This setting determines the protocol used for signaling encryption (SIP/SIPS) for communications with the provider.

Automatic

NAPTR (Naming Address Pointer) records are used for DNS resolution. In the DNS data, the provider specifies the use of transport protocols such as UDP, TCP or TLS. The provider can also specify weights or priorities.

If TLS is specified as the transport protocol for signaling encryption by NAPTR, voice encryption is also used automatically, regardless of the explicit configuration setting of voice encryption.

No (UDP)

All SIP packets are transmitted connectionless. Most providers support this setting.

No (TCP)

All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.

TLS

Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider. The TLS version selected in the configuration is taken as the minimum requirement for TLS encryption.

Speech encryption

This setting determines if and how the speech data (RTP/SRTP) is encrypted when communicating with the provider.

Speech encryption	
Reject	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are rejected. The speech channel is not encrypted.
Ignore	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are accepted. The speech channel is not encrypted.
Prefer	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are accepted. The speech channel is only encrypted if the remote peer also supports encryption.
Force	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are rejected. The speech channel is either encrypted or is not established.

If you require the encrypted transmission of speech data, the signaling must also use an encrypted channel. Please note that the use of SRTP is no guarantee of end-to-end encryption.

16.19 Auto provisioning LANCOM DECT 510 IP

LCOS facilitates the automatic installation and configuration of the base station with up to 6 DECT handsets. When connected to a LANCOM router, the LANCOM DECT 510 IP makes it easy to register the handsets and to assign them individual phone numbers.

The LANCOM DECT 510 IP base station can be configured via WEBconfig. This is not strictly required. If provisioning is enabled, your router configures the base station automatically. To enable the provisioning on your router, navigate to the LANconfig menu **Management** > **General** > **Advanced** > **Enable the provisioning server** and set the value to **Yes**. At the console, you set the corresponding parameters under **Setup** > **Provisioning-Server** > **Operating** (SNMP-ID 2.103.1).

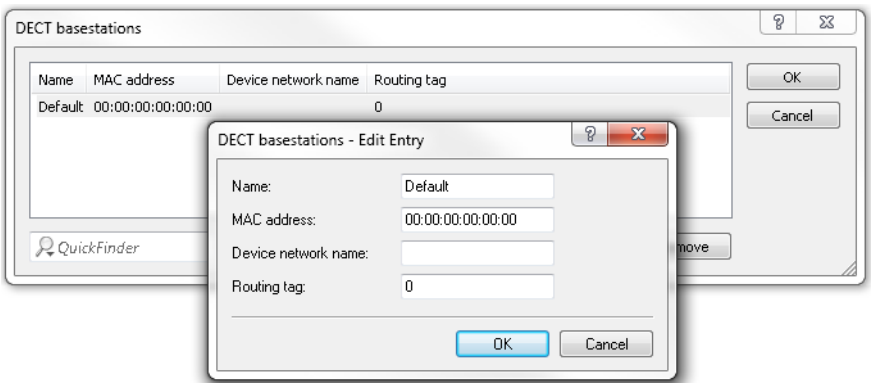
For the automatic configuration of the LANCOM DECT 510 IP, the base station needs to be connected to the router and the handsets registered with the base station.

You also have the option to configure the base station by means of the All-IP Wizard. Simply follow the instructions provided by the Wizard.

16.19.1 Configuring DECT base stations and handsets with LANconfig

To configure the DECT base station in LANconfig, go to **Voice Call Manager** > **Users** > **DECT base stations** and add a new entry to the table.

If auto-provisioning is to apply for all of the LANCOM DECT 510 IPs, or if they should all be configured the same, there is no need for any further entries in this table. The default entry takes care of everything.



Name

Specify a unique name for this base station here.

MAC address

Enter the MAC address of the base station.

If you wish to permit communications with any MAC address, enter `00:00:00:00:00:00` (default).

Network name

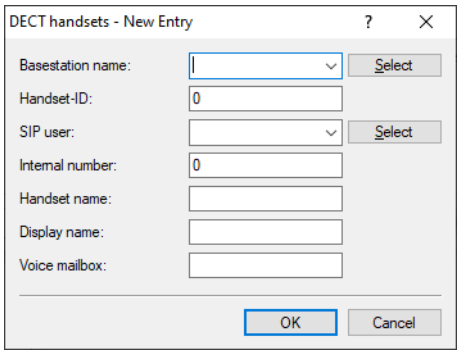
Here you optionally specify a network name that is displayed with the base station in the network.

Routing tag

The interface tag allows you to restrict the auto-provisioning of LANCOM DECT base stations to a specific network. This is particularly useful if your network contains IP addresses that are open to the public (e.g. via a Public Spot or DMZ). This restriction prevents SIP access credentials for the DECT base station from being unintentionally transmitted to third-party devices.

If you wish to use this service for all networks, enter the routing tag "0" here.

To configure the DECT handsets in LANconfig, go to **Voice Call Manager** > **Users** > **DECT handsets** and add a new entry to the table.



Base station name

Here you select the base station where the corresponding handset is registered.

Index

Enter here the number of the corresponding handset (e.g. "0" for handset 1, "1" for handset 2, etc.).

SIP user

Select the phone number of the handset here.

Internal Number

To use internal telephony via the LANCOM DECT base station, the handsets must be uniquely identifiable. This is done via a unique two-digit number (11–99), by which the handset can be dialed directly using the "Int" button. If the value 0 is set, the next available number is searched for and assigned automatically.

Handset name

Here you set the name to be shown in the display of the handset.

Display name

Here you set the name to be sent to a caller.

Voice mailbox

Enter the phone number of your voice mailbox here. This phone number is dialed by pressing and holding the button "1" on the handset.

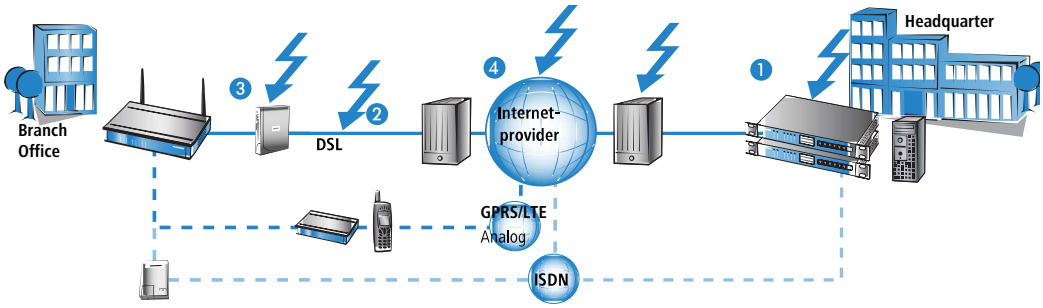
17 Backup solutions

17.1 High availability of networks

Networked cooperation between several offices or even between continents has become an everyday part of modern business. The paths of communication between headquarters, subsidiaries and field workers almost always rely upon public infrastructures. VPN has become established as the de facto standard for cost-effective and secure enterprise communications over the Internet.

However, many of important elements in these network structures remain susceptible to failure which could have severe consequences for business operations:

- The remote Internet gateway **1** can fail.
- The physical lines for the connection to the Internet or to a remote network can fail:
  - The Internet-access cable between the site and the provider **2** could fail; after damage from construction work, for example.
  - The DSL connection **3** may fail, while the ISDN/LTE connection remains functional.
- The provider's network **4** may malfunction or even fail.



Devices from LANCOM offer a range of security and backup functions that can be used for the protection of your network from faults.

17.1.1 How is a network-connection disturbance detected?

The first stage in protecting a network connection from the effects of a fault is to detect the fault itself. The following methods are available to check the connections:

- Check the PPP connection to the provider with PPP LCP echo monitoring.
- Checking the accessibility of arbitrary sites by name or IP address with ICMP polling (end-to-end ping).
- Check the tunnel end points with “dead-peer detection” (DPD).

17.1.1.1 PPP LCP echo monitoring

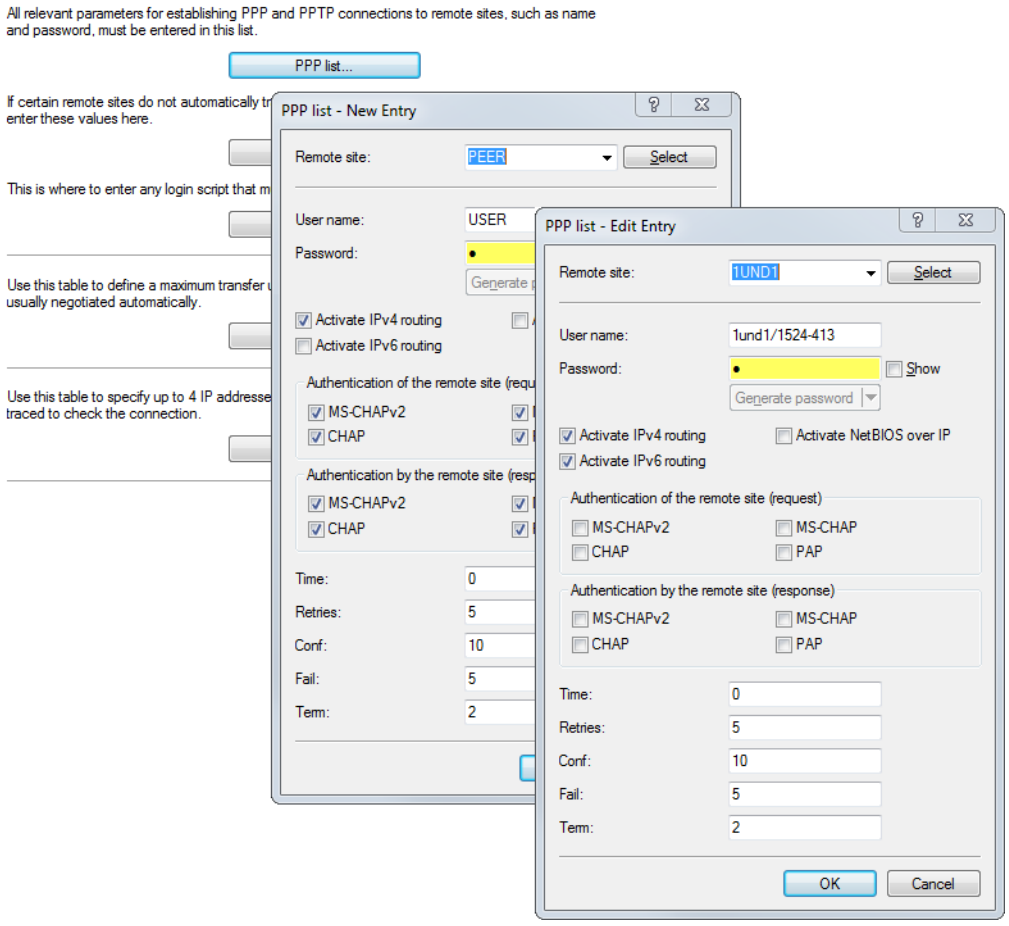
The method checks the PPP connection to a specific remote site with regular LCP requests. This method is typically used to check the connection to the Internet provider. The LCP requests are directed straight to the dial-in node.

In the PPP list, a time interval for the transmission of LCP requests to the remote site is defined for this connection. Further, for the event that LCP replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the line is considered to have failed.

- **Time:** The time entered into the PPP list must be multiplied by the factor 10 to arrive at the actual interval between two LCP requests. Entering the time as "5" means that an LCP request will be prompted every 50 seconds.
- **Retries:** If no reply to an LCP request is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. Entering "5" under retries means that the LCP request will be repeated 5 times before the connection is considered to have failed.

PPP LCP monitoring only checks the PPP connection path as far as the Internet provider.

The settings for LCP monitoring in LANconfig can be found in the configuration section **Communication** > **Protocols** > **PPP list**.



Command line: **Setup** > **WAN** > **PPP**

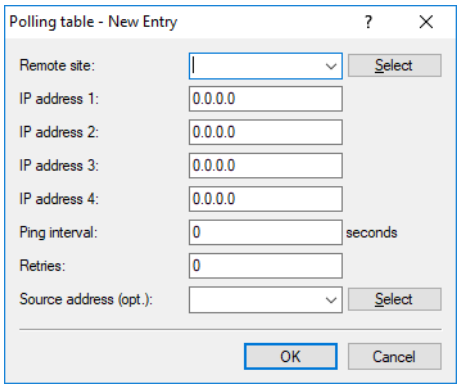
17.1.1.2 ICMP polling for IPv4

Similar to LCP monitoring, ICMP polling transmits regular requests to a remote site. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMP pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to have failed.

With the ICMP polling, an entire connection can be monitored from end to end.



The settings for ICMP polling in LANconfig can be found in the configuration section **Communication** > **Protocols** > **IPv4 polling table**.

Command line: **Setup** > **WAN** > **Polling-Table**

Remote site

Name of the remote site which is to be checked with this entry.

IP address 1-4

IP addresses for targeting with ICMP requests to check the remote site.

If no IP address is entered for a remote site that can be checked with a ping, then the IP address of the DNS server that was determined during the PPP negotiation will be checked instead.

Ping interval

The time entered into the polling table defines the time interval between ping requests. If the value "0" is entered, then the standard value of 30 seconds applies.

Retries

If no reply to a ping is received then the remote site will be checked in shorter intervals. The device then tries to reach the remote site once a second. The number of retries defines how many times these attempts are repeated. If the value "0" is entered, then the standard value of 5 retries applies.

Source address (opt.)

Optional source address sent with the ping; this is also the destination for the answering ping.

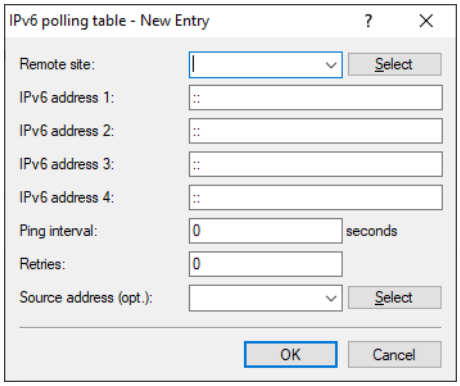
17.1.1.3 ICMPv6 polling

As with LCP monitoring or ICMP polling for IPv4, ICMPv6 polling regularly sends requests to a remote peer. Ping commands are transmitted and the answers to them are monitored. Unlike LCP monitoring, the target site for ICMPv6 pings can be freely defined. Pinging a router in a remote network thus provides monitoring for the entire connection and not just the section to the Internet provider.

A ping interval is defined for the remote site in the IPv6 polling table. Further, for the event that replies are missed, the number of retries before the transmission of a new LCP request is defined. Should the transmitter not receive any reply to the retries, the target for the ping requests is classified as unavailable.

Up to four different IPv6 addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IPv6 addresses are unavailable is the connection considered to have failed.

The settings for ICMPv6 polling in LANconfig can be found in the configuration section **Communication** > **Protocols** > **IPv6 polling table**.



Remote site

Here you select the name of a remote site from the list of remote sites.

IPv6 address 1- 4

Enter here up to 4 IPv6 addresses, which are pinged one after the other in order to check the connection for this peer. The connection is considered to be intact even if just one of the specified IPv6 addresses can be reached.

Be sure to choose IPv6 addresses that can be reached reliably to avoid unnecessary backup connections being initiated.

If you set all four IPv6 addresses as "::", the DNS server that is pinged is the one assigned via DHCPv6 or router advertisement.

Ping interval

Enter the ping interval in seconds here.

If you enter 0 both here and for retries, a default interval of 20 seconds and 5 repetitions is used.

Retries

Enter the number of tries each second if no response is received to a ping. If the repeated pings also go unanswered, the connection is terminated.

If you enter 0 both here and ping interval, a default interval of 20 seconds and 5 repetitions is used.

Source address (optional)

This is where you can configure an optional sender address to be used instead of the one that would normally be selected automatically for this target address.

17.1.1.4 Dead peer detection (DPD)

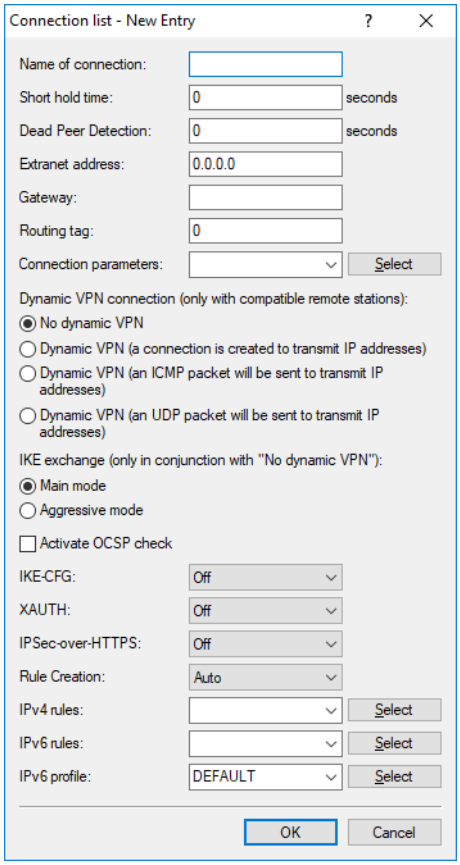
This method of connection monitoring is used when VPN clients dial-in to a VPN gateway. This is designed to ensure that a client is logged out if there is an interruption to the VPN connection, for example when the Internet connection

is interrupted briefly. If the line were not to be monitored, then the VPN gateway would continue to list the client as logged-on. This would prevent the client from dialing in again as, for example, the WLANmonitor does not allow a simultaneous dial-in using the same serial number.

For the same reason, without line monitoring a user with the same "identity" (user name) would be prevented from dialing in because the associated user would still be in the list for the logged-in client.

With dead-peer detection, the gateway and client regularly exchange "keep alive" packets. If no replies are received, the gateway will log out the client so that this ID can be registered again once the VPN connection has been re-established. The DPD time for VPN clients is typically set to 60 seconds. Possible values: 0 – DPD deactivated; 30 to 4,294,967,294 seconds

The settings for dead peer detection in LANconfig are located under **VPN** > **IKE/IPSec** > **Connection list**.



Command line: **Setup** > **VPN** > **VPN-Peers**

17.1.2 High-availability of lines – backup connections

If there is a disturbance to the connection with the Internet provider or to a remote network, a backup line can act as a temporary replacement for the normal data line. This requires the existence of a second physical connection which can be used to contact the remote site. Examples of backup lines are typically:

› Mobile connections via integrated 4G/5G modems

17.1.2.1 Configuration of the backup connection

The following steps are necessary to define a backup connection:

1. The backup connection requires the appropriate WAN interface to be set up so that the remote site can be reached via this alternative route. If, for example, the ISDN line is to serve as the backup connection, then the remote site is set up as an ISDN remote site (along with the necessary entries in the communications layers and in the PPP list).
2. If the connection to the remote site cannot be checked with LCP requests, the monitoring of the connection should be initiated with an entry in the polling table.
3. Assignment of the new backup connection to the remote site which is to be backed up. This entry is made in the backup table. Dedicated entries in the routing table are not required for a backup connection. The backup connection automatically takes over the source and target networks from the remote site that routes the data under normal operating conditions.

   A remote site can be assigned with multiple backup lines in the backup table. In the case of backup, the system decides which backup line is to be used first:

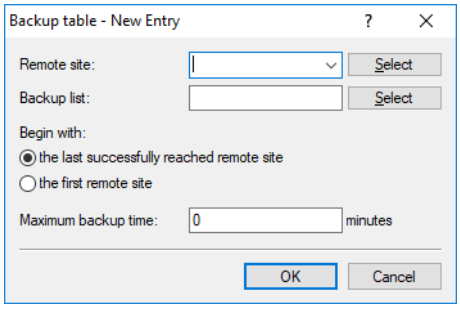
   - The last remote site that was reached successfully
   - The first remote site in the list

The **maximum backup time** specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

The backup table in LANconfig is located under **Communication** > **Backup** under **Backup table**.



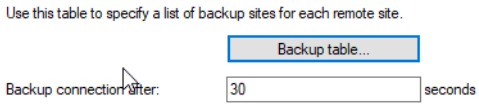
17.1.2.2 Triggering the backup connection

The backup is triggered when the monitoring mechanisms defined for the standard connection (LCP or ICMP polling) detect that contact to the remote site has been lost.

The backup connection will be established if:

- The backup delay time has expired and
- either
  - a data packet is to be transferred or
  - a hold time of 9999 seconds has been defined for the backup connection.

The backup delay time is entered in LANconfig in the configuration section **Communication** > **Backup** > **Backup connection after** or alternatively via the command line under **Setup** > **WAN** > **Backup-Delay-Seconds**.



The backup timer also controls the VRRP switchover time.

17.1.2.3 Return to the standard connection

The router constantly tries to establish the standard connection while the backup connection is active. As soon as the standard connection has been established, the backup connection is terminated and the line monitoring with LCP or ICMP polling is resumed.

Only keep alive connections return automatically!

The standard connection will only be automatically reestablished after a backup event if the hold time for the connection is configured properly:

- A hold time of "0" means that the connection will not be actively terminated. If the connection is terminated or interrupted due to interference, it will not be automatically established again. The connection will only be reestablished when communication is required of it.
- A hold time of "9999" means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to "9999" for connections to the Internet provider (in the corresponding name list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically reestablished and resumes data transfer after interruption.

17.1.3 High-availability of gateways – redundant gateways with VPN load balancing

Another cause of failure apart from the connection to the provider or to another network may lie with the local gateway. Severe effects can result from the failure of a central VPN gateway that is used, for example, to connect the networks of multiple remote locations with the central network at headquarters.

To ensure that the headquarters remains in contact, multiple VPN endpoints (generally identically configured VPN gateways operated in parallel) can be installed. Should line polling (with dead-peer detection, ICMP line polling) indicate a failure, then a variety of strategies (e.g. the random selection of one of the available gateways) can be used to enable communication to a different VPN end point. At the central headquarters, the new router and the local default gateway are propagated by dynamic routing (RIP V2).

To avoid the situation where the additional VPN gateways "remain unused", intelligent "load balancing" ensures that all of the devices share the load of incoming and outgoing connections also under normal operating conditions.

17.1.4 High availability Internet access – Multi-PPPoE

The third of the different basic sources of failures is the case where the gateways and connections are in order but the provider's own network is down. Such cases are handled by setting up multiple PPoE connections at the physical interface of a single device (Multi-PPPoE).

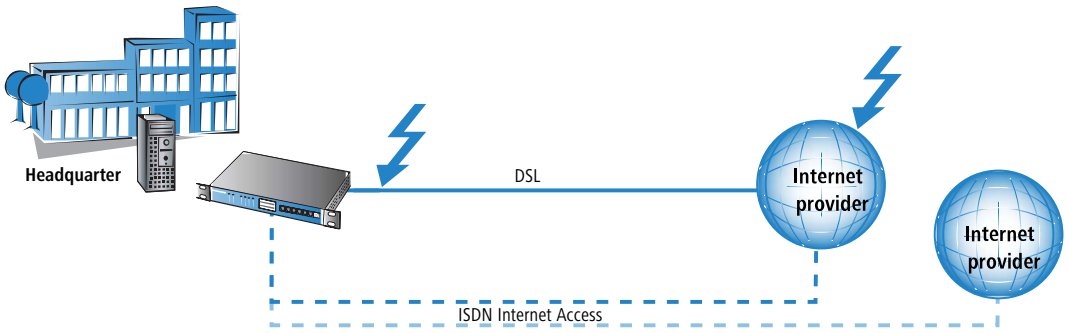
To define these backup solutions as alternative Internet accesses you can use, for example, the Setup Wizard to set up two Internet access accounts one after another. The standard Internet access for normal operations should be set up last. Consequently, the entries in the routing table will be associated with the appropriate remote site.

Additionally, an entry is made in the backup table that defines the alternative Internet access account as the backup to the remote site at the standard provider.

17.1.5 Example applications

17.1.5.1 Backing up DSL Internet access with ISDN Internet access

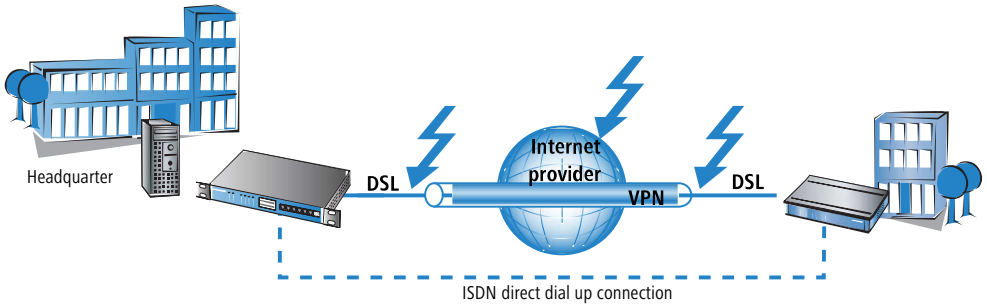
In this simple backup scenario, Internet access is realized via a DSL connection. An ISDN connection is defined as a backup in case of failure of the DSL Internet access.



This backup solution can be quickly and easily set up with the help of the LANconfig Setup Wizard, for example. A further degree of security is available by defining another Internet provider in addition to the standard provider. This solution caters for the contingency where the provider's network fails and the problem is not caused by the DSL connection.

17.1.5.2 Backing up dynamic VPN network connectivity with a direct ISDN dial-in connection

In the case that a branch office is connected to the headquarters via a VPN connection, the Internet-based VPN connection can be backed up by a direct ISDN dial-in connection. Should the Internet connection fail at either of the two routers, the data transmission is transferred to the ISDN link.



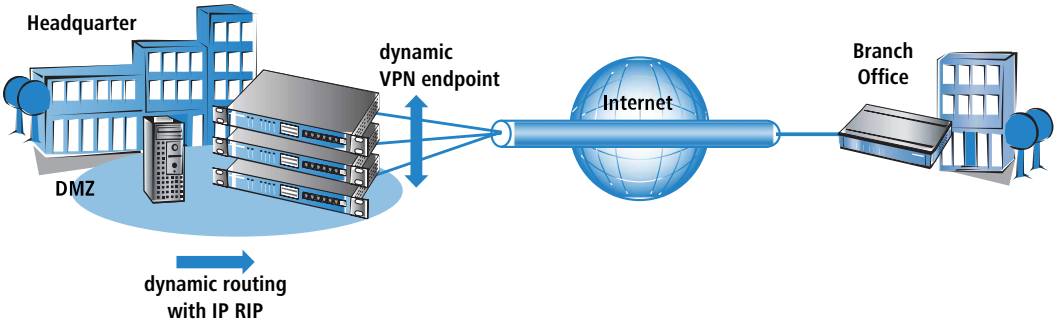
In this scenario we are assuming a fully configured VPN connection between the two networks.

- A LAN-LAN connectivity via ISDN is additionally set up between the two networks. Do **not** use the Setup Wizard to set up this network connectivity! The Wizard would change the entries in the routing table and would thus upset the function of the VPN network connection. Set up the ISDN network connectivity in both routers manually—with the appropriate entries in the list of remote sites, the PPP list, and with the necessary telephone numbers and access identifiers.
- In the gateway at the headquarters, create an entry in the backup table that acts to backup the VPN remote site via a directly dialed ISDN remote site.
- Further, the router at the headquarters requires an entry for the monitoring of a remote device in the network at the branch office: usually the LAN IP address of the remote VPN gateway. This entry ensures that the router at the headquarters can react immediately to a failure of the VPN connection.

Should there be a failure in the connection between the headquarters and branch office (on the way to the Internet provider or at the provider itself) then the ISDN connection takes over the data transfer independent of the Internet.

17.1.5.3 Redundant VPN gateways

In decentralized company structures that rely on VPN for networking the various locations, the availability of the central VPN gateway is of particular significance. The company-wide communications only remain reliable as long as these central dial-in nodes are working properly.



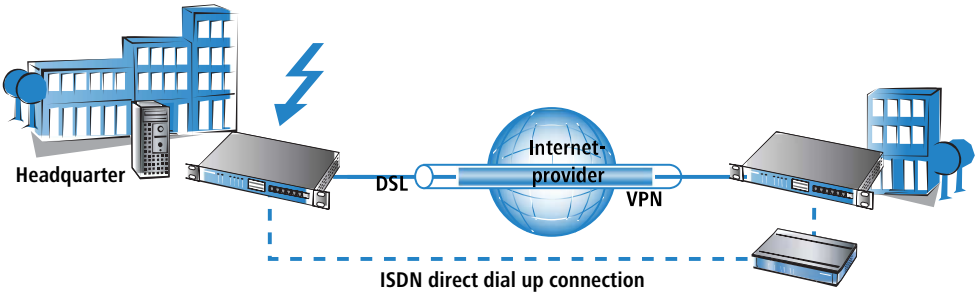
With the option of configuring several "remote gateway" addresses as the "dynamic VPN end point" for a VPN connection, LANCOM VPN gateways offer a high level of availability by using redundant devices. This involves multiple gateways at the headquarters being set up with identical VPN configurations. On location at the satellite sites, all of these available gateways are entered as possible remote sites for the VPN connection. If one of the gateways is unavailable, the remote router automatically redirects the request to one of the other routers.

To ensure that the computers in the LAN at the headquarters know which VPN gateway it to be used to reach a particular satellite station, the outband router currently connected to the remote site is propagated via RIPv2 to the network at the headquarters.

A powerful mechanism for load balancing between the VPN gateways at the headquarters is attained with the configuration of the satellite stations to select the remote site for VPN connection on a random basis ("VPN load balancing").

17.1.5.4 Backing up a VPN gateway with an ISDN gateway and RIP

Going a step further, the VPN gateways themselves can be backed up in case of failure. This case assumes the existence of a VPN connection between two gateways. In the event that one of the two VPN devices should fail, an ISDN connection is to take over the data transfer; in this case via a direct dial-in connection.



Regarding the configuration of this solution, we again assume a functional VPN connectivity of the two networks. The following additional steps are required:

- A standard ISDN network connectivity that routes the same subnets as the VPN connection is set up between the two ISDN routers. In the routing table, however, a distance is entered that is at least 1 higher than the corresponding route in the VPN gateway.
- The local RIP (RIP V2) is activated in all of the routers involved. This allows the VPN and ISDN routers to inform each other about the known routes to the remote sites. The higher distance of the route via the ISDN gateway is, under normal circumstances, the poorer route.

› It is not necessary to define backup connections in this case as a different device should take over the data transmission.

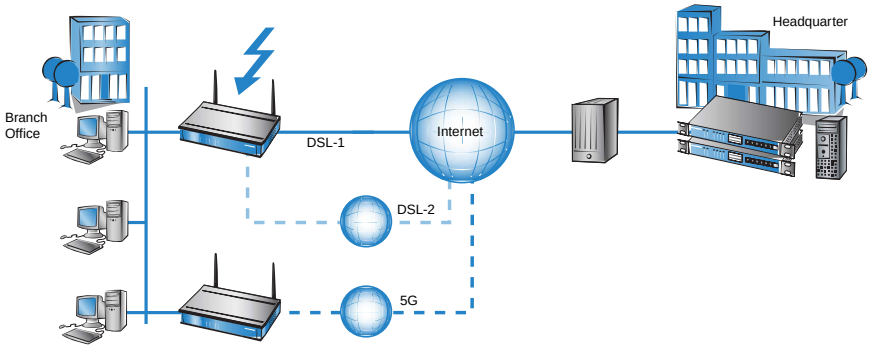
If there is a disturbance in the connection between the VPN devices, the value for the distance of the corresponding routes changes automatically: A route which is not available is marked with a distance of 16. Consequently, the route entered into the ISDN router automatically becomes the "better" solution and all data packets will be re-routed over the ISDN connection. As soon as the VPN connection is re-established, the distance changes to a value below that of the ISDN connection and the backup will be terminated as intended.

17.2 Backup solutions and load balancing with VRRP

17.2.1 Introduction

For businesses in particular, the high availability of data connections presents an essential requirement of the network components. The devices provide various mechanisms for securing data transfer as a backup solution:

- Various WAN interfaces (DSL, Fiber, 4G/5G) enable data transfer over a second physical medium if the primary WAN interface is disturbed or fails.
- In order to provide protection from failure of an Internet provider's network, different Internet access accounts can be configured with Multi-PPoE.
- Two or more VPN gateways in a network can share the VPN tunnels required, thus keeping data traffic alive even in cases of temporary failure of a VPN end point.
- VRRP can now also be used to implement a sophisticated backup system for protection against router hardware failure. Two or more routers are installed in a network, one of which can replace the other in case of device failure.
- In addition to the normal VRRP, the triggering of the backup event can be linked to the availability of a data connection. With this additional feature, devices with more than one WAN interface (e.g. two DSL interfaces) can be implemented flexibly into backup solutions. The backup event is triggered, for example, when the default route is no longer available via the first DSL interface. The device's second DSL interface can take its place further along in the backup chain should the the backup router also fail. However, the 5G interface of the device can take up another place in the backup chain if the backup router is also disrupted.



The VRRP failover time is influenced by the backup timer (see *Triggering the backup connection* on page 1495).

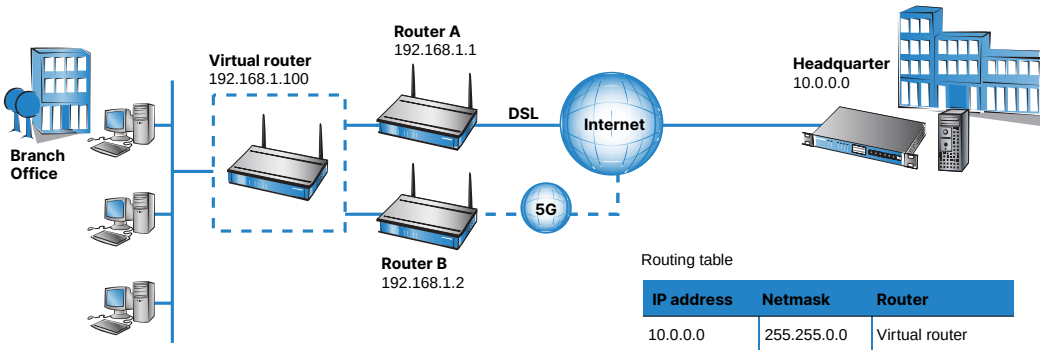
17.2.2 Virtual Router Redundancy Protocol

VRRP—Virtual Router Redundancy Protocol—enables multiple physical routers to appear as a single "virtual" router. Of the existing physical routers, one is always the "master". The master is the only router that establishes a data connection to the Internet, for example, and transfers data. The other routers only play a role when the master fails (e.g. due to a hardware defect or because its Internet connection is no longer available). Using the VRRP protocol, which is described in *RFC 5798*, they negotiate which device should assume the role of master. The new master completely takes over the tasks that were carried out by the previous master.

17.2.2.1 Virtual and physical routers

Dynamic routing protocols such as RIP adapt the entries in dynamic routing tables when, for example, a route is no longer available. When using VRRP, hosts in the LAN can use a static routing table even though the gateway IP address may change, for example, when a device fails due to a defect and another device takes over its functions. VRRP uses “virtual routers” in the routing tables so that the network users always find the right gateway nevertheless. A virtual router is announced on the network with the IP address '192.168.1.100' in the same way as a “normal” router would be and takes over the function of a gateway to certain remote sites. The actual work of data transfer is carried out by the physical routers behind the virtual router.

- Under normal operating conditions, for example, router A with the IP address '192.168.1.1' establishes the connection to the Internet.
- If router A fails, then router B with the IP address '192.168.1.2' takes over the functions of router A. The network clients do not notice this change; for them, the “virtual” router '192.168.1.100' is still the gateway.



From a more technical standpoint, a router in a network requires a unique MAC address in addition to an IP address. Therefore, when defining a virtual router, a virtual MAC address is defined simultaneously which the virtual router reacts to. The virtual MAC address is formed as '00-00-54-00-01-xx', whereby 'xx' stands for the unique router ID.

In order to determine which physical router reacts to the combination of virtual IP and MAC address, priorities are used for the physical routers. For this purpose, every physical router is assigned a priority. The router with the highest priority takes over the functions of the virtual router as master and thus reacts to the virtual IP and MAC addresses. If two physical routers have the same priority, then the router with the “higher” physical IP address is considered to be the master.

All physical routers report their availability on a regular basis so that, should the current master fail, the router with the next highest priority can take over the routing function at the end of this interval at the latest. If a device determines that it cannot complete the tasks required, it can actively log off before the end of the interval thereby triggering the transfer of the master role to the router with the next priority.

The major advantage of virtual routers is that they enable very flexible scenarios with backup and load balancing functions which remain virtually undetected by the LAN. Clients in the local network randomly select a DHCP server from those available and retrieve the required address information from this server.

Address assignment via DHCP with more than one DHCP server in the LAN

Several DHCP servers can be operated parallel to each other in a LAN without disrupting one another's functionality. Upon establishing a network connection, the DHCP clients request an IP address selecting one of the available DHCP servers. The DHCP server receiving the request checks to determine whether the address requested is available or already in use within the LAN before assigning the address. This check prevents address conflicts even when several DHCP servers are in use.

For the clients, it is irrelevant which physical router subsequently establishes the data connection. Similarly, the LAN clients do not notice when a router or WAN interface fails due to the fact that, in this case, another router steps in and is available under the same virtual addresses as before.

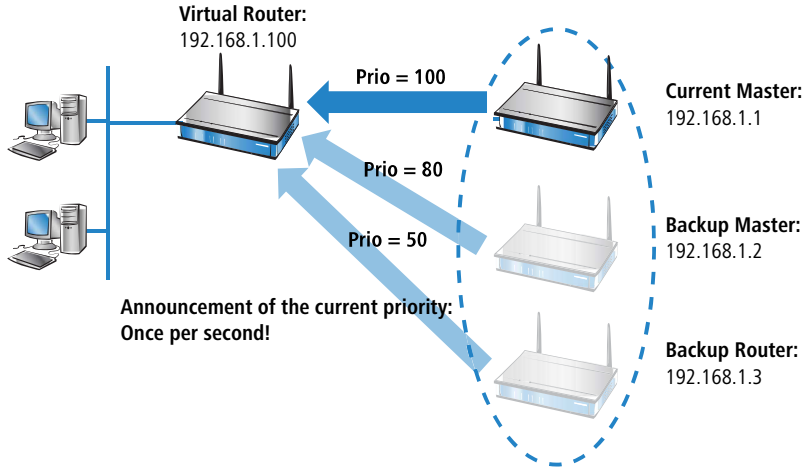
17.2.2.2 Device, connection or remote site backup

A device can disconnect itself from the VRRP group, an option which indicates that the possibilities offered by VRRP are not restricted only to the failure of a device.

VRRP only provides one backup mechanism which safeguards against device failure. In practice, however, the failure of a physical data transfer medium (e.g. DSL or 5G) or the unavailability of a remote site prevent the router from completing its tasks as planned. For this reason, the LANCOM-specific enhancements to VRRP also offer the ability to define the availability of a remote site as a trigger for the backup event—regardless of whether the data connection is denied due to device, connection or remote site problems.

For the definition of a virtual router, the IP address by which it can be accessed, its priority and its logical router ID are required as a minimum. The router ID serves to ensure that the regular messages from the physical routers can be assigned to the respective virtual routers.

- The router ID can assume a value between 1 and 255. The router ID also reveals the router's virtual MAC address as 00:00:5E:00:01:router ID. The router ID 0 is not permitted.
- The IP address for the virtual router can be chosen freely, however, it must obviously be within the local network. If the virtual router's address is the same as the physical router's address, then the physical router is the “main master” of the system. The main master automatically has the highest priority, that is, when it signals that it is ready for operation, it immediately becomes the active master.
- The priority can assume a value between 1 and 255. The values 0 and 255 have special meanings: With the priority 0, the virtual router is not active, with 255, this virtual router is the main master.

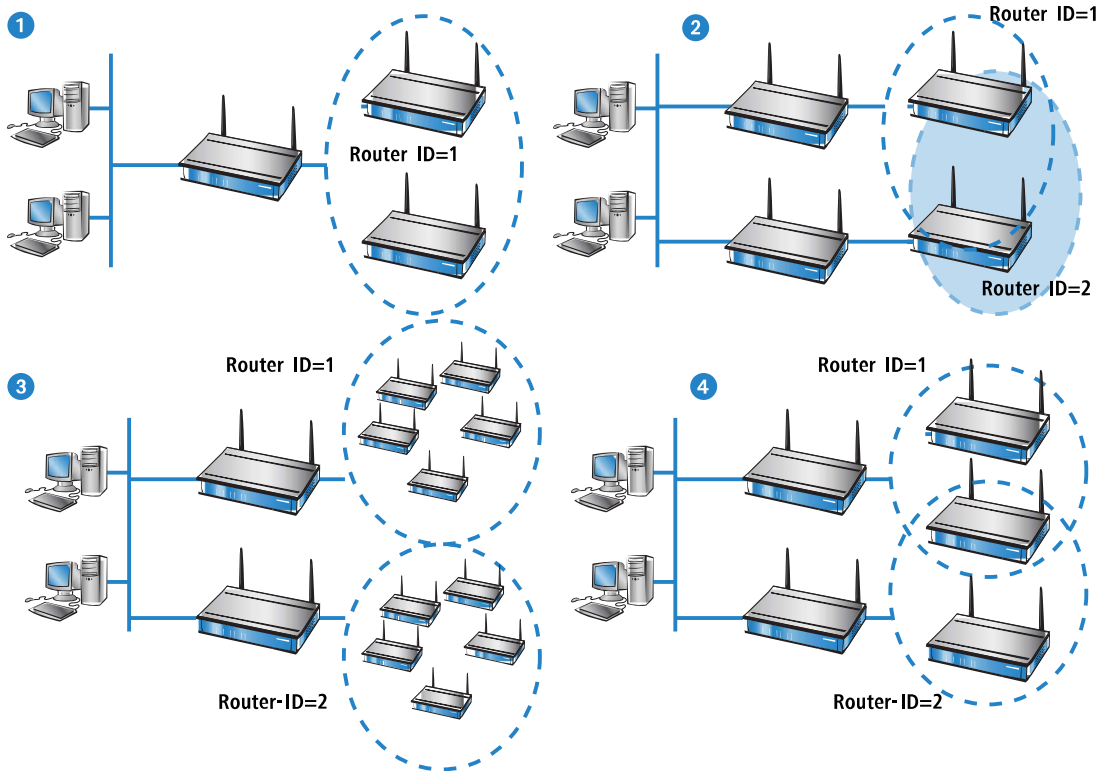


17.2.2.3 Router ID defines “standby groups”

The physical routers are assigned to the virtual routers by means of the router ID that is specified when defining the virtual router. All devices in which virtual routers are created with the same router ID form a “standby group” in which the devices act as replacements for one another. There are three different examples of standby groups:

- In a simple backup scenario, two or more routers form **one** standby group. A virtual router with the same router ID and the same virtual IP address is configured in all physical routers (item **1** in the following illustration).
- In order to perform load balancing, the same number of virtual routers with differing IDs and IPs are defined as there are physical routers planned for the VRRP group. For example, **two** devices would each belong to two standby groups (**2**).
- It is also possible to create more complex combinations with many devices. For example, two devices can form their own standby group with router ID 1 and two other devices can form another group with the ID 2 (**3**). Depending on

the requirements, it is also possible to selectively assign certain devices to a single group while other devices remain members of all groups (**4**).



17.2.2.4 The Priority System

With the analysis of the priorities, VRRP controls the order in which the physical routers take over the function of the master in a VRRP group. VRRP only considers the failure of an entire device to be a trigger for the backup event.

Since numerous devices have more than one WAN interface, the VRRP application in LCOS interprets not only the failure of a device as a trigger for the backup event, but also interruptions to the data connection or the unavailability of a remote site. In order to enable the backup behavior of the devices and the formation of backup chains, every virtual router is assigned two priorities: a main and a backup priority.

- The main priority is used (propagated into the network) as long as the device is in normal operating condition (i.e. the remote site for the standard connection is still available).
- The backup priority is propagated when the device is in backup mode (i.e. the backup delay has expired and the connection could not be reestablished).
- If '0' is set as the backup priority, the router will not send any signals until the end of the backup event, i.e. the device is not available to the VRRP router group when the remote site is not available.

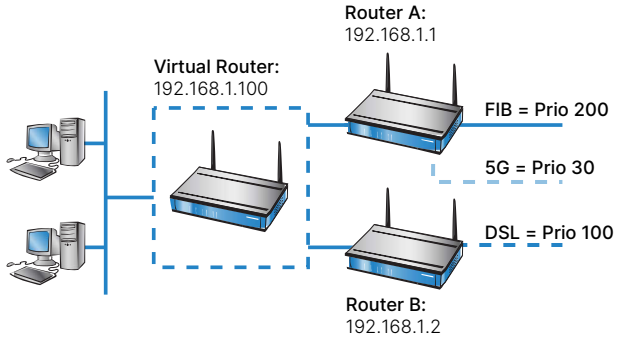
Since VRRP only knows "priorities" and does not differentiate between main or backup priority, it simply analyzes the priority that is currently being propagated by the device. The device with the currently highest priority is considered to be master.

Normally, priorities are configured so that the main priorities of the devices in a VRRP group are larger than the backup priorities used. However this is a general rule and not a requirement. The main priority of router A can be smaller than the backup priority of another router B. In this case, the backup connection of device B is used **before** the standard connection of router A in the backup chain.

The assignment of priorities to the various WAN interfaces can be determined from the configuration of the backup connections in the **Backup table** (under LANconfig in the configuration section **Communication** > **Call Management**).

- The main priority refers to the interface on which the standard connection is configured.

› The backup priority refers to the interface on which the backup connection is configured.



VRRP list Router A:

Main prio	Backup prio	Remote site
200	30	INTERNET-FIB

Backup list Router A:

Remote site	Backup list
INTERNET-FIB	INTERNET-5G

VRRP list Router B:

Main prio	Backup prio	Remote site
100	0	INTERNET-DSL

A master that has been activated due to the priority status will now attempt to establish a connection if this has been configured as a keep alive connection. If the connection is set up as a normal connection with a hold time, then it will not be established until the next packet is transmitted. If this connection fails, thereby triggering the backup event, then the router will also log off and then propagate itself with its backup priority.

17.2.2.5 Backup chains

The use of two priorities enables the formation of flexible backup chains by which each physical router does not merely take a single place within the chain but takes a place for every physical WAN interface:

› The first physical router, the main router in the network, has a DSL and an ISDN interface for example, the second router (backup router) has a DSL and a UMTS interface.
› The first router receives the main priority 255. Consequently, it will become the main router with the value 50 as its backup priority.
› The second router receives the main priority 150 and the value 100 as its backup priority.

Under normal operating conditions, data traffic is processed by the DSL interface on the first router. If the router or this interface fails, the second router attempts (due to the next highest main priority) to establish the connection via its own DSL interface. If this does not succeed, then both devices will propagate their backup priority. Since the second router has the higher backup priority, the connection is established using its UMTS interface. Only when this interface is also unable to establish a connection will the ISDN interface on the first router (with the lower backup priority) be used.

Only keep alive connections return automatically!

The standard connection will only be automatically reestablished after a backup event if the hold time for the connection is configured properly:

› A hold time of 0 means that the connection will not be actively terminated. If the connection is terminated or interrupted due to interference, it will not be automatically established again. The connection will only be reestablished when communication is required of it.
› A hold time of 9999 means that the connection is permanently held open. If it is interrupted, then the connection will be actively opened up again. This behavior is known as **keep alive**.

Set the hold time to 9999 for connections to the Internet provider (in the corresponding name list) and backed-up VPN connections (in the VPN connection list) to ensure that the connection is automatically reestablished and resumes data transfer after interruption.

17.2.2.6 Return to the VRRP group

After an adjustable amount of time (reconnect delay), a router that has logged off attempts to establish its main or backup connection again without propagating its priority first. If the main connection was successfully established, the backup event is terminated and the router returns to propagating its main priority. If only the backup connection was established, then the router falls back into the normal backup event and begins propagating its backup priority again.

As soon as a device can reestablish its primary connection, the router begins propagating with its main priority again and becomes the master:

- Devices that are in backup mode with a lower main priority than the active master can also leave backup mode and propagate their main priority due to the fact that their backup connection is not required in this state.
- Devices that are in backup mode with a higher main priority than the active master can remain in backup mode as long as they are not able to establish their higher-prioritized primary connection.
- Devices that have completely logged out of the VRRP group due to the unavailability of a VRRP remote site over the backup connection return to the normal backup mode.

17.2.2.7 Connection establishment

In order to allow coordinated connection establishment and prevent standby routers from attempting to establish connections, connections from a router are only established when this router:

- is the master **or**
- it is in backup mode and its primary connection is configured with a keep alive **or**
- it has completely logged off and the timer for the renewed connection attempt (reconnect delay) expires.

This simple rule allows the primary connection to be configured as a keep alive connection even in standby routers. It also makes it possible only to use connections with hold time even in the main router.

Connections are always established when all virtual routers connected to the remote site have switched to standby mode. This either happens because another router propagates a higher priority or a LAN connection is lost.

17.2.3 Application scenarios

VRRP is normally employed for two different uses:

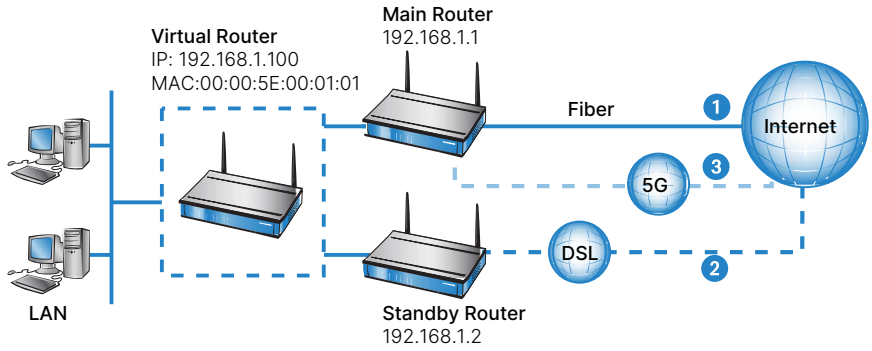
- In the simple backup case with two routers, one device under normal operation establishes the connection to the Internet. The second device is only operated in wait mode as a “standby device” and takes over the function of the main router should it fail.
- In the second case, two or more devices function parallel to each other as routers in the same network and distribute the incoming data connections using static load balancing. If one of these devices fails, the other router in the group can take over the failed device's functions.

17.2.3.1 Backup solution with VRRP

Possibly the most important application of VRRP is the provision of backup connections in which one or more routers serve as backup for the main router. These routers can use different physical media for the Internet connection, such as DSL in the main router and UMTS or ISDN in the backup routers. A normal backup chain thus resembles the following:

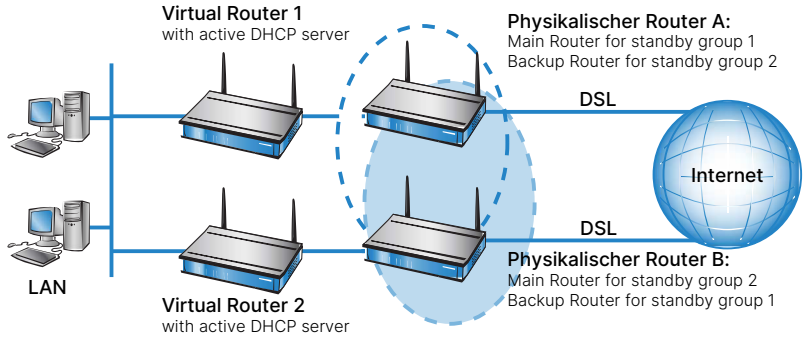
- If the DSL connection fails **1**, the UMTS router **2** takes over the function.
- If the UMTS connection **2** fails, the ISDN router **3** takes over the function.

Since almost all LANCOM devices with a DSL interface also have an ISDN interface, the main router can also take over ISDN backup functions at the end of the backup chain—as long as the hardware does not fail completely.



17.2.3.2 Load balancing

With load balancing, several routers exist which can accomplish the same tasks. These routers are pronounced to be the default gateway and evenly distributed among the computers in the LAN using the DHCP server active in every router. If one of the routers fails, then another can take over its functions providing both routers work with VRRP. On every router, as many virtual routers are defined as there are actual routers. The computers in the LAN are assigned one of the virtual routers as a gateway. Using the virtual router priorities, it is now defined in which order the other routers take over when a master fails. It is also possible to establish a backup chain using the main and backup priority here.



17.2.3.3 Example application: Secure Internet access via two DSL/ISDN combination routers

Two load-balancing default gateways that provide security for one another are to be the basis for operating the LAN at two DSL lines. On average, 50% of the LAN stations log in to router 1 and 50% to router 2. The failure of a router or the non-availability of a DSL connection is compensated for by the other router, which the takes over the full load.

Under normal operational circumstances, each router handles on average 50 % of users in the LAN (prio 250 for the DSL connection). Should a router or DSL connection fail, then the load is distributed to the other router (prio 100 for the DSL connection of the backup router). If both DSL connections fail, then the traffic is directed over the ISDN connections (each with backup prio 50, ISDN connections not illustrated).

Notes for the configuration of the virtual router

Router A		Router B	
	DHCP = On (10.1.1.x)		DHCP = On (10.1.1.x)
Router-ID = 1	Router IP = 10.1.1.1	Router-ID=1	Router IP=10.1.1.1
	Prio = 250		Prio = 100
	Backup prio = 50		Backup prio = 50

Router A		Router B	
	Peer = DSL INTERNET		Peer = DSL INTERNET
	Comment: Main router f. Group 1		Comment: Backup router for Group 1
Router-ID = 2	Router IP = 10.1.1.2	Router-ID = 2	Router IP = 10.1.1.2
	Prio = 100		Prio = 250
	Backup prio = 50		Backup prio = 50
	Peer = DSL INTERNET		Peer = DSL INTERNET
	Comment: Backup router for group 2		Comment: Main router for group 2

17.2.4 Interaction with internal services

Since virtual routers with virtual IP and MAC addresses are used when operating VRRP, this also affects the internal services of the LANCOM devices. These have to behave differently depending on whether a virtual router or a physical router is addressed. Depending on the service or protocol used, the answers to address requests must be changed or completely denied.

17.2.4.1 ARP

The most important protocol when dealing with virtual routers is ARP (Address Resolution Protocol), which provides the ability to match logical addresses such as IP addresses to hardware addresses such as MAC addresses. The use of virtual and physical IP and MAC addresses means that the router's reaction to ARP requests is of great importance:

- An ARP request to the virtual router's address may only be answered when the LANCOM router is the master. This request must be answered with the corresponding virtual MAC address. All other requests must be ignored.
- ARP requests that list a virtual router's address as the sender address must be ignored.
- When using proxy ARP, an ARP request must be checked in order to determine if a virtual router is associated with the remote site through which the requested address can be reached. If so, then the request may only be answered when the LANCOM router is the master. This also applies to virtual remote sites (i.e. PPTP or VPN) when they use a remote site that is associated with a virtual router as a physical connection.
- ARP requests sent by the LANCOM router itself are always sent with the real sender address, as long as this is not the address of a virtual router. In this event, the virtual MAC address must be entered in the ARP request.

Routing of local services/ARP handling switchable

17.2.4.2 ICMP

When using ICMP, echo requests and replies should be differentiated from error messages. For the error messages, ICMP redirect will require and additional inspection.

- An ICMP echo request directed to the virtual router's address may only be answered by the LANCOM router when it is the master.
- ICMP redirects may also be sent from virtual routers but the address of the router to which the packet was sent must be entered as the sender address. This is to be determined from the packet's target MAC address.
- If the LANCOM router is addressed via its physical MAC address and the target of the packet is linked to a virtual router, the address of which is connected to the receiving interface, then an ICMP redirect is returned and the sender receives the address of the virtual router.
- For all other error messages, it does not matter whether the virtual router's address or the real address is used as the sender address. To simplify matters, the real address is always used.

With the implementation of VRRP in LCOS, the previous option 'local routing' in the IP Router menu has been replaced with 'Send ICMP redirects'. If this option is enabled, ICMP redirects are sent, if the option is disabled, the packets are always forwarded.

17.2.4.3 DHCP

- Gateway address

  Although the computers in the LAN can use ICMP redirects to learn which router is the correct virtual router, it is still advisable to designate the correct router as gateway directly during the DHCP negotiation. This allows the assigning gateway address to be determined as follows:

  - If a gateway is explicitly defined for the interface in the DHCP module, then only this will be assigned.
  - If no explicit gateway is set, then the default route is looked up in the routing table. If the default route exists and is connected to a virtual router which is directly linked to the interface through which the DHCP request is received, then the virtual router's address is assigned as gateway.
  - If other remote sites are linked to virtual routers, then these will not be assigned via DHCP since there can only be one default gateway. A host can only learn the corresponding routers via ICMP redirects.
  - Otherwise, the address corresponding to the address pool or interface (intranet or DMZ) will be assigned.

  If more than one virtual router is connected by the default route, then the address of the router with the highest priority will be assigned. This allows for automatic load balancing through the selection of the DHCP server by the respective client. The DHCP server is to be activated on all routers involved in load balancing. All routers then define many virtual routers, each with different priorities. If the client randomly selects a DHCP server from those that answer, then it will also be randomly assigned a virtual router.

  Example with two routers

  Router A defines the following virtual routers:

Router ID	Virt. address	Prio	B-Prio	Peer
1	10.0.0.1	100	50	INTERNET
2	10.0.0.2	60	50	INTERNET

  and, correspondingly router B:

Router ID	Virt. address	Prio	B-Prio	Peer
1	10.0.0.1	60	30	INTERNET
2	10.0.0.2	100	30	INTERNET

  Depending on whether it chooses router A or router B, a DHCP client will now be assigned 10.0.0.1 or 10.0.0.2 as gateway and is initially distributed on both routers.

  Using this example, it becomes clear how load balancing can be combined with backup. If router A falls into backup mode, then router B will become the master for all clients. If router B fails, then router A will become the master for all clients and will attempt to establish its backup. If this fails, then it is LANCOM B's turn again (this signals the end of the backup chain).

- Further addresses

  If the DHCP server is to assign explicit addresses for certain services which the device provides, such as a DNS server, then either the configured addresses or the real addresses are assigned to the respective interfaces. Assigning a virtual router violates the RFC, which prohibits a virtual router from offering other services. A device may only respond to a virtual address if it is the “owner” of this address, i.e. if this address is also the real address of the interface. At the same time, this means that DNS must receive special treatment.

17.2.4.4 DNS server

Since the RFC prohibits a virtual router from offering additional services when the physical router is not the “owner” of the virtual IP address, the DNS server in the LANCOM router requires special treatment. The device offers two options.

- The solution which conforms to the RFC works in the DNS forwarder. If an external IP address is entered as primary or secondary DNS server, then forwarding to the responsible virtual router functions automatically using the ICMP redirect treatment since the packet is simply forwarded to the virtual router.

  However, if no address is entered and no connection has been made to the remote site to which the packet should be forwarded, then the DNS forwarder checks to see if a virtual router is connected to the remote site.

  - If this is the case and the device is also the master for one of the virtual routers, then the connection is established and the packet is forwarded to the DNS server assigned to this connection.
  - If the device is not the master for all connected routers, then the packet is forwarded to the master of the first connected router.

  This procedure only works when all routers behave in accordance with the RFC and use port forwarding. If all of the routers involved are LANCOM devices, then this requirement is fulfilled.
- With the second option, a virtual router reacts to DNS requests itself.

  - In order to enable this behavior, the option "Internal Services" must be enabled. The LANCOM device accepts the requests to the internal services (here, for example, DNS) via the virtual addresses as if it had been addressed through one of the physical addresses.
  - In the default setting **Off** the LANCOM behaves in accordance with the RFC and drops the corresponding packets.
  - The default setting is **On**.

  If a virtual router is connected to the default route when using the internal services, it will be assigned as DNS server by the DHCP server of the LANCOM router. If more than one virtual router is connected by the default route, then the router with the highest priority will be assigned (as is the case with gateway addresses).

  This option can only guarantee trouble-free operation if all of the routers involved are LANCOM devices.

17.2.4.5 RIP

The use of VRRP has a particularly strong influence on RIP, which is used to propagate information on the accessible routes and the corresponding routers.

- On the one hand, routes to remote sites which can be reached via a virtual router must be made known to the network.
- On the other hand, the routes that are propagated by the virtual routers themselves must be ignored.
- Ultimately, the propagated information is dependent upon the interface which it is to be passed on to.

The announcement of routing information via RIP is governed by the following rules:

- Routes are propagated on all virtual and physical interfaces and every virtual router counts as its own virtual interface.
- If routes are currently being propagated on a physical interface (LAN/DMZ) and a route that must be propagated is connected to a virtual router, then two cases must be differentiated:

  - When the virtual router is active on the interface, i.e. its address is in the address range of the respective interface, then the route will not be propagated.
  - If the virtual router on the interface is not active, then the route will be propagated normally, i.e. the physical interface address will be propagated as the best route.
- If routes are propagated on a virtual router, then only the routes that are connected to this virtual router may be propagated.
- If routes are propagated on a WAN interface, then all routes are propagated.
- Upon receiving a RIP packet, the sender address of the RIP packet must be taken into consideration. The routes contained in the packet must be ignored when they are propagated by a virtual router known by the LANCOM router.
- If the LANCOM router cannot establish a connection to the remote site because all channels are occupied, then RIP propagates the routes accessible through this remote site as "unavailable".

- In addition, the VRRP module is notified in this case so that it can log off of the router connected to this remote site allowing a new master to be determined.
- Similarly, VRRP receives notification when the connection is can be re-established in order to allow the virtual router to propagate with its main or backup priority again.

17.2.4.6 NTP

When the "Internal Services" switch is enabled, then the LANCOM device also accepts (S)NTP requests that are directed to virtual routers since the exact address of the time source is not relevant for an NTP client.

17.2.4.7 Other services

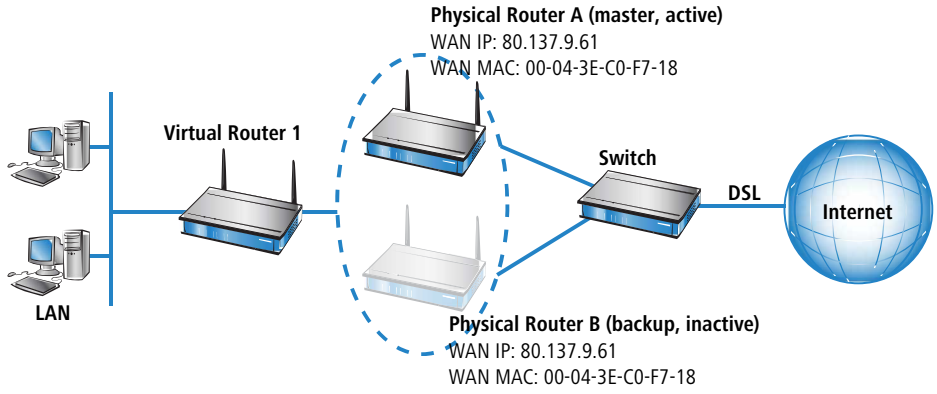
The LANCOM device only processes other services when it is addressed via its physical address.

17.2.5 VRRP in the WAN

The description of VRRP initially relates only to the LAN portion of data networks and leaves the regulation of the WAN portion to dynamic routing protocols such as RIP In order to enable WAN failover despite this, VRRP in the LANCOM router provides two alternatives.

17.2.5.1 Same IP and MAC addresses

The first possibility entails assigning the same MAC and the same IP address to all of the routers in the VRRP group on the WAN side. The routers are then connected to a commonly used DSL line, for example by a switch. In order to avoid address conflicts, only one router may actually react to these addresses on its WAN side, which is achieved through the use of VRRP.



- Since the router closes its WAN connection when the last virtual router switches to backup mode, this condition is guaranteed to be met if only one virtual router has been defined.
- In the backup scenario, the necessary requirement is also fulfilled because the primary connection is guaranteed to have been terminated or else the backup router would not have become master.

17.2.5.2 Routing protocols

In the load balancing scenario, however, there are two different WAN connections online simultaneously, which is why the use of the same MAC and IP address is not possible here. In this case, a routing protocol such as RIP, OSPF or BGP must be used as a second option.

In order to accelerate the switch using RIP, which is rather slow, a LANCOM router propagates to all networks that it is no longer available before the connection is terminated, thereby ensuring a quick change of routing priorities.

17.2.6 Interaction with the WAN backup module

The VRRP module is closely linked to the WAN backup module to enable interaction between the two functionalities. The interaction is in both directions: On the one hand, VRRP can request or prevent the establishment of WAN connections depending on the state of the virtual routers, and on the other hand, the connection state of a WAN connection (established/backup/disconnected) can influence the priority used by the virtual routers.

A virtual router in the VRRP interacts with a maximum of one WAN connection (and its backup connections), and only if the name of the WAN connection is entered in the column **Monitored interface** in the configuration table **Virtual routers**. If there is no entry for a virtual router, this router does not interact with the WAN backup module.

17.2.7 Control of WAN/WAN backup by VRRP

If virtual routers exist and are monitoring a WAN interface, but none of them is in the "Master" state, the VRRP requests a disconnect of the monitored WAN and prevents a reconnect. As soon as one of the routers changes to the Master state, the connection can be re-established and a connection attempt is started. Since WAN connections for IPv4 and IPv6 are established and terminated together, the IP version of the virtual routers is irrelevant. In general: If the VRRP control **VRRP activate** is not enabled, the VRRP has no influence on the WAN backup module.

Also note the switch **Setup** > **VRRP** > **WAN-Connection-Control** (2.141.7).

17.2.8 Configuration of VRRPv3

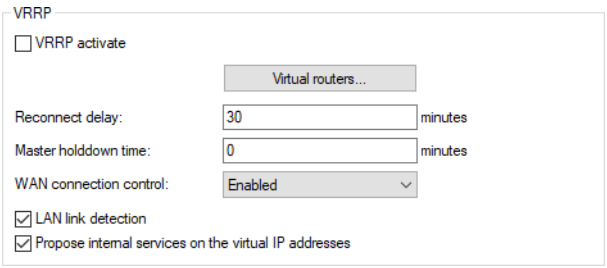
LCOS supports VRRPv2 and VRRPv3 (*RFC 5798* and also *RFC 9568*) for IPv4 and IPv6.

VRRP with IPv6 only works with static addresses or Network Prefix Translation (NPTv6) in the direction of the Internet provider.

VRRP operates independently for IPv4 and IPv6, even if configured together in a single line. This is even recommended to ensure that the advertisement interval and priorities are consistent.

The settings for VRRP can be found in LANconfig under **IP router** > **VRRP**.

Command line: **Setup** > **VRRP**



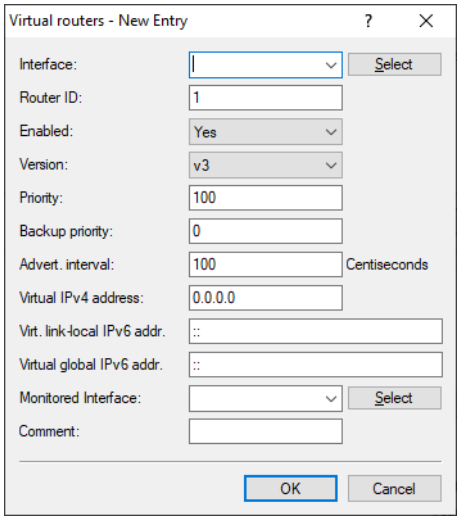
In order to configure failover (router redundancy) or load balancing with VRRP, the following parameters can be set:

VRRP activate

This switches the VRRP module on or off (default: Off).

Virtual routers

In the Virtual Routers table, the virtual routers can be defined for each interface.



Interface

Logical IPv4 or IPv6 interface or network on which VRRP should be enabled. In principle, only LAN interfaces are meaningful. Other interfaces can be selected but may lead to undefined behavior.

Router ID

Unique ID for the virtual router. Values between 1 and 255 are possible. The router ID is used to consolidate several physical routers into a single virtual router or a standby group. The router ID is sometimes called VRRP ID or VRID for short.

Enabled

Enables or disables VRRP for this configuration entry.

Version

Defines which VRRP version should be used. Supported are VRRPv2, VRRPv3, or VRRPv2 and VRRPv3. IPv6 is only supported with VRRPv3. IPv4 is supported in both VRRPv2 and VRRPv3.

The v2+v3 mode is intended as a transitional solution for the move from VRRPv2 to VRRPv3 operation under IPv4. It doubles the packet volume, since a virtual router configured in this way sends advertisements in both protocol versions.

A virtual router configured to use one protocol version will discard advertisements from other routers if they have the wrong protocol version, it will be output to the VRRP packet trace and add an entry to the event log table.

Priority

Specifies the priority with which the virtual router operates. This is transmitted in the advertisements and largely determines which device is the master for a VRRP network. The specified priority must be greater than 0. The value 255 has a special meaning:

- The value 255 is automatically set if the virtual router's address is the same as the address of the interface to which the router is bound. In all other cases, the priority is automatically lowered.

Backup priority

The backup priority of the virtual router refers to the interface for which a backup connection is configured, i.e. with routers with DSL and cellular support to the cellular interface. Values between 0 and the configured priority are permitted. The value 0 has a special meaning:

› 0 disables the virtual router in the backup event. Checks are conducted regularly in order to determine whether or not the standard connection can be reestablished. The inspection interval is defined in the reconnect delay.

When the backup connection cannot be established in backup mode, then the virtual router logs off completely and attempts to reestablish the standard or backup connection in intervals defined by the reconnect delay.

Advert. interval

The advertisement interval specifies the time until a virtual router is propagated again. The default value is 100 centiseconds (1 second).

Additionally, version v2 or v2+v3 require the interval to be an integer of 100, since for VRRPv2 the interval must be an integer number of seconds. If the version is subsequently changed, the advert interval is automatically adjusted to a valid value and should be checked.

With a propagation time of 1 second, the routers in the VRRP group can change quickly when a device or interface fails. An interruption of this type will usually remain undetected due to the fact that the TCP connection is not interrupted. Other routing protocols require up to 5 minutes or longer in order to conduct the transfer to a backup router.

Virtual IPv4 address

Defines the virtual IPv4 address of the virtual router. The address must be identical on all routers in the VRRP network.

To avoid conflicts, virtual IP addresses should only be IP addresses that are not dynamically assigned to end devices that do not speak VRRP.

If the assigned virtual IPv4 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

An unspecified IPv4 address (0.0.0.0) disables IPv4 for this configuration entry.

Virtual link-local IPv6 address

Defines the virtual link-local IPv6 address of the virtual router, for example fe80::1. The address must be identical on all routers in the VRRP network. This address is used as the sender address for sending router advertisements. The parameter is only supported in VRRPv3 mode.

Assigning a virtual link-local address is mandatory to define a virtual router for IPv6.

If the assigned link-local virtual IPv6 corresponds to the physical address of the device on the LAN interface, the configured priorities and backup priorities are ignored and priority 255 is always used instead, in compliance with RFC.

An unspecified IPv6 address (::) disables IPv6 for this configuration entry.

Virtual global IPv6 address

Defines the optional global IPv6 address of the virtual router, for example 2001:db8::1. The address must be identical on all routers in the VRRP network. The parameter is only supported in VRRPv3 mode.

This address is required for the VPN load balancer if it is to operate with IPv6.

Monitored interface

Name of the remote site that controls the virtual router behavior. The remote site can still also be assigned to other virtual routers.

Entering the remote site is optional. Linking the backup requirement to a remote site allows the use of the LANCOM-specific enhancement to VRRP not only to secure against device failure (VRRP standard) but also against interface failure or disruption at a remote site.

Comment

Enter a comment for this entry.

Reconnect delay

This specifies the number of minutes before a virtual router that has logged off attempts to reestablish its main connection. The router remains logged off during this connection attempt. It is only broadcasted with its main or backup priority after the connection has been established successfully. The default value is 30 minutes. Input is entered as <minutes>:<seconds>.

Master holddown time

If a time is configured here, the virtual router changes to the "Hold-Down" state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the "Hold-Down" state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the "Master-Holddown-Time" expires, the virtual router transitions to the "Standby" state, in which the monitored WAN connection can be reestablished.

The "Master-Holddown-Time" is a string with a maximum of 6 characters, which may include the digits 0-9 and a colon. This allows the entry of times of up to 999 minutes 59 seconds (999:59).

If there is no colon (e.g. "30") then the specification is interpreted as minutes. In this case the maximum is "999".

If a colon is present, the colon must be followed by two characters that are interpreted as seconds. The maximum possible value here is "59".

Correct time specifications are, for example "5" (5 minutes), "5:30" (5 minutes, 30 seconds) or "0:30" (30 seconds).

A value of "0" or "0:00" disables the Master-Holddown.

WAN connection control

Defines whether VRRP should suppress the connection establishment of the monitored WAN counterpart in the standby role. Possible values:

Enabled

In the standby role, the connection establishment of the monitored WAN counterpart is not suppressed, and the WAN connection is established. Additionally, in this case, the routes to the monitored WAN are not switched when the virtual router goes into standby.



Packets sent to the physical MAC address of the router are not forwarded to the master in the standby state.

Disabled

In the standby role, the connection establishment of the monitored WAN counterpart is suppressed.

LAN link detection

Specifies whether the WAN connection should be established if no LAN connection is available.

The feature is relevant for a scenario where the router is still in operation without a LAN connection, but management of the router should be possible via the WAN connection. In this scenario, the LAN-link detection has to be deactivated.

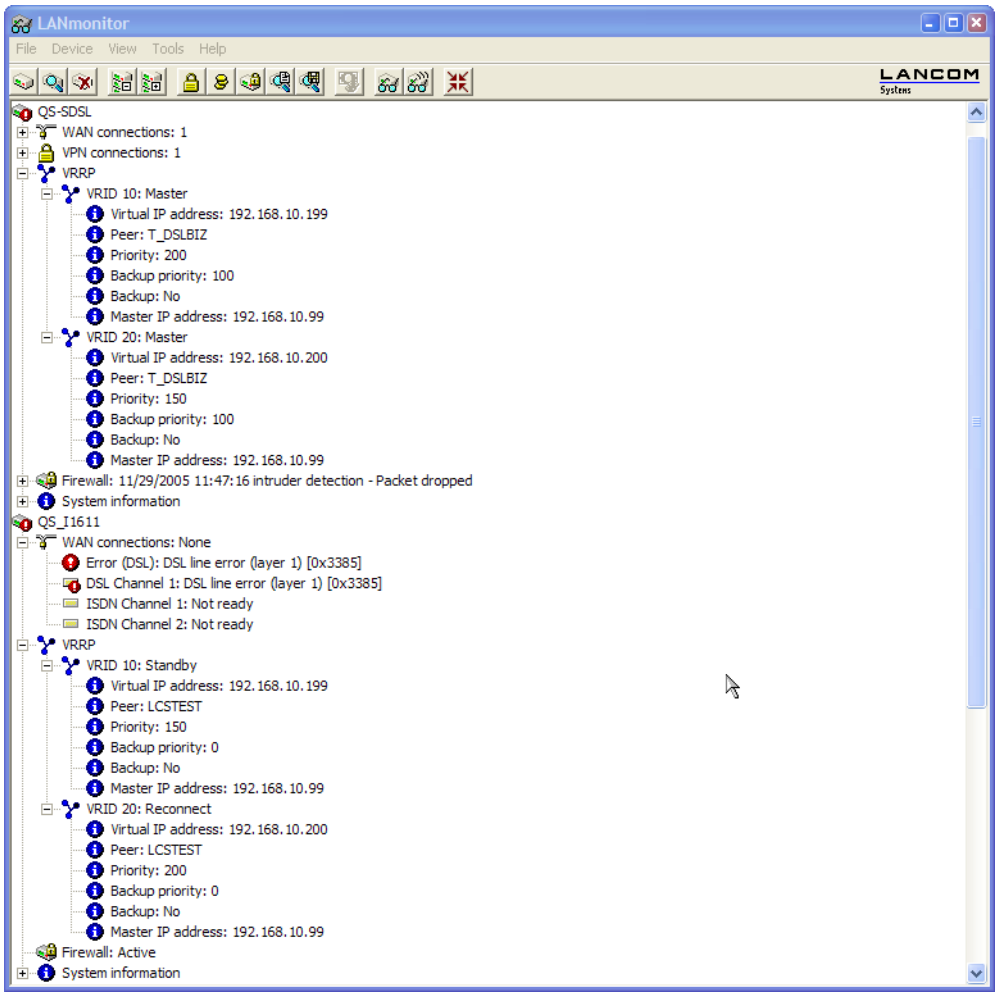
As soon as a logical LAN interface (LAN-X) is configured together with a WLAN interface (WLAN-X-Y) in a bridge group and the SSID is enabled, the bridge group will have the status “Link-Up”. LAN link detection is therefore only partially functional when used in combination with a bridge group (with WLAN). The link status of an active WLAN SSID is always “Up” as soon as the SSID is enabled—regardless of whether any clients are connected or not.

Propose internal services on the virtual IPs

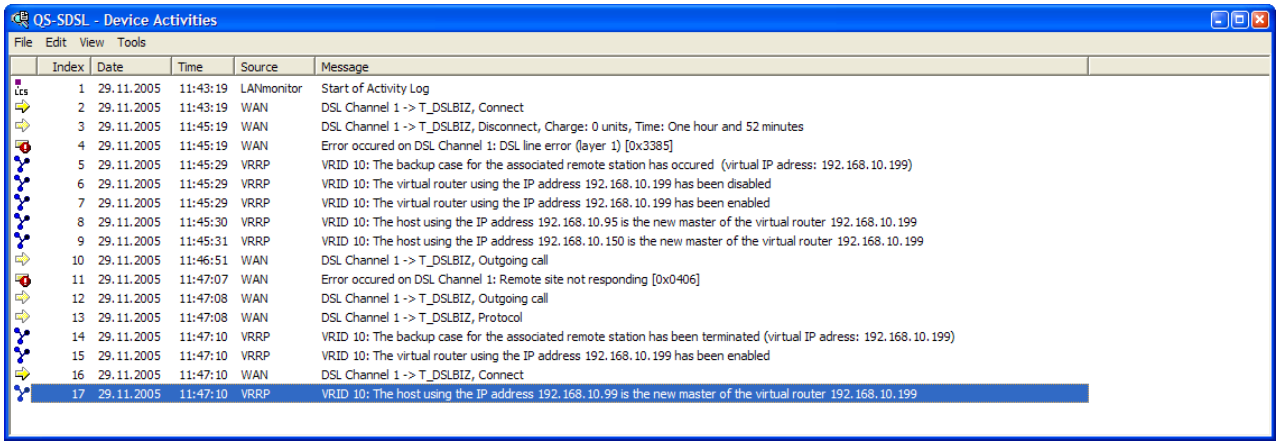
This item controls whether the virtual router is assigned as a DNS server in DHCPv4, DHCPv6 and Router Advertisement.

17.2.9 Status Information

The current status of the devices in the VRRP group is showed in LANmonitor as long as the VRRP module is activated:



In the device activity log, VRRP events can be viewed in chronological order.



Status information on VRRP can be found in the IP router's status menu and offers the following entries:

- The values Rx and Tx count the VRRP packets received or sent, respectively.
- Error counts all fatal protocol errors that are logged.
- Drop counts all VRRP packets that are dropped, e.g. when a serious error occurred.

In the Virtual Router table, all active virtual routers are listed with their current status. This table has the following fields:

- **Router-ID**: Unique ID for the virtual router.
- **Virt. address**: IP address for the virtual router.
- **Prio**: Main priority for the virtual router.
- **B-Prio**: Backup priority for the virtual router.
- **Peer**: Name of the remote site that controls the virtual router behavior.
- **State**: State of the virtual router. The following states are possible:
  - Init: The router is currently being set up.
  - Listen: The router is currently learning which device is the master.
  - Standby: The router is the standby router.
  - Master: The router is the master.
  - Down: The router is deactivated.
  - Reconnect: The reconnect timer is running and the router is currently not propagating itself.
- **Backup**: Shows if the remote site (peer) is in backup or not. If the remote site is in backup, then the device will propagate its backup priority, otherwise it will propagate its main priority.
- **Master**: Shows which of the physical routers is currently the master.

The MAC list table displays the MAC addresses for the virtual routers that are currently masters. This table has the following fields:

- **Virt. address**: IP address for the virtual router.
- **MAC-Address**: MAC address for the virtual router.
- **Router-ID**: Unique ID for the virtual router.

17.3 Interface bundling with LACP

Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle GB ports into a virtual link. Physical GB connections can be

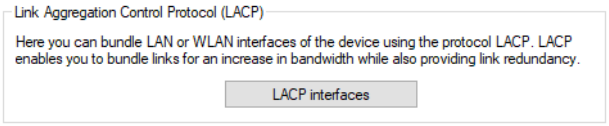
combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

For example, 11ac Wave 2 (4x4 MIMO) achieves a data throughput greater than 1 Gbps net per access point.

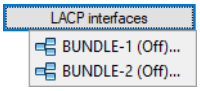
Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

17.3.1 Configuring the LACP interfaces

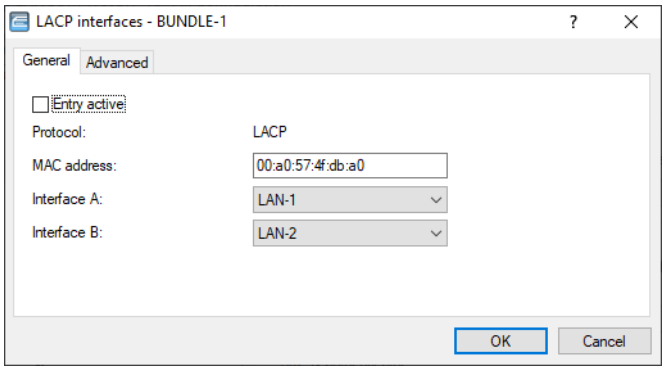
In LANconfig, you configure LACP interfaces under **Interfaces** > **LAN** in the section **Link Aggregation Control Protocol (LACP)**.



1. Click the button **LACP interfaces** to access the list of available bundles.



2. Choose a bundle.



3. Enter the MAC address of the device into the input field **MAC address**.

   The MAC address is used to identify the LACP partner within the LAG. If this is left empty or set to 0, the LAN MAC address of the device is set automatically. The MAC address does not necessarily have to belong to an interface of the bundle. In case of a reset of the configuration, the system-wide MAC address is entered here as the default.

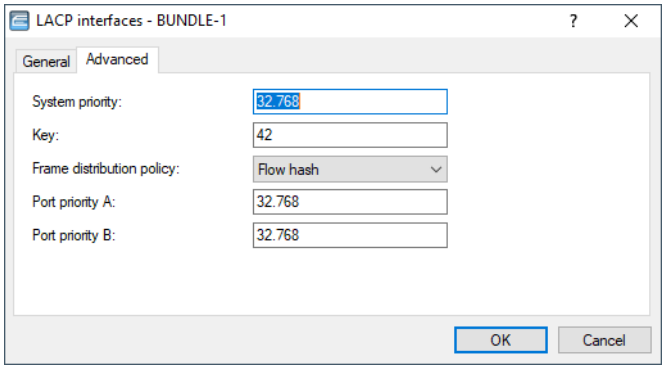
4. Select the first interface from the selection menu **Interface A**.
5. Select the second interface from the selection menu **Interface B**.
6. Activate the bundle by checking the checkbox **Entry active**.

   The remaining steps are optional.

   The default settings are suitable for most common applications.

   Further customizations to the configuration should only be performed by an experienced network technician.

7. Further configuration options are available on the **Advanced** tab.



8. In the **System priority** input field, enter a multiple of 4,096. The default value is 32,768.
9. Enter a value for the **Key**.

   The key is a number from 1 to 54 and is used to identify the bundle.

10. Select an entry from the drop-down menu **Frame distribution policy**. The default setting for most scenarios is Flow hash.
11. In the **Port priority A** input field, enter a multiple of 4,096. The default value is 32,768.
12. In the **Port priority B** input field, enter a multiple of 4,096. The default value is 32,768.

17.4 Support for vRouter redundancy in Amazon AWS

Cloud providers used for outsourcing virtual machines to the cloud, such as Amazon AWS, do not support layer-2 protocols such as VRRP. This means that common router redundancy concepts are not readily available and must be implemented differently. Amazon AWS offers an API that can be used to switch route entries to a secondary router in the event of a failover.

This scenario is structured as follows: One or more private virtual machines (EC2 instances) are available. Two redundant vRouters have a private subnet to the virtual machines and a public subnet to the Internet. Each vRouter has a VPN tunnel to the customer site, which thus provides access to the private machines. One vRouter is the primary router (active), the second router is secondary (passive). The latter is only involved in active routing in the event of a failover. An EC2 instance can only have one router as the next hop in the private subnet at a time. In case of failover, the AWS API uses the AWS routing table to switch from the primary vRouter to the secondary vRouter. If the primary vRouter is available again, it switches back to the primary router.

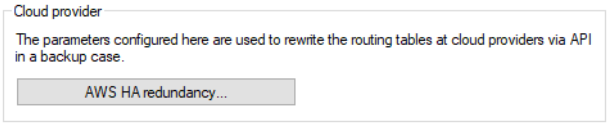
In order to access the AWS API, the vRouters require a role in the AWS Identity and Access Management (IAM).

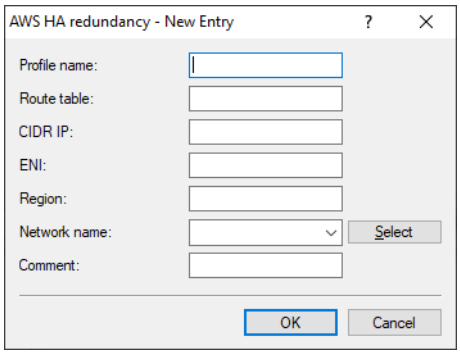
A VPN tunnel is established between the two vRouters in order to detect the failure of the primary router. The action table in the secondary vRouter sends AWS API commands when it detects that the VPN tunnel to the primary vRouter is being established or shut down. The only purpose of the VPN tunnel is to detect the availability of the primary router. No data is transmitted via this VPN tunnel.

The vRouter needs access to the Internet in order to access the AWS API.

17.4.1 Configuration

Configure vRouter redundancy for AWS in LANconfig under **Miscellaneous Services** > **Services** > **Cloud provider** > **AWS HA redundancy** or on the command line under **/Setup/Cloud-Provider/AWS/** in the table **HA-Redundancy**.





Profile name

Unique name of the profile. This name is used by the route-change command to reference the profile.

Route table

Name of the routing table to change in AWS, e.g. "rtb-099605ce6cb4ac319". This value can be taken from the AWS management interface.

CIDR IP

Prefix in the routing table for which the next hop is to be changed, e.g. "0.0.0.0/0".

ENI

Name of the AWS network adapter (Elastic Network Interface) that the command is to set as the next hop, e.g. "eni-00c734d6da1fd8968". This value can be taken from the AWS management interface.

Region

Region where the AWS route table is located, e.g. "eu-central-1"

Network name

Name of the interface or remote site used by the vRouter to reach the AWS API, e.g. "INTERNET".

Comment

Enter a descriptive comment for this entry.

17.4.2 Commands

Two commands are available under **/Setup/Cloud-Provider/AWS**:

- Switch-Route

  ```
  do /Setup/Cloud-Provider/AWS/Switch-Route <Profile-Name>
  ```

  This command uses the AWS API to switch the prefix in the AWS routing table to the new next hop as configured under <profile-name> in the table `/Setup/Cloud-Provider/AWS/`.

- Get-Remote-Route-Table

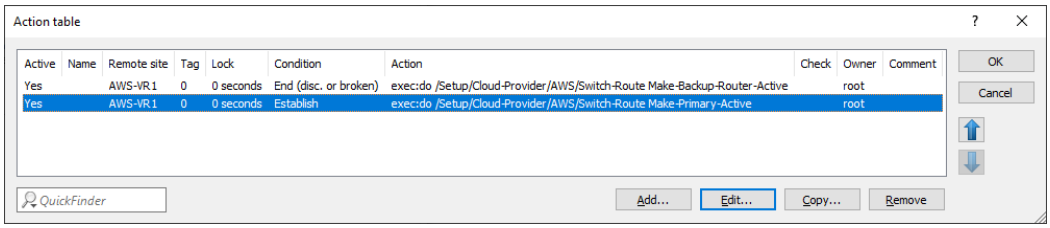
```
do /Setup/Cloud-Provider/AWS/Get-Remote-Route-Table <route-table-id>
   <region> <outgoing-network>
```

This command returns the current status of the AWS routing table <route-table-id> via the AWS API. Example:

```
do Get-Remote-Route-Table rtb-099605ce6cb4ac319 eu-central-1 INTERNET
```

Example: Using the commands in the action table

The backup vRouter has the following entries configured in the action table (**Communication** > **General** > **Action table**):



There are two profiles in the HA redundancy table that are referenced in the action table in the Switch-Route command. The first entry causes the backup vRouter to make itself the active router in the AWS routing table if the VPN tunnel (remote site AWS-VR1) to the primary router is disconnected or broken. If the VPN tunnel is reestablished, i. e. the primary router is available again, the primary router is reset as the next hop in the routing table.

17.4.3 Configuring the IAM role in AWS

In AWS, go to the IAM dashboard and click **Role** > **Create Role**.

The IAM role for the secondary vRouter requires the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateRouteTable",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:DisassociateRouteTable",
                "ec2:ReplaceRouteTableAssociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Create a new policy and assign the policies to the secondary vRouter so that it has the correct permissions to invoke the API.

18 RADIUS

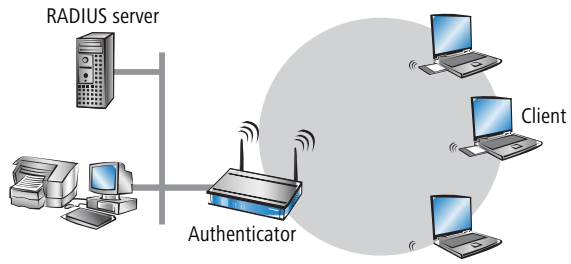
RADIUS stands for “Remote Authentication Dial-In User Service” and is referred to as a “triple-A protocol”. The three “A”s stand for

- Authentication
- Authorization
- Accounting (billing)

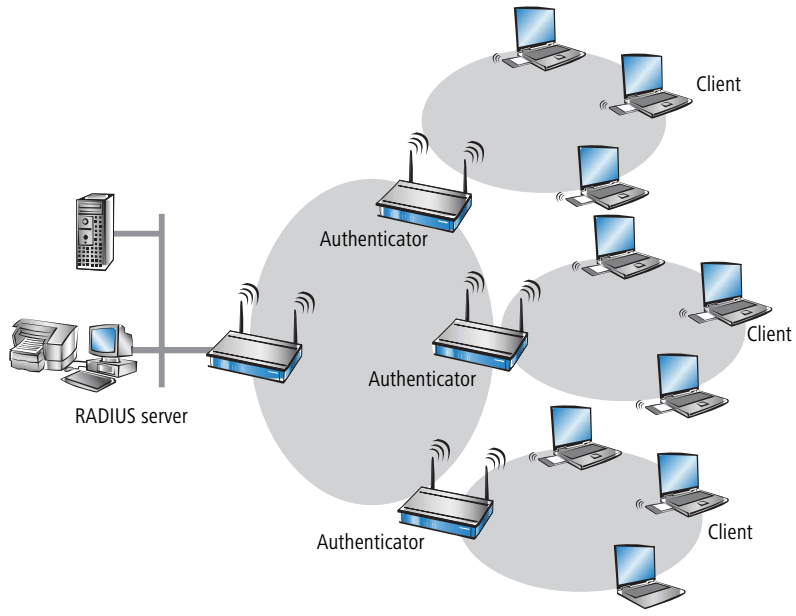
This protocol allow you to grant users access to a network, to assign them certain rights and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

3 different devices are required for RADIUS to work.

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.
- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by an access point, for example. The authenticator is referred to as the Network Access Server (NAS).



- Authentication server: RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of an access point for this task.



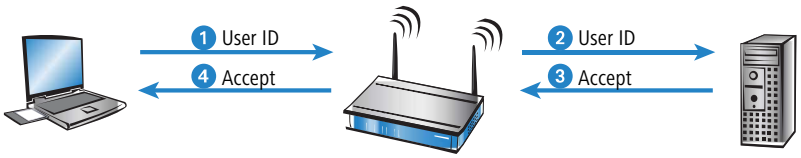
The authenticator has no initial information on the clients wanting to register. This is all stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database there and can vary from network to network. The authenticator has just the one task, that of transferring the information between the client and the RADIUS server.

Access to a RADIUS server can be configured in several ways:

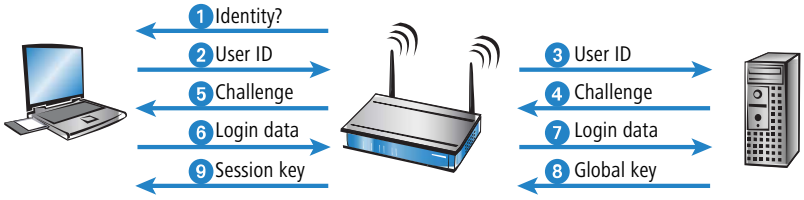
- Using PPP when dialing into a network
- Via WLAN
- Via a public spot for users who register using a browser
- Via the 802.1X protocol

18.1 How RADIUS works

The authentication process of a client using the authenticator on a RADIUS server can vary in complexity and is implementation dependent. In a simplified application, the client sends its registration data to the RADIUS server via the authenticator and receives back either an "Accept" or a "Reject".



In more complicated applications, the RADIUS server can request additional registration data using what is known as a "Challenge". The handshake sequence looks something like this:



18.2 Using RADIUS to login to the LCOS management GUI

There are currently three ways to login to the management interface of the device:

- Internal: The device handles over the overall user administration including the user login name, password, access rights, and privileges.
- TACACS+: User administration is handled by a TACACS+ server on the network.
- RADIUS: User administration is handled by a RADIUS server on the network.

With RADIUS, users can login via the following connections:

- Telnet
- SSH
- WEBconfig
- TFTP

› Outband

RADIUS authentication via SNMP is not currently supported.

A RADIUS authentication via LL2M (LANCOM Layer-2 Management Protocol) is not supported, because LL2M requires cleartext access to the password that is stored in the device.

The RADIUS server handles user management in terms of authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin access accounts in large network installations with multiple routers.

Logging in via a RADIUS server follows this procedure:

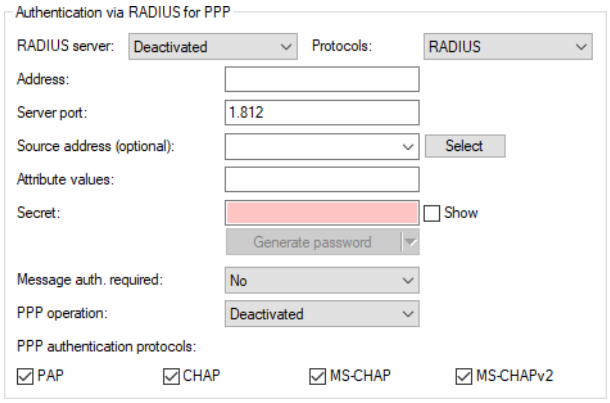
1. At login, the device sends the user's credentials to the RADIUS server on the network. The server data are stored in the device.
2. The server checks the credentials for validity.
3. If the data is invalid, the server sends a corresponding message to the device, which aborts the login process with an error message.
4. If the credentials are valid, the server returns the access rights and privileges to the device and the user then has access to the approved features and directories.
5. If the user's sessions are subject to budgeting by the RADIUS server (accounting), the device stores the session data including the start time, end time, user name, authentication mode and, if available, the port used.

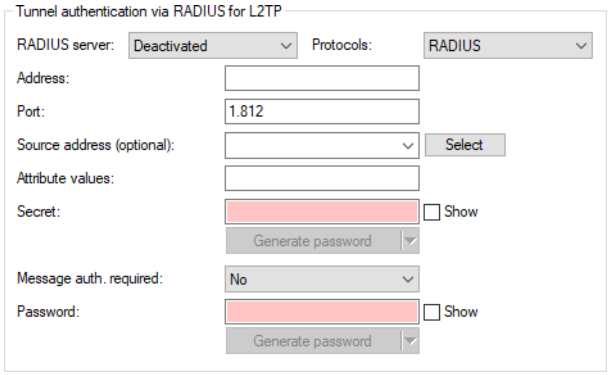
18.3 RADIUS as authenticator or network access server (NAS)

The RADIUS protocol is supported by the devices in a range of different applications. For each of these cases there is a specific set of parameters which may be configured independently of other applications. There are also general parameters which need to be configured for each of these applications. Not all devices support all applications.

18.3.1 General settings

The general settings under **Communication** > **RADIUS** apply to all RADIUS applications. The default values have been set to typical values and usually do not need to be changed.

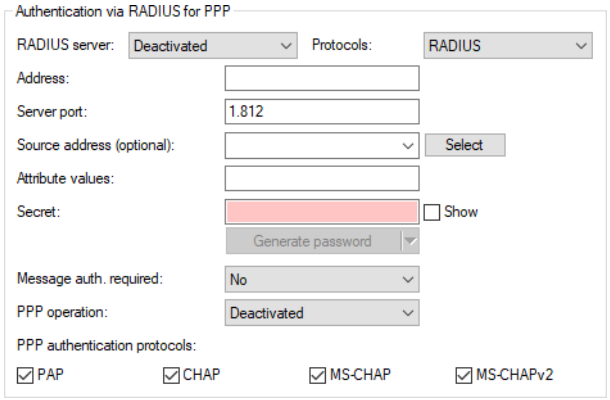




A RADIUS server address can be specified optionally as an IPv4 or IPv6 address, or as a DNS name.

18.3.2 Dial-in using PPP and RADIUS

When dialing-in using the PPP protocol (Point-to-Point protocol), RADIUS can be used to check client access authorizations. A client can dial-in to the network from anywhere. The resulting data transmission between client and authenticator is encrypted.



The configuration is carried out in LANconfig under **Communication** > **RADIUS** > **Authentication via RADIUS for PPP**.

Radius server

When authenticating using RADIUS, the user administration and authentication tasks are passed on to a RADIUS server.

- Disabled: The functionality of RADIUS is disabled and no requests are forwarded to the RADIUS server (default).
- Operating: The functionality of RADIUS is enabled and requests may be forwarded to the configured RADIUS server. Depending on the setting, other sources may be used for the authentication process (e.g. PPP list).

The appropriate RADIUS server must be configured to use the functionality of RADIUS. All user data, such as user name and password, is entered on the RADIUS server.

Protocols

The available protocols are the UDP-based RADIUS and the TCP-based RADSEC. See also *RADSEC* on page 1560.

Address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server used for central user management.

Server port

Specify here the port used for communication to your RADIUS server (default: 1,812).

Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the following form:

`<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Secret

Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

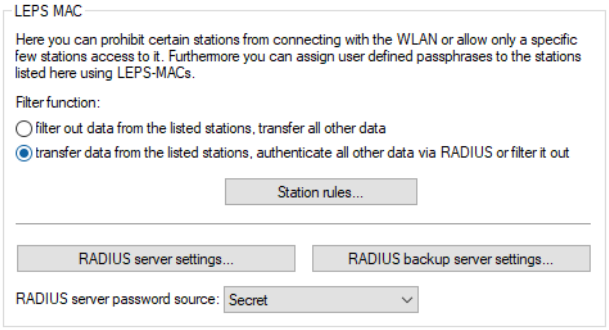
PPP operation

A RADIUS server may be used for the authentication process when dialing-in using PPP.

- Disabled: PPP clients are not authenticated using RADIUS. They are checked **exclusively** using the PPP list (default).
- Operating: RADIUS authentication for PPP clients is enabled. User data supplied by clients is **first** checked using the PPP list. If no matching entry is found in the PPP list, the client is checked by the RADIUS server. Authentication is successful if the PPP list check **or** RADIUS server check returns as positive.
- Exclusive: RADIUS authentication for PPP clients is enabled. User data supplied by clients is checked **exclusively** by the RADIUS server. In this mode, solely the advanced settings of the PPP list for the user are interpreted (e.g. check for PAP/CHAP – or the allowed protocols like IP).

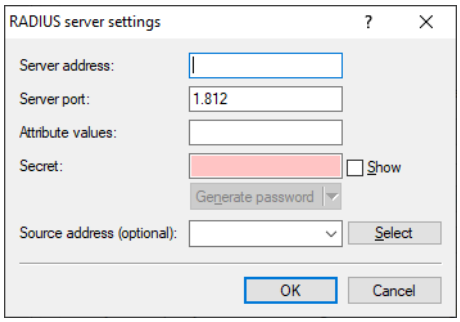
18.3.3 Dial-in using WLAN and RADIUS

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.



To use the RADIUS functionality for WLAN clients, go to the **LEPS-MAC** section and select the option **Transfer data from the listed stations, authenticate all other data via RADIUS or filter it out**.

The configuration is carried out with LANconfig under **Wireless LAN** > **Stations/LEPS**. The **RADIUS server settings** located there specify how the RADIUS server can be reached. Under **RADIUS backup server settings** the backup server is configured in the same way.



Server address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server used for central user management.

Server port

Specify here the port used for communication to your RADIUS server (default: 1,812).

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the following form:

`<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Secret

Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

Backup server address

Enter the IP address (IPv4, IPv6) or the hostname of the backup RADIUS server used for central user management.

Backup server port

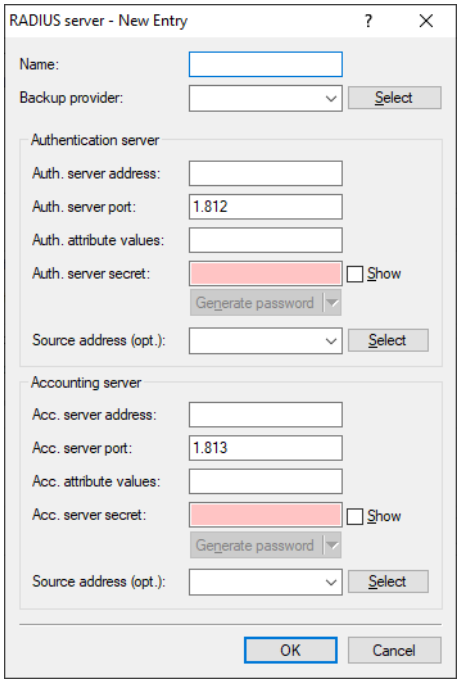
Specify here the port used for communication to your backup RADIUS server (default: 1,812).

Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

18.3.4 Dial-in using a public spot and RADIUS

When configuring a Public Spot (enable using software option for the access points, also see *Public Spot* on page 1216), user registration data can be forwarded to one or more RADIUS servers. These are configured in the provider list. The registration data individual RADIUS servers require from the clients is not important to the access point since this data is passed on transparently to the RADIUS server.



The configuration is performed in LANconfig under **Public Spot** > **Users** > **Users and RADIUS servers** > **RADIUS server**.

Name

Name of the provider for whom the RADIUS server is defined.

Backup provider

The name of a different provider can be selected as the backup from the current table. Using these types of entries, backup chains linking several RADIUS servers can be easily configured.

The generic values for retry and timeout must also be configured.

Authentication server

Auth. server address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server for this provider.

Auth. server port

The port over which the access point can communicate with the RADIUS server for this provider.

Auth. server attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

It is also possible to use a number of placeholders:

- `%n` – replaced by the configured device name.
- `%e` – replaced with the serial number of the device as displayed in the device system info.
- `%%` – replaced by a single % character.
- `%{name}` – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Auth. server secret

Key (shared secret) for access to the RADIUS server of the provider. The key must also be configured on the appropriate RADIUS server.

Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

Accounting server

Acc. server address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS accounting server for accessing the Public Spot.

Acc. server port

The port used by the access point to communicate with the accounting server.

Acc. attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

It is also possible to use a number of placeholders:

- `%n` – replaced by the configured device name.
- `%e` – replaced with the serial number of the device as displayed in the device system info.
- `%%` – replaced by a single % character.
- `%{name}` – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Acc server secret

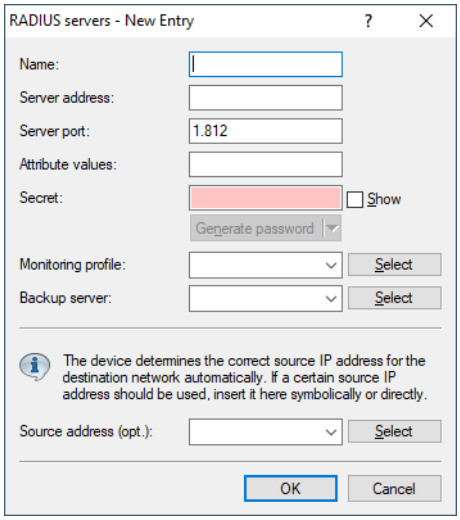
Key (shared secret) for access to the accounting server. The key must also be configured on the accounting server.

Source address

The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

18.3.5 Dial-in using 802.1X and RADIUS

WLAN clients can use the 802.1X protocol for network registration. The access point can use this protocol to forward the registration to the RADIUS server. The MAC address is used for user identification.



The configuration is carried out with LANconfig under **Interfaces** > **802.1X** > **RADIUS servers**.

Name

In this table, each RADIUS server needs a unique name. The name 'DEFAULT' is reserved for WLAN networks that use an authentication process in line with IEEE 802.1X and that have not specified their own RADIUS server.

By using the name defined in the 'Key 1/passphrase' field, each WLAN network using authentication in line with IEEE 802.1X can be assigned its own RADIUS server.

Server address

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server used for central user management.

Server port

Specify here the port used for communication to your RADIUS server.

Attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks ("<Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

It is also possible to use a number of placeholders:

- %n – replaced by the configured device name.
- %e – replaced with the serial number of the device as displayed in the device system info.
- %% – replaced by a single % character.
- %{name} – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Secret

Specify here the key to be used for coding data. The key must also be configured on the RADIUS server.

Monitoring profile

Here you set a profile to be used to monitor the RADIUS server for accessibility. See also *Availability monitoring for external RADIUS servers* on page 1531.

Backup server

Name of the backup server from the list of RADIUS servers configured so far.

The generic values for retry and timeout must also be configured.

WLAN clients must be entered as follows on the RADIUS server:

The user name is the MAC address in the format AABBCC-DDEEFF. The password for all users is identical to the key (shared secret) for the RADIUS server.

Source address

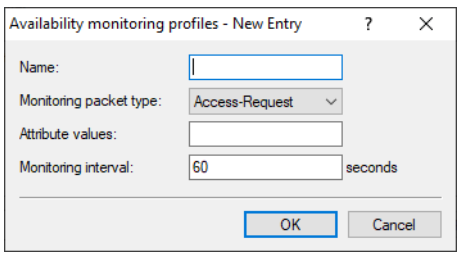
The device automatically determines the correct source IP address for the destination network. To use a fixed source IP address instead, enter it symbolically or directly here.

18.3.5.1 Availability monitoring for external RADIUS servers

Use this feature to monitor whether a RADIUS server is available. RADIUS requests are sent at regular intervals to check whether the RADIUS service is functional.

Monitoring can be performed as follows:

- By sending status server requests (DEFAULT). These are specifically used to check the availability of RADIUS services. However, they are not supported by all RADIUS servers (a positive example is FreeRADIUS).
- By sending access requests ("dummy requests"). Only use this method if the server does not support status server requests.



The configuration is carried out in LANconfig under **Interfaces** > **802.1X** > **RADIUS server availability monitoring** > **Availability monitoring profiles**.

Name

Enter the name of the availability monitoring profile here.

Monitoring packet type

Your choices are as follows:

Access request (default)

Only use this type if the server does not support status server requests.

Status server

This type is specifically for the availability monitoring of RADIUS services, but it is not supported by all RADIUS servers.

Attribute values

An attribute is only required for access requests. It is not required for status server requests.

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

It is also possible to use a number of placeholders:

- `%n` – replaced by the configured device name.
- `%e` – replaced with the serial number of the device as displayed in the device system info.
- `%%` – replaced by a single % character.
- `%{name}` – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Monitoring Interval

Here you define the interval in seconds used by the RADIUS server to check the availability.

The RADIUS servers monitored in this way and their status can be viewed in the table **Status** > **TCP-IP** > **RADIUS-Supervision-Servers** > **Servers**. An alternative is to view the status table under **Status** > **SLA-Monitor** > **RADIUS** > **Servers**.

18.3.6 Additional source ports for access requests

The RADIUS client uses a source port (UDP listener) for negotiating access requests with the RADIUS server. This port allows the simultaneous negotiation of up to 256 IDs. If a client is processing a large number of requests at the same time and the RADIUS server is far away, it is possible for all 256 access requests to be open at the same time, causing the RADIUS client to be unable to handle any further requests. This can happen, for example, in extensive Eduroam environments.

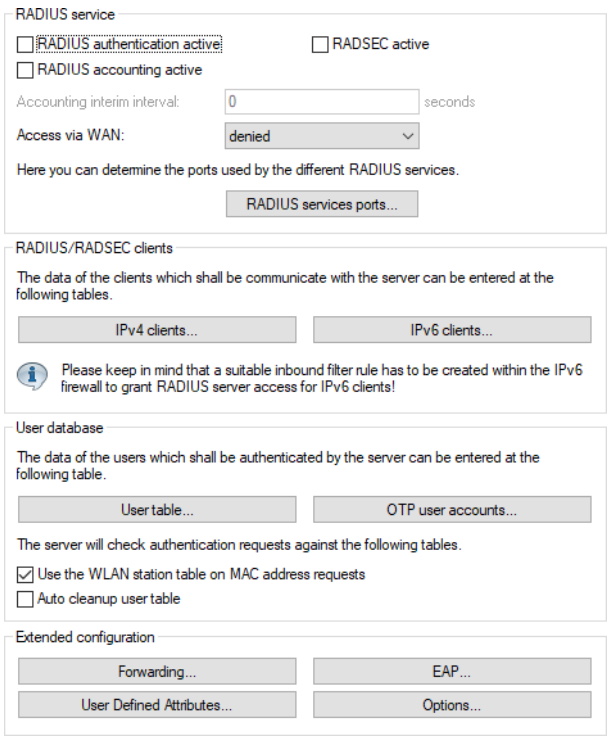
In this case, the RADIUS client opens the next highest source port to enable the access request negotiation for additional IDs. This is automatic and is not configurable.

18.4 RADIUS server

In addition to its function as RADIUS authenticator or NAS, an access point can also operate as a RADIUS server. When in this mode, information in the device on users authorized to register is made available to other access points in Authenticator mode.

The configuration of the RADIUS server requires the specification of the authenticator that can access the RADIUS server, the password required for this access, and the open port that is specifically used to communicate with the RADIUS server. The authentication port applies globally for all authenticators.

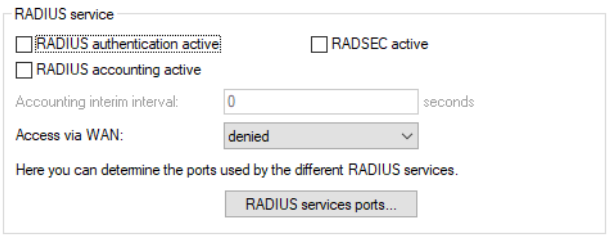
The configuration of the server is performed with **RADIUS** > **Server**.



18.4.1 RADIUS service

The configuration of the RADIUS server requires the specification of the authenticator that can access the RADIUS server, the password required for this access, and the open port that is specifically used to communicate with the RADIUS server. The authentication port applies globally for all authenticators.

The RADIUS service is configured via **RADIUS** > **Server** > **RADIUS service**



RADIUS authentication active

Enables the RADIUS authentication service.

RADIUS accounting active

Enables the RADIUS accounting service.

RADSEC active

Enables the RADSEC service. See also *RADSEC* on page 1560.

Accounting Interim Interval

Enter the value that the RADIUS server should output as "Accounting interim interval" after successful authentication. Provided that the requesting device supports this attribute, this value determines the interval (in seconds) at which an update of the accounting data is sent to the RADIUS server.

Access via WAN

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

RADIUS services ports

Authentication port

Specify here the TCP port used by the authenticators to communicate with the RADIUS server in the access point. That is usually the port "1812".

Accounting port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port "1813".

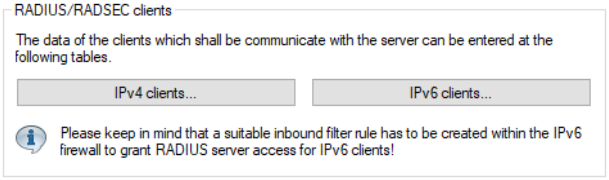
RADSEC port

Enter the TCP port used by the server to accept accounting or authentication requests that are encrypted using RADSEC. That is usually the port "2083".

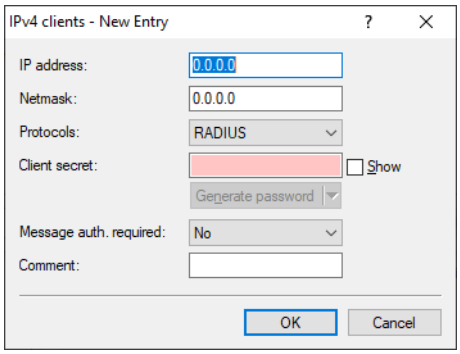
18.4.2 RADIUS / RADSEC clients

The clients that can communicate with the server are entered into this table. Use the corresponding table depending on the network protocol.

The RADIUS / RADSEC clients are configured via **RADIUS** > **Server** > **RADIUS / RADSEC clients** under **IPv4 clients** and **IPv6 clients**.



IPv4 clients



The following values are entered for each client:

IP address

IP address (or address range) of the clients for which the password entered in this dialog applies.

Netmask

IP netmask of the clients

Protocols

Protocol for communication between the internal server and the clients.

Client secret

Password required by the clients for access to the internal server.

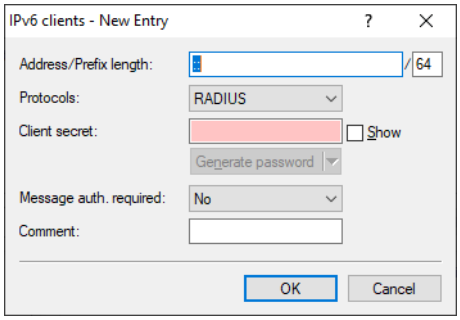
Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Comment

Comment on this entry.

IPv6 clients



The following values are entered for each client:

Address / prefix length

IP address (or address range) of the clients for which the password entered in this dialog applies.

To use an address, the prefix length must be 128 bits. The entry “fd00::/64”, for example, permits access to the entire network, the entry “fd00::1/128” permits exactly one client only.

Protocols

Protocol for communication between the internal server and the clients.

Client secret

Password required by the clients for access to the internal server.

Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Comment

Comment on this entry.

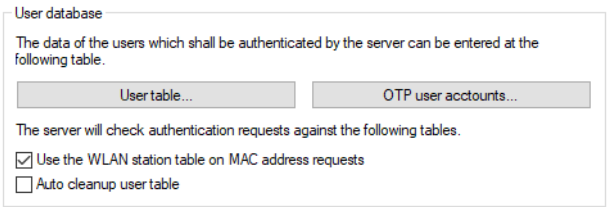
In order for IPv6 clients to access the RADIUS server, a corresponding inbound rule must be entered in the IPv6 firewall, if necessary.

18.4.3 User database

The RADIUS user database is used to enter the user accounts that the RADIUS server can authenticate without any further databases. This database uses the RADIUS server for local requests, also for requests with usernames without a realm.

Please note that the number of users the database can accommodate depends on the model. The maximum possible number of user accounts can be found in the product description of your device. For devices without a limit, we recommend an upper limit of max. 2,500 users.

The RADIUS user database is configured via **RADIUS** > **Server** > **User database**.



Use the WLAN station table for MAC address requests

This parameter specifies whether the WLAN access list is to be used as an information source for the RADIUS server in the access point. The WLAN access list contains the user name in the form of the MAC address and the password ("WPA passphrase"). In addition to this access data, the access list provides information such as bandwidth restriction and association to a specific VLAN.

The WLAN access list can be found under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules**. Up to 512 WLAN clients may be entered here so they can associate with the access point. When operating in RADIUS server mode, this list can also be used to check on RADIUS clients wanting to register at other access points. In an installation having several access points, client access authorizations can be maintained centrally.

Once a WLAN client is logged on after authentication by RADIUS, it remains active until it logs off itself or is logged off by the RADIUS server. By specifying a recheck cycle [minutes], the RADIUS server can regularly check whether the WLAN clients logged in are still in the access list. If a WLAN client is removed from the access list, it remains logged in to the WLAN up to the point when the recheck cycle runs again. You can adjust the recheck cycle from the CLI under **Setup** > **WLAN** > **RADIUS-Access-Check** > **Recheck-Cycle**.

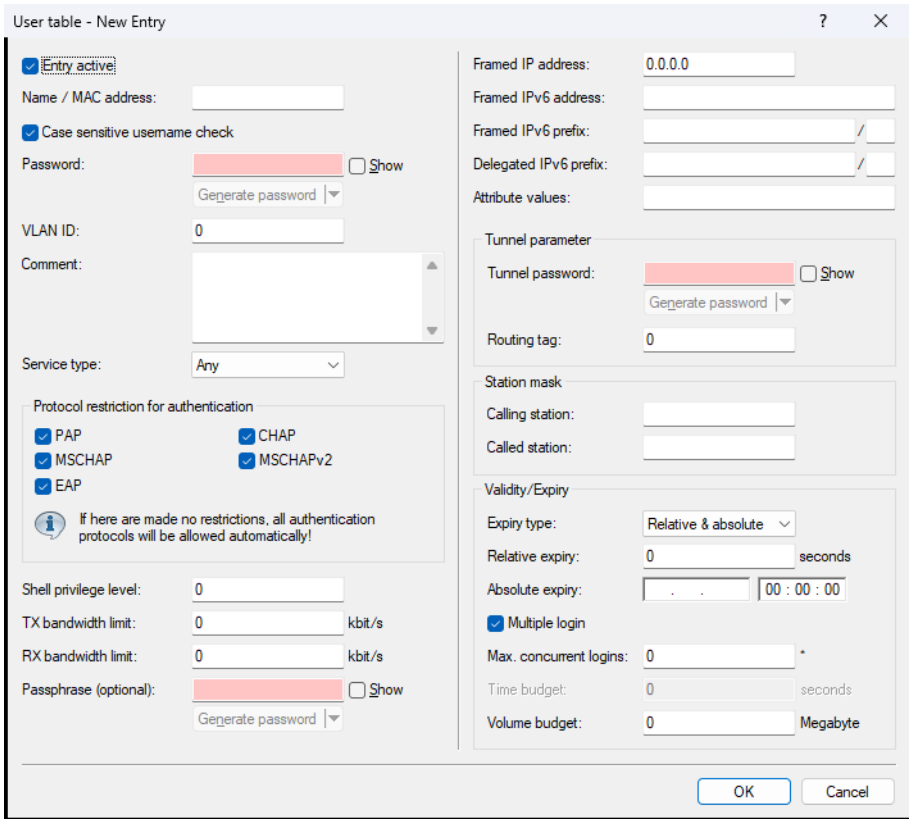
A recheck cycle of '0' disables regular checking. WLAN clients remain logged in until they log themselves out.

Auto cleanup user table

Enabling this option causes expired user accounts to be deleted from the user table automatically. This considers user accounts with validity periods that are absolute and relative.

The device must operate as an accounting server and as an authentication server in order to process accounts with a relative validity period and accounts with a time or volume budget.

With **User table** you define the entries for local requests.



Entry active

Using this option, you specifically enable or disable an individual RADIUS user account. This makes it possible to disable individual accounts temporarily without deleting the entire account, for example.

Name / MAC address

Enter the name or MAC address of the user

The MAC address is used in combination with the passphrase for LEPS-MAC authentication.

Cast-sensitive user name check

When enabled, the RADIUS server distinguishes between uppercase and lowercase. “User12345” and “user12345” are therefore two different users.

Password

User password.

VLAN-ID

This option allows a certain VLAN ID to be assigned to the user on successful authorization. A value of 0 means that no VLAN ID is assigned to the user.

Comment

Additional information about the user.

Service type

The service type is a special attribute of the RADIUS protocol, which the NAS (Network Access Server) transmits with the authentication request. The request will only receive a positive response if the requested service type fits the service type of the user account. Possible values include:

- `Any`: The service type can be any type.
- `Framed`: For checking WLAN MAC addresses via RADIUS or IEEE 802.1X.
- `Login`: For Public Spot authentications.
- `Authentication only`: For RADIUS authentication of dialup peers via PPP.
- and various others that are defined by the RADIUS protocol.

Please note that, depending on the device, the number of entries can be limited with the service type `Any` or `Login`. If your device is able to manage a total of 64 Public Spot users, for example, the LANconfig rejects any after 64. User account with the service type `Any`/`Login` requires the creation of additional user accounts with these service types.

Protocol restriction for authentication

This option limits the selection of authentication methods allowed for the user. Possible values are:

PAP

The NAS passes the user name and password. The RADIUS server searches its data sets for an entry matching the user name, compares the password, and responds with a RADIUS accept or RADIUS reject.

CHAP

The NAS passes the user name, the CHAP challenge and characteristics of the password (but not the password itself). The RADIUS server searches its data sets for an entry matching the user name; it uses the associated password and the CHAP challenge from the NAS to compute the CHAP response. If this computed response and the answer sent by the client via the NAS correspond, then the RADIUS server sends a RADIUS accept; otherwise it sends a RADIUS reject.

MSCHAP

The NAS passes the user name, the MS-CHAP challenge and the MS-CHAP password characteristics. The method continues in the same way as CHAP, although the responses are computed with the MS-CHAP algorithm (*RFC 2433*).

MSCHAPv2

The NAS passes the user name, the MS-CHAP challenge and the MS-CHAPv2 response. The method continues in the same way as CHAP and MS-CHAP, although the responses are computed with the MS-CHAPv2 algorithm (*RFC 2759*). Furthermore the RADIUS server transmits an MS-CHAPv2 confirmation once the authentication was successful. This confirmation contains the server's response to the client's challenge, so enabling a mutual authentication.

EAP

The NAS passes the user name and an EAP message. Unlike the methods outlined above, EAP is not stateless, i.e. in addition to sending an access accept or access reject, the RADIUS server issues its own challenge before authentication is completed. EAP itself is a modular authentication protocol that accommodates various methods of authentication.

Shell privilege level

Vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept (default: 0).

TX bandwidth limit

Bandwidth limitation for sending data.

RX bandwidth limit

Bandwidth limitation for receiving data

The bandwidth limitation for sending and receiving applies regardless of the interface used (LAN and WLAN).

Passphrase

The respective WPA passphrase assigned to the registered user. This enables a LAN-connected device to operate as a central RADIUS server and benefit from LEPS-MAC (LANCOM Enhanced Passphrase Security MAC).

The configuration of LEPS-MAC involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. This is done either with an entry in the list under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules** (see *LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)* on page 966) or in the RADIUS server. One entry is generated per MAC address—from the point of view of the RADIUS server, the MAC address is therefore a user. It is also necessary to activate the MAC filter under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**, i.e. data will be transmitted for the WLAN clients entered here.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

If you are storing client-specific passphrases in the user table of a RADIUS server, a LAN-based device can serve as the central RADIUS server and take advantage of LEPS-MAC.

Framed IP Address

Defines the Framed IP Address attribute (according to *RFC 2865*, attribute type 8) for this RADIUS user.

Framed IPv6 Address

Defines the Framed IPv6 Address attribute (according to *RFC 6911*, attribute type 168) for this RADIUS user.

Framed IPv6 Prefix

Defines the Framed IPv6 Prefix attribute (according to *RFC 3162*, attribute type 97) for this RADIUS user.

Delegated IPv6 Prefix

Defines the Delegated IPv6 Prefix attribute (according to *RFC 4818*, attribute type 123) for this RADIUS user.

Attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

It is also possible to use a number of placeholders:

- `%n` – replaced by the configured device name.
- `%e` – replaced with the serial number of the device as displayed in the device system info.
- `%%` – replaced by a single % character.
- `%{name}` – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Tunnel-Password

This entry sets the connection password for each user.

Routing tag

Specify the routing tag for this connection.

Calling station

This mask limits the validity of the entry to certain IDs transmitted by the calling station (WLAN client). When authenticating via 802.1X the calling station's MAC address is transmitted in ASCII format (capital letters only) with a hyphen separating pairs of characters (for example, “00-10-A4-23-19-C0”).

Called station

This mask limits the validity of the entry to specified IDs as transmitted by the called station (BSSID and SSID of the access point). When authenticating via 802.1X the called station's MAC address (BSSID) is transmitted in ASCII format (capital letters only) with a hyphen separating pairs of characters. The SSID is appended using a colon as a separator (e.g., “00-10-A4-23-19-C0:AP1”).

Expiry type

This option specifies the type of the validity period of the user account. Possible values are:

- `Relative & absolute:`
- `Relative`
- `Absolute`
- `Never`

Relative expiry

Validity period in seconds from the initial successful login.

Absolute expiry

Validity period in hours, minutes and seconds from a certain date.

Multiple login

Activates the option for the client to register more than once

Maximum number

Maximum number of concurrent logins by the client

Time budget

Specifies the time in seconds available to the client if **Multiple login** is not enabled.

Volume budget

Specifies the data volume available to the client.

18.4.3.1 Importing and exporting RADIUS user data by CSV file

The internal RADIUS server is basically a user database. Here we describe an easy way to import and export the user entries. This is particularly relevant for Public Spots, where users are generated in large numbers by an external system. For LEPS-MAC, too, this is an easy way to import the data. The format used for the data exchange is csv (comma separated values), whereby a semicolon serves as the default separator of the individual data fields.

Exporting RADIUS user data by CSV file

To export the user data of the RADIUS server via WEBconfig, proceed as follows.

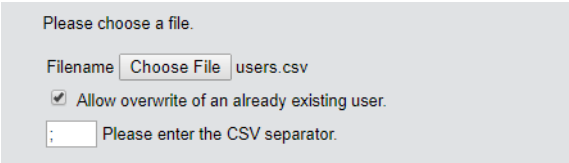
Click on **Extras** > **Export RADIUS users**.<draft-comment author="mkoser">Englisch: Extras > Export RADIUS users</draft-comment>
The user data is downloaded as the file `users.csv`. The semicolon is the separator; the first row contains the identifiers of the database fields.

Importing RADIUS user data by CSV file

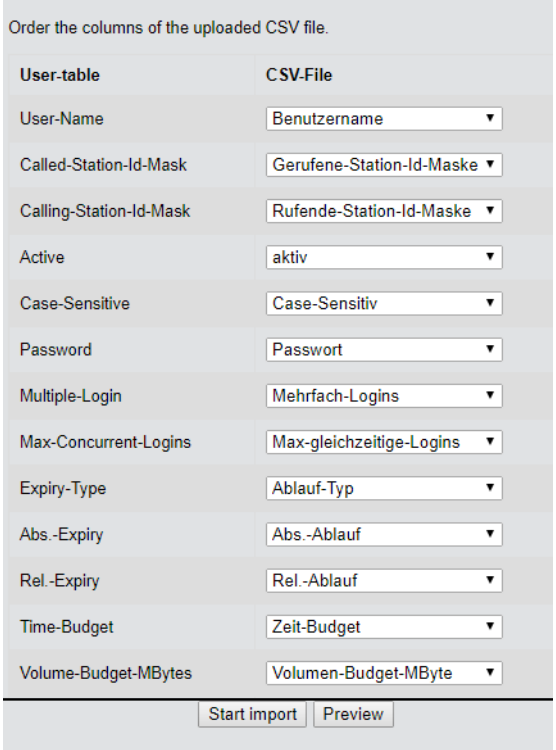
To import the user data of the RADIUS server via WEBconfig, proceed as follows.

1. Generate a file with the required header for the user data by performing an export of the user data as described in *Exporting RADIUS user data by CSV file* on page 1541.
2. Create a CSV import file with a header containing the correct database field identifiers determined in the previous step. The import file does not have to contain all the columns.
3. Navigate to the menu item **Extras** > **Import RADIUS users**.
4. Use **Choose file** to select the CSV file to be imported.

5. Enter the CSV separator. By default this is already preset to ";".



6. Start the upload.
7. Now check that the columns detected in the CSV file are correctly aligned with the supported columns. You can adjust the alignment in this dialog. No adjustment should be necessary if you used the column names from the previously exported CSV file.

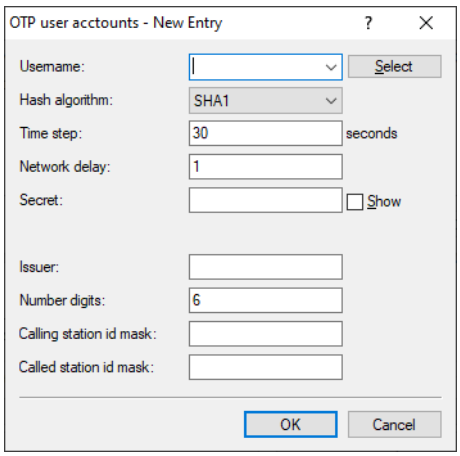


8. Click **Start import** to complete the process and accept the user data.

18.4.3.2 OTP user accounts

The OTP users are defined in the OTP user accounts table. For EAP-OTP, the user must be created with his normal password in the table of *RADIUS user accounts*, as well as additionally created in this table with the OTP secret.

The configuration of the OTP user accounts is done via **RADIUS** > **Server** > **User database** > **OTP user accounts**.



Username

Enter the name of the OTP user here. This must already be contained in the RADIUS user accounts table with the same name.

Hash algorithm

Defines the hash algorithm used.

Note that the Authenticator app supports the maximum possible hash algorithm. For example, Google Authenticator currently supports only SHA1 on certain Android platforms.

Time step

Defines the interval in seconds after which a new OTP is calculated. Default: 30 seconds

Network delay

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Secret

Defines the actual shared secret that must be shared with the Authenticator app. The secret must be different for each user. There are currently three possible entries in the table:

Base32 (Default)

Prefix "base32:" followed by the base32 encoded secret. The prefix "base32:" may also be omitted.

Hexadezimal

Prefix "hex:" followed by an even number of hex digits.

Plain text passphrase

Prefix "ascii:" and then the characters.

For Google Authenticator, the secret must be 16 characters long (80 bit, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G

Issuer

Freely definable text used in Authenticator to keep multiple keys apart when the same username is used. Must not contain a colon.

Number digits

Length of OTPs. Default: 6.

For Google Authenticator, the value 6 should be used.

Calling station id mask

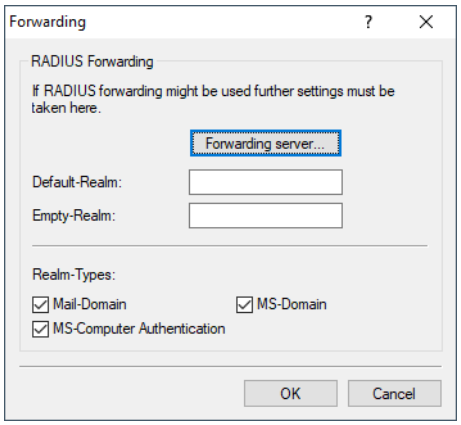
This mask restricts the validity of the entry to certain IDs transmitted by the calling station.

Called station id mask

This mask restricts the validity of the entry to certain IDs transmitted by the called station.

18.4.4 Forwarding

Forwarding is configured via **RADIUS** > **Server** > **Extended configuration** > **Forwarding**



In the case of "multi-layer" EAP protocols such as TTLS or PEAP, the actual "internal" authentication can be performed by a separate RADIUS server. Thus an existing RADIUS server can continue to be operated to provide user tables, even though it is not EAP(/TLS) capable itself. In this situation the TLS/TTLS/PEAP tunnel is managed from the LCOS RADIUS server.

The configuration of multi-layer protocols of this type is an element of a general method for the forwarding of RADIUS requests, whereby a LCOS RADIUS server can also be used as a RADIUS proxy. The concept of "realms" is the basis for request forwarding and the proxy function. A realm is a character string which defines the validity of a series of user accounts. The device considers the following parts of a user name to be the realm:

Mail domain

`User@company.com`: `company.com` is the realm and is separated from the name of the user by an @ character.

MS computer authentication

`company\user`: `company` is the realm and is separated from the name of the user by a backslash ("\").

This form of authentication is used for a Windows login, for example.

MS domain

`Host/user.company.com`: If the user name starts with the string `host/` and the rest of the name contains at least one dot/period, the device considers everything after the first dot to be the realm (in this case `company.com`).

The realm can be seen as a pointer to the RADIUS server where the user account is managed. The realm is removed from the string prior to the search of the RADIUS server's user table. Realms allow entire networks which are mutually trustworthy to work with common RADIUS servers located in partner networks, and to authenticate users who move

between these networks. The LCOS RADIUS server stores any connected RADIUS servers along with their associated realms in a forwarding table. The realm is searched for in this table in connection with the communicated user name. If no entry is found, the request is answered with an access reject. An empty realm is treated as a local request, i.e. the LCOS RADIUS server searches its own user tables and generates its response accordingly.

To support the processing of realms the LCOS RADIUS server uses two special realms:

Default realm

This realm is used where a realm is communicated for which no specific forwarding server has been defined. Importantly, an entry for the default realm itself must be present in the forwarding table.

Empty realm

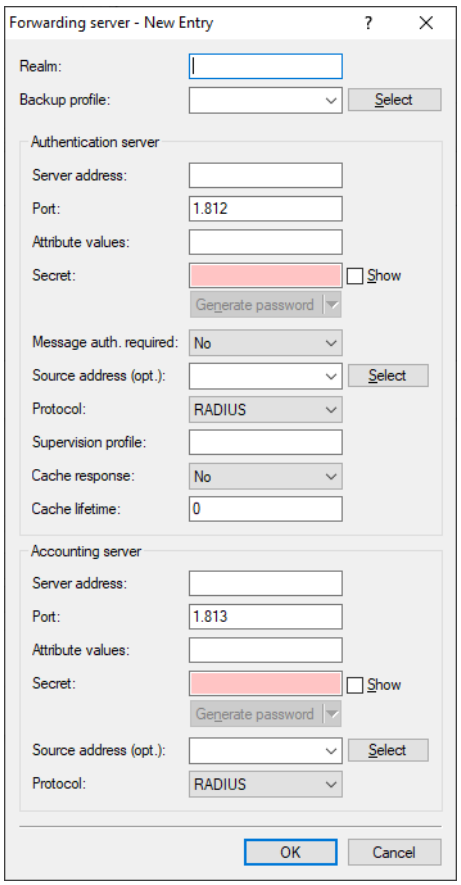
This realm is used when **no** realm is communicated, but the user name only.

In the default state the forwarding table has no entries, i.e. the default and empty realms are empty. This means that all requests are treated as local requests and any realms which are communicated are ignored. To operate the LCOS RADIUS server purely as a forwarding server or RADIUS proxy, the default and empty realms must be set to a value that corresponds with a server defined in the forwarding table.

Please note that the forwarding of RADIUS requests does not alter the user name. No realm is added, changed or removed. The next server may not be the last one in the forwarding chain, and the realm information may be required by that server to ensure that forwarding is carried out correctly. Only the active RADIUS server which processes the request resolves the realm from the user name, and only then is a search made of the table containing the user accounts. Accordingly the LCOS RADIUS server resolves the realm from the user name for processing requests locally.

The processing of tunneled EAP requests using TTLS and PEAP makes use of a special EAP tunnel server, which is also in the form of a realm. Here you select a realm that will not conflict with other realms. If no EAP tunnel server is defined then the LCOS RADIUS server forwards the request to itself, meaning that both the internal and the external EAP authentications are handled by the LCOS RADIUS server itself.

If necessary, set up the **Forwarding server**.



Realm

Character string identifying the forwarding destination.

Backup profile

Alternative forwarding server in case the first forwarding server is not available.

Authentication server and accounting server

You can configure parameters for the two possible RADIUS applications (access management and accounting) so that the router can forward RADIUS queries to an external RADIUS server.

If no forwarding is required for the access management or accounting, leave the corresponding address field empty.

Server address

IP address of the RADIUS server to which the request is to be forwarded.

Port

The same port number must be set for the port that is configured in the corresponding RADIUS server. This is usually 1812 for access management and 1813 for accounting.

Attribute values

Here you can assign user-defined values to RADIUS attributes. The individual name-value pairs must have the form <Name>=<Value>, and they are separated by semicolons.

<Name> identifies the RADIUS attribute by its name or number. The associated attribute names can be found in the corresponding RADIUS RFCs. Attribute names can be abbreviated as long as the identifiers are unequivocal.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

It is also possible to use a number of placeholders:

- `%n` – replaced by the configured device name.
- `%e` – replaced with the serial number of the device as displayed in the device system info.
- `%%` – replaced by a single % character.
- `%{name}` – replaced by the original value of the corresponding RADIUS attribute. Any new / re-definitions within this attribute list are ignored. The identifier can be truncated as long as it remains unique.

Secret

The key (secret) must also match the one configured in the RADIUS server so that this router can authenticate against it.

Message Auth. required

Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

Protocol

Protocol for communication between the internal RADIUS server and the forwarding server.

Supervision profile

Specify a monitoring or supervision server for Dynamic RADIUS Caching here. See **Cache response**.

Cache response

Dynamic RADIUS Caching allows client authentication via IEEE 802.1X even when no data connection to the RADIUS server is available. RADIUS Accept messages are cached and retained for a defined period (see **Cache lifetime**) to enable re-authentication of the respective clients. Using MAC-based authentication, clients can re-authenticate at the port even if the RADIUS server is temporarily unavailable.



Only PAP is supported.

Only MAC-based authentication is supported.

For monitoring purposes, a supervision server must be configured (see **Supervision profile**).

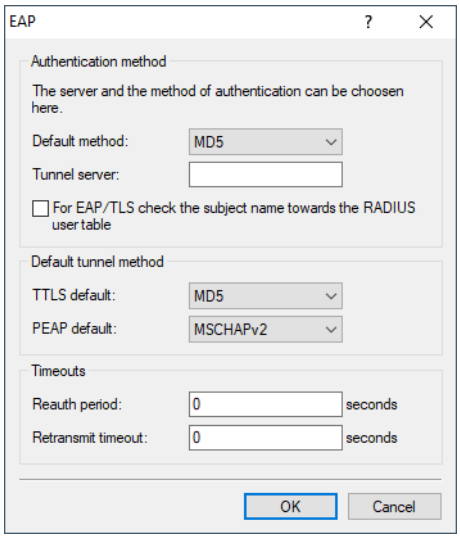
Under **Status** > **TCP-IP** > **RADIUS-Server** > **Access-Control** > **Cached-Responses** you can view the current Dynamic RADIUS Cache. The command-line instruction `show radius-server response-cache` shows all entries in full detail. You can narrow the results using wildcards. Example: `show radius-server response-cache * testuser` shows only entries for the user "testuser".

Cache lifetime

Specify the time period for Dynamic RADIUS Caching here. See **Cache response**.

18.4.5 EAP authentication

EAP authentication is configured via **RADIUS** > **Server** > **Extended configuration** > **EAP**



EAP is not a specific authentication mechanism, it is more like a framework for various authentication methods.

Default method

The LCOS RADIUS server supports a range of EAP methods:

MD5

Defined in *RFC 2284*. EAP/MD5 is a simple challenge/response protocol. It does not cater for mutual authentication nor does it offer a dynamic key such as those required for 802.1X authentication in wireless networks (WLANs). Thus it is only used for the authentication of non-wireless clients or as a tunneled method as a part of TTLS.

GTC

Generic Token Card. EAP-GTC is an EAP method defined in *RFC 3748*, also known as PEAPv1. It is based on a text sent by an authentication server, which must be processed by a security token sent back. The entire transmission is not encrypted.

MSCHAPv2

As opposed to EAD/MD5, EAP/MSCHAPv2 does supports mutual authentication but does not support dynamic keys, making it just as prone to dictionary attacks as EAP/MD5. This method is usually used within PEAP tunnels.

TLS

Defined in *RFC 2716*. The use of EAP/TLS requires the use of a root certificate, a device certificate and a private key in the device. EAP/TLS provides outstanding security and the dynamic keys necessary for wireless connections; its implementation is complex, however, because each individual client requires a certificate and a private key.

Please note that the TLS implementation in LCOS does not support certificate chains or certificate revocation lists (CRLs).

TTLS

TTLS is based on TLS; it does not make use of client certificates and it utilizes the existing TLS tunnel to authenticate the client. The LCOS RADIUS server supports the following TTLS methods:

- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP, preferably EAP/MD5

PEAP

Similar to TTLS, PEAP is based on TLS and works with an EAP negotiation inside the TLS tunnel.

Please note that although PEAP enables the use of any authentication method, the LCOS RADIUS server only supports MSCHAPv2 for tunneling.

OTP

One Time Password. This value must be used with EAP-OTP for *two-factor authentication in the VPN*, because with the LANCOM Advanced VPN Client the EAP method is specified by the EAP server.

At this time, authentication methods cannot be suppressed. The EAP supplicant and the RADIUS server negotiate the EAP method with the standard EAP mechanism. Clients requesting a non-EAP method will be rejected by the RADIUS server.

Tunnel server

To process the tunneled EAP requests used for TTLS and PEAP, simply specify an account that is listed in the forwarding table.

Choose a realm that does not conflict with other configured realms. If this field is left empty, the local RADIUS server handles the request itself. This means that the internal and external EAP phase is performed by the local RADIUS server.

For EAP/TLS, check the subject name against the RADIUS user table

TLS authenticates the client via certificate only. If this is selected, the RADIUS server additionally checks to see if the certificate username (common name, CN in the subject) is included in the RADIUS user table.

If the corresponding entry in the RADIUS user table also contains a VLAN ID, this is transmitted to the authenticator as well.

Default tunnel method

TTLS default / PEAP default

When either TTLS or PEAP is used, two authentication methods are negotiated. First, a secure TLS tunnel is negotiated via EAP. Then a second authentication method is negotiated in this tunnel. In each of these negotiating processes the server offers a method that the client can either accept (ACK) or reject (NAK). If the client rejects it, it sends the server a proposal for a method that it would like to use. If enabled in the server, the method proposed by the client is will be used. Otherwise the server breaks off negotiation.

This parameter is used to determine the method that the server offers to clients for authentication in the TLS tunnel. The value specified here can help to avoid rejected proposals and thus speed up the process of negotiation.

Timeouts

Reauth period

When the internal RADIUS server responds to a client request with an ACCEPT (negotiation of authentication method completed successfully), the RADIUS server can inform the authenticator how long it should wait (in seconds) before triggering repeat authentication of the client.

If the value is 0, no timeout is sent to the authenticator.

Retransmit timeout

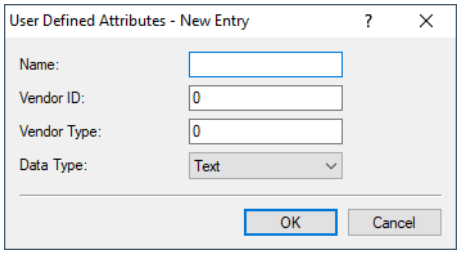
When the internal RADIUS server responds to a client request with a CHALLENGE (negotiation of authentication method not yet completed), the RADIUS server can inform the authenticator how long it should wait (in seconds) for a response from the client before issuing a new CHALLENGE.

If the value is 0, no timeout is sent to the authenticator.

18.4.6 User-defined attributes

RADIUS attributes are managed in what is known as a dictionary. LCOS supports many different attributes by default; however, there is a huge variety of manufacturer-specific attributes, which the administrator can enter into the LCOS configuration here. These attributes can then be used in the LCOS at any point where attributes can be added to a RADIUS request or response, e.g. in the RADIUS user management.

The user-defined attributes are configured via **RADIUS** > **Server** > **Extended configuration** > **User-defined attributes**



Name

The name used to reference the attribute in other places in LCOS.

Vendor ID

The specific vendor ID of the attribute.

Vendor type

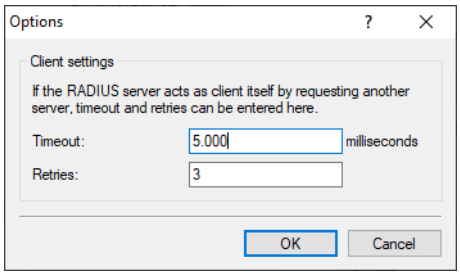
The specific type ID of the attribute.

Data type

The data type of the attribute.

18.4.7 Options

EAP authentication is configured via **RADIUS** > **Server** > **Extended configuration** > **Options**



If the RADIUS server itself works as a client and sends requests to another server, the corresponding settings can be made here.

Timeout / Retries

These values indicate after how many milliseconds a RADIUS authentication should be repeated and how many attempts are made before it is rejected.

18.5 RADIUS attributes

The RADIUS client can request RADIUS attributes, such as the "Framed-IP-Address", from an external RADIUS server and provide these, for example, to a PPPoE server in order to authenticate them at PPPoE, PPTP or L2TP servers.

For more information about RADIUS attributes, see the following technical documents:

- *RFC 2865*
- *RFC 3162*
- *RFC 4679*
- *RFC 4818*
- *RFC 7268*

The device transmits the following attributes in access request messages:

Table 42: Overview of the supported RADIUS attributes

ID:	Name	Meaning	Possible values in LCOS
1	User-Name	The name entered by the user.	Used with 802.1X WLAN, PPPoE server, L2TP, PPTP, VPN
2	User-Password	The password entered by the user.	Used with 802.1X WLAN, PPPoE server, L2TP, PPTP, VPN
4	NAS-IP-Address	Specifies the IPv4 address of the device requesting access for a user.	<IPv4 address of the device>

ID:	Name	Meaning	Possible values in LCOS
6	Service-Type	Specifies the type of service that the device requests or expects as a response.	› Authenticate-Only › Framed
7	Framed-Protocol	Specifies the protocol to be used.	PPP
8	Framed-IP-Address	Specifies the IP address that is assigned to the client.	<IP address of the client>
26	Vendor 2356(LCS) ID 2	MAC address of the client if authentication using the MAC address is enabled. In contrast to the Calling-Station-Id, this value is transmitted as a 6-byte binary string. This attribute only exists for the login mode **Authenticate with name, password and MAC address**.	<MAC address of the client>
30	Called-Station-Id	Specifies the identifier of the called station (e.g. the VPN server).	› Server IP address (for VPN connections via PPTP or L2TP) › Service name (for PPPoE) › BSSID:SSID (for WLAN) › MAC address of the device (for Public Spot)
31	Calling-Station-Id	Specifies the identifier of the calling station (e.g. the VPN client).	› Client IP address (for VPN connections via PPTP or L2TP) › Client MAC address (for PPPoE, WLAN and Public Spot)
32	NAS identifier	Specifies the name of the device being managed by the RADIUS server.	<Device-Name>
61	NAS-Port-Type	Specifies the physical port through which the device authenticates the user.	› Virtual (for VPN connections via PPTP or L2TP) › Ethernet (with PPPoE) › Wireless 802.11 (for WLAN)
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	› 13 (VLAN; for Public Spot)
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	› 6 (802; for Public Spot)
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	› 1-4096 (for Public Spot)
87	NAS-Port-Id	Description of the interface over which the client is connected to your device. This may be a physical and a logical interface.	For example › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27
95	NAS-IPv6-Address	Specifies the IPv6 address of the device requesting access for a user.	<IPv6-address of the device>
96	Framed-Interface-ID	This attribute conveys the IPv6 interface identifier that should be configured for the user in the IPv6CP.	
97	Framed-IPv6-Prefix	Prefix, which is sent to the user via router advertisements.	
99	Framed-IPv6-Route	This attribute conveys the route to be used for this user. The device supplements the IPv6 routing table with this route and the next hop to this user.	

ID:	Name	Meaning	Possible values in LCOS
100	Framed-IPv6-Pool	This indicates the IPv6 pool from which a prefix is to be taken for the user. The IPv6 pool is referenced by its name and must be present under **Ipv6** > **Router advertisement** > **Prefix pools**.	
123	Delegated-IPv6-Prefix	Prefix, which is sent to the user via DHCPv6 prefix delegation.	
177	Mobility-Domain-ID	Identifies the mobility domain where the client is located.	
181	WLAN-HESSID	Contains the HESSID of the 802.11u SSID.	
182	WLAN-Venue-Info	Contains information about the category of the site.	This is configured under **Wireless-LAN** > **802.11u** > **Venue information**.
183	WLAN-Venue-Language	Contains information about the language of the site.	This is configured under **Wireless-LAN** > **802.11u** > **Venue information**.
184	WLAN-Venue-Name	Contains the name of the site (venue name).	This is configured under **Wireless-LAN** > **802.11u** > **Venue information**.
186	WLAN-Pairwise-Cipher	Contains information about the pairwise key used by the client and AP.	
187	WLAN-Group-Cipher	Contains information about the group key used by the client and AP.	
188	WLAN-AKM-Suite	Contains information about the access management (authentication and key management) between the client and AP.	
189	WLAN-Group-Mgmt-Cipher	Contains information about the group management key/cipher used to secure a connection via RSNA (robust security network association) between an AP and mobile client.	
190	WLAN-RF-Band	Contains information about the frequency band used by the client.	

In addition to these attributes, there is an almost endless variety of manufacturer-specific attributes. LCOS allows these attributes to be used once they have been defined. See *User-defined attributes* on page 1550

An example for a PPP user `test` with IPv6 in the FreeRADIUS is as follows:

```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP,
     Framed-IPv6-Prefix := "fec0:1:2400:1::/64",
     Delegated-IPv6-Prefix := "fec0:1:2400:1100::/56",
     Framed-IP-Address := 172.16.3.33
```

The user `test` in a dual-stack PPP session receives the IPv4 address `172.16.3.33`, the prefix `fec0:1:2400:1::/64` via router advertisement, and the prefix `fec0:1:2400:1100::/56` via DHCPv6 prefix delegation.

The following vendor-specific RADIUS attributes use the IANA Private Enterprise Number "3561" of the Broadband Forum. The remaining entries are LANCOM-specific attributes!

Table 43: Overview of all supported manufacturer-specific RADIUS attributes in the access request

ID:	Name	Meaning	Possible values in LCOS
1	ADSL-Agent-Circuit-Id, Vendor 3561	Specifies the interface of the device being managed by the RADIUS server. Only transmitted if agent-relay info is included in the PPPoED packet (see *PPPoE snooping*).	<Device interface>
2	ADSL-Agent-Remote-Id, Vendor 3561	Specifies the identifier of the device being managed by the RADIUS server. Only transmitted if agent-relay info is included in the PPPoED packet (see *PPPoE snooping*).	<Device identifier>
8	LCS-TxRateLimit, Vendor 2356	Defines a maximum downstream rate in kbps on Layer 2 from the perspective of the PPPoE server (NAS) toward the PPPoE client. The PPPoE server supports the vendor-specific RADIUS attributes LCS-TxRateLimit and LCS-RxRateLimit with vendor ID 2356 (LANCOM Systems GmbH) in the RADIUS Access-Accept message. This allows the upstream and downstream bandwidth of a PPPoE client to be limited at Layer 2. This feature is only supported when the PPPoE client is connected via LAN interfaces. It is not supported when the PPPoE client is connected via Layer-2 tunnel interfaces such as Ethernet-over-GRE (EoGRE) or L2TPv3.	
9	LCS-RxRateLimit, Vendor 2356	Defines a maximum upstream rate in kbps on Layer 2 from the perspective of the PPPoE server (NAS) coming from the PPPoE client.	
16	LCS-Orig-NAS-Identifier, Vendor 2356	NAS-identifier of the original access point in WLC mode.	<Device-Name>
17	LCS-Orig-NAS-IP-Address, Vendor 2356	NAS IP address of the original access point in WLC mode.	<IPv4 address of the device>
18	LCS-Orig-NAS-IPv6-Address, Vendor 2356	NAS IPv6 address of the original access point in WLC mode.	<IPv6-address of the device>

An overview of the attributes used to support RADIUS with IKEv2 is available under *RADIUS support for IKEv2* on page 903.

18.5.1 RADIUS attributes configurable

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified by means of a semicolon-separated list of attribute numbers or names (as per *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) and a corresponding value in the following form.

```
<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>
```

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark in a value requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

`%{name}`

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

18.5.2 RADIUS attribute extensions for IPv6 RAS services

The RADIUS client can request RADIUS attributes, such as the "Framed-IP-Address", from an external RADIUS server and provide these, for example, to a PPPoE server in order to authenticate them at PPPoE, PPTP or L2TP servers. The device accepts the following attributes in access-accept messages:

96

Framed-Interface-ID

This attribute conveys the IPv6 interface identifier that should be configured for the user in the IPv6CP.

97

Framed-IPv6-Prefix

Prefix, which is sent to the user via router advertisements.

99

Framed-IPv6-Route

This attribute conveys the route to be used for this user. The device supplements the IPv6 routing table with this route and the next hop to this user.

100

Framed-IPv6-Pool

This indicates the IPv6 pool from which a prefix is to be taken for the user. The IPv6 pool is referenced by its name and must be present under **Ipv6** > **Router advertisement** > **Prefix pools**.

123

Delegated-IPv6-Prefix

Prefix, which is sent to the user via DHCPv6 prefix delegation.

The newly available RADIUS attributes are implemented according to *RFC 3162* and *RFC 4818*. An example for a PPP user `test` with IPv6 in the FreeRADIUS is as follows:

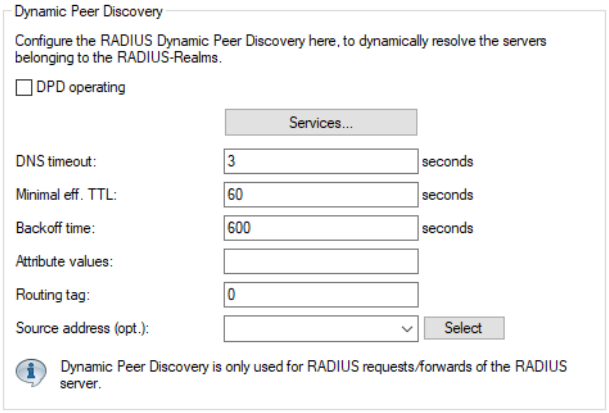
```
test Cleartext-Password := "1234"
     Service-Type := Framed-User,
     Framed-Protocol := PPP,
```

```
    Framed-IPv6-Prefix := "fec0:1:2400:1::/64",
    Delegated-IPv6-Prefix := "fec0:1:2400:1100::/56",
    Framed-IP-Address := 172.16.3.33
```

The user "test" in a dual-stack PPP session receives the IPv4 address 172.16.3.33, the prefix fec0:1:2400:1::/64 via router advertisement, and the prefix fec0:1:2400:1100::/56 via DHCPv6 prefix delegation.

18.6 Dynamic Peer Discovery

Support for *RFC 7585* "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)". Instead of statically forwarding RADIUS requests to one or more RADIUS servers, Dynamic Peer Discovery dynamically finds the correct RADIUS server based on the realm/NAI. If a request arrives, the correct server is found via DNS NAPTR/SRV record.



LANconfig: **RADIUS** > **Dyn. Peer Discovery**

Console: **Setup** > **RADIUS** > **Dynamic-Peer-Discovery**

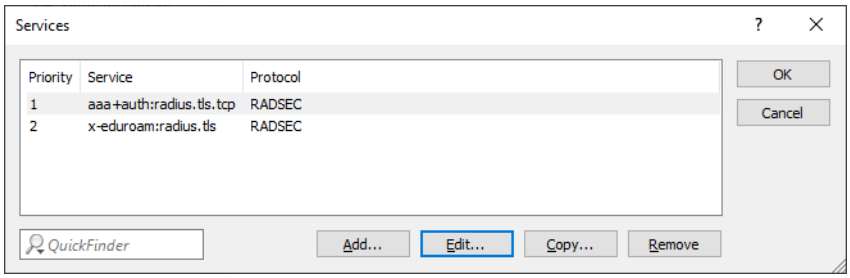
DPD operating

Switch Dynamic Peer Discovery on or off. As soon as Dynamic Peer Discovery is enabled, the RADIUS server branches to dynamic resolution if a specific realm is not defined in its forwarding table. dynamic resolution if a particular realm/NAI is not defined in its forwarding table. Local definitions for realms always have priority.

Services

TTable with the services. The service is what is delivered in the NAPTR response in the service. All NAPTR entries are extracted and are extracted and further resolved, which have as service the one with the highest priority from this table. If the default setting, for example, NAPTR records for both service types are supplied, those for "x-eduroam:radius.tls" are ignored. The table is automatically sorted by the LCOS so that higher prioritized services are placed higher up. The protocol that must be used to such a server (RADIUS or RADSEC) is explicitly specified. In case the NAPTR request does not return any usable records, this table still has the meaning, which prefix is put in front of the NAI for the fallback SRV request. The highest priority entry is taken from the table for which a prefix is defined in an internally fixed table. Currently the services radius.tls,

radius.tls.tcp, radsec.tcp and radius.udp are defined, which respond to a prefix of _radiustls._tcp., _radsec.tcp. or _radius._udp. respectively.



Priority

Priority of this service.

Service

The services themselves. The defaults are “aaa+auth:radius.tls.tcp” and “x-eduroam:radius.tls”.

Protocol

The protocol (RADIUS or RADSEC) used for this service.

DNS timeout

The amount of time in seconds within which all DNS requests for an NAI must be handled. This also includes the two-step variant via NAPTR and subsequent SRV queries. Default: 3 seconds

Minimal eff. TTL

TTL values reported by the DNS server that are shorter than this time are raised to this value. Default: 60 seconds

Backoff time

If a resolution ends in an error (DNS response with error, timeout…), this is the time in seconds for which no new resolution attempts should be made for this realm. Default: 600 seconds

Attribute values

RADIUS attributes to be added or changed when forwarding to servers discovered by Dynamic Peer Discovery.

Routing tag

The routing tag that Dynamic Peer Discovery should use for its DNS queries. Default: 0

Source address (opt.)

The loopback address to use when forwarding to RADIUS servers determined by Dynamic Peer Discovery.

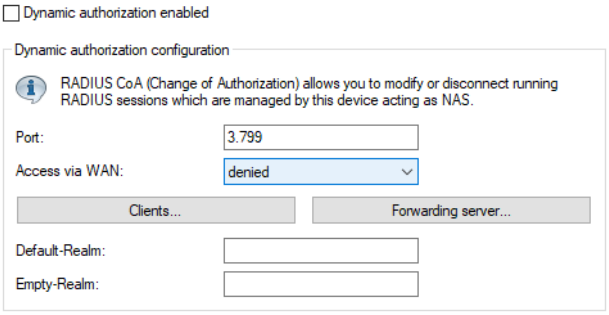
18.7 Dynamic authorization by RADIUS CoA (Change of Authorization)

Dynamic authorization provides the capability to modify current RADIUS sessions. A modification is initiated when the CoA client sends a CoA message to the NAS. This message contains the identifying characteristics for the session to be modified, the attributes to be modified, and their new values.

Another option is to disconnect the current session. This is done with a disconnect message (DM) sent to the NAS, whereupon the NAS terminates the connection.

18.7.1 Configuring dynamic authorization with LANconfig

In order to configure dynamic authorization (CoA) with LANconfig, navigate to **RADIUS** > **Dyn. Authorization**.



Dynamic authorization enabled

Activate or deactivate dynamic authorization here.

Port

Contains the default port where CoA messages are received.

Access via WAN

This entry specifies whether messages are accepted from the WAN, via VPN only, or prohibited.

Clients

Enter all of the CoA clients here that are permitted to send messages to the NAS.

Forwarding server

To forward CoA messages, the forwarding servers are specified here.

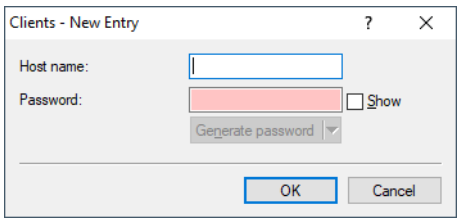
Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Empty realm

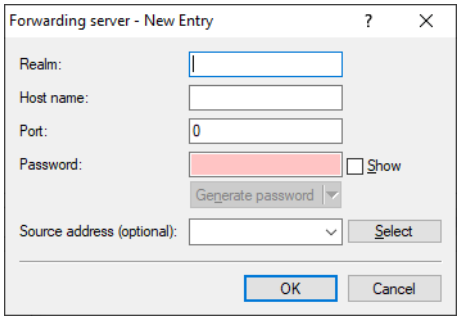
This realm is used when the specified username does not contain a realm.

To add CoA clients for dynamic authorization, click the button **Clients** and add a new entry to the table.



Enter a host name for the client and set a password for the client to access the NAS.

To add new forwarding servers for dynamic authorization, click the button **Forwarding server** and add a new entry to the table.



Realm

Here you enter the realm used by the RADIUS server to identify the forwarding destination.

If applicable, enter any existing forwarding servers that are specified under **RADIUS** > **Server** > **Extended configuration** > **Forwarding** > **Forwarding server**.

Host name

Specify the host name of the forwarding server.

Port

Specify the server port used to forward the requests.

Password

Set a password that is required by the client to access the RADIUS server.

Source address (optional)

Optionally, specify a source address.

Specify which logical WLAN interfaces should use dynamic authorization. You enable or disable them under **Wireless LAN** > **General** > **Logical WLAN settings** > **Network** with the checkbox **RADIUS CoA activated** for the appropriate interface.

18.7.2 RADIUS CoA for 802.1X Authenticator Ethernet Ports

The 802.1X Authenticator for Ethernet ports supports RADIUS Change of Authorization (CoA) and Disconnect Messages (DM) for 802.1X, as well as for authentication based on MAC addresses.

The shared configuration for Dynamic Authorization is used. In LANconfig under **RADIUS** > **Dyn. Authorization** and on the CLI under **Setup** > **RADIUS** > **Dyn-Auth.**. This configuration is also used by Public Spot or IKEv2.

The following CoA functions are supported:

- Disconnecting the session of a current user (Disconnect Message)
- Changing the current user session by modifying the VLAN via a CoA message

Examples:

1. The currently active sessions can be displayed via the status menu:

```
root@test-8021x-dm:/
> ls /Status/LAN/IEEE802.1x/Authenticator-Ifc-Status/

Ifc   Operating Mode        State         MAC-Auth.-Bypass MAC-Address  VLAN-ID Auth-Count Conflicting-MAC
==============-------------------------------------------------------------------------------------------
ETH-2 Yes       Single-Host authenticated No               e89c255b7b86 0       1          000000000000


Conflict-Age
```

```
-----------------
0
```

2. The status for CoA can be displayed with the show command “show ethernet-dynauth”:

```
> show ethernet-dynauth
MAC address e8:9c:25:5b:7b:86 on ETH-2: NAS-Identifier 'test-8021x-dm', User-Name 'test'
```

3. A user session can be disconnected using the CLI command “Radclient” under **Setup** > **RADIUS** > **Dyn-Auth.** in the LCOS, for example:

```
do Radclient 192.168.1.112 disconnect 12345678 "NAS-Identifier=test-8021x-dm;User-Name=test;"
```

   Where:

   - “192.168.1.112” is the IP address of the NAS, i.e., the router
   - “disconnect” is the disconnect message to be sent
   - “12345678” is the configured Dyn-Auth/CoA password
   - “NAS-Identifier” is the name of the router or the unique identifier of the NAS
   - “User-Name” is the 802.1X username used by the client during authentication

   All of these parameters are required.

4. The VLAN of an active session for a MAC-authenticated user can be changed as follows:

```
do Radclient 192.168.1.112 coa 12345678 "NAS-Identifier=test-8021x-dm;User-Name=e89c255b7b86;
   Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200;
```

   Where:

   - “192.168.1.112” is the IP address of the NAS, i.e., the router
   - “coa” is the CoA message to be sent
   - “12345678” is the configured Dyn-Auth/CoA password
   - “NAS-Identifier” is the name of the router or the unique identifier of the NAS
   - “Tunnel-Type:0=VLAN;Tunnel-Medium-Type:0=IEEE-802;Tunnel-Private-Group-Id:0=200” are the required RADIUS attributes to move the client into VLAN 200

   All of these parameters are required.

   For analyzing CoA functionality, the traces “DYN-AUTH-Client” and “DYN-AUTH-Server” are available.

18.8 RADSEC

RADIUS has become established as the standard for server-based authentication, authorization and billing. RADIUS is now being used for applications outside of its original design purpose, for example in combination with EAP/802.1X, and a number of deficits have become apparent:

- RADIUS operates via UDP and thus offers no native procedure for packet-loss detection. Although this is no problem in a LAN environment, it is becoming increasingly important over WAN connections or on the Internet.
- RADIUS is equipped only with simple procedures for authentication by means of a “shared secret” and a low level of confidentiality.

RADSEC is an alternative protocol that transmits RADIUS packets through a TLS-encrypted tunnel. TLS is based on TCP, thus providing a proven mechanism for monitoring packet loss. Furthermore, TLS is highly secure and it features a method of mutual authentication by means of X.509 certificates.

18.8.1 Configuring RADSEC for the client

18.8.1.1 Device as a RADIUS client

To function as a RADIUS client, a device is set up to use RADIUS via UDP or RADSEC via TCP with TLS. Additionally the port to be used has to be set. 1812 for authentication with RADIUS, 1813 for billing with RADIUS and 2083 for RADSEC.

The RADSEC protocol can be selected at any point where a device is configured as a RADIUS client.

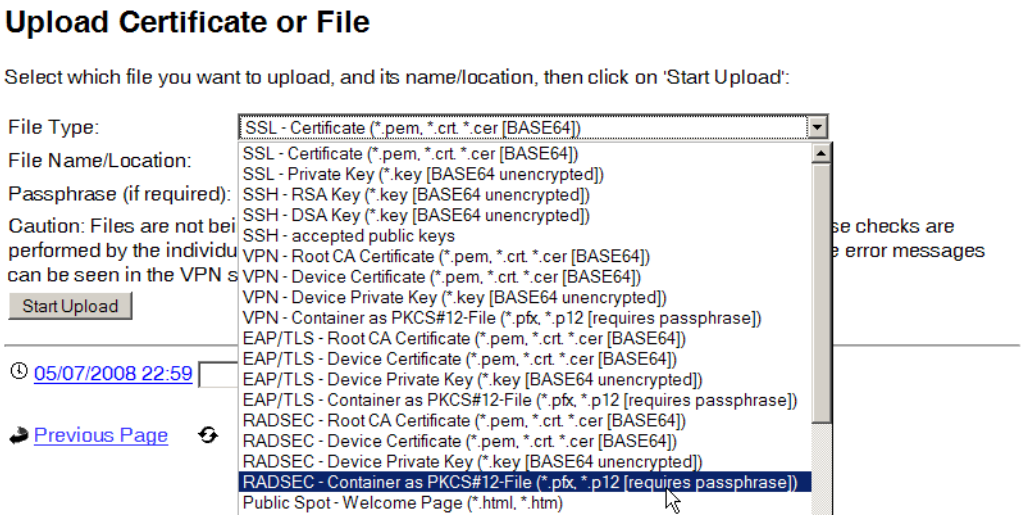
18.8.1.2 Device as a RADIUS server

If a device operates as a RADIUS server, the RADSEC port can be set up for receiving logins. In addition to that, the protocol to be used (RADIUS, RADSEC or all) can be set for each of the RADIUS clients in the client list. On the one hand RADIUS can be used for the clients in the LAN, for example. Additionally, the more reliable RADSEC variant based on TCP can be used for external logins over the Internet.

18.8.2 Certificates for RADSEC

Separate X.509 certificates are required for TLS encryption of the RADSEC connection. The individual certificates (root certificate, devices certificate and private key) can be uploaded to the device individually or as a PKCS#12 container.

WEBconfig: **Upload certificate or file**



19 IoT – the Internet of Things

Here you will find the settings for IoT technologies supported by LCOS, such as Wireless ePaper, iBeacon and Bluetooth Low Energy.

IoT networks interconnect physical and virtual objects to facilitate the exchange of data and information. Typical examples include sensors, smart home appliances, digital room signs, and electronic shelf labels. IoT devices are largely networked by radio, using a variety of wireless technologies such as modified ZigBee variants (retail IoT), Bluetooth Low Energy (BLE), or the various cellular offshoots. There is no uniform "IoT wireless standard", and new IoT radio technologies are emerging in rapid cycles.

The special settings for IoT are made in LANconfig under **IoT**.

19.1 Wireless ePaper

LANCOM Wireless ePaper Displays provide a variety of options for displaying information. You can automatically and remotely update the calendar schedule for your conference rooms, you can create dynamic notices and direction signs, or you can control the price labels of goods on your shelves from a central location in real time. The wide range of different settings allows you to set up your very own customized use case.

The settings for operating Wireless ePaper Displays are to be found in LANconfig under **Tools** > **Options** > **Wireless ePaper**. Under IP/Hostname you enter the IP address and the port of the Wireless ePaper Server. The recommended port number is 8001.

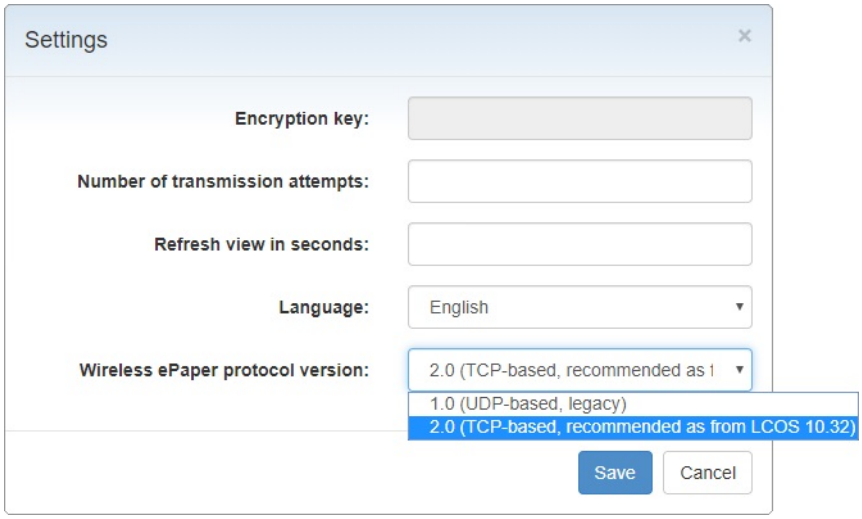
You invoke the Wireless ePaper management in LANconfig under **Tools** > **Start Wireless ePaper management**.

Centralized management of your Wireless ePaper infrastructure

As of LCOS 10.32, LANCOM access points with Wireless ePaper support a new protocol that ensures efficient and reliable communications between the Wireless ePaper server and access points. Thanks to the support of this new protocol, your LANCOM Wireless ePaper Displays can now be managed remotely from the Wireless ePaper Server at your data center and controlled via VPN. The new protocol will be used if both ends support the protocol and it is enabled on the Wireless ePaper server.

From LCOS 10.40 the LANCOM access points with Wireless ePaper support optionally use an extension of the TCP protocol that allows the establishment of TLS-encrypted connections (from Wireless ePaper access points, or routers with a USB interface and a Wireless ePaper USB stick) to the Wireless ePaper Server. To use this extension, both the Wireless ePaper Server and the Wireless ePaper device (access point or router with Wireless ePaper USB) have to be configured accordingly.

In the upper-right corner of the Wireless ePaper management, click on the gear-wheel icon to access the **general settings** for the Wireless ePaper Server. You can activate the new protocol here.



In LANmonitor, the display of the device under **IoT** > **Wireless ePaper** > **Protocol version** displays the protocol that is in use:

- None – there is no connection to a controller/server
- ThinAP1.0/UDP – protocol version 1.0 (UDP-based, legacy)
- ThinAP2.0/TCP – protocol version 2.0 (TCP-based, from LCOS 10.32)

Activating a TCP-based protocol on the Wireless ePaper Server

The Wireless ePaper Server supports "protocol version 2.0" as of version 1.91 and the TLS encryption based on it as of version 1.101. If you already use a supported Wireless ePaper Server and yet only "protocol version 1.0" or, from version 1.101 only "protocol version 2.0" is displayed here, the protocol was probably not yet enabled in the settings for the Wireless ePaper server. In this case you first have to activate the protocol version.

Follow these steps to activate "protocol version 2.0 (ThinAP2.0/TCP)":

1. Check the following prerequisites:
   - LANCOM Wireless ePaper Server version 1.91 or higher is installed
   - cURL is installed
2. Open the command line on your operating system and enter the following command:
   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
   ```
3. Restart the Wireless ePaper Server.
4. Then enter the following command to verify that the feature was successfully enabled:
   ```
   curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
   ```

If activation was successful the output is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

Follow these steps to activate "protocol version 2.0 (ThinAP2.0/TLS)":

1. Check the following prerequisites:
   - LANCOM Wireless ePaper Server version 1,101 or higher is installed
   - cURL is installed
   - "Protocol version 2.0 (ThinAP2.0/TCP)" is activated
   - The Wireless ePaper Server address is configured in the Wireless ePaper supporting device.

The LANCOM Wireless ePaper Server must accept the connection or the Wireless ePaper supporting device must establish the connection, therefore the device must also be configured.

2. Open the command line on your operating system and enter the following command:

   ```
   curl -X PUT http://<server-ip>:8001/service/configuration/accessPointUseThinMode?value=true
   curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinOutboundMode?value=true
   curl -X PUT http://<server-ip>:8001/service/configuration/accessPointThinUseOutboundMode?value=true
   ```

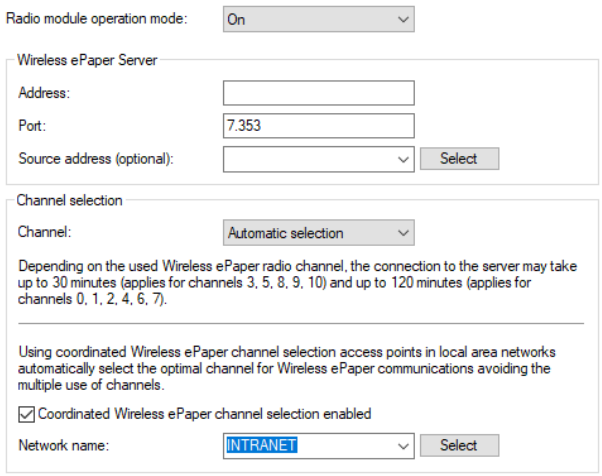
3. Restart the Wireless ePaper Server.
4. Then, as with the TCP protocol check, enter all three parameters with "GET" as the command to check whether the activation was successful. The output must be "`value="true"`"

To deactivate the function on the command line, enter the commands with the parameter "`value=false`" instead of the parameter "`value=true`". The command would look like this:

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

19.1.1 Settings for Wireless ePaper

Activate the Wireless ePaper radio module in LANconfig under **IoT** > **Wireless ePaper**,



Radio module operation mode

Select the basic operating mode of your Wireless ePaper radio module here:

Managed by WLC

In this mode, the radio module of the device is configured by a central WLAN controller (WLC). Any settings made here will be overwritten.

On (stand-alone)

The radio module of the device is switched on and operates autonomously.

Off

The radio module of the device is switched off.

Wireless ePaper Server

From LCOS 10.40 the LANCOM access points with Wireless ePaper support optionally use an extension of the TCP protocol that allows the establishment of TLS-encrypted connections (from Wireless ePaper access points,

or routers with a USB interface and a Wireless ePaper USB stick) to the Wireless ePaper Server. The ThinAP2.0/TLS protocol must be set up on the Wireless ePaper Server (see *Activating a TCP-based protocol on the Wireless ePaper Server* on page 1563) and the IP address of the Wireless ePaper Server must be specified here.

Address

IP address of the Wireless ePaper Server.

Port

Here you set the port for communication between the Wireless ePaper device, e.g. access point or router, and the Wireless ePaper Server. The default port is 7353 for establishing a connection from the Wireless ePaper Server to the Wireless ePaper device. If the connection from the Wireless ePaper device to the Wireless ePaper Server is to be established using TLS, set the port to 7354.

Source address

Enter loopback address here.

Channel selection

Either you let the radio automatically select a channel, or you specify a fixed channel.

Coordinated channel selection

Coordinated channel selection is necessary if your site operates multiple Wireless ePaper access points.

Each access point requires its own ePaper channel, so collisions or multiple assignments need to be avoided.

For this reason, ePaper access points automatically discover neighboring ePaper access points within a broadcast domain by means of a TCP-based protocol that is transmitted in a multicast group. One of these access points is automatically set as the master AP. The remaining access points become slave access points. If the master AP fails, one of the slave APs is automatically designated as the new master AP.

Each slave AP regularly sends an assessment of its current ePaper channel to the master AP. Based on the assessments from all the slaves, the master decides whether or not a slave needs to change channel.

The ePaper AP assesses all of the ePaper channels. This takes into account the locally used WLAN channel (which the ePaper channel should not overlap) and whether the ePaper channel is a preferred channel.

Preferred channels are: 3, 5, 8, 9 and 10.

Based on the channel assessments received, the ePaper channels are optimized as follows:

The master AP selects the best of the free channels and assigns it to the ePaper AP with the lowest ePaper AP ID. The master also assigns a channel to itself. This is performed successively for all of the ePaper APs.

Channels are only switched if the evaluation of the competing channel is better by a certain, configurable threshold. This avoids unnecessary channel changes.

If the network contains one or more ePaper APs with statically assigned ePaper channels, the master can still perform coordinated channel selection. If this is enabled on an access point with a static channel, the master performing the channel allocation will consider this channel to be already assigned and will not assign it to any other access point.

The status menu of the Wireless ePaper feature contains a peer table. This lists the access points involved in channel coordination.

The peer table contains the ePaper access point ID, the role of the AP (slave or master), the channel assessment, and the assigned ePaper channel.

The channel assessment is shown as a list of the ePaper channels 0 to 10 followed by the assessment value. The value range is 0 to 255, a higher value being a better rating.

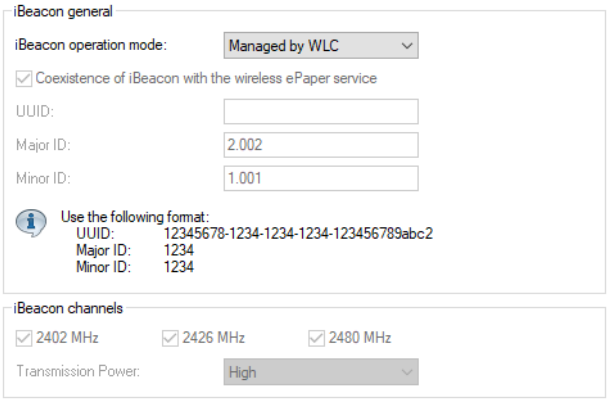
```
root@LN-830E PM:/Status/Wireless-ePaper
> ls -a Channel-Coordination/Peer-Table/

ID    State    IP-Address    Rtg-Tag  Connected  Assessment  Assignment
==============-------------------------------------------------------
66122  SLAVE  172.16.26.7      1        Yes       0:108|1:096|2:073|3:196
66123  MASTER 172.16.26.6      1        No                  3
66124  SLAVE  172.16.26.8      1        Yes       0:127|1:127|2:127:3:255
```

19.2 iBeacon

The operating principle of a beacon, including the iBeacons. is based on a transmitter-receiver principle. For this purpose, small transmitters (beacons) are positioned and they send signals at fixed time intervals. If a receiver, such as a smartphone equipped with an app configured to receive iBeacon signals, comes into range of a transmitter, it can identify the transmitter's Universally Unique Identifier (UUID) and measure its signal strength. With at least three beacons in range, the position of the receiver can be calculated in two-dimensional space. Determining a location in three-dimensional space requires four beacons to be within range. iBeacons themselves cannot send push notifications to receivers, or collect or store user data. They only send information about their own identity (the values UUID, Major and Minor). Data transmission is based on Bluetooth Low Energy (BLE), which is extremely energy efficient. Furthermore, targeted location-related information can be displayed on the smartphone. iBeacon modules achieve a range of up to 30 meters and are characterized by low power consumption.

Settings for iBeacon on E-series devices are adjusted in LANconfig under **IoT** > **IBeacon**.



iBeacon operation mode

Select the basic operating mode of your iBeacon radio module here:

Managed by WLC

In this mode, the radio module of the device is configured by a central WLAN controller (WLC). Any settings made here will be overwritten.

On (stand-alone)

The radio module of the device is switched on and operates autonomously.

Off

The radio module of the device is switched off.

Coexistence of iBeacon with the Wireless ePaper service

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

UUID

Assigns a "Universally Unique Identifier" (UUID) to the iBeacon module.

Major ID

Assign a unique major ID to the iBeacon module.

Minor ID

Assign a unique minor ID to the iBeacon module.

iBeacon channels

Here you select the channels used to broadcast the iBeacon.

Transmission power

Select the transmission power here. The exact meaning of the values that can be selected here is explained in the iBeacon specification. The following values are possible:

High

The module sends with maximum power (default).

Medium

The module sends with medium power.

Low

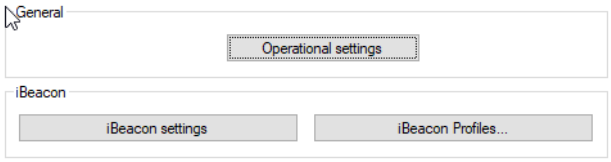
The module sends with minimum power.

19.3 BLE scanner and beacon

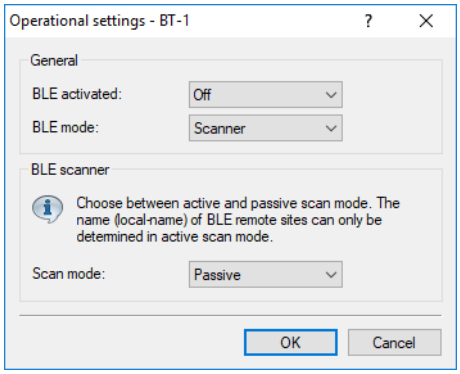
B-series wi-fi devices feature Bluetooth Low Energy (BLE) support for the following technologies: Beacon transmission (e.g. iBeacon) and BLE environment scanning, which in combination with a suitable processing system can be used for applications such as asset tracking or visitor counting.

19.3.1 Settings for BLE

The settings for BLE are made in LANconfig under **IoT** > **Bluetooth LE**.



Operational settings



BLE activated

Activate the BLE module here.

BLE mode

This entry allows you to set the operating mode of the BLE module. Choose whether to use the Bluetooth interface for sending beacons or for scanning the environment.

The two operating modes cannot be operated simultaneously.

Scanner

The BLE module is used for scanning the environment.

BLE-Beacon

The BLE module sends out beacons.

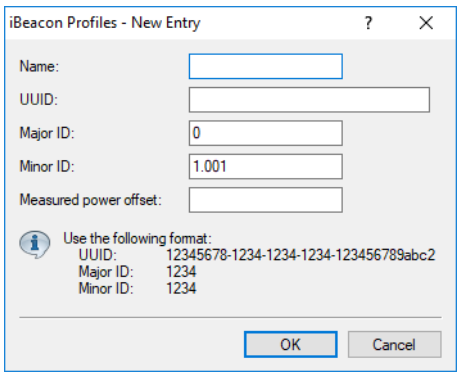
Scan mode

Select here whether to use active or passive scanning. With active scanning, requests are sent actively and any BLE clients in the surroundings can respond to them. This is necessary to determine the names of the clients, for example.

Please note that continuously responding to scan requests can affect client battery life. With passive scanning, no scan requests are sent but only passively listened for.

iBeacon profiles

Here you define profiles that you can later assign to a BLE interface.



Name

Give the iBeacon profile a name.

UUID

A 16-byte identifier used to group together larger groups of beacons. For example, all iBeacons of a company could share the same iBeacon UUID.

Major ID

A 2-byte identifier used to distinguish subgroups of iBeacons. For example, all iBeacons at a company branch office could share the same major identifier.

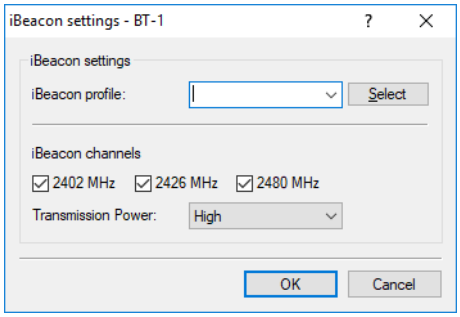
Minor ID

A 2-byte identifier used to distinguish individual iBeacons. For example, each individual iBeacon in a branch office could have its own minor identifier.

Empfangsleistungsverschiebung

Normally, a power value measured according to the set transmit power is used to detect the approximation and exact distance of devices emitting a beacon. On the basis of the corresponding measurement series, a deviation can be determined between the measured reception power and actual distance from the device emitting the beacon. Based on this deviation, experts can specify a offset of the reference value of the device in order to increase the measurement accuracy.

iBeacon settings



iBeacon profile

Here you select iBeacon profile to set the UUID, Major ID and Minor ID, etc.

iBeacon channels

Here you select the channels used to broadcast the iBeacon.

Transmission power

Select the transmission power here. The exact meaning of the values that can be selected here is explained in the iBeacon specification. The following values are possible:

High

The module sends with maximum power (default).

Medium

The module sends with medium power.

Low

The module sends with minimum power.

19.3.2 Monitoring

19.3.2.1 Monitoring on the CLI

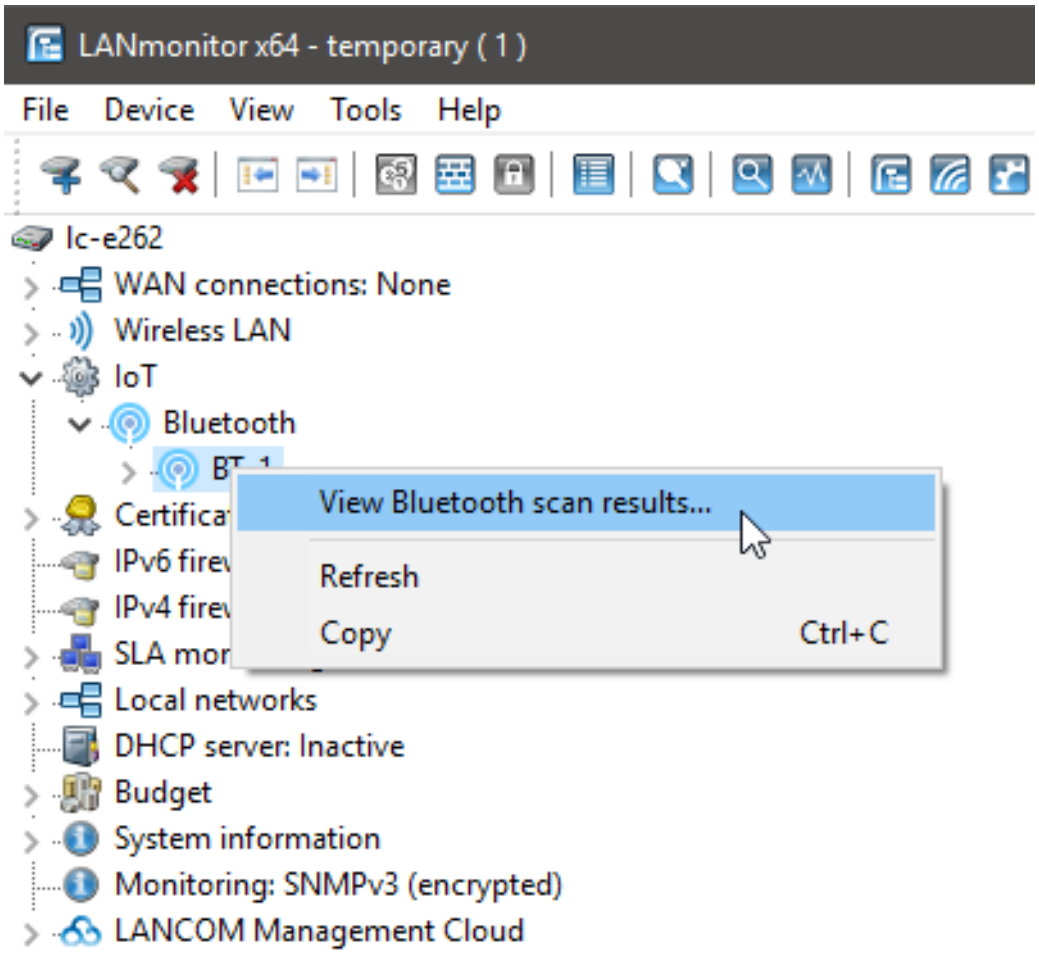
In scanning mode, the scan results are viewed in the table **Status** > **IoT** > **Bluetooth** > **Scan-Results**.

Note that the iBeacon-related values are only filled in when the scanned client actually is an iBeacon.

The implementation of applications such as asset tracking requires these values to be read out by an external system. This can be done with the usual methods for accessing LANCOM devices, preferably by SNMP.

19.3.2.2 Monitoring with LANmonitor

In Scanning mode, the scan results in LANmonitor can be viewed in tabular form. The scan result table can be accessed via the context menu of the corresponding Bluetooth module:



Note that the iBeacon-related values are only filled in when the scanned client actually is an iBeacon.

The implementation of applications such as asset tracking requires these values to be read out by an external system. This can be done with the usual methods for accessing LANCOM devices, preferably by SNMP.

20 Other services

A device offers a range of services for PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Time server

20.1 Automatic IP address administration with DHCP

20.1.1 Introduction

20.1.1.1 DHCP server

All devices in a local area network require a unique IP address in order for a TCP/IP network to function smoothly. They also require the addresses of DNS servers and also of a standard gateway that can route data packets to addresses not located on the local network.

In a small network it is still possible to enter these addresses on all the computers in the network manually. However, in a large network with many workstations this soon becomes an unmanageable task. This is where the use of DHCP (dynamic host configuration protocol) comes in. A DHCP server in a TCP/IP-based LAN can use this protocol to assign the required addresses to the individual workstations dynamically.

The devices have an integrated DHCP server that can assume the task of assigning IP addresses. This process involves communicating the following parameters to the workstations:

- IP address
- Netmask
- Broadcast address
- Default gateway
- DNS server
- Lease (validity period) of the assigned parameters

The DHCP server must first know which IP addresses it can use to assign before it can actually assign them to workstations in the network There are three different methods for selecting possible addresses:

- An IP address can be taken from the defined address pool (Start address pool to End address pool). Any address can be entered provided it is valid for the IP network segment.
- If “0.0.0.0” is entered, the DHCP server determines the relevant first and last addresses itself using the settings for the IP network (network address and netmask).
- The device will be in a special operating mode if no IP network has yet been defined. It then uses the IP address “172.23.56.254” and the address pool “172.23.56.x” for assigning IP addresses to the network.

When a client is activated in the network and requests an IP address via DHCP, the device with an activated DHCP server will offer to assign an address. This address is selected from the pool of valid IP addresses. A computer which received an IP address in the past requests this address again and, assuming the DHCP server has not assigned this number to another computer in the meantime, it will attempt to issue this address again.

The DHCP server also checks the LAN to confirm that the selected address is free. Once the address is confirmed as unique, it is assigned to the requesting computer.

Therefore in the most basic scenario you only need to connect a new out-of-the-box device to a network without a DHCP server and switch it on. The DHCP server will then manage all further address assignment in the LAN by itself in cooperation with LANconfig using a Wizard.

DHCP settings can be different for each network. It is possible to define several IP networks in LCOS in conjunction with advanced routing and forwarding (ARF). DHCP settings therefore apply to a particular IP network, with the exception of a few general settings.

20.1.1.2 DHCP relay

If another DHCP server is located in the LAN, a device can obtain the address information it requires from the other DHCP server if it is in DHCP client mode.

The device can also operate as a DHCP relay agent and as a DHCP relay server.

DHCP relay agent

As a DHCP relay agent, the device forwards DHCP requests to another DHCP server.

DHCP relay server

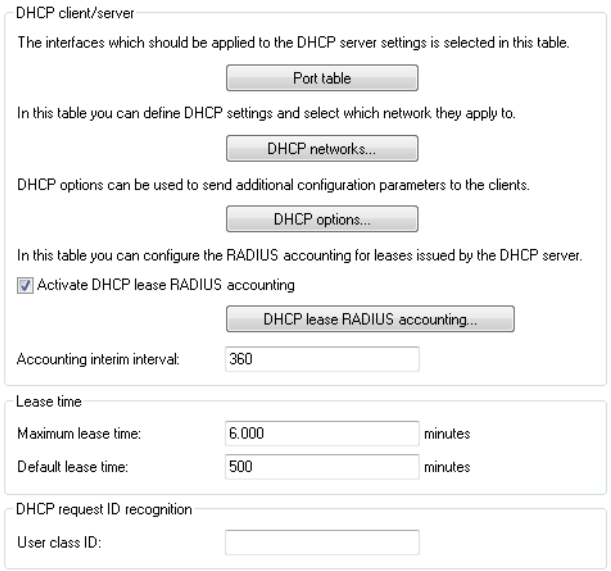
As a DHCP relay server the device processes DHCP requests forwarded from DHCP relay agents.

20.1.1.3 BOOTP

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. Workstations without hard drives can use BOOTP to load a boot image, i.e. a complete operating system, from a boot server (ARF).

20.1.2 Configuring DHCPv4 parameters with LANconfig

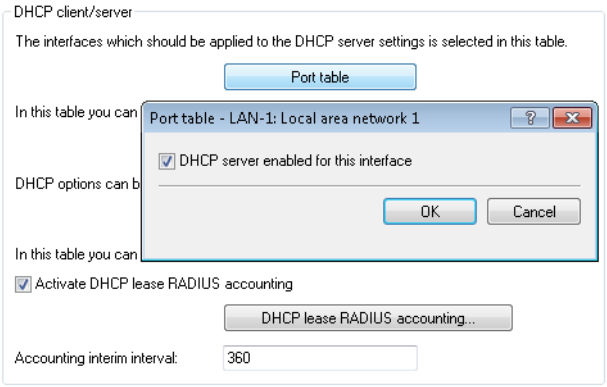
The DHCPv4 settings in LANconfig are configured under **IPv4** > **DHCPv4**.



Information on configuring the DHCPv6 settings is available in the section *IPv6*.

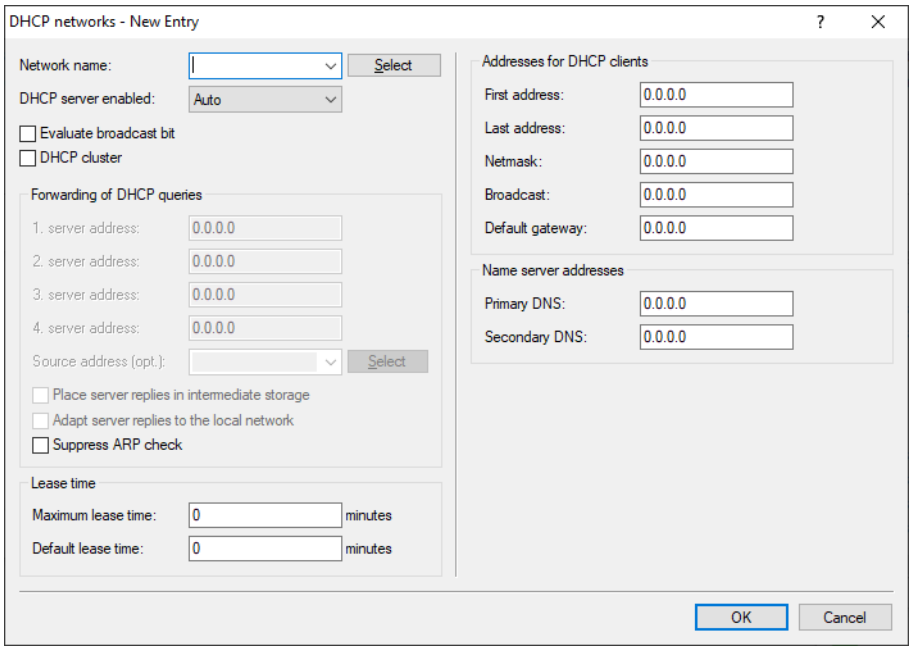
20.1.2.1 Port table

The DHCP server can be enabled or disabled separately for each logical interface (e.g. LAN-1, WLAN-1, P2P-1-1 etc.). To do this, select the appropriate logical interface from the configuration menu under **IPv4** > **DHCPv4** > **Port table** and switch the DHCP server on or off for this interface.



20.1.2.2 DHCP networks

DHCP settings can be specified separately for any IP network defined in the device. To find the parameters that define the DHCP networks, click on **DHCP networks**.



Network name

Select here the name of the network to which the settings are to apply.

The configuration of IP networks is located in the LANconfig configuration menu under **IPv4** > **General** > **IP networks**.

DHCP server enabled

The DHCP server can be configured to run in the following modes:

On

DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked.

- If the configuration is correct then the device starts operating as a DHCP server in the network.
- Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be disabled and switched to the "Off" state.

Only use this setting if you are certain that no other DHCP server is active in the LAN.

Off

DHCP server is permanently switched off.

Auto (default)

With this setting, the device regularly searches the local network for other DHCP servers. The "LAN-Rx/Tx" LED flashes briefly when this search is in progress.

- If another DHCP server is discovered the device switches its own DHCP server off. If the router is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally.
- If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the router will be disabled.

Client mode

The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN.

Only use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

Forward queries

The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.

Stateless relay

The device accepts requests from DHCP clients in the local network. However, the device does not answer these requests itself, but forwards them to a central DHCP server in another network section (DHCP relay agent mode).

The Stateless Relay Agent does not modify DHCP packets from the client to the server and back. In particular, unlike the Relay Agent, the DHCP server identifier is not modified.

The status of the DHCP server is available in the DHCP statistics.

Evaluate broadcast bit

Select here whether the DHCP server should evaluate the broadcast bit reported by the client.

If the bit is not evaluated, all DHCP responses are sent as broadcasts.

DHCP cluster

Enable or disable the operation of a DHCP server in a cluster here.

Enabled

With cluster mode activated, the DHCP server monitors all of the ongoing DHCP negotiations in the network, and it additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster. These stations are flagged as “cache” in the DHCP table.

Disabled (default)

The DHCP server manages information only for the stations connected to it.

If the lease time for the information supplied by DHCP expires, the station requests a renewal from the DHCP server which supplied the original information. If the original DHCP server does not respond, the station then emits its rebinding request as a broadcast to all available DHCP servers. DHCP servers in a cluster ignore renew requests, which forces a rebinding. The resulting broadcast is used by all of the DHCP servers to update their entries for the station. The only DHCP server to answer the rebind request is the one with which the station was originally registered. If a station repeats its rebind request, the all DHCP servers in the cluster assume that the original DHCP server is no longer active in the cluster, and they respond to the request. The responses received by the station will have the same IP address, but the gateway and DNS server addresses may differ. From these responses, the station selects a new DHCP server to connect with, and it updates its gateway and DNS server (and other relevant parameters) accordingly.

Forwarding of DHCP requests

Address of 1st, 2nd 3rd and 4th Servers

Configure the IP addresses of up to four parent DHCP servers. If the network's DHCP operating mode is set to “Forward queries”, the device forwards DHCP requests to these addresses.

Source address (optional)

Here you assign an optional source address to a relay agent. This address (the name of an ARF network, named loopback address) is used to forward client messages.

Put server replies into intermediate storage

If you enable this option, the device stores responses from the parent DHCP server so that it can directly respond to subsequent requests.

This avoids unnecessary connections if the parent server is on a remote network.

Adapt server replies to the local network

If you enable this option, the device modifies the responses from the parent DHCP server, so as to adapt them to the local network.

This means that it replaces the values for “default gateway” and “DNS server”.

Suppress ARP check

Before the DHCP server assigns an IP address, an ARP request is usually used to check whether the address has been assigned already. If there is no response to the ARP request within 3 seconds, the assignment goes ahead. This query is especially useful when computers are booting in normal networks that use fixed IP addresses. In a Public Spot network where, for example, a smartphone has to recognize that there is no Internet connection in order to display the login popup, this ARP request leads to an unnecessary delay. For scenarios such as this, this check can be disabled here.

Lease time of address assignments

In addition to the global default lease time configured under **IPv4** > **DHCPv4**, it is possible to configure a lease time specifically for this DHCP network only.

Maximum lease time

Here you specify the maximum lease time that a client may request.

Default lease time

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

Addresses for DHCP clients

First address

Here you enter the first IP address of the pool of addresses that you want to provide to DHCP clients.

If you do not specify a range, the DHCP server automatically uses all of the free addresses on its own network.

Last address

Here you enter the last IP address of the pool of addresses that you want to provide to DHCP clients.

Netmask

Specify here the netmask associated with the selected address range.

If no mask is entered, the device attempts to determine the netmask as far as possible from its own address and netmask.

Broadcast

As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case, you enter the broadcast address to be used here.



We recommend that only experienced network specialists change the pre-setting for the broadcast address. Errors in the configuration here can lead to unwanted and potentially costly connections being established.

Default gateway

As standard, the device issues its own IP address as the gateway address to computers making requests. If necessary, you can configure the IP address of another gateway by entering the appropriate address here.

Name server addresses

Primary/secondary DNS

Specify here the address of a name server and an alternative name server, to which DNS requests are to be forwarded.

You can leave this field empty if you have an Internet provider or other remote site that automatically assigns a name server to the router when it logs in.

When configuring DHCP networks, the addresses are defined that can be assigned to the DHCP clients (address pool). When a client is activated in the network and requests an IP address via DHCP, the device with an activated DHCP server will offer to issue an address. This address is selected from the pool of valid IP addresses. A computer which received an IP address in the past requests this address again and, assuming the DHCP server has not assigned this number to another computer in the meantime, it will attempt to issue this address again.

The DHCP server also checks the LAN to confirm that the selected address is free. Once the address is confirmed as unique, it is assigned to the requesting computer.

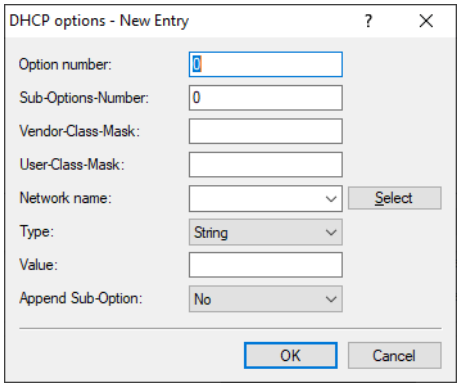
The device factory settings include the IP networks 'Intranet' and 'DMZ', although there are no settings for IP addresses and netmasks. The device is in a special operating mode. It then uses the IP address "172.23.56.254" and the address pool "172.23.56.x" for assigning IP addresses to the network.

Multiple networks on one interface: With the configuration of IP and DHCP networks, multiple networks with different DHCP settings can be active at a logical interface. In this case, the DHCP settings for the first suitable network are applied. A prioritization of networks may be necessary here.

20.1.2.3 DHCP options

The DHCP server uses the DHCP options to transmit additional configuration parameters to the DHCP clients. The vendor class ID (DHCP option 60) shows e.g. the type of device. DHCP option 43 is used by various device manufacturers to distribute additional information about network devices during the initial startup. The parameters themselves are manufacturer-specific. For the LANCOM Rollout Agent, for example, see *Configuring the zero-touch rollout* on page 152.

In LANconfig, the DHCP options are configured under **IPv4** > **DHCPv4** > **DHCP options**. Click on **Add** to create a new entry.



Option number

Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP.

You can find a list of all DHCP options in *RFC 2132 – DHCP Options and BOOTP Vendor Extensions* of the Internet Engineering Task Force (IETF).

Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. For example, DHCP requests from LANCOM devices always contain the string "LANCOM" in the vendor-class ID, which is supplemented by the exact device type, if required. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The

wildcards “*” (any number of characters) and “?” (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

For LANCOM devices, the entry here would be “*LANCOM*”.

User class mask

Filter criterion used by some manufacturers for requests to the DHCP server. See also Vendor-class mask. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards “*” (any number of characters) and “?” (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

Network name

Name of the IP network where this DHCP option is to be used.

Type

Entry type. This value depends on the respective option. For example, RFC 2132 defines the option “35” (ARP cache timeout) as follows:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

This description tells you that this the type “32-bit integer” is used for this option.

You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Value

With this field you define the contents of the DHCP option.

IP addresses are specified with the usual notation for IPv4 addresses, e.g. as “123.123.123.100”, integer types are entered as normal decimal numbers, and strings as simple text.

Multiple values in a single field are separated with commas, e.g. “123.123.123.100, 123.123.123.200”.

You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Append Sub-Option

For each sub-option of option 43, a separate option is created and transmitted. This switch allows several sub-options of DHCP option 43 to be appended. To do this, set this to **Yes**. Appending occurs when:

- **Option-Number** equals 43
- **Sub-Option-Number** is not equal to zero
- Above that in the table an option 43 with a sub-option number not equal to zero

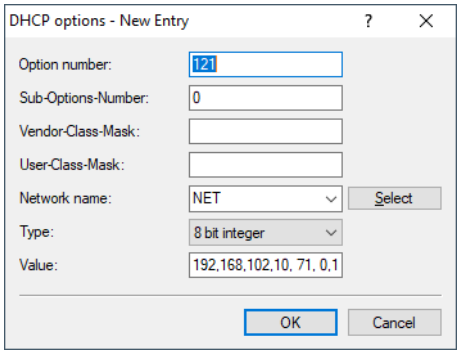
Note that each option can have a maximum of 255 characters.

Example: Transmit the “Classless Static Route” option from the DHCP server

To transmit the route 192.168.102.0/24 via 10.71.0.1 as a Classless Static Route Option (121) from the DHCP server, place the following entry in the table **IPv4** > **DHCPv4** > **DHCP options**:

- **Option number** – 121

- **Network name** – name of the network to which the option should be transmitted to clients.
- **Type** – 8-bit integer
- **Value** – 24,192,168,102,10, 71, 0,1

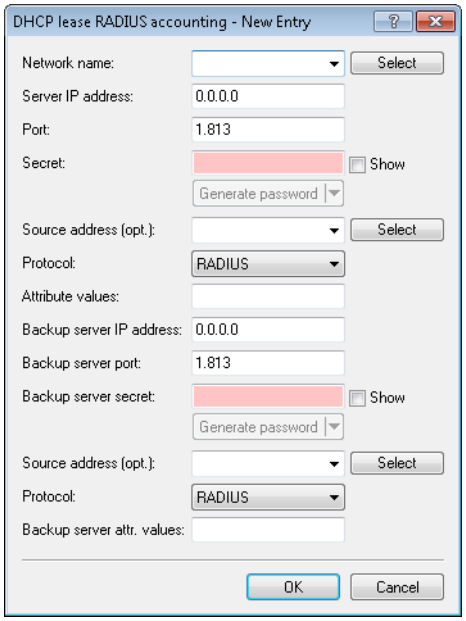


20.1.2.4 DHCP lease RADIUS accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a `RADIUS accounting start` to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a `RADIUS accounting stop`. In between these two events, the DHCP server regularly sends the RADIUS server a `RADIUS accounting interim update` in a configurable interval.

To enable or disable RADIUS accounting for the DHCP server, go to **IPv4** > **DHCPv4** and click on the option **Activate DHCP lease RADIUS accounting**.

The input box **Accounting interim interval** configures the interval for the RADIUS interim updates. You configure the RADIUS accounting server and the corresponding backup server by clicking on **DHCP lease RADIUS accounting**.



Network name

Select here the name of the network for which RADIUS accounting messages are to be sent.

Server IP address

Enter the IP address or the DNS name of the RADIUS server (IPv4 or IPv6).

Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port "1813".

Key

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Source address (optional)

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Protocol

Use this entry to specify the protocol used by the DHCP server to communicate with the RADIUS accounting server.

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

`%n`

Device name

`%e`

Serial number of the device

`%%`

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup server IP address

Enter the IP address or the DNS name of the backup RADIUS server.

Backup server port

Enter the TCP port used by the backup RADIUS server to receive accounting information. That is usually the port "1813".

Backup server secret

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Source address (optional)

Here you optionally specify an alternative source address that the DHCP server transfers to the backup RADIUS server.

Protocol

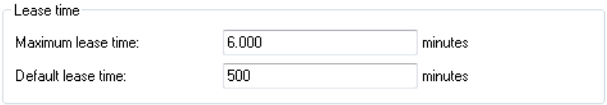
Use this entry to specify the protocol that the DHCP server uses for the RADIUS accounting server.

Backup server attr. values

Here you specify any additional attribute values for the RADIUS communication with the backup server.

20.1.2.5 Lease time of address assignments

When a DHCP client requests an IP address from a DHCP server, it can also ask for a lease period for the address. In this section you configure how the DHCP server handles these requests.



Maximum lease time

This values governs the maximum length of lease that the client may request.

Default lease time

When a client requests an address without asking for a specific lease period, the DHCP server assigns the address with the lease period given here.

20.1.2.6 Vendor Class and User Class Identifier on the DHCP Client

The DHCP client in the device can supplement the transmitted DHCP requests with additional information to simplify the recognition of request within the network.

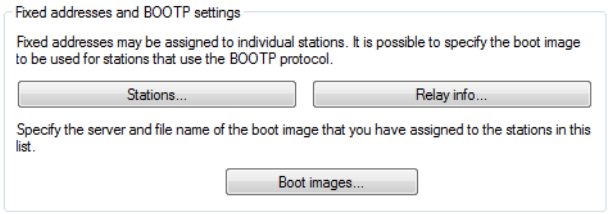
› The vendor class ID (DHCP option 60) shows the type of device. The vendor class ID is always transmitted.

› The user class identifier (DHCP option 77) displays a user-defined string, which can be entered under `Setup/DHCP` or in LANconfig in the configuration section **IPv4** > **DHCPv4** in the **User class ID** field (default: blank). The user class ID is only transmitted when the user has configured a value.

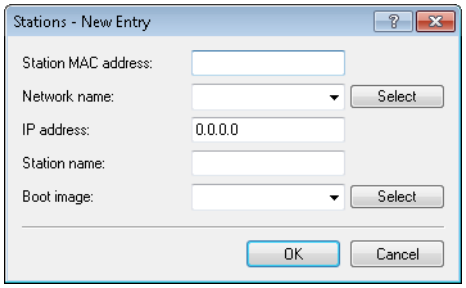


20.1.2.7 BOOTP: Configuring the assignment of fixed IP addresses to specific clients

The parameters for configuring BOOTP in LANconfig is located under the configuration menu **IPv4** > **BOOTP**.



Enter the MAC address of the client that is to be assigned a fixed IP address into the **Stations** list.



The client's MAC address

Enter the node ID of the client here.

The node ID is the physical identifier of the client network adapter and corresponds to the MAC address.

Network name

Select here the name of the ARF network to which the settings are to apply.

If you leave this entry blank, the device will assign the configured address from the ARF network that the DHCP request arrived from. If the request arrives from an ARF network that you have not configured with a special address, the device dynamically assigns an address from the address pool.

If an assigned IP address is outside of the address range of the configured ARF network, the assignment is rejected and, instead, an IP address is used from the address pool of the ARF network that the request arrived from.

IP address

Enter the IP address that the device assigns to the client.

Station name

Enter the name used by the device to identify the client.

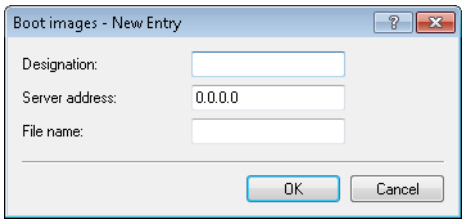
If the client does not communicate its name, the device will use the name entered here.

Boot image

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

You must enter the server providing the boot image and the name of the file on the server in the boot image table.

You can define a boot image in the list of **boot images** that you optionally wish to assign to a client.



Designation

Specify a unique identifier for this entry.

Server address

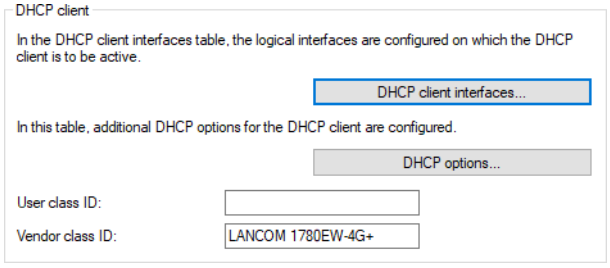
Enter the IP address of the server that provides the boot image.

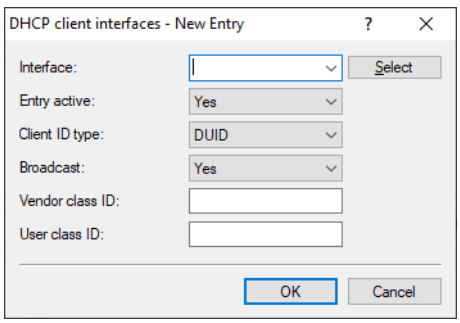
File name

Enter the name of the file containing the boot image.

20.1.2.8 DHCPv4 client interfaces

You can configure the client interfaces of the DHCP client for IPv4 under **IPv4** > **DHCPv4** > **DHCP client** > **DHCP client interfaces**.





Interface

Name of the interface on which the client is active (LAN, physical WAN, or WWAN interface). Depending on the device, default entries for Zero Config exist after a system reset: “INTERNET-DHCPDEF”, “INTERNET-DEFAULT”, or “WWAN-DEFAULT”.

Entry active

Switch to specify whether this entry is active.

Client ID type

Switch that specifies the type of client ID.

Broadcast

Switch that specifies the type of client ID.

Vendor class ID

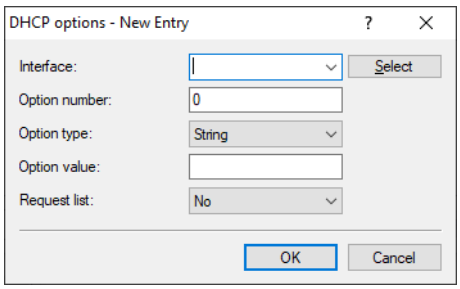
String containing the vendor class identifier to be reported on this interface. If this value is empty, the (global) value under **IPv4** > **DHCPv4** > **DHCP client** > **Vendor class ID** will be used.

User class ID

String containing the user class identifier to be reported on this interface. If this value is empty, the (global) value under **IPv4** > **DHCPv4** > **DHCP client** > **User class ID** will be used.

20.1.2.9 DHCPv4 client options

Certain options can be configured for the DHCPv4 client, which are then transmitted. This is required if the Internet provider expects certain data in DHCP messages. The options is found in the DHCP Options table under **IPv4** > **DHCPv4** > **DHCP client** > **DHCP options** and can be freely configured.



Interface

Interface that the DHCPv4 client should use for this option, e.g. WAN remote site or IPv4 LAN network.

Option number

Specifies the assigned IANA number of the DHCP option as defined in the RFC.

Option type

Specifies the type of the DHCP option. Possible values: String, Integer8, Integer16, Integer32, or IP address

Option value

Specifies the content of the DHCP option

A comma and/or space-separated list can also be specified, except in the case of a string. C-coding applies to integer values, i.e. for numbers 0x gives a hex value and, if the number starts with 0, it is an octal value. With the Integer8 type, it is additionally possible to specify a single hex string (of even length) without a separator. Values from the default options can be overwritten. The following options cannot be overridden

or configured: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57), and end (255).

Request list

Specifies whether the DHCP request should request the option number. The behavior is defined via the respective RFC of the DHCP option. Possible values: Yes, No

20.1.3 Configuring DHCP clients

It is standard in a Windows network environment for nearly all settings to be configured in such a way that required parameters can be requested via DHCP. You can check your Windows settings by clicking on **Start** > **Settings** > **Control Panel** > **Network**. Select the entry for **TCP/IP** on your network adapter and open **Properties**. You can now see on the various tabs whether there are special entries for e.g. the IP address or the standard gateway. If you wish to have all the values assigned by the DHCP server, just delete the corresponding entries.

If a client is to use a different parameter from the one assigned (e.g. for a standard gateway), this parameter must be configured at the workstation itself. The client will then ignore the corresponding parameter(s) in those assigned by the DHCP server. Under Windows this can be effected for example via the properties of the network environment. Click on **Start** > **Settings** > **Control Panel** > **Network**. Select the entry for **TCP/IP** on your network adapter and open **Properties**. You can now enter the desired values on the various tabs.

20.1.4 DHCP-client option Classless Static Route

The DHCPv4 option Classless Static Route allows a DHCP server to pass a list of static routes to a DHCP client, which then enters those routes into its routing table. The routes in this list are "Classless", i.e. a subnet mask or prefix length is transmitted for each route. According to RFC 3442, the option number 121 is used for this purpose.

On receiving this list, the DHCP client does not install a default route to the specified router, but only the list of the static routes in its routing table.

This feature is used, for example, by ISPs in scenarios where multiple virtual connections are separated by VLAN according to the individual service, e.g. with one VLAN each for Internet, VoIP and IPTV. In this case, the default route is used for the Internet connection (e.g. via PPPoE or DHCP), while the routes for IPTV are directed via a different VLAN as communicated by DHCP Classless Static Route Option.

By default, the LANCOM DHCPv4 client requests both the router option and the "Classless Static Routes" option. If the DHCP server sends a "Classless Static Routes" option, the client ignores any router option and only installs the list of routes. This behavior conforms with RFC 3442.

For a provider scenario with IPTV, you create a new DSL remote site with hold time 9999, layer DHCPOE and the corresponding VLAN according to provider specifications. Activate the switch **Establish remote site even without route (keepalive without route)** under **Communication** > **Remote Sites**. No entries are required in the routing table as the DHCP client provides the necessary routes by means of the "Classless Static Route" option.

The LANCOM DHCP server can also use a user-defined option to assign the "Classless Static Route" option to DHCP clients. Refer to section *DHCP options* on page 1577 for information on this.

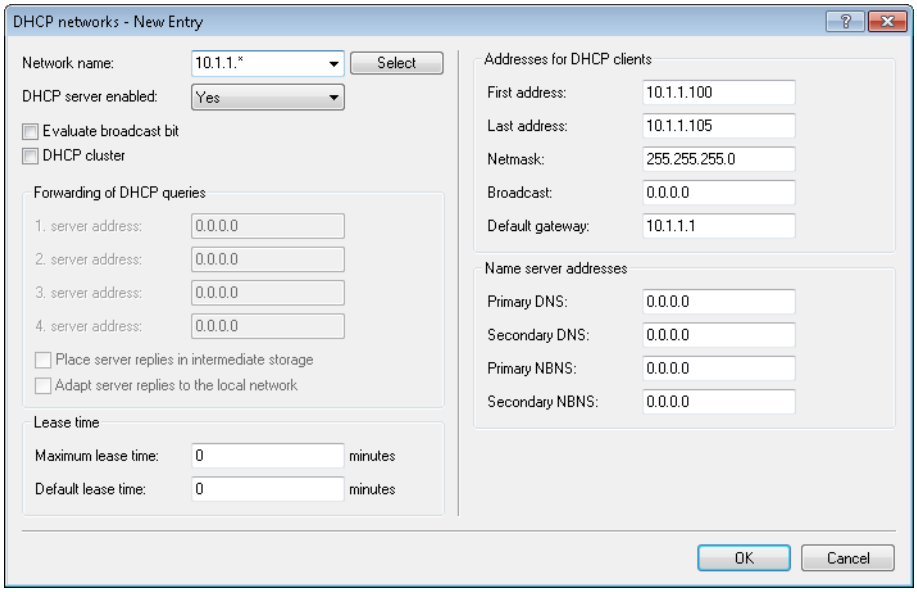
20.1.5 DHCP relay server

A device is not limited to forwarding DHCP requests to upstream DHCP servers; it can also function as a central DHCP server (DHCP relay server).

In order for a device to operate as a DHCP relay server to other networks, the relay agent IP address (GI address) is entered as the network name in the table of IP networks.

If the same network is being used by several relay agents (e.g. multiple access points are forwarding requests to a central DHCP server) then the GI address can also be abbreviated with a "*". If for example clients in the remote network `10.1.1.0/255.255.255.0` are to be assigned with addresses and several relay agents are available in this

network, all of which use the device as upstream DHCP server, then the assignment of IP addresses and standard gateway to the clients can take place as follows:



In DHCP relay server mode, the address pool, the netmask and the broadcast address must be specified.

20.1.5.1 DNS resolution of names learned via DHCP

The DNS server considers the interface tags when resolving names learned via DHCP, i.e. the only names to be resolved are those which were learned from a network with the same interface tag as the requesting computer. If the request arrives from an untagged network, then all names are resolved, including those that were learned via tagged networks. Similarly, all names that were learned from untagged networks are visible for tagged networks.

Names learned from relay agents are handled as though they were learned from an untagged network, i.e. these names are visible to all networks.

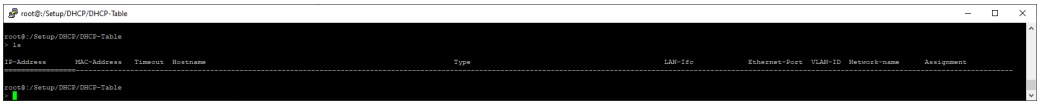
20.1.6 Displaying status information from the DHCP server

You can view a summary of the LAN IP addresses in the Status table of the DHCP server. It shows the following information about the devices that to which the DHCP server has assigned IP addresses:

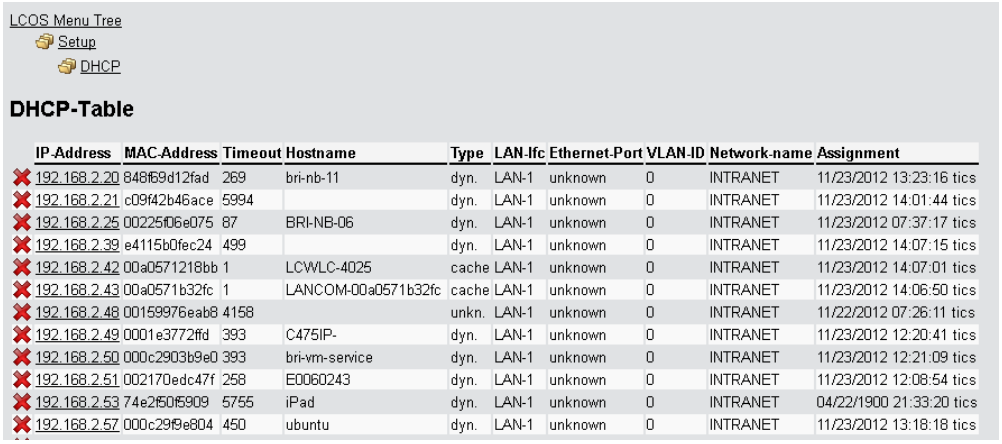
- IP address, which the DHCP server has assigned to the network device
- MAC address of the network device
- Timeout, remaining validity period in minutes
- Host name
- Type of address assignment, dynamic or from cache
- LAN-Ifc, logical interface over which the DHCP server assigned the IP address to the network device
- Ethernet port, physical interface over which the DHCP server assigned the IP address to the network device
- VLAN ID of the network
- Network name
- Assignment, date and time when the DHCP server assigned the IP address to the network device

You can find the status information for the DHCP server at the following locations:

› CLI: **Setup** > **DHCP** > **DHCP-Table**



› WEBconfig: **Setup** > **DHCP** > **DHCP-Table**



LCOS Menu Tree

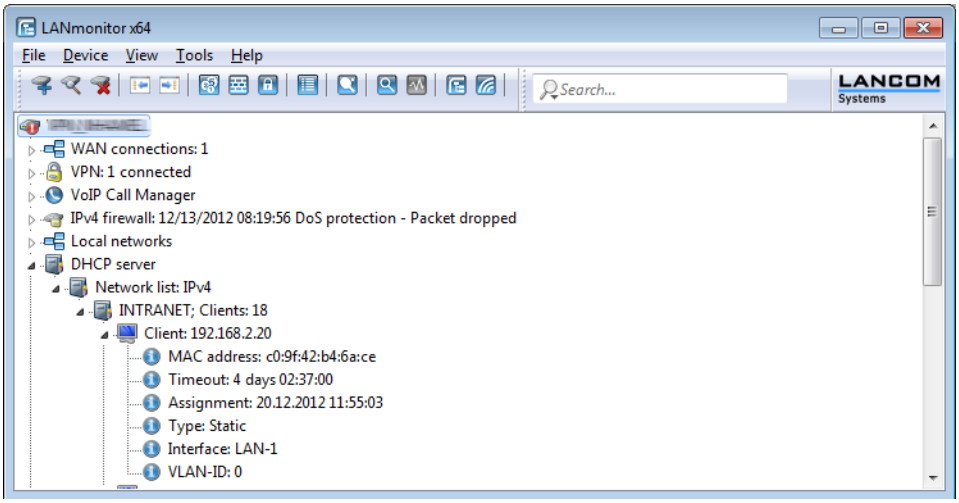
Setup

DHCP

DHCP-Table

IP-Address	MAC-Address	Timeout	Hostname	Type	LAN-Ifc	Ethernet-Port	VLAN-ID	Network-name	Assignment
192.168.2.20	848f69d12fad	269	bri-nb-11	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 13:23:16 tics
192.168.2.21	c09f42b46ace	5994		dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 14:01:44 tics
192.168.2.25	00225f06e075	87	BRI-NB-06	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 07:37:17 tics
192.168.2.39	e4115b0fec24	499		dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 14:07:15 tics
192.168.2.42	00a0571218bb	1	LCWLC-4025	cache	LAN-1	unknown	0	INTRANET	11/23/2012 14:07:01 tics
192.168.2.43	00a0571b32fc	1	LANCOM-00a0571b32fc	cache	LAN-1	unknown	0	INTRANET	11/23/2012 14:06:50 tics
192.168.2.48	00159976eab8	4158		unkn.	LAN-1	unknown	0	INTRANET	11/22/2012 07:26:11 tics
192.168.2.49	0001e3772ffd	393	C475IP-	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 12:20:41 tics
192.168.2.50	000c2903b9e0	393	bri-vm-service	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 12:21:09 tics
192.168.2.51	002170edc47f	258	E0060243	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 12:08:54 tics
192.168.2.53	74e2f50f5909	5755	iPad	dyn.	LAN-1	unknown	0	INTRANET	04/22/1900 21:33:20 tics
192.168.2.57	000c29f9e804	450	ubuntu	dyn.	LAN-1	unknown	0	INTRANET	11/23/2012 13:18:18 tics

› LANmonitor: Broken down by network name under **DHCP server** > **Network list**



20.1.7 DHCP cluster

If multiple DHCP servers are active in a network, the stations “divide” themselves equally between them. However, the DNS server in devices can only properly resolve the name of the station which was assigned the address information by the DHCP server. In order for the DNS server to be able to resolve the names of other DHCP servers, these can be operated in a cluster. In this operating mode, the DHCP server monitors all DHCP negotiations in the network. It additionally supplements its table with the stations which are registered at the other DHCP servers in the cluster.

Activate the setting for the DHCP cluster under **IPv4** > **DHCPv4** in the settings for the **DHCP networks**.

20.1.8 Alternative DHCP server for forwarding

The DHCP server offers various operating modes. In the forwarding mode, the device acts in the local network like a DHCP relay and forwards requests to one of more pre-defined DHCP servers. This setting facilitates the operation of central DHCP servers in another network.

All DHCP messages sent by DHCP clients as a broadcast are forwarded to all predefined DHCP servers. The client selects the first server to answer and sends all subsequent messages as unicasts directly to that server. If the selected server becomes unavailable, the client once again transmits broadcast messages and selects another DHCP server.

You configure the DHCP forwarding servers under **IPv4** > **DHCPv4** in the settings for the **DHCP networks**.

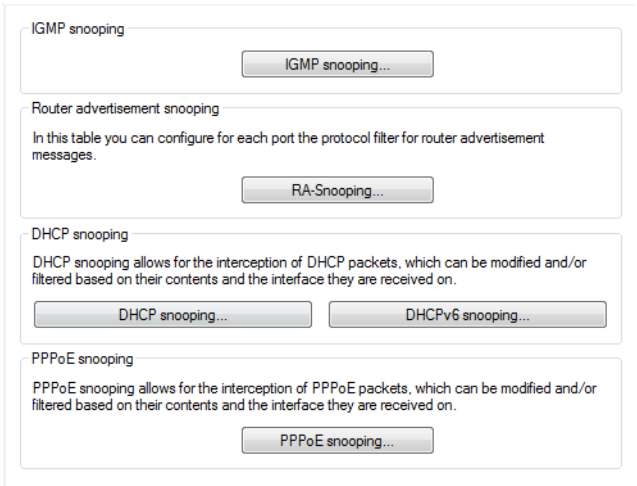
20.1.9 DHCP snooping and DHCP option 82

In its original form, DHCP has no safeguards to protect from attacks on the assignment of the network configuration. For example, if a client sends a 'DHCP discover' packet on the network in order to retrieve a valid network configuration from a DHCP server, an attacker can send the client fake 'DHCP offer' packets and trick it into using a false default gateway (DHCP spoofing).

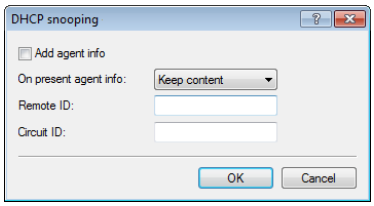
With DHCP snooping, the devices that receive and redirect DHCP packets are able to analyze and change these data packets, and to filter them by certain criteria. Additionally inserted information about the origin of the DHCP packets improves a DHCP server's capacity to manage extensive networks. Further, as this additional information is missing from the attacker's DHCP packets, they can no longer be used to interfere with the DHCP negotiations between DHCP servers, DHCP relay agents and the DHCP clients.

The access point supports DHCP snooping on layer 2. This enables it, for example, to add information (such as the SSID) to the DHCP packets received from the client on the WLAN before forwarding them to the LAN. The access point then adds the DHCP relay agent information option (option 82) according to RFC 3046.

In LANconfig you can set up DHCP snooping for each interface under **Interfaces** > **Snooping** and a click on **DHCP snooping**.



After selecting the appropriate interface, you can set the following:



Add DHCP agent info

Here you decide whether the DHCP relay agent appends incoming DHCP packets with the DHCP option "relay agent info" (option 82), or modifies an existing entry, before forwarding the request to a DHCP server.

The "relay agent info" is composed of values for the **Remote ID** and the **Circuit ID**.

On present agent info

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets. The following settings are possible:

- Keep content: In this setting, the DHCP relay agent forwards a DHCP packet and any existing "relay agent info" unchanged to the DHCP server.
- Replace content: In this setting, the DHCP relay agent replaces any existing "relay agent info" with the values specified in the fields **Remote ID** and **Circuit ID**.
- Drop packet: In this setting, the DHCP relay agent deletes any DHCP packet containing "relay agent info".

Remote ID

The remote ID is a sub-option of the "Relay agent info" option. It uniquely identifies the client making a DHCP request.

Circuit ID

The circuit ID is a sub-option of the "Relay agent info" option. It uniquely identifies the interface used by the client to make a DHCP request.

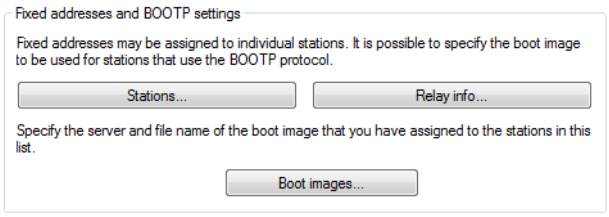
You can use the following variables for **Remote ID** and **Circuit ID**:

- `%%`: Inserts a percent sign.
- `%c`: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%i`: Inserts the name of the interface where the relay agent received the DHCP request.
- `%n`: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%r`: Inserts the interface-independent (i.e. valid throughout the system) MAC address of the device that received the DHCP request.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

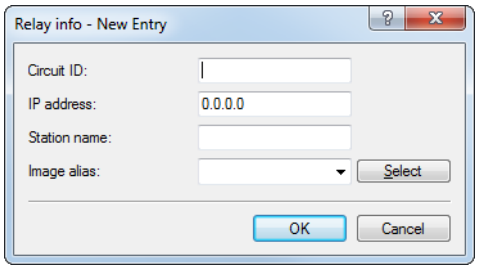
20.1.10 Assigning IP addresses based on DHCP option 82

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. The switch in question uses DHCP option 82 to supplement the DHCP request with the Circuit ID, which identifies the port that this device is connected to. This information is then used by the DHCP server to assign a specific IP address. This establishes a relationship between an IP address and a location, which simplifies network monitoring.

In LANconfig under **IPv4** > **BOOTP**, you can set the switch-port based assignment of IP addresses for each port separately by clicking on **Relay info**.



After selecting the switch port that is automatically added by the DHCP option 82, you can set the following:



Circuit-ID

This is the storage location for the "Circuit ID" used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the "Circuit ID" is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires "negative" bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8}{2/8}{30/16}MES-3728
- {0x00/8}{0x02/8}{0x1e/16}MES-3728
- {00/8}{02/8}{036/16}MES-3728

IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

Station name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Image alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

20.1.11 Delivering LANCOM Management Cloud parameters with the DHCP server

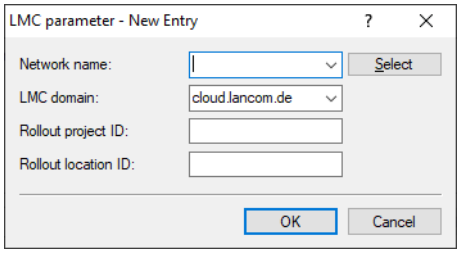
The DHCP server enriches its DHCP packets with the DHCP option 43 (vendor specific option) to distribute this information to requesting clients on the network. This includes the domain name, which is required for the device to operate with the LANCOM Management Cloud (LMC). In this way, a LANCOM device is able to communicate directly with a private LMC installation without having to be configured first.

If you operate a LCOS as a DHCP server, you enter the necessary LMC URLs into the configuration in cleartext. The DHCP server in LCOS adds the URLs to the DHCP option 43 and delivers them in the response packets sent to requesting LCOS devices. To do this, the DHCP server evaluates DHCP option 60 (vendor class identifier) in the DHCP requests from the clients. A DHCP option 43 configured in this way takes precedence over a DHCP option 43 that was manually configured in the DHCP options table on the DHCP server.

The vendor class identifier in the request must contain `LANCOM`. If a device from a different manufacturer sends a request to the LCOS-internal DHCP server, the response packet does not offer DHCP option 43.

20.1.11.1 Configuration

In LANconfig, the LMC domain for the individual networks is configured under **IPv4** > **DHCPv4** > **LMC parameter**.



Network name

Here you specify the network to which the device delivers the LMC domain via DHCP option 43.

LMC domain

Enter the domain name for the LANCOM Management Cloud here.

By default, the domain is set to the public LMC for the first connection. If you wish to manage your device with your own Management Cloud (private cloud or on-premises installation), please enter your LMC domain.

20.2 Domain Name Service (DNS)

The Domain Name Service (DNS) links the computer names or network names (domains) with the IP addresses in TCP/IP networks. This service is vital for communication on the Internet. But within a local network or for LAN connectivity, too, it is useful to uniquely assign the IP addresses in the LAN to the names of the computers.

20.2.1 What does a DNS server do?

Each name requested from a DNS server consists of different parts: One part consists of the actual name of the host or service to be reached, another part identifies the domain. Within a local network, specifying the domain is optional. Examples of these names would be “www.domain.com” or “ftp.domain.com”.

Without a DNS server in the local network, every name that is not known locally would be searched for on the default route. By using a DNS server, any name that has a known IP address can be found directly at the correct peer. In principle, the DNS server can be a separate computer in the network. However, the DNS server is best located directly in the device for the following reasons:

- When operated as a DHCP server, the device can independently distribute the IP addresses for the computers in the local network. The DHCP server is therefore already familiar with all of the computers on its own network by their computer name and IP address. An external DNS server might have difficulties keeping the relationships between IP address and name up to date in case of dynamic address assignment by the DHCP server.
- The DNS server in the device can also be used as a convenient filter mechanism. Requests for undesirable domains can be blocked for the entire LAN, for certain subnets only, or even for individual computers, simply by specifying the domain name.

20.2.1.1 How does the DNS server react to a request?

When searching for a specific name, the DNS server searches using all of the information available to it:

- First the DNS server checks whether access to this name is prohibited by the filter list. If so, an error message informs the requesting computer that it is not permitted access to this name.
- The server then searches its own static DNS table for entries with the corresponding name.
- If the DNS table has no entry for this name, the dynamic DHCP table is searched. Use of the DHCP information can be disabled if necessary.
- Finally, the DNS server checks whether the request should be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

If the name is still not found after searching all of the available information, the DNS server forwards the request to a further DNS server (e.g. at the Internet provider) using the general DNS forwarding mechanism. Otherwise it will send an error message to the requesting computer.

20.2.2 DNS forwarding

If a request cannot be answered using the DNS tables, the DNS server forwards the request to further DNS servers. This process is called DNS forwarding.

A distinction is made between

- Special DNS forwarding

  Requests for specific name spaces are forwarded to specific DNS servers.

- General DNS forwarding

  All other unspecified names are forwarded to the “higher-level” DNS server.

20.2.2.1 Special DNS forwarding

With special DNS forwarding, name zones can be defined that use specific DNS servers to resolve them.

A typical use case for special DNS forwarding is the home office: The user would like to be able to directly access the company's intranet and the Internet at the same time. The requests sent into the intranet must be routed to the company DNS server, and all other requests to the DNS server of the provider.

20.2.2.2 General DNS forwarding

DNS queries that cannot be resolved in any other way are forwarded to a general DNS server. These can be configured in the following menus or command-line paths:

LANconfig	**IPv4** > **Addresses** > **Name server addresses** > **Primary DNS** | **Secondary DNS**
CLI	**Setup** > **TCP-IP** > **DNS-Default**
	Setup > **TCP-IP** > **DNS-Backup**

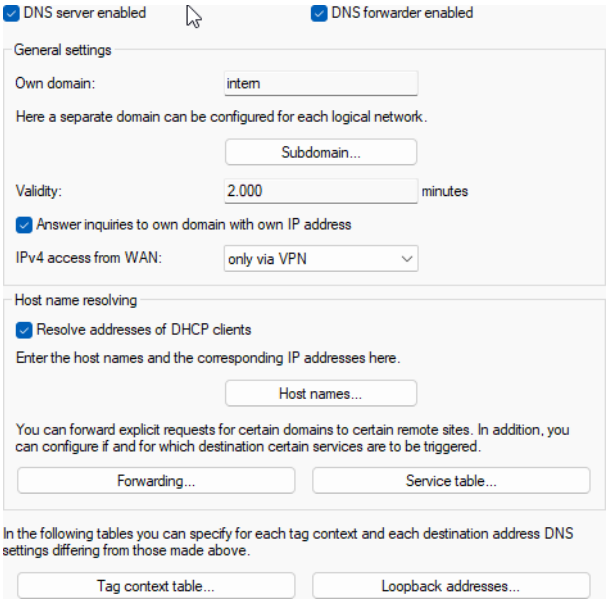
If a DNS server is specified here, it must be entered as the **primary DNS**. Optionally, an additional DNS server can be specified as the **secondary DNS** for redundancy.

- For DNS forwarding, a DNS server that has been assigned to the Internet connection (manually or automatically) is always used first.
- If no DNS server has been assigned to the Internet connection or none of the assigned DNS servers respond, the system falls back to the general DNS server.

With this procedure, you do not need to know the addresses of a DNS server. All you need to do to enable name assignment is to set up each workstation computer with the intranet address of your router as the DNS server. This also automatically updates the DNS server address. For example, should the provider with this address rename their DNS server, or if you switch to another provider, your local network will always receive up-to-date information.

20.2.3 Setting up the DNS server

The settings for the DNS server can be found in LANconfig under **DNS** > **General**.



1. Enable the DNS server by checking the **DNS server enabled** option.

   If the DNS server is to forward the DNS request to another DNS server (DNS forwarding), additionally check the **DNS forwarder enabled** option.

2. Enter your own domain where the DNS server is located.

   With the help of this domain, the DNS server recognizes during DNS queries whether the name searched for is located in its own LAN or not. Specifying the domain is optional.

3. Specify whether the DNS server should use the client information from the DHCP server.

4. Under **IPv4 access from WAN**, specify whether access from WAN interfaces to the DNS server or DNS forwarder via IPv4 is generally allowed. Access to these services via IPv6 is controlled exclusively through the IPv6 inbound firewall.

   Access can be controlled globally for the corresponding interface types using this switch. For more granular control than this level, corresponding IPv4 firewall rules can be configured.

   Access to the DNS service must be allowed via VPN if VPN clients are to use the router as a DNS server or DNS forwarder, for example, to resolve locally configured station names.

   Access to the DNS service via WAN must be allowed if clients are to connect to the router using PPPoE, L2TP, or PPTP. In this case, it is recommended to configure granular control for the local DNS service via firewall rules.

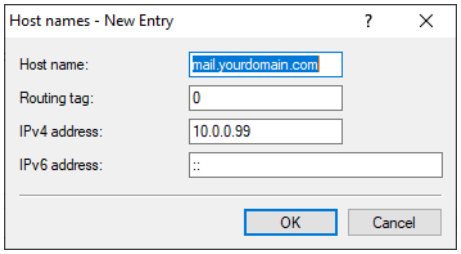
   VPN interfaces include IPSec VPN (IKEv1/IKEv2) and WireGuard. WAN interfaces include all WAN counterparts such as Internet connections and RAS dial-ins to the LANCOM router acting as a PPPoE, PPTP, or L2TP server.

5. Enter known remote stations and their IP addresses in the **Host names** table.

   The main purpose of the DNS server is to separate requests for public addresses on the Internet from requests for addresses at other remote sites. Therefore, enter all computers in the table

   - whose name and IP address you know,
   - which are not located in your own LAN,
   - that are not on the Internet and
   - that are accessible via the router.

   For example, if you're working in an external office or in a branch office and the employees want to reach the mail server in the head office (name: "mail.yourdomain.com", IP: "10.0.0.99") via the router, enter:



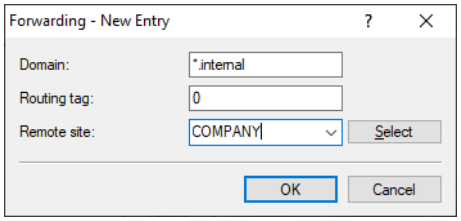
   Specifying the domain is optional, but recommended.

   When an employee now starts his mail program, it automatically searches for the server "mail.yourdomain.com". The DNS server then returns the IP address "10.0.0.99". The mail program then starts a connection to this IP address. With corresponding entries in the IP routing table and remote peer list of the router, the mail program establishes the connection to the mail server in the network of the central office.

6. To have entire name ranges resolved by a different DNS server, add a forwarding record consisting of the name range and remote site.

   When specifying the name ranges, you may use the wildcards "?" for single characters and "*" for multiple characters.

   To redirect all domains ending with ".internal" to a DNS server on the remote "COMPANY" LAN, create the following entry:



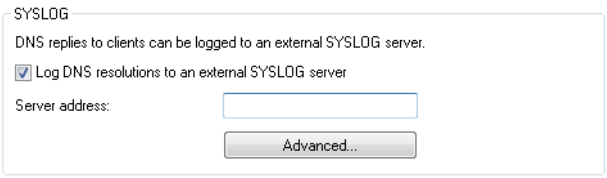
The DNS server can be specified either by the name of the remote station (for automatic configuration via PPP) or the explicit IP address of the responsible name server.

20.2.4 Logging DNS queries with SYSLOG

In order to document the requests from the clients to the DNS server in the device, this option allows the server to additionally send its responses to clients as SYSLOG messages to a SYSLOG server on a continual basis.

Please be aware that recording DNS requests must be performed in accordance with the applicable data privacy regulations in your country.

In LANconfig, you configure the documentation of DNS requests under **DNS** > **Filter/Aliases/SYSLOG** in the section **SYSLOG**.



Log the DNS resolutions on an external SYSLOG server

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under **Log & Trace** > **General** > **SYSLOG**. Thus, if you enable this option to log DNS requests, the DNS server sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (`ANSWER` record or `ADDITIONAL` record) generates a SYSLOG message with the following structure `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record`.

The parameters have the following meanings:

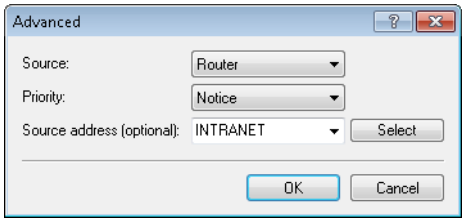
- The `TID` (transaction ID) contains a 4-character hexadecimal code.
- The `{host name}` is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The `resource record` consists of three parts: The request, the type or class, and the IP resolution (for example `www.mydomain.com STD A resolved to 193.99.144.32`)

Server address

Enter the address of the SYSLOG server. You can enter an IPv4/IPv6 address or a DNS name.

The use of the IP addresses `127.0.0.1` and `::1` to force the use of an external server is not permitted.

To configure the SYSLOG message, click on **Advanced**.



Source

Here you select which source is entered in the SYSLOG messages.

Priority

Here you select the source that is entered in the SYSLOG messages.

Source address (optional)

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

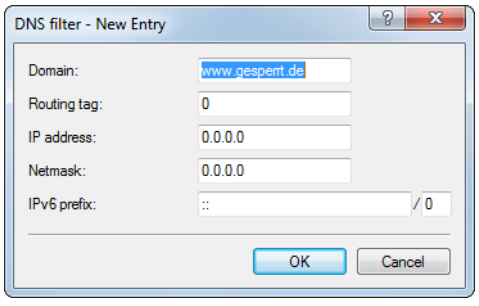
For more information on SYSLOG and the available settings, see the section *The SYSLOG module*.

20.2.5 URL blocking

1. The filter list allows you to block access to specific names or domains.

   Blocking the domain “www.blocked.com” for all computers on the LAN requires the following commands and inputs:

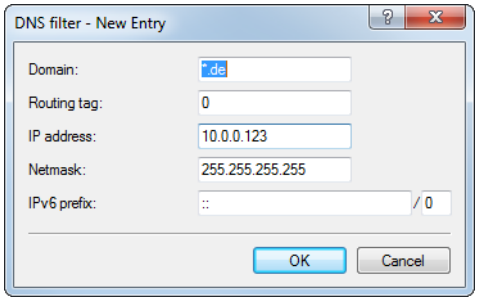
LANconfig	**DNS** > **Filter/Aliases** > **DNS filters** > **Add**
CLI	`cd Setup/DNS/Filter-List set 001 www.blocked.com 0.0.0.0 0.0.0.0`



   The index “001” can be freely selected when carrying out the configuration via CLI and serves only to uniquely identify the entry.

   Entering domains can also be done with the help of the wildcards '?' (which stands for exactly one character) and '*' (for any number of characters).

In order to block a particular computer (e.g. with IP 10.0.0.123) from accessing COM domains, enter the following values:



In CLI mode, the command is:

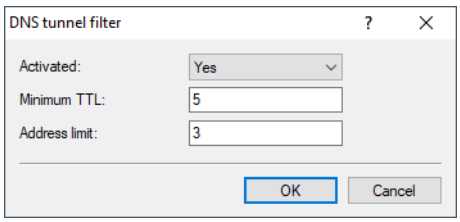
```
set 002 *.com 10.0.0.123 255.255.255.255
```

The hit list in the DNS statistics shows you the 64 most requested names, which gives you useful information for setting the filter list.

The appropriate choice of IP addresses and netmasks can also be used to filter individual departments when using subnetting in your LAN. The IP address “0.0.0.0” stands for all computers in a network, the netmask “0.0.0.0” for all networks.

20.2.6 DNS filter for DNS data tunnels

Methods and tools exist that use DNS packets to smuggle in data and avoid checks, for example by the firewall. This data tunnel can then be used to transport any data via the DNS protocol. Although this method conforms to the protocol’s standards, the establishment of these tunnels should be prevented under certain circumstances. The data tunnels are detected according to certain characteristics or properties of the DNS packets.



LANconfig: **DNS** > **Filter/Aliases** > **DNS tunnel filter**

Command prompt: **Setup** > **DNS** > **Tunnel-Filter**

Activated

The tunnel filter can be switched on and off with this switch.

Minimum TTL

Minimum TTL after which resource records are accepted. If a record (with the exception of A and AAAA) has a smaller TTL, the entire packet is discarded.

Area: 0-99; Default: 5

Address limit

Maximum number of A and AAAA records with a TTL smaller than the minimum TTL that are still accepted before the complete packet is discarded.

Area: 0-99; Default: 3

20.2.7 Dynamic DNS

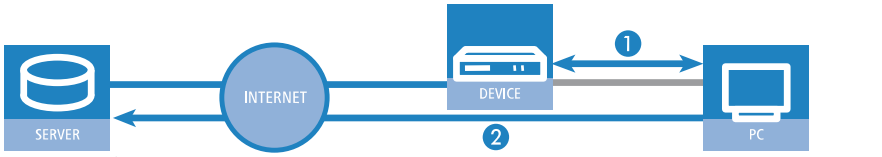
Systems with dynamic IP addresses can be made available for access via the WAN, for example via the Internet, by using the services of commercially available dynamic DNS servers (such as www.dynDNS.org) or the LANCOM Management Cloud service.

Consequently, a device can always be reached under a specific name (FQDN - Fully Qualified Domain Name) (e.g. "http://MyDevice.dynDNS.org").

The advantage is obvious: For example, if you want to use a VPN client to access a branch office with a dynamic IP address, you only need to know the dynamic DNS name.

20.2.7.1 How to deposit the current IP address at the Dynamic DNS server?

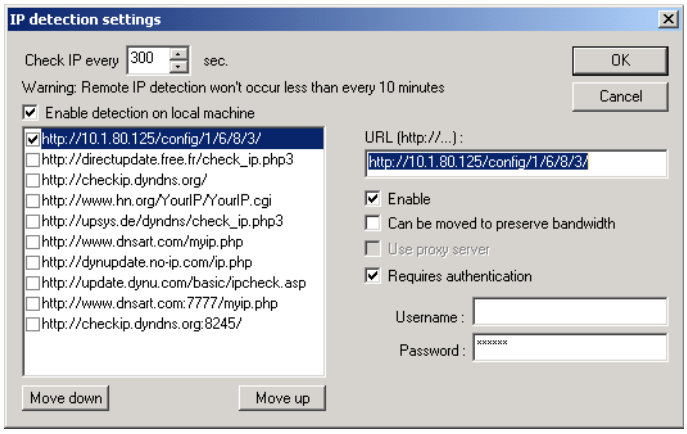
All Dynamic DNS provider support a set of client programs, which can determine the current assigned WAN IP address of a device via different methods **1**, and transfer this address—in case of a change—to their respective Dynamic DNS server **2**.



DynDNS provider DynDNS client program

The current WAN IP address of a device can be picked under the following address:

```
http://<address of device>/config/1/6/8/3/
```



Alternatively the device can directly transmit the present WAN IP to the DynDNS provider.



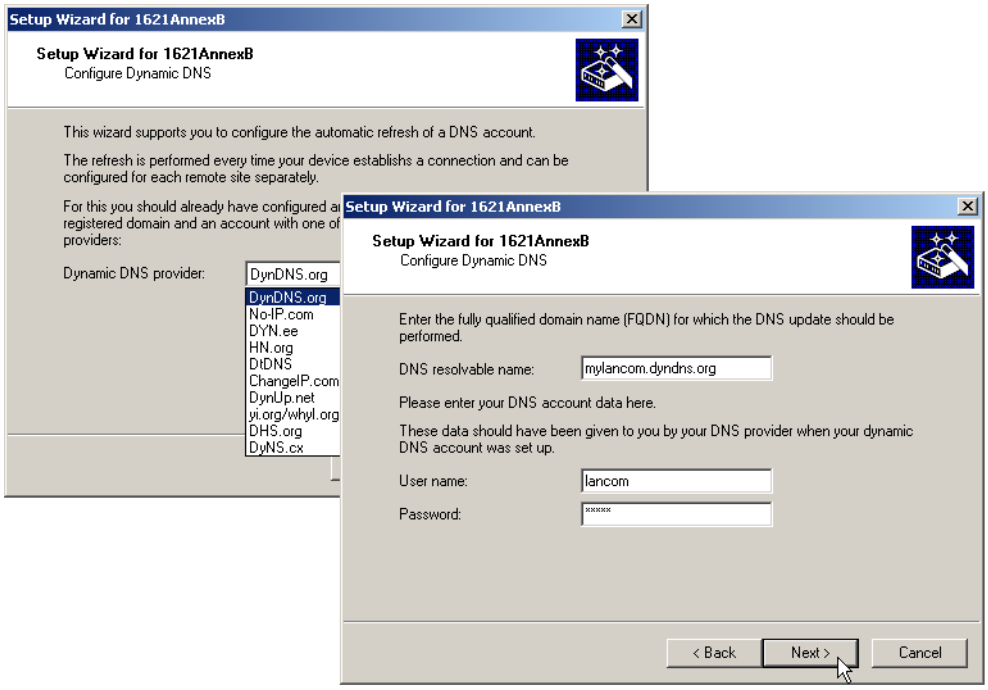
DynDNS provider

For this purpose, an action is defined that, for example, automatically sends an HTTP request to the DynDNS server after each connection establishment, thereby transmitting the required information about the DynDNS account and thus triggering an update of the registry. Such an HTTP request to the provider DynDNS.org looks like this, for example:

› http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a

This will send the hostname of the action and the current IP address of the device to the account at DynDNS.org specified by Username and Password, the corresponding entry will be updated.

The required settings can be changed comfortably with the Setup Wizard:



The Setup Wizard adds further vendor-specific parameters to the basic action described, which are not described in detail here. In addition, the setup wizard creates further actions to control the behavior of the device in case the update could not be performed successfully in the first run.

20.3 Accounting

Information on connections between clients in the local network and various remote sites is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

Along with IPv4, IPv6 is of course also supported. There is also a function for displaying the current data throughput of individual stations or logical interfaces in the network. This function is particularly suitable for analyzing which station on the network is currently causing which data traffic. For example, this allows stations that are using the Internet connection to be identified, or to see how much traffic is running via which interface at the current time.

For performance reasons, it is recommended to only activate this function while the analysis is running and to deactivate it again afterwards. For more extensive traffic monitoring, Netflow is recommended in conjunction with an external collector.

To use the analysis function, use the command line and set the “Operating” item under /setup/accounting to “Yes”.Set the “Intermittent-Reporting-Interval” to a small value in seconds, e.g. 5 seconds.

To deactivate the function again after the analysis, set the “Active” switch to “No”.

To display the current throughput per user, use the command “show accounting users”

```
show accounting users

Username   Interface      Rx-Total     Tx-Total      Rx-IPv4      Tx-IPv4  Rx-IPv6  Tx-IPv6
=============================================================================================
192.168.1.7 INTERNET       0 Bit/s    115 Bit/s      0 Bit/s    115 Bit/s  0 Bit/s  0 Bit/s
192.168.1.9 INTERNET   9.38 KBit/s  3.92 KBit/s  9.38 KBit/s  3.92 KBit/s  0 Bit/s  0 Bit/s
```

```
Next update of accounting bandwidth data in: 3s
```

As an alternative to the show command, the status table /Status/Accounting/User-Bandwidth-Usage can also be accessed.

The show command has a number of options that can be displayed by entering ?:

```
> show accounting ?
Displays short-term bandwidth usage statistics based on accounting.
NOTE: Accounting must be enabled and the Intermittent-Reporting-Interval must be set. All bandwidth data is
updated according to that interval.
USAGE:
show accounting-bandwidth <COMMAND> [FLAGS]:

COMMANDS:
  interfaces:              Displays accounted bandwidth usage per interface
  users:                   Displays accounted bandwidth usage per user per interface

FLAGS:
  -bps:                    Displays all data as bps without decimals
  -kbps:                   Displays all data as kbps with 3 fixed decimal places
  -mbps:                   Displays all data as mbps with 3 fixed decimal places
  -gbps:                   Displays all data as gbps with 3 fixed decimal places
        NOTE: You can only choose one of the unit display flags. If none is given, the correct output unit is
 automatically determined. All numbers are given with 3 significant digits.
  -compact:                Reduces output to bandwidth usage totals per traffic direction
  -totals-only:             (Only for command 'users') Does not show bandwith usage per interface, but as a
total value
```

Examples:

“show accounting interfaces” shows the load or current data throughput of the interfaces. This information can also be found in the /Status/Accounting/Interface-Bandwidth-Usage table

With the command “repeat 5 show accounting users” on the CLI you can have the command displayed automatically every 5 seconds.

20.3.1 Operating principles

Accounting users are identified by their user name. Potential accounting users are:

- All stations on the LAN (user name is their IPv4 or IPv6 address, or if known to the router via DNS, the station's hostname)
- All VPN peers (user name is the peer name)
- All dialed-in RAS clients (user name is the RAS client ID; multiple dial-ins are mapped to the same ID)

The data traffic counted by accounting is any data traffic that takes place between a user and an IP address behind one of the following interface types (regardless of whether Rx or Tx traffic):

- WAN
- RAS
- VPN

When connecting VPN to VPN, for example, the traffic is counted and booked separately for both VPN users.

The accounting records the data traffic with each remote site separately for each user. What this means is: Traffic, for example, from VPN to WAN1 and traffic from VPN to WAN2 are separate records.

From the user's point of view, the accounting records incoming and outgoing data as well as IPv4 and IPv6 traffic separately. This means that an IPv6 data packet from VPN1 to VPN2 is counted as IPv6-Tx for VPN1, and as IPv6-Rx for VPN2.

Also, the accounting records the number of data streams (sessions) that have occurred, but not separately according to Rx and Tx.

Bidirectional traffic is counted as 2 sessions because there are 2 streams. One incoming and one outgoing data stream from the user's point of view.

20.3.2 Switching accounting on or off on the fly

The check as to whether a data connection is reported by accounting takes place when the connection is established (first data packet). Data connections that already exist when accounting is switched on are not considered by accounting.

If accounting is switched off during operation, the data connections that are currently running are no longer included in the accounting data.

20.3.3 Data traffic counting

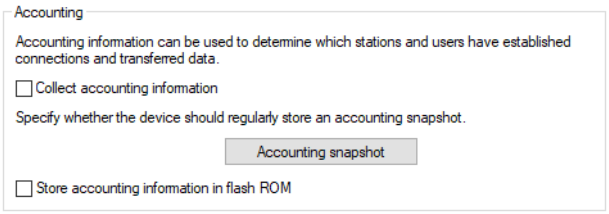
In the default setting, traffic is always reported to accounting when a data connection (in the form of a firewall session) ends, for example after a timeout within the firewall or when a TCP connection is closed. In the case of long-running connections, this can lead to a considerable delay before data traffic actually appears in the accounting status tables. To handle this problem, accounting has an "intermittent reporting" function, which enters partial recordings at fixed intervals in the accounting. How often this happens is configured via the intermittent reporting interval. By default this is set to 0; i.e. the feature is disabled. If a value between 1 and 30 is entered there, this setting defines the interval in seconds at which intermediate data-connection reports are received by accounting.

The intermediate reports increase the system load depending on the number of active data connections. The intermediate reports of the data connections are carried out independently of each other (i.e. not all at once) in order to avoid peak loads.

Intermittent reporting can be switched on at any time while accounting is running. The first intermittent report then contains the complete data traffic of the individual data flows measured up to the time when enabled.

20.3.4 Configuring accounting

When configuring accounting, the general parameters must be defined:



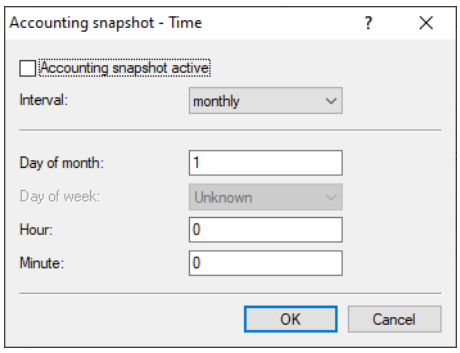
Configuration tool	Request
LANconfig	**Management** > **Costs**
CLI	**Setup** > **Accounting**

Collect accounting information

Turn accounting on or off.

Accounting snapshot

Configuring the snapshot sets the interval at which the accounting data are temporarily stored:



Accounting snapshot active

Turn intermediate storage of accounting data on or off.

The snapshot function can only be used when the device is set with the correct system time.

Interval

Daily, weekly or monthly.

Day of month

The day of the month on which caching is performed. Only relevant if the interval is **monthly**.

Day of week

The weekday on which caching is performed. Only relevant if the interval is **weekly**.

Hour

The hour on which caching will take place: 0 to 23

Minute

The minute in which caching will take place: 0 to 59

Store accounting information in flash ROM

Turn accounting data in flash memory on or off. Accounting data saved to flash will not be lost in the event of a power outage.

20.4 Call charge management

The capability of the router to automatically establish connections to all desired remote sites and to close them again when no longer required provides users with extremely convenient access, e.g. to the Internet. However, quite substantial costs may be incurred by data transfer over paid lines if the router is not configured properly (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

To reduce these costs, LCOS provides various options:

› The available online minutes can be restricted to a specific period.

20.4.1 Connection limits for DSL and cable modem

Even though a DSL or cable modem connection behaves like a leased line, which is always online, depending on the provider connection charges can be accounted by the time.

In this section all connections over a ethernet WAN port of the device, e.g. cable modem connection, will be referred as DSL connection.

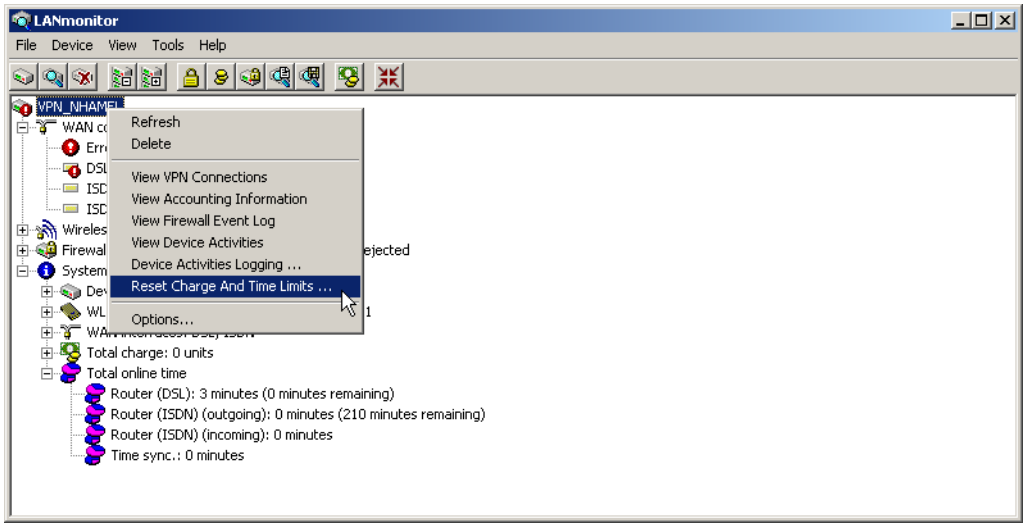
To limit the costs, the maximal connection duration can be controlled with time, by arranging a time limit for DSL connections for a period of time. By default the DSL connections can only be used for a maximum of 600 minutes in six days.

If the limit is reached, all DSL connections are automatically terminated. As soon as the current period has passed the time count is reset and the connection enabled. The administrator can of course reset the time count and enable the connection beforehand.

If the connection has a charge limit and a short hold of "0" or "9999" seconds, the charge control is switched off and the connection is kept even if the limit is exceeded.

If in an exceptional case you would like to extend the online budget, e.g. to download a large file from the internet, you do not necessarily have to change the time limit. In this case you can manually reset the limit.

Click with the right mouse button on the error in LANmonitor and select in the menu the entry **Reset Charge And Time Limit**.



If you cannot see the system information in LANmonitor, activate the view with **View** > **Show Details** > **System Information**.

In WEBconfig and in the console the commands to activate the additional time limit are as follows:

Configuration tool	Call
WEBconfig	**LCOS menu tree** > **Setup** > **Charges** > **Activate-additional-budget**

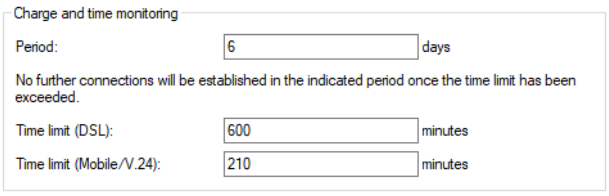
CLI	`cd /Setup/Charges`
	
	`do Activate-additional-budget`

The additional time limit is activated for the current period, in the following period normal time limit is set.

20.4.2 Settings in the charge module

In the charges module, the online time can be monitored and used to control call establishment.

Configuration tool	Path
LANconfig	**Management** > **Costs**
CLI	**Setup** > **Charges**



Period

The duration of the monitoring period in days can be specified here.

Online minutes budget

The maximum number of online minutes in a monitoring period.

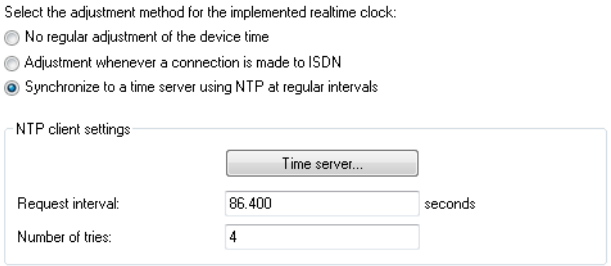
The current charge and connect-time information is retained when rebooting (e.g. when installing new firmware) is not lost until the unit is switched off. All the time references here are in minutes.

20.5 Time server for the local net

Routers can get exact information of time either over ISDN or over public time servers on the internet (NTP-Server with "Open Access" policy). The device makes the time determined in this way available to all stations in the local network.

20.5.1 Configuring the time server under LANconfig

In order for a device to broadcast the current time on the network, go to **Date & Time** > **Synchronization** and enable the regular synchronization with a time server.



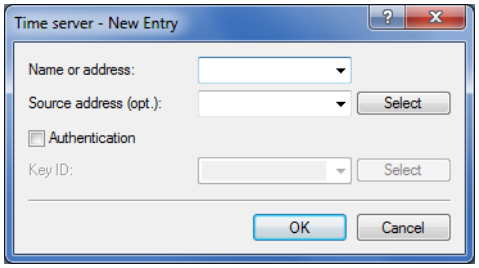
Request interval

Specify the time interval in seconds after which the internal clock of the device is re-synchronized with the specified time server (NTP).

Number of tries

Enter the number of times that the device should try to synchronize with the time server. By setting this value to zero, the device attempts to connect until it achieves a valid synchronization.

Then go to the section **NTP settings** and, under **Time server**, configure the settings for synchronizing the time with the server.



Name or address

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.

If you specify more than one time server in the list, you set the order in which they are queried in the overview of entries.

Source address (optional)

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

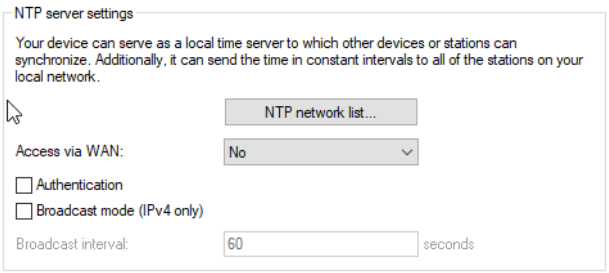
Authentication

Enables or disables MD5 authentication by the client.

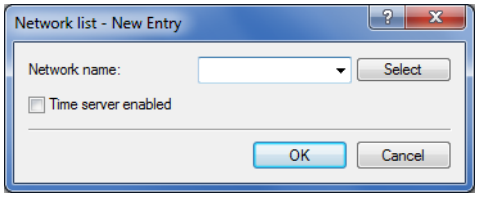
Key ID

Identifies the key that the client uses for MD5 authentication.

With these settings, the device initially retrieves the time from the public time servers for its own use only. To broadcast the current time to other devices in the LAN, go to **Date & Time** > **Synchronization** and, in the section **NTP server settings**, enable the time server on the device.



You configure the list of networks to which your device forwards the current time under **NTP network list**.



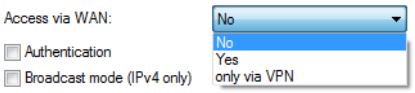
Netzwork name

Defines the name of the network.

Time server enabled

Enable this option if the device is to work as a time server on the network.

You configure access from the WAN via the selection list **Access via WAN**.



Possible options are:

No

Access from the WAN to the NTP server is disabled.

Yes

Access from the WAN to the NTP server is possible via unmasked connections, but generally not possible with masked WAN connections.

only via VPN

Access via VPN to the NTP server is enabled.

Activate support for MD5 authentication under **Authentication**.

Broadcast mode (IPv4 only)

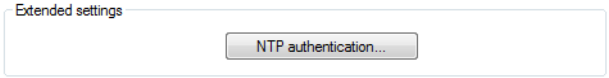
If the device should regularly operate as a time server and send the current time to all stations in the network, enable the "send mode" here.

The send mode of the device only supports IPv4 addresses.

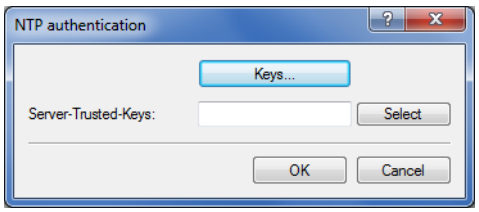
Broadcast interval

Specify the time interval in seconds after which the time server broadcasts the current time to the accessible stations on the network.

You configure the list of trusted keys in the section **Extended settings**

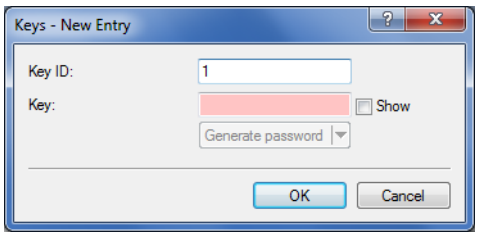


under **NTP authentication**.



The available keys are located in the list **Server-Trusted-Keys** and are selected via **Select**.

Edit or add a key via **Keys**.

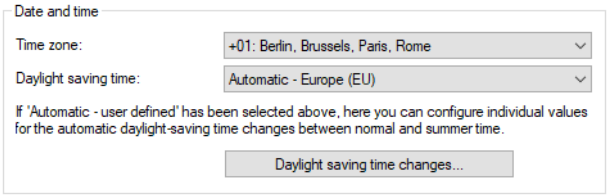


20.5.2 Configuring the NTP client

NTP clients have to be configured to use the time information from the device. Not all operating systems have an integrated NTP client: with Linux distributions, NTP has to be installed.

The **Date and time settings** in a Windows system are accessed by double-clicking on the clock at the bottom right of the screen. The settings allow a server for time synchronization to be selected, if one has not already been specified in a group policy.

The device works internally with the coordinated universal time (UTC). For protocol displays and time-related settings (e.g. cron jobs), the local time is taken as calculated from the defined time zone. To take local daylight-saving time into account, settings can be configured according to requirements.



LANconfig: **Date/time** > **General**

Daylight-saving time

Off

The system time will not be adjusted to daylight-saving time.

On

As long as this option is enabled, one hour is added statically to the current system time (comprised of UTC and time zone).

Automatic – Europa (EU)

In this setting, the daylight-saving time change is performed automatically in conformance with the time zone of the device's location.

Automatic – USA

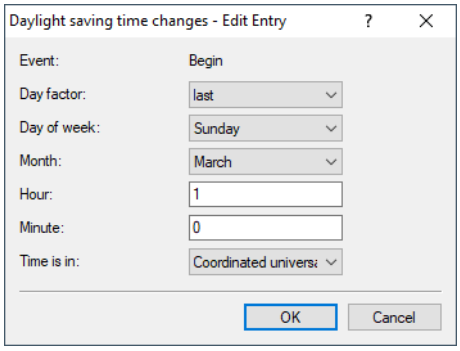
In this setting, the daylight-saving time change is performed automatically in conformance with the time zone of the device's location.

Automatic – user-defined

If the device is located in an area that is not listed here, then the daylight-saving time change options can be manually defined by the user.

20.5.2.1 User-defined daylight-saving time change

User-defined values can be set for the beginning and the end of the automatic daylight-saving time change.



LANconfig: **Date & time** > **General** > **Daylight-saving time**

Day factor

First, second, third, fourth, last, second to last, third to last, fourth to last: The time change will take place on this recurring day of the month.

Day of week

Monday to Sunday: The day on which the change will take place.

Month

January to December: The month on which the change will take place.

Hour

0 to 23: The hour in which the change will take place.

Minute

0 to 59: The minute in which the change will take place.

Time is in

Local standard time or UTC: Defines the time zone the data refers to.

In the last hour of daylight-saving time or the first hour that follows in standard time, it is possible for time entries to be ambiguous. If the time is acquired via ISDN or set manually during this time, then it is always assumed that the time entry is in daylight-saving time.

20.5.3 Retrieving Device Time via GPS

You can automatically retrieve the device time via GPS as an alternative to an NTP server. The prerequisites for retrieving the device time via GPS are:

› The operating mode of the cellular modem is set to WWAN

- The GPS module is enabled
- The retrieval method for the device time is set to GPS

You can find the current GPS time in LANmonitor (*Displaying GPS Time*) or in the device's status section.

This function is only available on devices with an internal WWAN module. Please check the technical specifications of your model to determine whether your device supports this function.

The time is only available once the device has successfully obtained a "GPS fix". This requires receiving signals from at least 4 satellites with sufficient quality.

The time received via GPS may differ by a few seconds from the actual time due to propagation delays.

20.6 Scheduled Events

20.6.1 Regular Execution of LCOS-Commands

This feature is intended to allow the device to execute predefined commands, at times defined by the user. The functionality is equivalent to the UNIX cron service. Subject of execution can be **any** command line command. Therefore, the full feature set of all devices can be controlled by this facility.

Application examples:

- scheduled connection

  Many leased lines disconnect automatically after 24 hours of continuous operation. This enforced disconnection can have some unwanted side-effects for example if it happens to an unsuitable time during the day, because e.g. the VPN tunnel is disconnected and the IP address of the device is changed. To control the disconnecting time a manual disconnection can be set e.g. at midnight, so it can not happen at an unsuitable time.

  As a second example devices with a distributed network with only dynamic IP addresses can build up a connection at a certain time to a VPN gateway, so that data can be transferred safely. This way a protected access is even possible without an ISDN connection.

- time-dependant firewall or QoS rules

  The firewall and QoS rules are at first temporally constant. But it can be useful to make variable settings for different daytimes or weekdays. At e.g. off-hours or weekends different priorities for guaranteed bandwidths can be set than at business hours.

- regular firmware or configuration updates

  Time-controlled rules do not only provide the settings of particular values, it is even possible to switch to a whole different configuration. This possibility allows you to pool a whole string of settings and change them all at once with one command. Therefore changing the configuration of the device with completely different values at the weekend and switching back on monday mornings can be done with just one command.

  Additionally the regular update of the newest firmware from one single source is adjustable.

- Email messages

  With the time-controlled rules you have the option that the device informs the administrator by email not only about specific firewall events, but even to set times. The email can e.g. inform about building up an internet connection successfully after an enforced disconnection or after booting the device because of a restart.

- time-dependant interfaces

  The time dependant use of interfaces for a set duration is also provided by the time-controlled rules. Therewith e.g. a WLAN interface can permit the wireless access to the network only at certain times.

› Deleting certain tables

It can be useful to delete the content of some tables in LCOS regularly. If your internet access for example has a monthly limited transfer volume, you can delete your accounting table monthly to have a survey of the present transferred data volume.

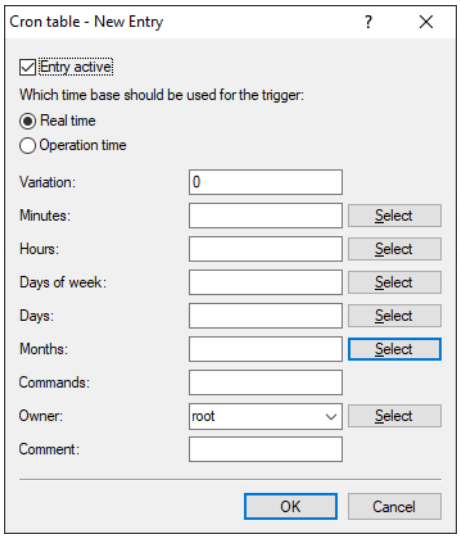
20.6.2 CRON jobs with time delay

CRON jobs are used to carry out recurring tasks on a LANCOM automatically at certain times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result if, for example, all devices try to establish a VPN connection at once. To avoid these effects, the CRON jobs can be set with a random delay time between 0 and 59 minutes.

20.6.3 Configuring the scheduler

This tutorial demonstrates how to create a new CRON job and details the available parameters.

1. Open the configuration for your device in LANconfig.
2. Navigate to the **Cron table** in the dialog **Date & Time** > **General** and click **Add** to create a new CRON job.



3. Specify a time basis.
   The time basis determines whether LCOS executes the scheduled action based on the real-time clock or the device's runtime. In the **Real time** setting, the system evaluates all time and date inputs. In the **Operation time** setting, the system only evaluates the minute and hour values since the last device restart.
4. Enter a delay under **Variation** in minutes to set the maximum delay of a CRON job execution relative to the defined start time.
   The actual delay is determined randomly by the device, between zero and the entered time. If the variation is set to zero, the CRON job is executed exactly at the specified time.

   Real-time-based rules can only be executed if your device has a valid time reference, such as via NTP.

5. Specify the minute(s), hour(s), day(s) of the week, day(s) of the month, and month(s) when your device should execute the specified command.

   If no value is entered, the device will not consider that time parameter in its scheduling. For each parameter, you can optionally enter a comma-separated list of values or a range (formatted as `<day>-<day>`, e.g., 1-5). A step value can be defined using /. If a range precedes the step value, it applies to the defined range.

   The syntax of the **Weekdays** field corresponds to the standard CRON interpretation:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0	1	2	3	4	5	6

The weekday field is also relevant for operation-time-based rules. This is useful for actions you want to execute only once at device start (i.e., at zero days of runtime). For example, this allows you to align the weekday against the days of operation time.

6. Enter the command(s) to execute under **Commands**.
   Any command-line function can be executed.
7. Specify the **Owner** of the CRON job.
   An administrator defined on the device can be selected as the owner. If an owner is specified, the CRON job commands are executed with the owner's permissions.
8. Enter a brief description of the CRON job in the **Comment** field.
9. Click **OK** to save the entry. Then write the configuration back to the device.

Additional configuration examples:

Time Basis	Min.	Hr.	Wk. Days	Mo. Days	Months	Command
Real time	0	4	0-6	1-31	1-12	do /so/man/disconnect internet
Real time	59	3	0-6	1-31	1-12	mailto:admin@example.com?subject=Forced-disconnect?body=Manual Internet discconnect
Real time	0	0		1		do /setup/accounting/delete
Real time	0	18	1,2,3,4,5			do /so/man/connect MAINOFFICE
Real time	/10					do command

- The first entry disconnects from the internet provider every morning at 4:00 AM (forced disconnection).
- The second entry sends an info email to the admin every morning at 3:59 AM, just before the forced disconnection.
- The third entry deletes the accounting table on the first day of every month.
- The fourth entry establishes a connection to headquarters at 6:00 PM on weekdays.
- The fifth entry executes a command every 10 minutes.

The device executes scheduled rules with a precision of one minute. Ensure that the language of the entered commands matches the console language, as the device will otherwise ignore the automation commands.

20.7 PPPoE server

The PPPoE server in the LCOS can authenticate PPPoE clients, e.g., routers or clients such as PCs with an integrated PPPoE client.

Possible use cases:

- In a student residence hall, students should be allowed to install their own routers and authenticate centrally in the network at the PPPoE server; access rights and bandwidth limitations should be applied
- In an office building, multiple tenants should share a common Internet connection while using their own routers; access rights and routing rules should be defined; as cabling, for example, a fiber-optic network or an existing copper cable network can be used

In all scenarios, users should be authenticated, clearly separated from each other, and a rights concept should be enforced through rules.

PPPoE sessions can be accepted on LAN interfaces in the LCOS. PPPoE users can be authenticated via the integrated PPP user table or a RADIUS server. It is possible to first search for a user in the local PPP user table in the router and then query the RADIUS server in a second step. It is also possible to use only the local user table or only a RADIUS server (exclusive mode).

User attributes, such as the IP address or the IPv6 prefix (router advertisement and/or delegated DHCPv6 prefix), can either be taken from the local configuration or outsourced to a RADIUS server. A combination of local configuration and RADIUS is also possible, whereby attributes from the RADIUS server take precedence for the corresponding user.

For multiple users, the use of a RADIUS server is generally recommended, as it enables centralized user configuration. Both an external RADIUS server and the RADIUS server integrated in the LCOS can be used.

Access rights for individual PPPoE users can be implemented via the firewall (IPv4/IPv6).

As authentication methods, the following are supported:

- PAP
- CHAP-MD5, MS-CHAPv1, and MS-CHAPv2

20.7.1 VLAN Support

PPPoE sessions can be accepted on a LAN interface in the following ways:

- Untagged PPPoE sessions (without VLAN)
- Tagged PPPoE sessions (with VLAN)
- Double-tagged PPPoE session (Q-in-Q / 802.1ad, configurable, e.g., Ethertype 0x8100 or 0x88a8)

The Ethertype for VLANs (C-VLAN / S-VLAN) can be configured under **Interfaces** > **VLAN** using the options **VLAN protocol ID** and **S-VLAN protocol ID**.

For PPPoE sessions over VLAN, PPPoE interfaces with the corresponding VLAN are created automatically at runtime and do not need to be configured statically.

20.7.2 Multiple Logins

It is recommended to configure an individual username and password for each user and to allow only one PPPoE session of the user to be active at a time per MAC address (set the parameter **Communication** > **General** > **Session limit** to 1).

In principle, multiple logins are supported by the PPPoE server, but they should be avoided, especially if individual parameters such as a fixed IP address are to be assigned to a user.

20.7.3 LCP Polling

To prevent inactive or expired PPPoE sessions on the PPPoE server, LCP polling is used. Inactive sessions mainly occur when a PPPoE client (e.g., a router) is disconnected from power without properly terminating the PPPoE session. LCP polling, or LCP echo request, is used to check the reachability of the PPPoE client. This ensures that an inactive PPPoE session on the PPPoE server is terminated. For this purpose, under (**Communication** > **Protocols**) in the **PPP list** for the DEFAULT entry—and, in the case of a local entry for a PPP user—the **LCP Polling** must be set for the parameter **Time**, e.g., to 3 (internally multiplied by 10 for 30 seconds), and for **Retries**, e.g., to 5 for 5 attempts. It is recommended to use the parameter **Communication** > **General** > **Session limit** with the value 1 and to enable **LCP Polling** at the same time.

20.7.4 IPv6

The PPPoE server generally supports IPv4 / IPv6 dual-stack scenarios. While IPv4 and the assignment of parameters such as the IP address are handled in PPP via IPCP (*RFC 1332*), IPv6 is implemented in several different functional components:

1. In IPv6CP according to *RFC 5072*, the link-local interface identifiers are negotiated between client and server

2. The PPPoE server sends the prefix (length /64) for the WAN connection toward the client via router advertisement. The prefix can be assigned either individually or from a pool. DNS servers can optionally also be assigned via router advertisement
3. The DHCPv6 server assigns the client its delegated DHCPv6 prefix (typically a /48 or /56) as well as the DNS server. The delegated DHCPv6 prefix can be assigned either individually or from a pool
4. In the IPv6 firewall, the access rights at the network level of the PPPoE client are defined

For IPv6, LCOS supports the concept of "RAS templates" for interfaces. This allows common parameters to be defined for all PPPoE clients, e.g., firewall configuration, router advertisements, or DHCPv6 server configurations.

20.7.5 Supported Standard RADIUS Attributes

The following standard RADIUS attributes are supported by the PPPoE server:

RADIUS ID	Attribute name / description	Access Request	Access Accept	Example
1	User-Name Username of the PPPoE client to be authenticated.	x		
2	User-Password User password (PAP) of the PPPoE client to be authenticated.	x		
3	CHAP-Password Value transmitted by the PPPoE client as part of password authentication in the case of CHAP.	x		
4	NAS-IP-Address Transmits the IPv4 address of the NAS/PPPoE server.	x		
6	Service-Type Specifies the service type that the device requests or expects in response. For PPPoE, the service type is "Framed-User".	x		
7	Framed-Protocol Specifies which protocol is used. The PPPoE server transmits the value "PPP".	x		
8	Framed-IP-Address Defines the IPv4 address to be assigned to the PPPoE client via IPCP.		x	Framed-IP-Address=100.64.1.2
18	Reply-Message Message transmitted to the PPPoE client by the PPPoE server in a PAP Authenticate-ACK or CHAP-Success.		x	
30	Called-Station-ID Transmits the device name of the router/NAS.	x		
31	Calling-Station-ID Specifies the ID of the calling station. For PPPoE, the MAC address of the client is transmitted.	x		
32	NAS-Identifier Specifies the device name of the NAS/PPPoE server.	x		

RADIUS ID	Attribute name / description	Access Request	Access Accept	Example
61	NAS-Port-Type Specifies the physical port through which the device authenticates the user. For PPPoE, the type “Ethernet” is transmitted.	x		
80	Message-Authenticator Additional attribute to protect the integrity of the RADIUS message exchange and prevent message spoofing. The attributes are set automatically.	x	x	
95	NAS-IPv6-Address Transmits the IPv6 address of the NAS/PPPoE server.	x		
96	Framed-Interface-ID This attribute defines the IPv6 interface identifier that is to be assigned or used for the user in IPv6CP.		x	
97	Framed-IPv6-Prefix Prefix transmitted to the user via router advertisements.		x	Framed-IPv6-Prefix=2001:db8::/64
99	Framed-IPv6-Route This attribute defines the route to be set for this user. The device creates this route in the IPv6 routing table with the next hop to this user.		x	Framed-IPv6-Route=2001:db8::/64
100	Framed-IPv6-Pool Specifies the IPv6 pool from which a prefix is to be provided to the user via router advertisement. The IPv6 pool is referenced by name and must exist under **IPv6** > **Router Advertisement** > **Prefix pools**. The pool name must be specified in uppercase.		x	Framed-IPv6-Pool=MYPOOL
123	Delegated-IPv6-Prefix Prefix transmitted to the user via DHCPv6 prefix delegation.		x	Delegated-IPv6-Prefix=2001:db8::/56

20.7.6 Supported Vendor-Specific RADIUS Attributes

The following vendor-specific RADIUS attributes from LANCOM Systems (Vendor 2356) are supported by the PPPoE server:

RADIUS ID	Attribute name / description	Access Request	Access Reply	Example
2356-8	LCS-TxRateLimit Defines a maximum downstream rate in kbps at Layer 2 from the perspective of the PPPoE server (NAS) toward the PPPoE client. This can be used to limit the download bandwidth of a PPPoE client at Layer 2. This function is only supported when the PPPoE client is connected via LAN interfaces. It is not supported when the PPPoE client is connected via Layer 2 tunnel interfaces such as Ethernet-over-GRE (EoGRE) or L2TPv3.		x	LCS-TxRateLimit=10000

RADIUS ID	Attribute name / description	Access Request	Access Reply	Example
2356-9	LCS-RxRateLimit Defines a maximum upstream rate in kbps at Layer 2 from the perspective of the PPPoE server (NAS) from the direction of the PPPoE client. This can be used to limit the upload bandwidth of a PPPoE client at Layer 2. This function is only supported when the PPPoE client is connected via LAN interfaces. It is not supported when the PPPoE client is connected via Layer 2 tunnel interfaces such as Ethernet-over-GRE (EoGRE) or L2TPv3.		x	LCS-RxRateLimit=10000

The following vendor-specific attributes from the Broadband Forum (Vendor 3561) are supported.

The values are inserted by an external access node such as a DSLAM, OLT, or switch and are transmitted as user-specific PPPoE tags in PADI/PADR messages. The PPPoE server transfers the existing attributes from the PPPoE tags into RADIUS attributes according to *RFC 4679* (e.g., in the Access Request) toward the RADIUS server.

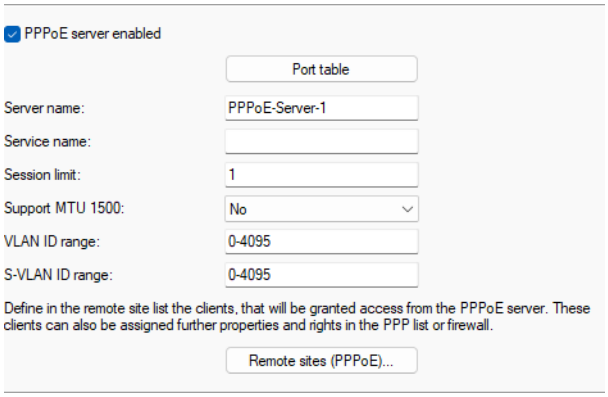
The values 3561-129 to 3561-144 contain general status values (e.g., attainable data rate in DSL) about the condition of the line to the router.

RADIUS ID	Attribute name / description	Access Request	Access Reply
3561-1	Agent-Circuit-Id This attribute contains the logical port name of the access node from which the PPPoE client's requests are initiated.	x	
3561-2	Agent-Remote-Id This attribute contains an operator-specific, statically configured string that uniquely identifies the subscriber on the corresponding access node port.	x	
3561-129	Actual data rate Upstream	x	
3561-130	Actual data rate Downstream	x	
3561-131	Minimum Data Rate Upstream	x	
3561-132	Minimum Data Rate Downstream	x	
3561-133	Attainable Data Rate Upstream	x	
3561-134	Attainable Data Rate Downstream	x	
3561-135	Maximum Data Rate Upstream	x	
3561-136	Maximum Data Rate Downstream	x	
3561-137	Minimum Data Rate Upstream in low power state	x	
3561-138	Minimum Data Rate Downstream in low power state	x	
3561-139	Maximum Interleaving Delay Upstream	x	
3561-140	Actual interleaving Delay Upstream	x	
3561-141	Maximum Interleaving Delay Downstream	x	
3561-142	Actual interleaving Delay Downstream	x	
3561-144	Access loop encapsulation	x	

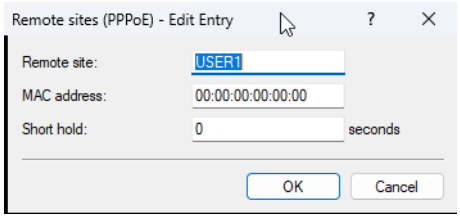
20.7.7 Tutorial: Setting Up a PPPoE Server with a Local User Table for IPv4 and IPv6

This tutorial describes how to configure a (dual-stack) PPPoE client in the router's local user table. The client receives an IPv4 address from the address pool, optionally an IPv6 prefix via router advertisement, and a delegated DHCPv6 prefix.

1. Open the configuration under **Communication** > **General**.
   a) Enable the **PPPoE server enabled** option.
   b) Under **Server name**, assign a name to the PPPoE server. This name is displayed to the PPPoE clients for identification in the status display

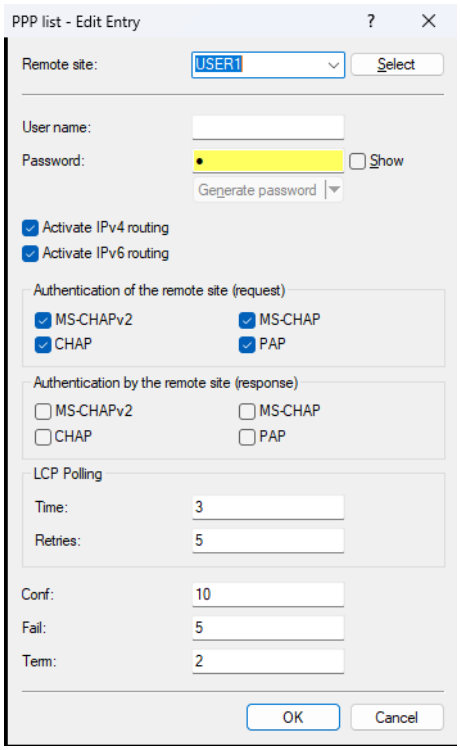


2. Open the **Remote sites (PPPoE)** table.
   a) Add a **Remote site** and assign it a name. This is also the username of the PPPoE client and must be provided to the user as part of the access credentials.
   b) Leave the **MAC address** field empty.
   c) Set the **Short hold** to 0. This means that the PPPoE client actively establishes the connection, and the server does not actively terminate it, except in the event of an LCP polling timeout



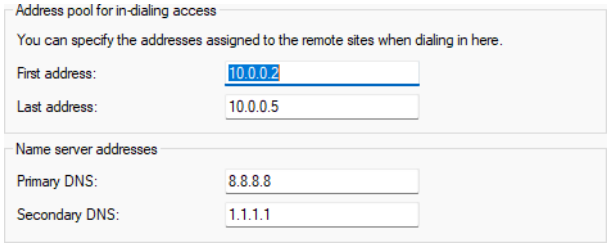
3. Open the **PPP list** under **Communication** > **Protocols**. Add a new entry and make the following adjustments:
   a) For **Remote site**, select the remote site created in the previous step.
   b) The **User name** field is not used for PPP dial-in in the role of PPPoE server on the LCOS and must therefore be left empty here.
   c) In the **Password** field, enter the password of the PPPoE client.
   d) Use **Activate IPv4 routing** to enable or allow IPCP negotiation and the assignment of IPv4 addresses to the client.
   e) Optionally, you can also use **Activate IPv6 routing** to allow IPv6CP negotiation and the use of IPv6 for the PPPoE client.
   f) Under **Authentication of the remote site (request)**, enable the permitted authentication methods with the PPPoE client.
   g) Under **Authentication by the remote site (response)**, the selection must be left empty. The PPPoE server is not supposed to authenticate itself to the client.

h) Under **LCP Polling**, set the **Time** value to 3 (internally multiplied by 10 for 30 seconds) and the **Retries** value to 5.

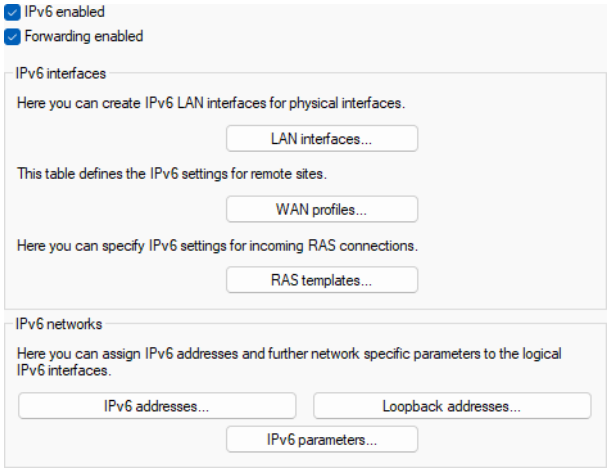


4. The address pool for PPPoE clients is defined under **IPv4** > **Addresses**:

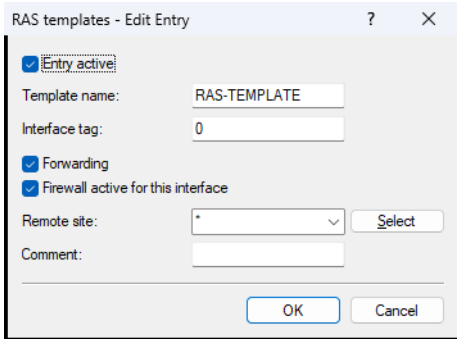
Option	Description
First address	First IPv4 address of the dial-in pool, e.g. 10.0.0.2.
Last address	Last IPv4 address of the dial-in pool, e.g. 10.0.0.5.
Primary DNS	First IPv4 DNS server to be assigned to the PPPoE clients.
Secondary DNS	Optional specification of a second IPv4 DNS server to be assigned to the PPPoE clients.



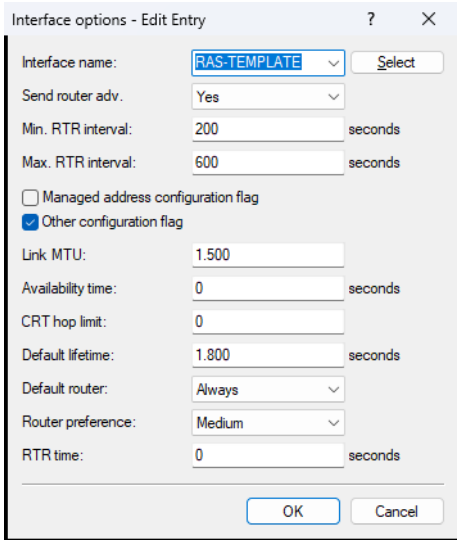
5. Optionally, also enable IPv6 under **IPv6** > **General** > **IPv6 enabled**.



a) Enable the IPv6 RAS templates under **IPv6** > **General** > **RAS templates** > **Edit the RAS-TEMPLATE** > **Entry active**.

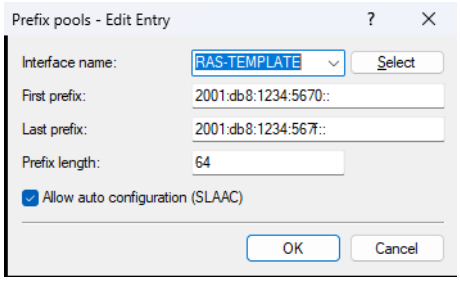


b) Under **IPv6** > **Router Advertisements** > **Interface options**, create a new table entry. For **Interface name**, select the "RAS-TEMPLATE" you just activated, and for **Default router** select "Always".

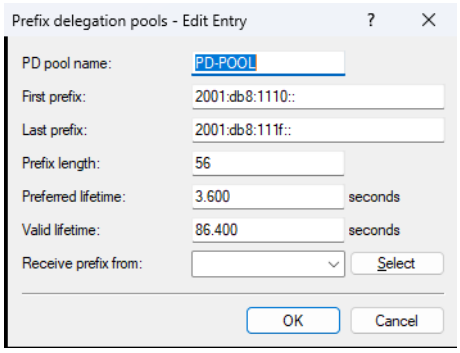


c) Under **IPv6** > **Router Advertisements** > **Prefix pools**, create a new table entry. For **Interface name**, select the "RAS-Template", and for **First prefix**, enter the first IPv6 prefix of the pool to be assigned to clients. For

Last prefix, enter the last IPv6 prefix of the pool to be assigned to clients. The **Prefix length** must be exactly /64.

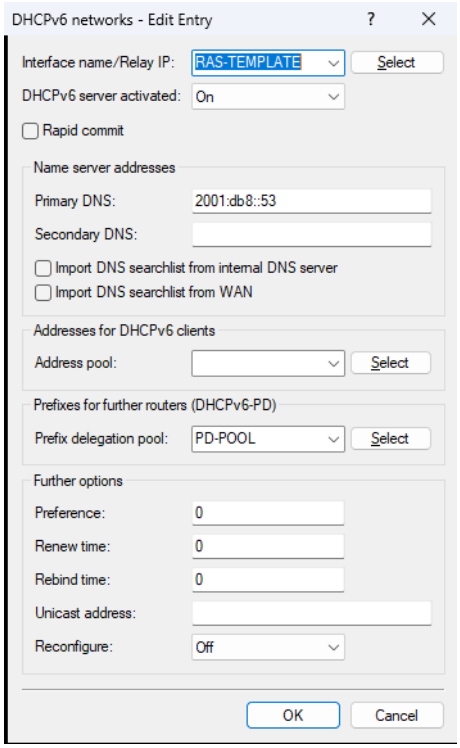


d) Under **IPv6** > **DHCPv6** > **DHCPv6 server** > **Prefix delegation pools**, create a new table entry. For **PD pool name**, use the name "PD-POOL", and for **First prefix**, enter the first IPv6 prefix of the PD pool to be assigned to clients. For **Last prefix**, enter the last IPv6 prefix of the PD pool to be assigned to clients. Under **Prefix length**, configure the prefix length of the DHCPv6 prefix to be assigned to a client. Usually, /56 is used as the prefix length.



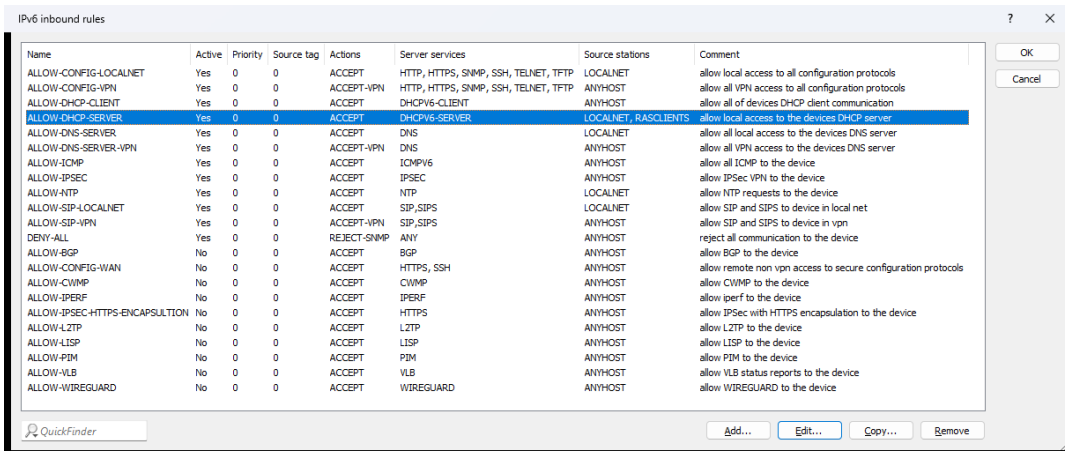
e) Under **IPv6** > **DHCPv6** > **DHCPv6 server** > **DHCPv6 networks**, create a new table entry. For **Interface name/Relay IP**, select "RAS-TEMPLATE". Set the option **DHCPv6 server activated** to "On". Under **Primary**

DNS, configure which IPv6 DNS server address is to be assigned to the client. Under **Prefix delegation pool**, configure the name of the previously created DHCPv6 PD pool “PD-POOL”.

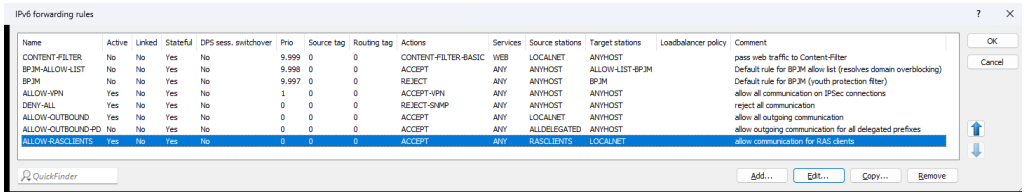


f) Open the configuration under **Firewall/QoS** > **IPv6 Rules** and make sure that the prefixes and services used are also enabled in the IPv6 firewall. The predefined object “RASCLIENTS” applies to PPPoE clients created via the “RAS-TEMPLATE” interface.

g) Check in the **IPv6 inbound rules** that “Allow-DHCP-Server” is allowed from the source stations “RASCLIENTS”. In addition, “Allow-DNS-Server” must be allowed from the source stations “RASCLIENTS” if the LANCOM router itself is to act as the IPv6 DNS server for the PPPoE clients.



h) Check in the **IPv6 forwarding rules** that the "Allow-RASCLIENTS" rule is allowed. The IPv6 prefixes used in this scenario for router advertisements or DHCPv6 PD pools must generally be allowed by a firewall rule in the forwarding case and must not be blocked by a DENY-ALL rule



Status information for all active PPPoE clients is displayed in the table under **Status** > **PPPoE Server** > **Connections**.

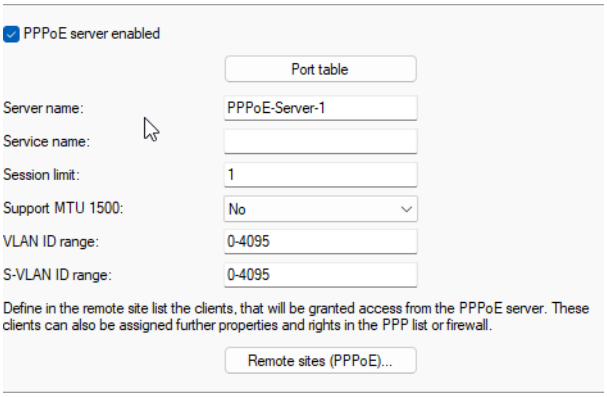
Detailed information about an individual client can be displayed with the show command "show pppoe-user-detail <user-name>".

Analysis options are provided by the trace command "trace # ppp".

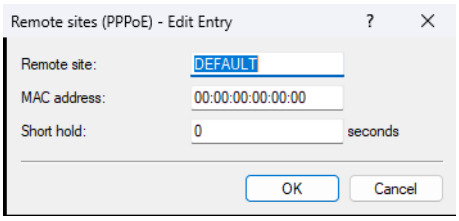
20.7.8 Tutorial: Setting Up a PPPoE Server with RADIUS for IPv4 and IPv6

This tutorial describes how to configure a (dual-stack) PPPoE client via RADIUS. The client receives an IPv4 address, optionally an IPv6 prefix via router advertisement, and a delegated DHCPv6 prefix.

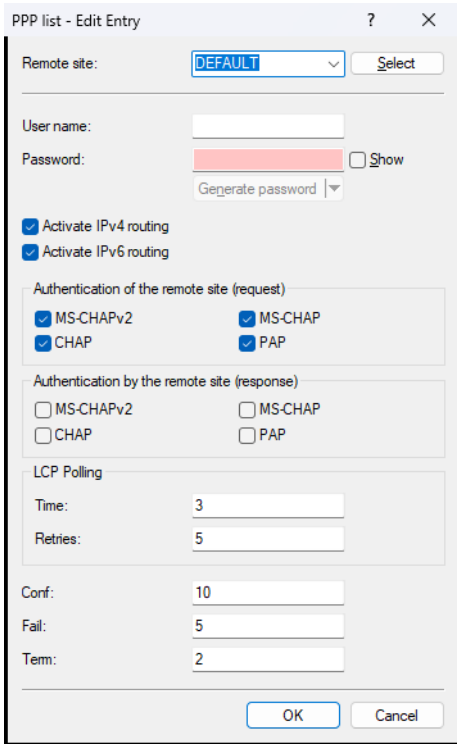
1. Open the configuration under **Communication** > **General**.
   a) Enable the **PPPoE server enabled** option.
   b) Under **Server name**, assign a name to the PPPoE server. This name is displayed to the PPPoE clients for identification in the status display



2. Open the **Remote sites (PPPoE)** table.
3. Edit the DEFAULT remote site.
   a) Leave the name of the **Remote site** as "DEFAULT". This entry is used for all PPPoE clients that are to be authenticated via RADIUS.
   b) Leave the **MAC address** field empty.
   c) Set the **Short hold** to 0. This means that the PPPoE client actively establishes the connection, and the server does not actively terminate it, except in the event of an LCP polling timeout



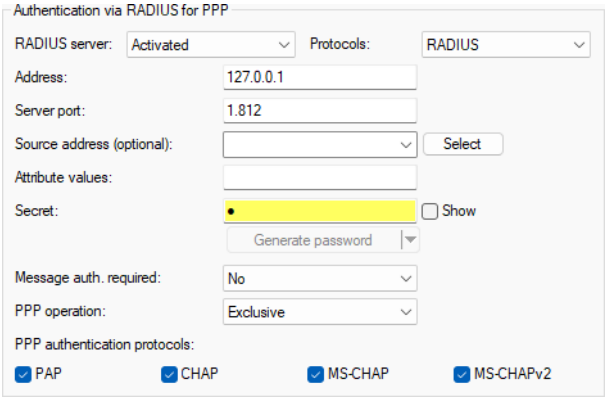
4. Open the **PPP list** under **Communication** > **Protocols**. Edit the DEFAULT remote site and make the following adjustments:
   a) Use **Activate IPv4 routing** to enable or allow IPCP negotiation and the assignment of IPv4 addresses to the client.
   b) Optionally, you can also use **Activate IPv6 routing** to allow IPv6CP negotiation and the use of IPv6 for the PPPoE client.
   c) Under **Authentication of the remote site (request)**, enable the permitted authentication methods with the PPPoE client.
   d) Under **Authentication by the remote site (response)**, the selection must be left empty. The PPPoE server is not supposed to authenticate itself to the client.
   e) Under **LCP Polling**, set the **Time** value to 3 (internally multiplied by 10 for 30 seconds) and the **Retries** value to 5.



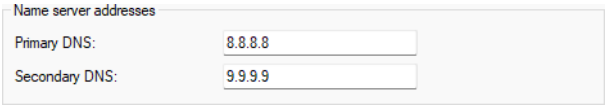
5. Open the configuration under **Communication** > **RADIUS**.
6. Configure the necessary settings for **Authentication via RADIUS for PPP**:

Option	Description
RADIUS server	Activated
Address	IP address of the RADIUS server. If the internal RADIUS server is to be used, 127.0.0.1 can be entered as the IP address.
Secret	Password for communication with the RADIUS server.

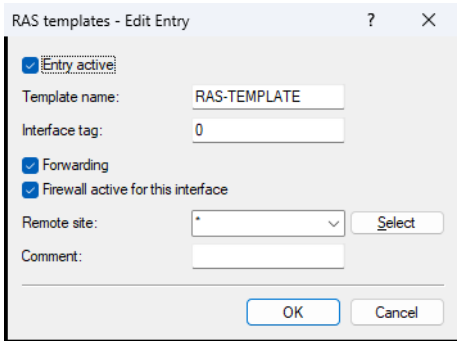
Option	Description
PPP operation	Exclusive. This means that only the RADIUS server is to be used for authentication and not the internal PPP user table as well.



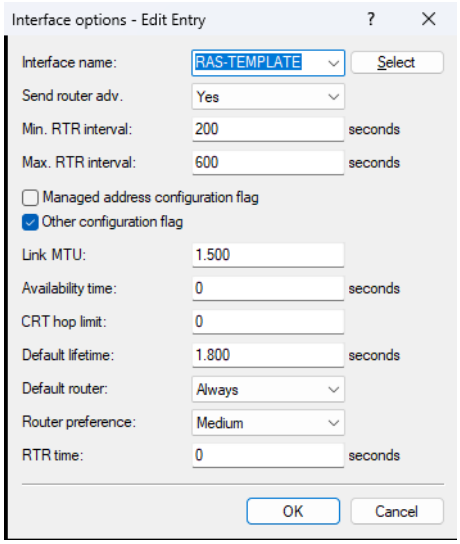
7. Open the configuration under **IPv4** > **Addresses**.
8. Configure the DNS server addresses for the clients as **Primary DNS** and **Secondary DNS**.



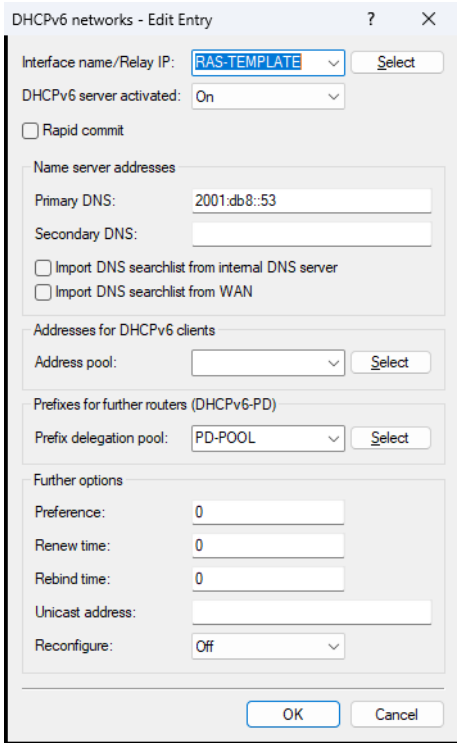
9. If the optional IPv6 was enabled above, then also carry out the following steps:
   a) Enable the IPv6 RAS templates under **IPv6** > **General** > **RAS templates** > **Edit the RAS-TEMPLATE** > **Entry active**.



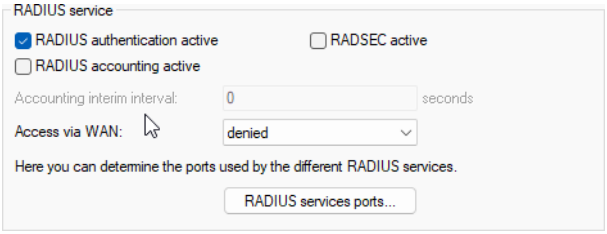
b) Under **IPv6** > **Router Advertisements** > **Interface options**, create a new table entry. For **Interface name**, select the "RAS-TEMPLATE" you just activated, and for **Default router** select "Always".



c) Under **IPv6** > **DHCPv6** > **DHCPv6 server** > **DHCPv6 networks**, create a new table entry. For **Interface name/Relay IP**, select "RAS-TEMPLATE". Set the option **DHCPv6 server activated** to "On". Under **Primary DNS**, configure which IPv6 DNS server address is to be assigned to the client. Under **Prefix delegation pool**, configure the name of the previously created DHCPv6 PD pool "PD-POOL".



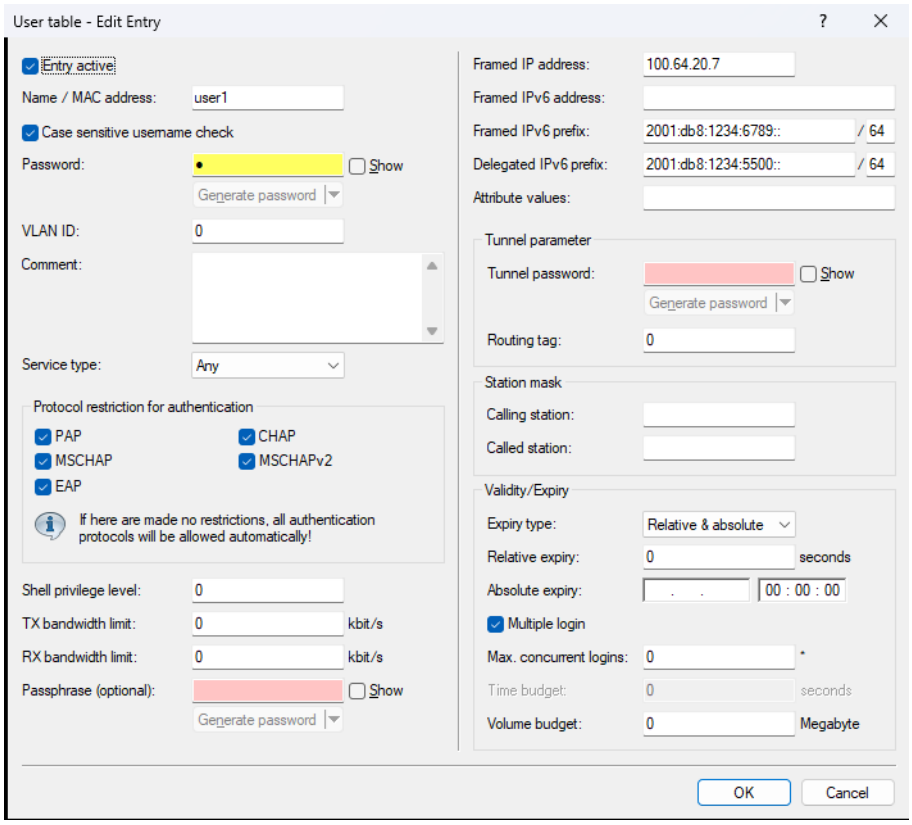
10. Enable **RADIUS authentication active** under **RADIUS** > **Server** > **RADIUS service**.



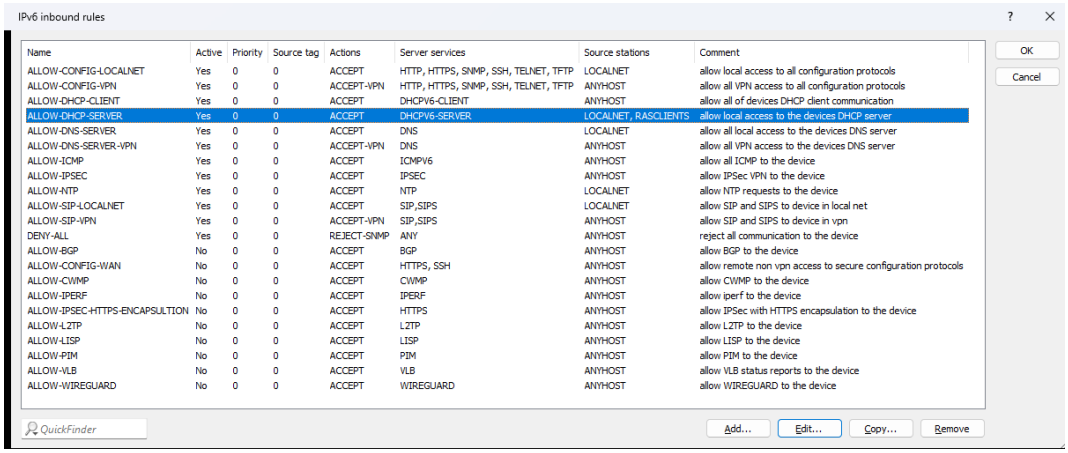
11. Create a new user on the RADIUS server under **RADIUS** > **Server** > **User database** > **User table** with the following attributes:

Option	Description
Name / MAC address	Required.
Password	Required.
Framed IP address	Required for assigning the IPv4 address.
Framed IPv6 prefix	Required for IPv6 for the IPv6 router advertisement prefix.
Delegated IPv6 prefix	Optional. Used for IPv6 DHCPv6.
TX bandwidth limit	Optional.
RX bandwidth limit	Optional.
Routing tag	Optional. The PPPoE client is created in the corresponding routing context.
Attribute values	Optional. E.g. “Reply-Message=SRU=10000#SRD=60000#”. Certain information can be transmitted here to the PPPoE client during

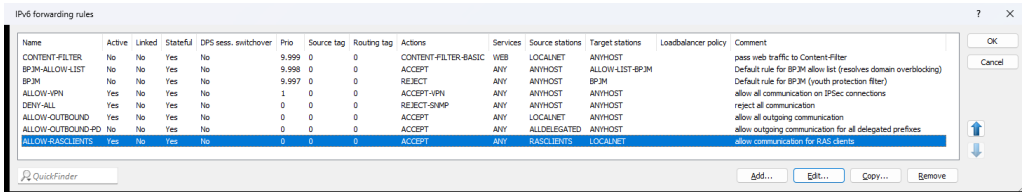
Option	Description
	authentication, e.g. the bandwidth information for correct QoS functionality.



12. Open the configuration under **Firewall/QoS** > **IPv6 Rules** and make sure that the prefixes and services used are also enabled in the IPv6 firewall. The predefined object “RASCLIENTS” applies to PPPoE clients created via the “RAS-TEMPLATE” interface.
13. Check in the **IPv6 inbound rules** that “Allow-DHCP-Server” is allowed from the source stations “RASCLIENTS”. In addition, “Allow-DNS-Server” must be allowed from the source stations “RASCLIENTS” if the LANCOM router itself is to act as the IPv6 DNS server for the PPPoE clients.



14. Check in the **IPv6 forwarding rules** that the “Allow-RASCLIENTS” rule is allowed. The IPv6 prefixes used in this scenario for router advertisements or DHCPv6 PD pools must generally be allowed by a firewall rule in the forwarding case and must not be blocked by a DENY-ALL rule



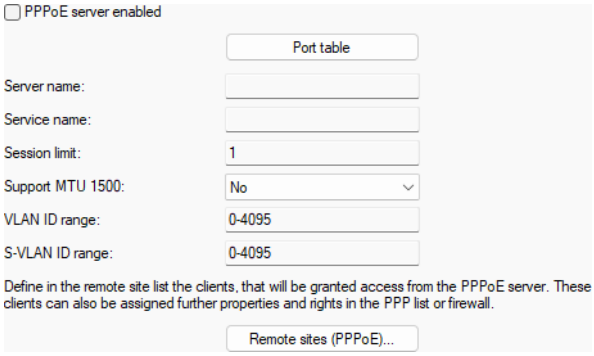
Status information for all active PPPoE clients is displayed in the table under **Status** > **PPPoE Server** > **Connections**.

Detailed information about an individual client can be displayed with the show command “show pppoe-user-detail <user-name>”.

Analysis options are provided by the trace command “trace # ppp”.

20.7.9 Configuration

The PPPoE server settings are adjusted in LANconfig under **Communication** > **General**.



In this view, you have the following configuration options:

PPPoE server enabled

Using these settings you globally enable or disable the PPPoE server.

Port table

Using this table the PPPoE server can be independently enabled or disabled for every physical or logical interface.

Server name

This input field provides the option to give the PPPoE server a name that is independent of the device name (AC-Name = access concentrator name). If you leave this field blank, the PPPoE server uses the device name as the server name.

Service name

Enter the name of the service being offered in this input field. The service name makes it possible for a PPPoE client to select a specific PPPoE server. Configure the service name directly on the client.

Session limit

This setting specifies how often a client can be logged on simultaneously with the same MAC address. Once the limit has been reached, the server no longer responds to any client requests it receives. A Session limit of `0` stands for an unlimited number of sessions.

Support MTU 1500

Defines, if the devices should negotiate a PPPoE MTU of 1500 based on *RFC 4638*. The remote peer must support this extension as well.

VLAN ID range

The PPPoE server supports Q-in-Q VLANs, i.e. double-tagged VLANs. For incoming PPPoE packets, LCOS automatically creates the corresponding peers in LCOS.

A range for permitted VLANs can be specified here. A string of up to 64 characters consisting of the digits 0 to 9 and the character '-' for a range, as well as ',' for a list, can be specified.

The list is validated on input. A maximum tag of 4095 may be entered. Tag 0 means "untagged". With the default "0-4095", all tags are permitted.

Possible entries are individual values, ranges, as well as lists of values and ranges, e.g. "0,1,20-60,70,100-200,4095". For ranges, the second value must always be greater than (or equal to) the first value, i.e. "123-123" is valid, whereas "123-122" is not.

If a packet is received with a tag that is not permitted, the PPP trace outputs this accordingly, e.g.

```
[PPP] 2025/03/19 18:19:16,051

Received PADI frame from peer b2:8d:ef:36:03:fd for session 0000 on LAN-1
 (VLAN-ID 8 not allowed) => Discard
```

Default: 0-4095

S-VLAN ID range

The PPPoE server supports Q-in-Q VLANs, i.e. double-tagged VLANs. For incoming PPPoE packets, LCOS automatically creates the corresponding peers in LCOS.

A range for permitted S-VLANs can be specified here. A string of up to 64 characters consisting of the digits 0 to 9 and the character '-' for a range, as well as ',' for a list, can be specified.

The list is validated on input. A maximum tag of 4095 may be entered. Tag 0 means "untagged". With the default "0-4095", all tags are permitted.

Possible entries are individual values, ranges, as well as lists of values and ranges, e.g. "0,1,20-60,70,100-200,4095". For ranges, the second value must always be greater than (or equal to) the first value, i.e. "123-123" is valid, whereas "123-122" is not.

Default: 0-4095

Remote sites (PPPoE)

In this table you define the individual clients which the PPPoE server allows to access the desired services (such as Internet, e-mail) or specific remote stations.

The **MAC address**`000000000000` allows a remote station to login to the device with any MAC address. If a specific MAC address is entered, then the PPP negotiation is terminated if the user logs on from a different MAC address.

After login, the device attempts to set the **Hold time** of the remote station. If there is no entry, the device uses the remote site `DEFAULT`. To prevent the device (as a PPPoE server) from automatically terminating the connection, the hold time must be set to 0.

In addition to this table, you must make an entry into the PPP table containing the password, the permissions (IP), and other PPP parameters (LCP polling, etc.). Alternatively, you also have the option to authenticate users through a RADIUS server. To do this, you configure the server under **Communication** > **RADIUS** > **Authentication via RADIUS for PPP**. Set the operating mode to **Activated** (mixed data storage, RADIUS/PPP table).

20.7.10 PPPoE snooping

PPPoE snooping enables devices that receive and forward PPPoE discovery (PPPoED) packets to analyze these packets and to supplement them with additional information. This information can be used by a PPPoE access concentrator (AC) to process the PPPoED data packets accordingly. This role is called the "PPPoE-Intermediate-Agent".

PPPoE snooping in the LCOS processes the following PPPoED packets:

- PADI (PPPoE Active Discovery Indication)
- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

The PPPoE intermediate agent, which is responsible for the PPPoE snooping, supplements the PPPoED packet with manufacturer-specific attributes (circuit ID and remote ID), and any existing IDs in received packets are replaced with its own values.

- The remote ID: Uniquely identifies the client making a PPPoE request.
- Circuit ID: Uniquely identifies the interface used by a client to make a PPPoE request.

PPPoE snooping is configured for each LAN/WLAN interface.

20.8 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) enables devices on a network to be monitored and configured from a central instance. Since the initial release of SNMPv1 in 1988, it has continued to evolve with the versions SNMPv2 and SNMPv3 to meet the needs of increasingly complex network infrastructures and the demands for user-friendliness, security and flexibility.

The protocol SNMP (simple network management protocol) meets the highest standards for convenient management and monitoring of a network. It allows for the early detection of problems and errors on a network and offers support in eliminating them. The simple network management protocol allows a central instance to monitor and configure the devices on a network from, and it regulates the communication between the monitored devices and the monitoring station. This means that parameters such as the status of the device, CPU utilization, the temperature of a device, its connection status, errors, and others can be monitored and analyzed, for example with LANmonitor. The administrator benefits from active support with network management and is helped to detect problems at an early stage. The latest SNMPv3 version of the protocol, in contrast to the previous versions SNMPv1 and SNMPv2, now enables encrypted data communication between the network and its management system, which provides a crucial security factor. By offering different user accounts for authentication, the integrated user administration provides optimal control over access to the configurations. You have precise control over the rights to the different levels of access that administrators receive, and the network is optimally protected.

SNMP components

The typical SNMP architecture consists of three components:

SNMP manager

The SNMP manager sends SNMP requests to the SNMP agent and evaluates the SNMP responses from it. LANconfig and LANmonitor act as this type of SNMP manager. LCOS devices comply with the standards SNMPv1, SNMPv2, and SNMPv3, so it is possible to use an alternative SNMP administration and management software.

SNMP agent

The SNMP agent is a module that is active on the managed device. When it receives a request from the SNMP manager, it retrieves the requested status data from the MIB in the device and returns this information to the SNMP manager as an "SNMP response". Depending on the configuration, an SNMP agent that detects certain

changes of state in the managed device can independently act to send an "SNMP trap" to the SNMP manager. It is also possible to send a notification to the device administrator by means of a SYSLOG message or e-mail.

Managed device

The status of this device is stored in its Management Information Base (MIB). When requested by the SNMP agent, the device reads out this information and returns it to the SNMP agent.

By default, SNMP requests and SNMP responses are exchanged between the SNMP manager and SNMP agent by the User Datagram Protocol (UDP) on port 161. SNMP traps are transmitted with the UDP via port 162 by default.

SNMP versions

The differences between the various versions of SNMP can be summarized as follows:

SNMPv1

Version 1 was launched in 1988 and has long been regarded as the de facto standard for network management. In SNMPv1, the SNMP manager authenticates at the SNMP agent by means of a community string, which must be identical on both components. The security of this is very limited, as the community strings are transmitted in cleartext. The increase in demands for secure network communication necessitated a revision of version 1.

SNMPv2

After 1993, the main improvements in version 2 were to its user-friendliness. Numerous intermediate steps and the repeated rejection of concepts eventually led to the version SNMPv2c. This version allows large amounts of data to be requested via a `GetBulkRequest` command and also the communication between SNMP managers. However, the exchange of the community strings was still as cleartext as with version 1.

SNMPv3

From 1999, version 3 finally met the by then much-needed security requirements. Among other things, the communication was encrypted and the communication partners first had to authenticate and authorize themselves. Also, the structure of SNMP became more modular so that improvements, for example in encryption technologies, can be incorporated into SNMPv3, without having to completely redesign the standard.

LCOS supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

20.8.1 SNMPv3 basics

The SNMP protocol structure has changed significantly with version 3. SNMPv3 is now divided into a number of modules with clearly defined interfaces that communicate with one another. The three main elements in SNMPv3 are "Message Processing and Dispatch (MPD)", "User-based Security Model (USM)" and "View-based Access Control Mechanism (VACM)".

MPD

The MPD module is responsible for the processing and dispatch of inbound and outbound SNMP messages.

USM

The USM module manages security features that ensure the authentication of the users and the encryption and integrity of the data. SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may

be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

VACM

VACM ensures that the sender of an SNMP request is entitled to receive the requested information. The associated access permissions are found in the following settings and parameters:

SNMPv3-Views

"SNMPv3-Views" collect together the content, status messages, and actions of the Management Information Base (MIB) that are permitted to receive or execute an SNMP request. These views can be single values, but also complete paths of the MIB. This content is specified by the OIDs of the MIB entries.

In this way, a successfully authenticated sender of an SNMP request only has access to that data specified in the applicable SNMPv3 views.

SNMPv3-Groups

"SNMPv3-Groups" collect users with the same permissions into a specific group.

Security-Levels

"Security levels" relate to the exchange of SNMP messages. The following levels can be selected:

NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

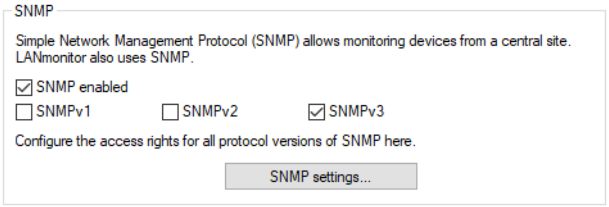
SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Context

"Context" is used to distinguish the various SNMP entities.

20.8.2 Configuring SNMP

In LANconfig you configure SNMP under **Logging/Monitoring** > **Protocols** in the section **SNMP**.



SNMP enabled

Enable SNMP for the SNMP protocol versions specified below, which the device should support for SNMP requests and SNMP traps.

SNMPv1

Enables SNMPv1.

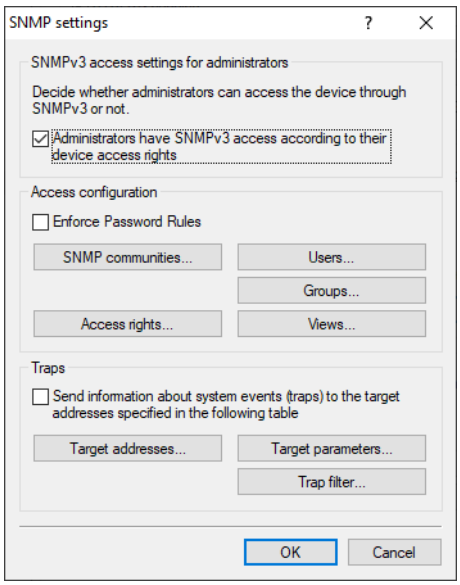
SNMPv2

Enables SNMPv2c.

SNMPv3

Enables SNMPv3.

Click on **SNMP settings** to open the configuration settings.



20.8.2.1 SNMP settings

SNMPv3 access settings for administrators

Administrators have SNMPv3 access according to their access rights

Enable this option if registered administrators should also have access via SNMPv3.

Password rules

Enforce password rules

This entry gives you the option to disable or enable the enforcement of password rules. The following rules then apply for SNMPv3 authentication and the password for SNMPv3 encryption:

- The length of the password must be at least 16 characters.
- The password must contain at least 3 of the 4 character classes, i.e. lowercase letters, uppercase letters, numbers, and special characters.

Note that turning on this feature does not cause current passwords to be verified immediately. Only future password changes will be checked for compliance with the policy.

SNMP communities

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a "community". Authentication is optionally handled

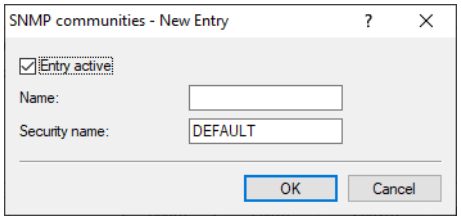
- by the `public` community (unlimited SNMP read access),
- by a master password (limited SNMP read access), or
- a combination of user name and password, separated by a colon (limited SNMP read access)

.

A community collects certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community `public`. Because this represents a potential security risk, especially with external access, LANconfig gives you the option of defining your own communities.

This configuration is relevant for the SNMP versions v1 and v2c only.



Entry active

Activates or deactivates this SNMP community.

Name

Enter a descriptive name for this SNMP community.

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

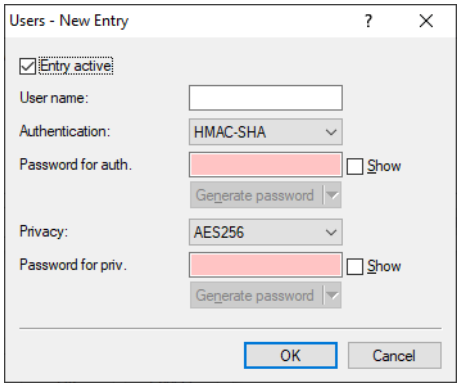
For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the `public` community in the list of the SNMP communities. This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community `public` has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

SNMP write access is reserved exclusively for administrators with the appropriate permissions.

Users

Individual users can be granted access to the device in addition to the administrators registered on it. Here you configure the authentication and encryption settings for these users when operating SNMPv3.



Entry active

Activates or deactivates this user.

User name

Enter a descriptive name for this user.

Authentication

Specify the method that the user is required to use to authenticate at the SNMP agent. The following options are available:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA (default)

Authentication is performed using the hash algorithm HMAC-SHA (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

Password for auth.

Enter the user password necessary for authentication here and repeat it in the box below.

Encryption

Specify which encryption method is used for encrypted communication with the user. The following options are available:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits)

AES192

Encryption is performed with AES192 (key length 192 bits)

AES256 (default)

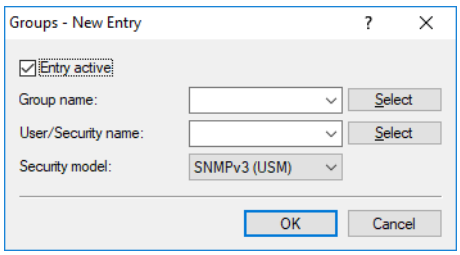
Encryption is performed with AES256 (key length 256 bits)

Password for priv.

Enter the user password required by the encryption here and repeat it in the box below.

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.



Entry active

Activates or deactivates this group.

Group name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

User / security name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Security model

SNMPv3 introduced the principle of the “security model”, so that the SNMP configuration in LCOS primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the “security model” accordingly. Select one of the following entries accordingly:

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv2

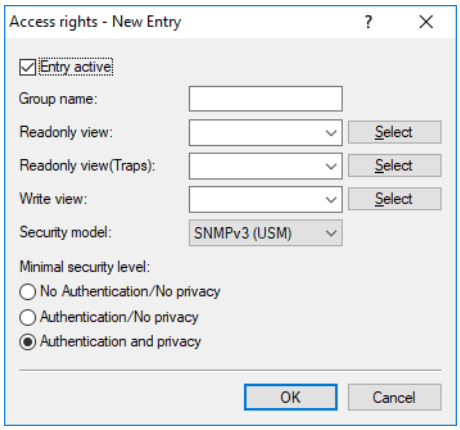
Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv3 (USM)

Data is transmitted by SNMPv3. Security levels for the user’s authentication and communication are possible, and these levels are activated with the **access rights**.

Access rights

This table brings together the different configurations for access rights, security models, and views.



Entry active

Activates or deactivates this entry.

Group name

Here you select the name of a group that is to receive these assess rights.

Read-only view

Set the view of the MIB entries for which this group is to receive read rights.

Read-only view (traps)

Set the view of the MIB entries for which this group is to receive read rights for traps.

Write view

Set the view of the MIB entries for which this group is to receive write rights.

Security model

Activate the appropriate security model here.

Minimal security level

Specify the minimum security level for access and data transfer.

No authentication/No privacy

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

Authentication/No privacy

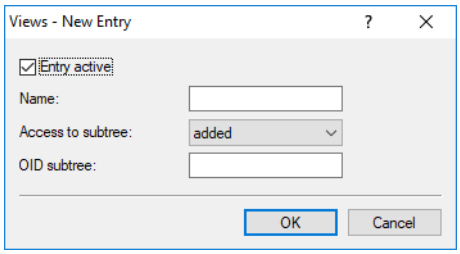
Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

Authentication and privacy

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

Views

Here you collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with the corresponding access rights.



Entry active

Activates or deactivates this view.

Name

Give the view a descriptive name here.

Access to subtree

Here you decide whether the OID subtrees specified in the following are “added” or “removed” from the view.

OID subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in or excluded from this view.

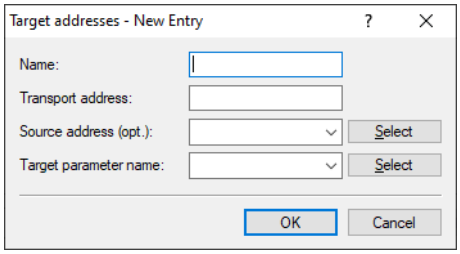
The OIDs are taken from the device MIB, which you can download with WEBconfig under **Extras** > **Get Device SNMP MIB**.

Traps

If you enable the option **Send information about system events (traps) to the target addresses specified in the following table**, the recipients configured under **Target addresses** and **Target parameters** will receive the corresponding information. The system events that trigger a message can be restricted by trap filters.

Target addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.



Name

Give the entry a descriptive name here.

Transport address

Configure the address of the recipient here. This address describes the IP address and port number of a recipient of an SNMP trap and is specified in the syntax "<IP address> : <Port>" (e.g. 128.1.2.3:162). UDP port 162 is used for SNMP traps.

Source address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

If you have configured loopback addresses, you can specify them here as source address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

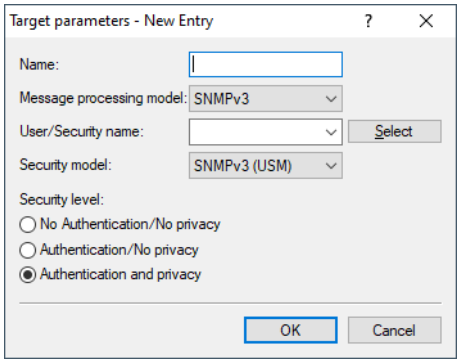
If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Target parameter name

Here you select the desired entry from the list of recipient parameters.

Target parameter name

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.



Name

Give the entry a descriptive name here.

Message processing model

Here you specify the protocol for which the SNMP agent structures the message.

User / security name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Security model

SNMPv3 introduced the principle of the "Security Model", so that the SNMP configuration in LCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to allow for the versions SNMPv2c or even SNMPv1, and to select these accordingly. Select one of the following entries accordingly:

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv2

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv3 (USM)

Data is transmitted by SNMPv3. This can only be selected together with SNMP users. The effective possible security level depends on the user's chosen authentication and encryption methods.

Security level

Set the security level that applies for the recipient to receive the SNMP trap.

No authentication/No privacy

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Authentication/No privacy

Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

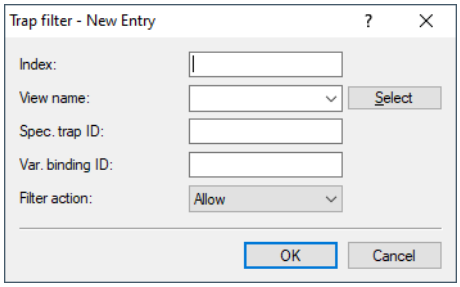
Authentication and privacy

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

Trap filter

Certain SNMP traps or even large numbers of SNMP traps can be unwanted on the receiving servers. For this reason, you can add an SNMP filter list that allows you to selectively pass or withhold SNMP traps based on their manufacturer-specific OIDs or the OIDs contained in the variable bindings.

Traps for the user “root” cannot be filtered. Filtering requires the use of a separate SNMP user.



Index

The position of this entry in the filter list. The list is checked from the smallest to the largest value until the first

hit.

View name

The **View name** is the name of a **view** that this filter rule applies to. If **Access to subtree** for the relevant view is set to “added”, the corresponding traps can be prevented by the **filter action** “deny” in a related filter rule. However, if **Access to subtree** of the relevant view is set to “removed”, the **filter action** “Allow” still sends the messages as an exception. Since the **views** can contain multiple entries of the same name with different access settings, it must be possible to set the **filter action** irrespective of the value of the corresponding setting for **Access to subtree**.

Spec. trap ID

Specifies a certain trap ID that can contain wildcards and ranges. An empty entry applies to all specific trap IDs of the device. See the examples in the following table.

OID	Description
	Applies to every OID.
1.2.3	Applies to all OIDs that start with “1.2.3”.
1.*.3	Applies to all OIDs that start with “1”, then contain any value, and then continue with “3”.
1.2-3.4	Applies to all OIDs that start with “1”, continue with a number ranging from “2 to 3”, and then a “4”.
1.2.3-4,7-8	Applies to all OIDs that start with “1.2” and continue with a number ranging from “3 to 4” or “7 to 8”.

Wildcards and ranges can occur anywhere in an OID, and an OID may also contain multiple wildcards or ranges. However, each position may only contain either a wildcard or a range.

A LANCOM device maps the generic trap OIDs of the SNMP protocol to certain vendor-specific OIDs:

Name	Generic OID	OID at LANCOM
coldStart	0	1.3.6.1.6.3.1.1.5.1
warmStart	1	1.3.6.1.6.3.1.1.5.2
linkDown	2	1.3.6.1.6.3.1.1.5.3
linkUp	3	1.3.6.1.6.3.1.1.5.4

Name	Generic OID	OID at LANCOM
authenticationFailure	4	1.3.6.1.6.3.1.1.5.5
egpNeighborLoss	5	1.3.6.1.6.3.1.1.5.6

Var. Binding ID

Specifies an OID that must be in the trap's variable bindings, which in turn may contain wildcards and ranges. Also see **Spec. trap ID**, An empty entry applies to all variable bindings of the device.

Filter action

In case of a match with the set IDs, you can either "Allow" the trap to so send it, or "Deny" it so that it is discarded.

20.9 Netflow / IPFIX

NetFlow is a feature that allows network devices such as routers or switches to export information about their inbound and outbound IP traffic. The so-called IP flows are transmitted by UDP. An IP flow contains information about the source IP address, destination IP address, ports, timestamp and packet counters, among others. This information is received, stored and processed on a NetFlow collector. NetFlow can be used either permanently or temporarily for network analysis.

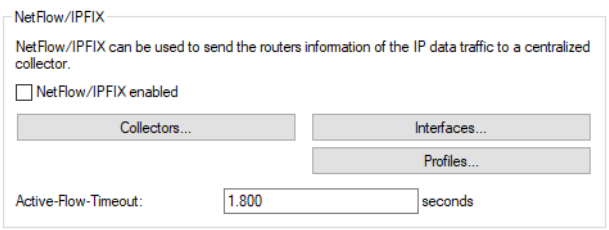
LANCOM supports the standards NetFlow 9 (*RFC 3954*) as well as IPFIX (*RFC 7011*), which is an extension of NetFlow Version 9, via the transport protocol UDP.

Notes on use:

- You need an external NetFlow collector that supports NetFlow 9 or IPFIX.
- The firewall must be activated.
- The only flow information collected with IPv4 is that being passed from one logical interface to another logical interface. Packets generated by or addressed to the router itself are not captured. For IPv6, this restriction does not apply.
- Only unicast IP flow information is collected, multicast (e.g. IPTV) is not supported.
- Depending on the scenario, using NetFlow/IPFIX increases CPU load and reduces the overall performance of the router.

20.9.1 Configuring NetFlow / IPFIX

In LANconfig you configure NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** in the section **NetFlow/IPFIX**.



NetFlow/IPFIX enabled

Enable NetFlow/IPFIX on the device.

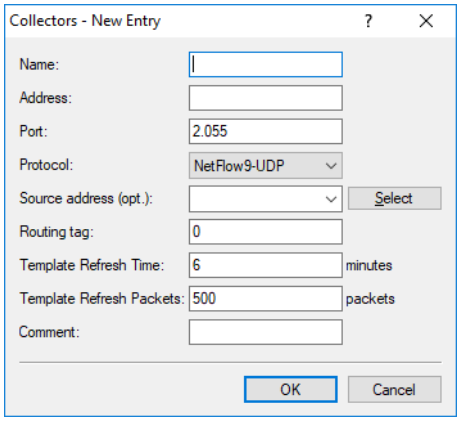
Active-Flow-Timeout

Defines the interval in seconds after a running data stream is exported via Netflow. This makes it possible to run longer sessions, e.g. to export large downloads at runtime. Subsequent traffic is classified as a new data flow, and the logging of the data traffic by the collector starts again.

Possible values: 60–1800 seconds (0 turns the function off)

20.9.1.1 Collectors

You can configure the collectors for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Collectors**.



Name

Unique name of the NetFlow collector. This name is referenced in other tables.

Address

IPv4, IPv6 address or host name of the collector.

Port

NetFlow collector port. Usually port 2055 for NetFlow 9 and 4739 for IPFIX.

Protocol

Protocol version used by the NetFlow collector. Possible values are NetFlow 9 over UDP or IPFIX over UDP.

Source address

Optionally, specify a source address.

Routing tag

Specify a routing tag if a particular route is to be used to the collector.

Template refresh time

Specifies the time in minutes after which a NetFlow template record is refreshed. The value 0 deactivates the periodic refresh of template records.

A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Template refresh packets

Specifies the number of packets after which a NetFlow template record is refreshed. The value 0 deactivates the refresh of template records based on a packet counter.

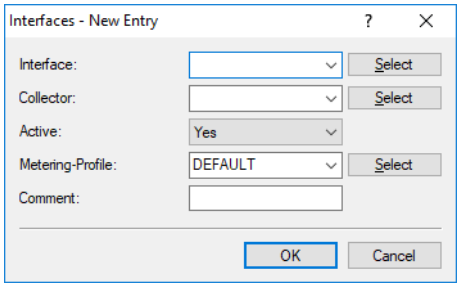
A NetFlow template packet is refreshed either after the specified time in minutes or after the corresponding number of Flow packets, whichever comes first.

Comment

Optionally enter a meaningful comment as a description.

20.9.1.2 Interfaces

You can configure the interfaces for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Interfaces**.



Interface

Logical interface on which NetFlow/IPFIX is to be activated. Possible values: IPv4, IPv6 LAN interfaces, remote sites, IPv6 RAS template. IPv4 remote sites can use a wildcard, e.g. Company*

Collector

This references an entry in the list of collectors.

Active

Enables/disables NetFlow/IPFIX for this entry for the interface and the collector.

Metering profile

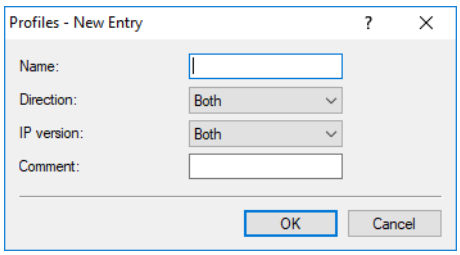
This references an entry in the Profiles list.

Comment

Optionally enter a meaningful comment as a description.

20.9.1.3 Profiles

You can configure the profiles for NetFlow/IPFIX under **Logging/Monitoring** > **Protocols** > **NetFlow/IPFIX** > **Profiles**.



Name

Unique name of the metering profile. This name is referenced in other tables.

Direction

IP flow direction to be monitored by NetFlow/IPFIX. Possible values from the perspective of NetFlow/IPFIX: Ingress, Egress, Both

IP version

IP protocol version(s) to be monitored by NetFlow/IPFIX, possible values: IPv4, IPv6, Both

Comment

Optionally enter a meaningful comment as a description.

20.10 Operating printers at the USB connector of the device

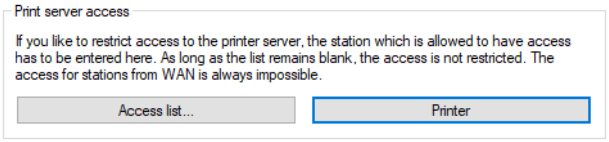
With the USB port of various models, printers can be connected to the device and provided to the entire network. The device features a print server to manage the printing jobs from the network. Supported protocols are RawIP and LPR/LPD.

Parallel print jobs arriving from different stations are saved on the respective computer. The print server in the device processes the waiting jobs sequentially.

20.10.1 Configuring the printer server in the device

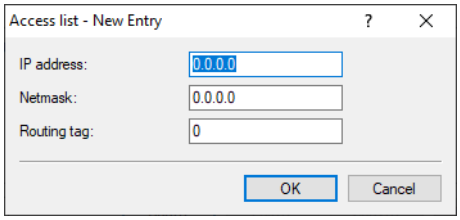
When configuring the USB port for the connection of a printer, the first thing is to define the ports which will receive the print jobs as transported by the various protocols.

In LANconfig you configure the printer server under **Management** > **Advanced** in the section **Printer server access**.



20.10.1.1 Access list

Up to 16 networks that have access to the configured printer can be entered into the access list. In LANconfig you configure the print server under **Management** > **Advanced** > **Access list**.



IP address

IP address of the network with clients requiring access to the printer.

If the access list is empty, any computer with any IP address can use the printer at the USB port of the device.

For reasons of security, access to the printer at the USB port of the device is not permitted from the WAN.

Netmask

Netmask of the permitted networks.

Routing tag

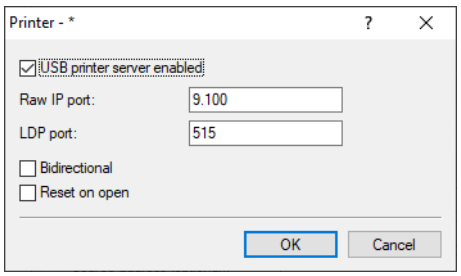
Routing tag of the network.

If you specify a routing tag for this access rule, the only packets that will be accepted have received the same tag in the firewall or they are from a network with the corresponding interface tag.

It follows that the use of routing tags only makes sense in combination with the appropriate rules in the firewall or tagged networks.

20.10.1.2 Printer

Normally there will be no need to adjust the printer settings. With the default settings, the print server works with RawIP and LPR/LPD and reacts to the standard ports as suggested by Windows when the printer connection is being configured. If printer operation does not work with these settings, the printing parameters can be adjusted. In LANconfig you configure the settings for the connected printers under **Management** > **Advanced** > **Printer**.



USB printer server enabled

Activate the print server here.

Raw IP port

This port can be used to accept print jobs over Raw IP.

Raw IP is a standard used by Windows and is recommended for operating printers at a USB port.

LDP port

This port can be used to accept print jobs over LDP.

The protocol and port options entered here must agree with the settings for the printer connection in the corresponding computer's operating system.

Bidirectional

If you activate this option, the device sends the printer status to the connected computers at regular intervals.

Reset on open

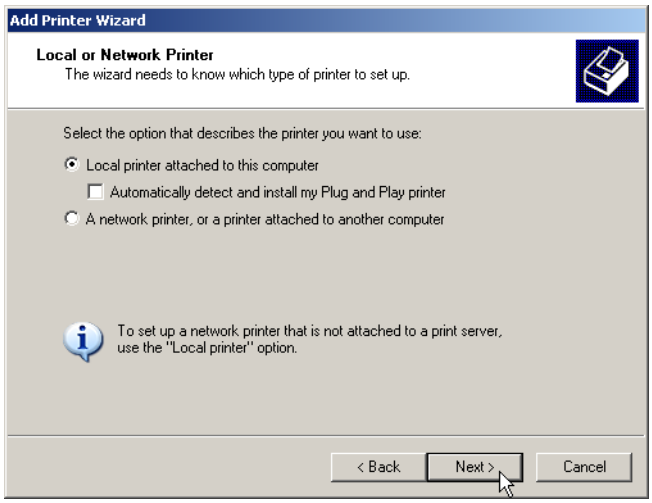
If this option is activated the device will send a reset command to the printer before opening a printer session.

Activate this option if the connection to the printer does not work as expected.

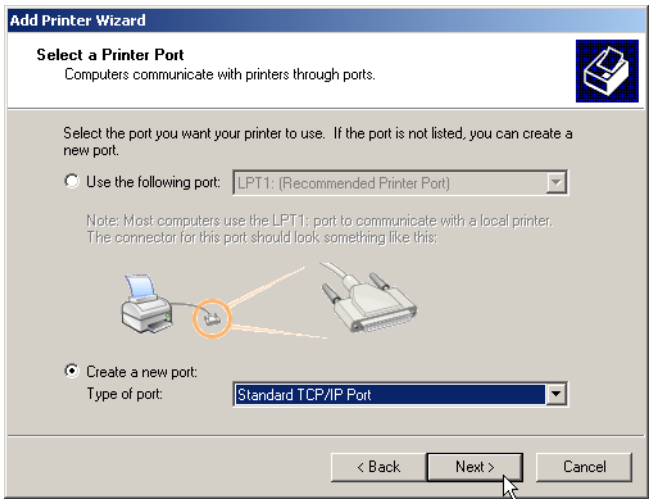
20.10.2 Printer configuration at the computer

To use the printer at the USB port over the network, the printer drivers on the computers have to be connected with a corresponding printer connection. The following is a description of the setup under Windows XP; the configuration under Windows 2000 is similar. Controlling printers via TCP/IP ports with older version of Windows is rather unsatisfactory.

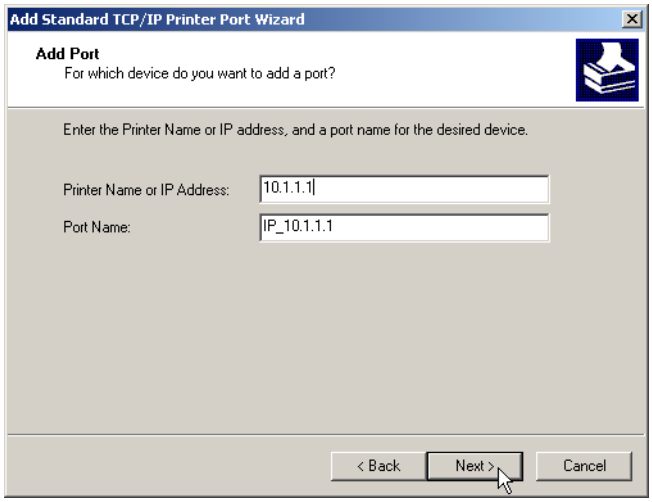
1. In the Control Panel, open the dialog for the configuration of a new printer and start the Wizard to add a new printer.
2. Select the option for a local printer and deactivate Plug&Play.



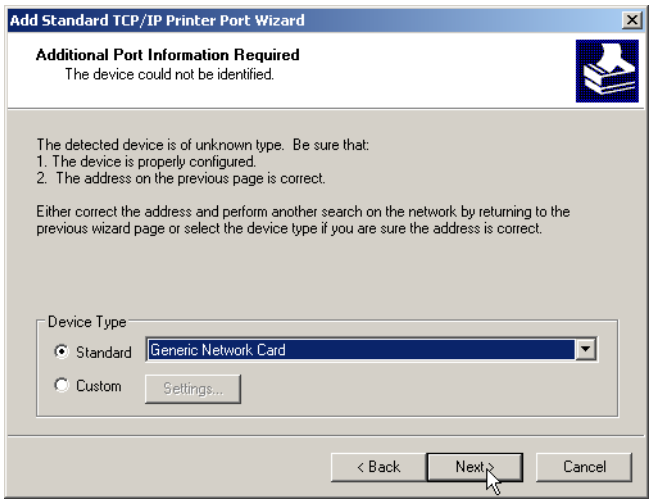
1. Select the option to add a new printer port.



1. Enter the IP address of the LANCOM as the IP address of the printer port. The name for the printer port will automatically be filled out with 'IP_<IP address of the LANCOM>'.

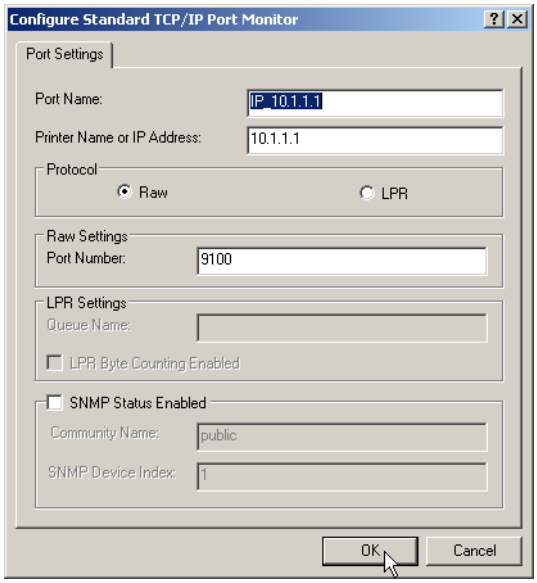


1. As the device type, select the option 'Standard' for a 'Generic Network Card'. If you wish to keep the standard settings (recommended), press on **Next** to proceed to the next dialog.



1. Alternatively, you can select 'Custom' and press on the **Settings** button to open an additional dialog. In this dialog, you can select the protocol to be used for transmitting the print jobs to the printer at the USB port of the LANCOM

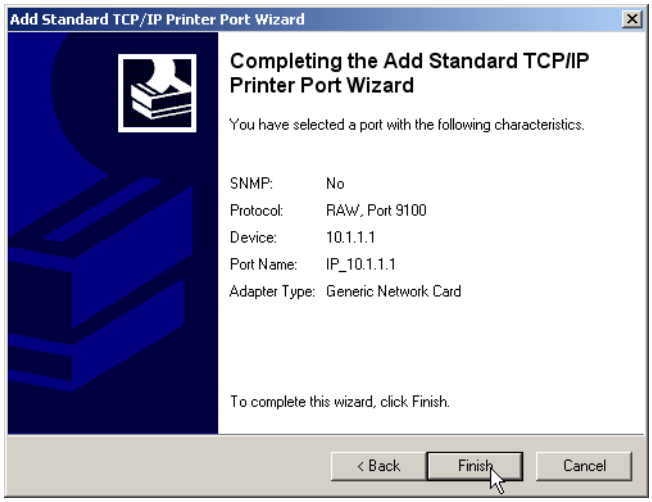
('Raw' for RawIP or 'LPR').. The port to be used can be entered here too (for RawIP only). For LPR, port '515' is always used as standard.



The protocol and port options entered here must agree with the settings for the printer in the LANCOM configuration.

The dialog for selecting the protocol and port can also be accesses via the Control Panel by opening the Printer Properties and accessing the 'Ports' tab.

1. Once the settings have been made, the printer port is set up. The Wizard now goes on with the selection of the printer driver.



Further information about the installation of a printer driver is available in the documentation for the printer.

20.11 LANCOM Security Essentials

20.11.1 Introduction

With LANCOM Security Essentials, you can filter specific content in your network to prevent access to, for example, illegal, dangerous, or offensive websites. Additionally, you can restrict private browsing on certain sites during working hours. This not only boosts employee productivity and network security but also ensures that full bandwidth is available exclusively for business processes.

LANCOM Security Essentials is an intelligent, dynamic website filter. It contacts a rating server that reliably and accurately evaluates websites based on the categories you selected.

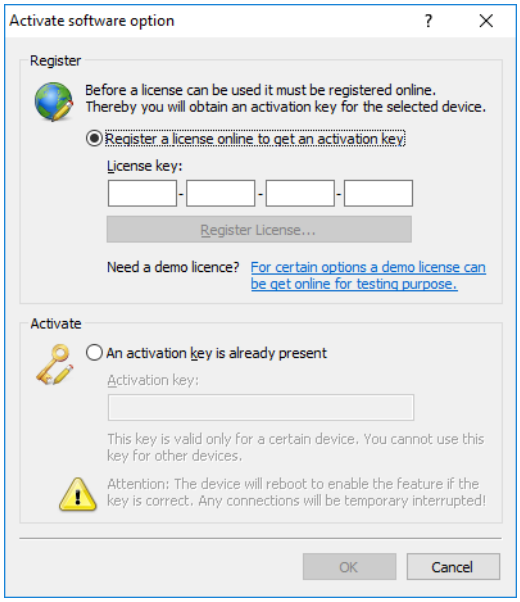
The functionality of LANCOM Security Essentials is based on checking the IP addresses determined from the entered URLs. For many pages, subdirectories within a domain are also evaluated separately so that different sections of a URL can be rated differently.

Users cannot bypass website verification by LANCOM Security Essentials by entering the IP address of a site in the browser. LANCOM Security Essentials checks both unencrypted (HTTP) and encrypted (HTTPS) websites.

The BPjM module is part of the LANCOM Security Essentials or can be obtained separately via the LANCOM BPjM Filter Option software license. The BPjM module is published by the Federal Agency for the Protection of Children and Young People in the Media (Bundeszentrale für Kinder- und Jugendmedienschutz) and blocks domains that must not be made accessible to children and adolescents in Germany.

The license you purchased for LANCOM Security Essentials applies to a specific device category and a specific time period (either one year or three years). The number of users is unlimited. You will be notified in advance when your license is about to expire.

You can test the LANCOM Security Essentials on any router that supports this function. To do so, you must activate a time-limited 30-day demo license once per device. Demo licenses are created directly from within LANconfig. Right-click the device, select **Activate Software Option** from the context menu, and in the following dialog, click the link next to **Need a demo license?**. You will automatically be connected to the LANCOM registration server website, where you can select and register the desired demo license for the device.



Category profiles store all settings related to categories. You select from predefined main and subcategories in your LANCOM Security Essentials: 73 categories are grouped into 12 thematic groups, e.g., “Pornography”, “Shopping”, or “Illegal”. Each group allows you to enable or disable the included categories. Subcategories for “Pornography” include “Pornography”, “Sex toys”, “Sexual content”, “Nudity”, “Lingerie”, and “Sex education”.

Additionally, administrators can enable an override option for each category during configuration. When override is active, users can temporarily access a blocked site by clicking a corresponding button—but the administrator will receive a notification via e-mail, SYSLOG, and/or SNMP trap.

Using the category profile you created, along with the whitelist and blacklist, you can create a content filter profile that can be assigned to users via the firewall. For example, you can create the profile “Employees_Department_A”, which is then assigned to all computers in that department.

During installation, LANCOM Security Essentials automatically sets up useful default settings that only need to be activated for initial operation. In subsequent steps, you can further adapt the behavior of LANCOM Security Essentials to your specific use case.

Useful default settings are also automatically configured for the BPjM module. For example, there is a default firewall rule in the IPv4 or IPv6 firewall with the system object “BPJM” as the destination station. Define the source stations as the networks that should be protected by the BPjM module. By activating the rule, the BPjM module is started.

20.11.2 Requirements for using LANCOM Security Essentials

The following requirements must be met in order to use LANCOM Security Essentials:

1. The LANCOM Security Essentials option is activated.
2. The firewall must be enabled.
3. A firewall rule must select the content filter profile.
4. The selected content filter profile must define a category profile and optionally a white and/or blacklist for every time period of the day. To cover different time periods, a content filter profile can consist of multiple entries.

   If a specific time period is not covered by an entry, unrestricted access to websites will be possible during that time.

   If the content filter profile is renamed later, the firewall rule must also be adjusted.

20.11.3 Quick start

After installing the LANCOM Security Essentials, all settings are preconfigured for quick commissioning.

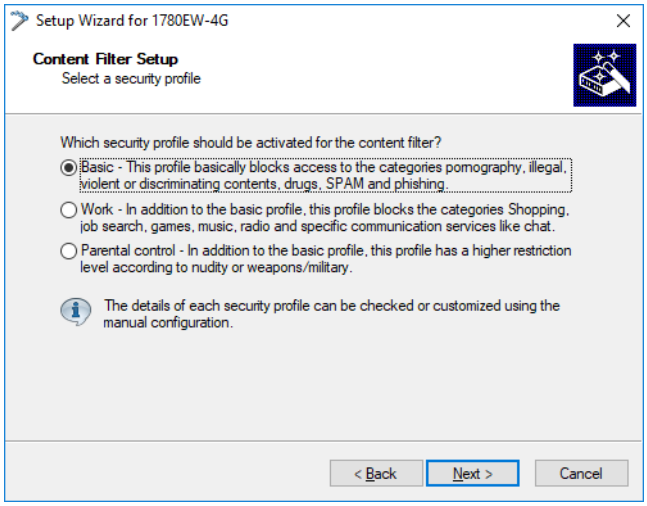
The operation of the LANCOM Security Essentials may be subject to data protection regulations in your country or to company policies. Please check applicable rules before commissioning.

In LANconfig, the settings of the LANCOM Security Essentials are listed under **Content Filter**.

Activate the content filter using the following steps:

1. Launch the setup wizard for the corresponding device.

2. Select the setup wizard for configuring the content filter.



3. Select one of the predefined security profiles (Basic Profile, Corporate Profile, Parental Control Profile):

   - Basic profile: This profile mainly blocks access to categories such as pornography, illegal, violent or discriminatory content, drugs, spam, and phishing.
   - Work profile: In addition to the Basic Profile settings, this profile also blocks categories such as shopping, job search, games, music, radio, and certain communication services like chat.
   - Parental control profile: In addition to the Basic Profile settings, this profile includes stricter blocking for nudity and weapons.

   If the firewall is disabled, the wizard will enable it. The wizard then checks whether the firewall rule for the content filter is set correctly and adjusts it if necessary. With these steps, the content filter is activated, and the default settings will apply to all stations in the network using the selected content filter profile with empty blacklists and whitelists. Adjust these settings to suit your needs if necessary. The wizard activates the content filter for the time frame ALWAYS.

20.11.4 Standard settings in the Content Filter

The following elements have been created in the default configuration of the Content Filter:

Firewall rule

The preset firewall rule is named CONTENT-FILTER and uses the action object CONTENT-FILTER-BASIC.

Firewall action objects

There are three firewall action objects:

- CONTENT-FILTER-BASIC
- CONTENT-FILTER-WORK
- CONTENT-FILTER-PARENTAL-CONTROL

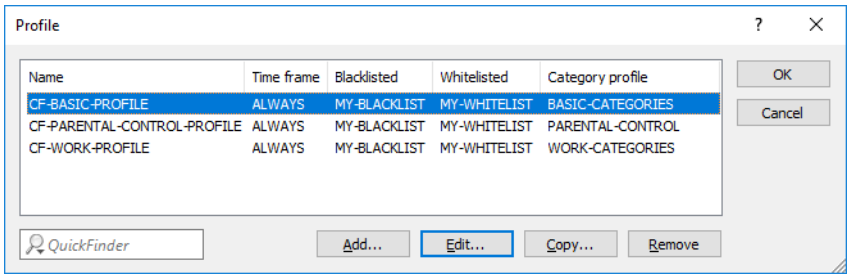
These action objects work with the corresponding content-filter profiles.

Content filter profiles

There are three content filter profiles. All content-filter profiles use the timeframe ALWAYS, the blacklist MY-BLACKLIST and the whitelist MY-WHITELIST. Each content-filter profile uses one of the predefined category profiles:

- CF-BASIC-PROFILE: This content-filter profile features a low level of restrictions and works with the category profile BASIC-CATEGORIES.

- CF-PARENTAL-CONTROL-PROFILE: This content-filter profile protects minors (e.g. trainees) from unsuitable Internet content, and it works with the category profile PARENTAL-CONTROL.
- CF-WORK-PROFILE: This content-filter profile is intended for companies wishing to place restrictions on categories such as Job Search or Chat. It works with the category profile WORK-CATEGORIES.



Timeframe

There are two predefined timeframes:

- ALWAYS: 00.00-23.59 hrs
- NEVER: 00.00-0.00 hrs

Blacklist

The preset blacklist is named MY-BLACKLIST and it is empty. Here you can optionally enter URLs which are to be forbidden.

Whitelist

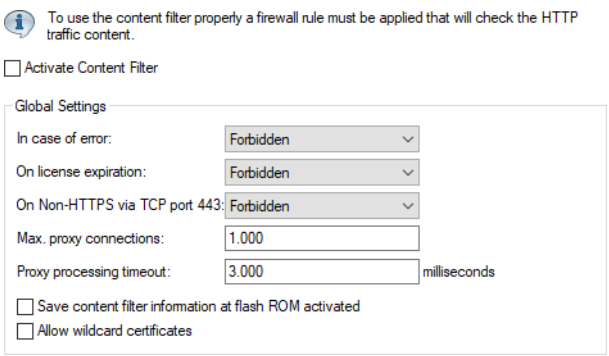
The preset whitelist is named MY-WHITELIST and it is empty. Here you can optionally enter URLs which are to be allowed.

Category profiles

There are three category profiles: BASIC-CATEGORIES, WORK-CATEGORIES and PARENTAL-CONTROL. The category profile specifies the categories which are to be allowed and forbidden, and for which one an override can be activated.

20.11.5 General Settings

You can make global content filter settings in LANconfig under **Content Filter** > **General**:



Activate Content Filter

This allows you to activate the content filter.

In case of error

This lets you define what happens in the event of an error. For example, if the rating server cannot be reached, this setting determines whether the user can browse freely or if all web access is blocked.

On license expiration

The license for using LANCOM Security Essentials is valid for a specific period. You will be reminded of the upcoming license expiration 30 days, one week, and one day in advance (to the email address configured in LANconfig under **Log & Trace** > **General** > **E-mail addresses** > **E-mail for license expiry reminder**).

Here, you can specify whether websites should be blocked or passed through unchecked after license expiration. Based on this setting, the user can either browse freely after the license expires or all web access will be denied.



To ensure the reminder is actually sent to the specified email address, you must configure the appropriate SMTP account.

On Non-HTTPS via TCP port 443

Forbidden

Disallows non-HTTPS traffic on port 443.

Allowed

Allows non-HTTPS traffic on port 443.

TCP port 443 is reserved by default exclusively for HTTPS connections.

Some applications that do not use HTTPS still use TCP port 443. In such cases, you can allow TCP port 443 to accept non-HTTPS traffic.



If you allow non-HTTPS connections on port 443, the traffic will not be classified but instead generally permitted. By default, non-HTTPS traffic on port 443 is not allowed.

Max. proxy connections

Set the maximum number of simultaneous proxy connections allowed. This helps limit system load. A notification is triggered if this number is exceeded. You can configure the type of notification under **Content Filter** > **Options** > **Event notification**.

Proxy processing timeout

Specify the time in milliseconds the proxy is allowed for processing. If this time is exceeded, a timeout error page is returned.

Save Content Filter information to flash ROM activated

If enabled, this option stores content filter information in the device's Flash ROM.

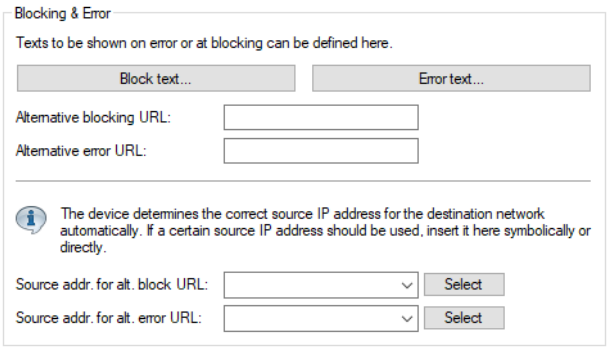
Allow wildcard certificates

For websites using wildcard certificates (with CN entries such as `*.mydomain.de`), enabling this function uses the main domain (`mydomain.de`) for filtering. The filtering process occurs in the following order:

- Check the server name in the "Client Hello" (depending on the browser used)
- Check the CN in the received SSL certificate
- Wildcard entries are ignored
- If the CN is not usable, the "Alternative Name" field is evaluated
- DNS reverse lookup of the corresponding IP address and evaluation of the resulting hostname
- If wildcards are included in the certificate, the main domain is used instead (as described above)
- Check the IP address

20.11.6 Settings for blocking

You adjust the website-blocking settings here:



LANconfig: **Content filter** > **Blocking / Override** > **Blocking & error**

Command line: **Setup** > **UTM** > **Content-Filter** > **Global-Settings**

Alternative blocking URL:

This is where you can enter the address of an alternative URL. If access is blocked, the URL entered here will be displayed instead of the requested web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the blocking text. If you do not make any entry here, the default page stored in the device will be displayed..

Possible values:

› Valid URL address

Default:

› Blank

Alternative error URL:

This is where you can enter the address of an alternative URL. In the event of an error, the URL entered here will be displayed instead of the usual web site. You can use this external HTML page to display your company's corporate design, for example, or to perform functions such as JavaScript routines, etc. You can also use the same tags here as used in the error text. If you do not make any entry here, the default page stored in the device will be displayed..

Possible values:

› Valid URL address

Default:

› Blank

Source addr. for alt. block URL:

This is where you can configure an optional sender address to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

Default:

› Blank

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

Source addr. for alt. error URL:

This is where you can configure an optional sender address to be used instead of the one that would normally be automatically selected for this target address. If you have configured loopback addresses, you can specify them here as sender address.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

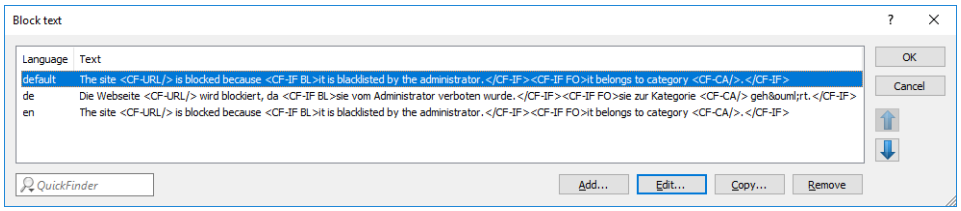
Default:

- Blank

If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

20.11.6.1 Block text

This is where you can define text to be displayed when blocking occurs. Different blocking texts can be defined for different languages. The display of blocking text is controlled by the language setting transmitted by the browser (user agent).



Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

Text

Enter the text that you wish to use as block text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use special tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for a forbidden URL
- <CF-CATEGORIES/> for the list of categories why the web site was blocked
- <CF-PROFILE/> for the profile name
- <CF-OVERRIDEURL/> for the URL used to activate the URL (this can be integrated in a simple <a> tag or in a button)
- <CF-LINK/> adds a link for activating the override
- <CF-BUTTON/> for a button for activating the override
- <CF-IF att1 att2> … </CF-IF> to display or hide parts of the HTML document. The attributes are:
  - BLACKLIST: If the site was blocked because it is in the profile blacklist
  - CATEGORY: If the site was blocked due to one of its categories
  - ERR: If an error has occurred.
  - OVERRIDEOK: If users have been allowed an override (in this case, the page should display an appropriate button)

    Since there are separate text tables for the blocking page and the error page, this attribute only makes sense if you have configured an alternative URL to show on blocking.

If several attributes are defined in one tag, the section will be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

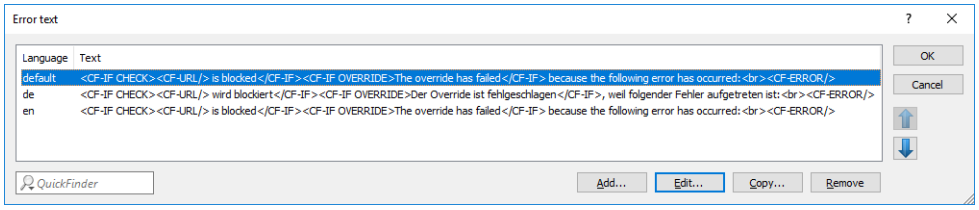
- Example:

  <CF-URL/> is blocked because it matches the categories <CF-CA/>. Your content profile is <CF-PR/>. <CF-IF OVERRIDEOK> <CF-BU/></CF-IF>

The tags described here can also be used in external HTML pages (alternative URLs to show on blocking).

20.11.6.2 Error text

This is where you can define text to be displayed when an error occurs.



Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

Text

Enter the text that you wish to use as error text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use HTML tags for the error text.

The following empty element tags can be used as tag values:

- <CF-URL/> for a forbidden URL
- <CF-PROFILE/> for the profile name
- <CF-ERROR/> for the error message
- Example:

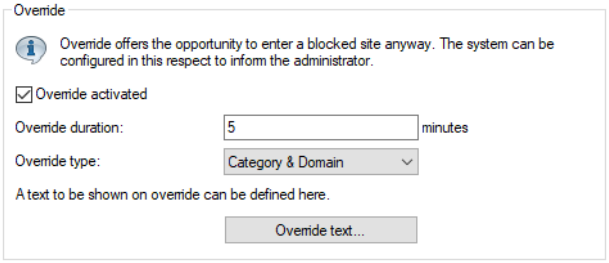
  <CF-URL/> is blocked because an error has occurred: <CF-ERROR/>

20.11.7 Override settings

The override function allows a website to be accessed even though it is classified as forbidden. The user must click on the override button to request the forbidden page to be opened. You can configure this feature so that the administrator is notified when the override button is clicked (LANconfig: **Content filter** > **Options** > **Events**).

If the override type "Category" has been activated, clicking on the override button makes **all** of the categories for that URL accessible to the user The next blocking page to be displayed has just one category explaining why access to the URL was blocked. If the override type "Domain" has been activated, then the entire domain can be accessed.

The settings for the override function are to be found here:



LANconfig: **Content filter** > **Blocking / Override** > **Override**

Command line: **Setup** > **UTM** > **Content-Filter** > **Global-Settings**

Override-Active

This is where you can activate the override function and make further related settings.

Override duration

The override duration can be restricted here. When the period expires, any attempt to access the same domain and/or category will be blocked again. Clicking on the override button once more allows the web site to be accessed again for the duration of the override and, depending on the settings, the administrator will be notified once more.

Possible values:

- 1-1440 (minutes)

Default:

- 5 (minutes)

Override type:

This is where you can set the type of override. It can be allowed for the domain, for the category of web site to be blocked, or for both.

Possible values:

Category

For the duration of the override, all URLs are allowed that fall under the affected categories (as well as those which would already have been allowed even without the override).

Domain

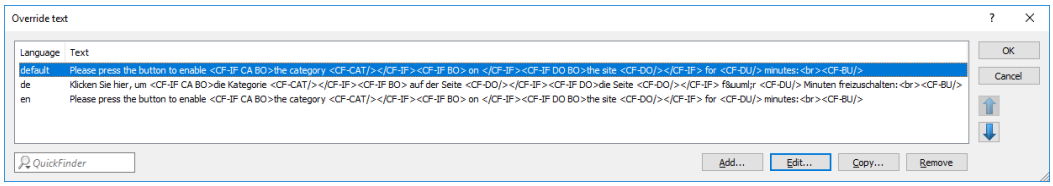
For the duration of the override all URLs in this domain are allowed, irrespective of the categories they belong to.

Category-and-Domain

For the duration of the override, all URLs are allowed that belong to this domain and also to the allowed categories. This is the highest restriction.

20.11.7.1 Override text

This is where you can define text that is displayed to users confirming an override.



Language

Entering the appropriate country code here ensures that users receive all messages in their browser's preset language. If the country code set in the browser is found here, the matching text will be displayed.

You can add any other language.

Examples of the country code:

- de-DE: German-Germany
- de-CH: German-Switzerland
- de-AT: German-Austria
- en-GB: English-Great Britain
- en-US: English-United States

The country code must match the browser language setting exactly, e.g. “de-DE” must be entered for German (“de” on its own is insufficient). If the country code set in the browser is not found in this table, or if the text stored under that country code is deleted, the predefined default text ("default") will be used. You can modify the default text.

Possible values:

- 10 alphanumerical characters

Default:

- Blank

Text

Enter the text that you wish to use as override text for this language.

Possible values:

- 254 alphanumerical characters

Default:

- Blank

Special values:

You can also use HTML tags for blocking text if you wish to display different pages depending on the reason why the web site was blocked (e.g. forbidden category or entry in the blacklist).

The following tags can be used as tag values:

- <CF-URL/> for the originally forbidden URL that is now allowed
- <CF-CATEGORIES/> for the list of categories that have now been allowed as a result of the override (except if domain override is specified).
- <CF-BUTTON/> displays an override button that forwards the browser to the original URL.
- <CF-BUTTON/> displays an override link that forwards the browser to the original URL.
- <CF-HOST/> or <CF-DOMAIN/> displays the host or the domain for the allowed URL. The tags are of equal value and their use is optional.
- <CF-ERROR/> generates an error message in the event that the override fails.
- <CF-DURATION/> displays the override duration in minutes.
- <CF-IF att1 att2> … </CF-IF> to display or hide parts of the HTML document. The attributes are:
  - CATEGORY when the override type is "Category" and the override was successful
  - DOMAIN when the override type is "Domain" and the override was successful
  - BOTH when the override type is "Category-and-Domain" and the override was successful
  - ERROR when the override fails
  - OK if either CATEGORY or DOMAIN or BOTH are applicable

  If several attributes are defined in one tag, the section should be displayed if at least one of these conditions is met. All tags and attributes can be abbreviated to the first two letters (e.g. CF-CA or CF-IF BL). This is necessary as the blocking text may only contain a maximum of 254 characters.

  - Example:

    <CF-IF CA BO>The categories <CF-CAT/> are</CF-IF><CF-IF BO> in the domain <CF-DO/></CF-IF><CF-IF DO>The domain <CF-DO/> is</CF-IF><CF-IF OK> released for <CF-DU/> minutes. <CF-LI/></CF-IF><CF-IF ERR>Override error: <CF-ERR/></CF-IF>

20.11.8 Profiles in the Content Filter

Under **Content Filter** > **Profiles** you can create content-filter profiles that are used to check web sites for prohibited content. A content-filter profile always has a name and, for various time periods, it activates the desired category profile and, optionally, a blacklist and a whitelist.

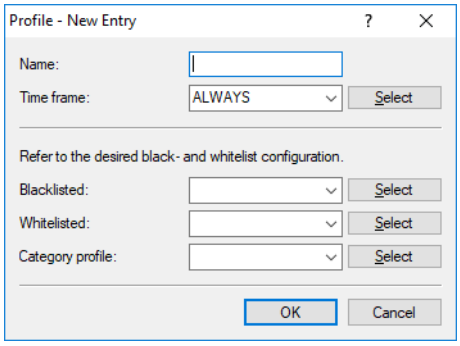
In order to provide different configurations for the various timeframes, several content-filter profile entries are created with the same name. The content-filter profile is thus made up of the sum of all entries with the same name.

The firewall refers to this content-filter profile.

Please note that you must make corresponding settings in the firewall in order to use the profiles in the LANCOM Content Filter.

20.11.8.1 Profiles

The settings for the profiles are to be found here:



LANconfig: **Content filer** > **Profiles** > **Profile**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Profile**

Name

The profile name that the firewall references must be specified here.

Timeframe

Select the timeframe for this category profile and, optionally, the blacklist and the whitelist. The timeframes ALWAYS and NEVER are predefined. You can configure other timeframes under:

LANconfig: **Date & time** > **General** > **Time frame**

Command line: **Setup** > **Time** > **Timeframe**

One profile may contain several lines with different timeframes.

Possible values:

- Always
- Never
- Name of a timeframe profile

If multiple entries are used for a content-filter profile and their timeframes overlap, then all pages contained in the active entries will be blocked for that period of time. If multiple entries are used for a content-filter profile and a time period remains undefined, access to all web sites will be unchecked for this period.

Blacklist

Name of the blacklist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the blacklist table.

Possible values:

- Name of a blacklist profile
- New name

Whitelist

Name of the whitelist profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the whitelist table.

Possible values:

- Name of a whitelist profile
- New name

Category profile

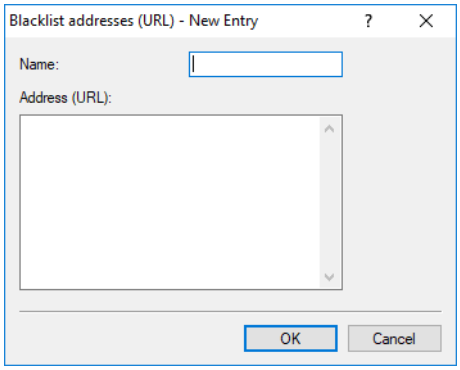
Name of the category profile that is to apply for this content filter profile during the period in question. A new name can be entered, or an existing name can be selected from the category table.

Possible values:

- Name of a category profile
- New name

20.11.8.2 Blacklist addresses (URL)

This is where you can configure those web sites that are to be blocked.



LANconfig: **Content files** > **Profiles** > **Blacklist addresses (URL)**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Blacklist**

Name

Enter the name of the blacklist for referencing from the content-filter profile.

Possible values:

- Blacklist name

Address (URL)

Access to the URLs entered here will be forbidden by the blacklist.

Possible values:

- Valid URL address

The following wildcard characters may be used:

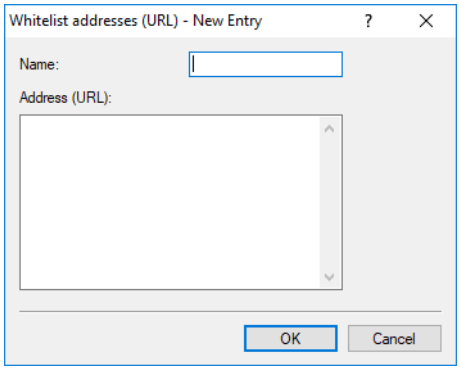
- * for any combination of more than one character (e.g. www.lancom.* encompasses the web sites www.lancom.com, www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)

URLs must be entered **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. "www.mycompany.de/". For this reason it is advisable to enter the URL as: "www.mycompany.de*".

Individual URLs are separated by a blank.

20.11.8.3 Whitelist addresses (URL)

This is where you can configure web sites to which access is to be allowed.



LANconfig: **Content files** > **Profiles** > **Whitelist addresses (URL)**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Whitelist**

Name

Enter the name of the whitelist for referencing from the content-filter profile.

Possible values:

- Name of a whitelist

Address (URL)

This is where you can configure web sites which are to be checked locally and then accepted.

Possible values:

- Valid URL address

The following wildcard characters may be used:

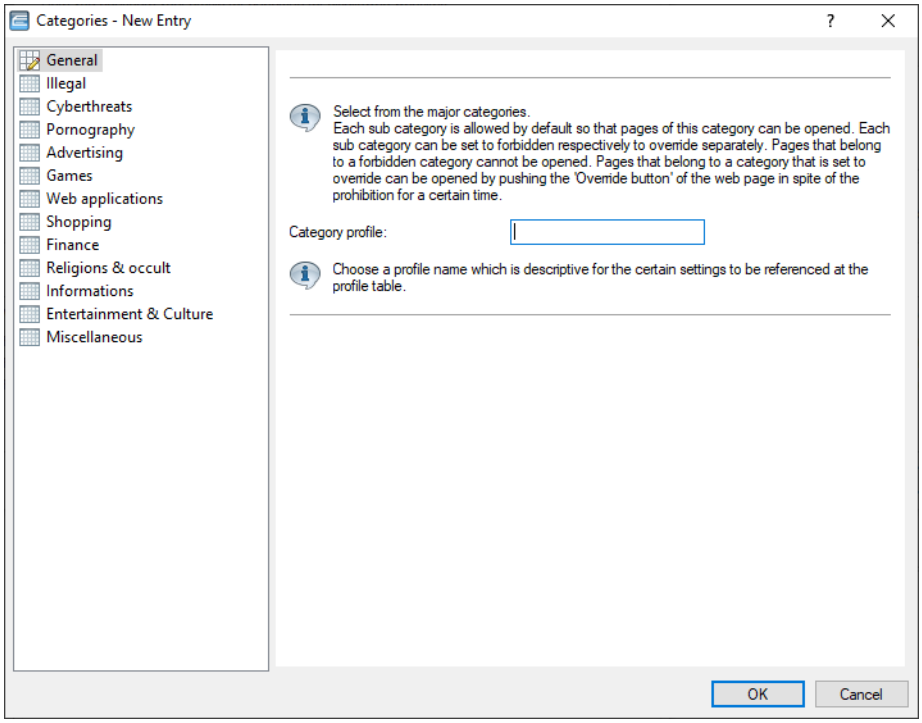
- * for any combination of more than one character (e.g. www.lancom.* encompasses the web sites www.lancom.com, www.lancom.de, www.lancom.eu, www.lancom.es, etc.)
- ? for any one character (e.g. www.lancom.e* encompasses the web sites www.lancom.eu, www.lancom.es)

URLs must be entered **without** the leading http://. Please note that in the case of many URLs a forward slash is automatically added as a suffix to the URL, e.g. "www.mycompany.de/". For this reason it is advisable to enter the URL as: "www.mycompany.de*".

Individual URLs are separated by a blank.

20.11.8.4 Category profiles

Here you create a category profile and determine which categories or groups should be used to rate web sites for each category profile. You can allow or forbid the individual categories or activate the override function for each group.



LANconfig: **Content Filter** > **Profiles** > **Categories**

Command line: **Setup** > **UTM** > **Content-Filter** > **Profiles** > **Category-Profile**

Category profile

The name of the category profile for referencing from the content-filter profile is entered here.

Possible values:

- Name of a category profile

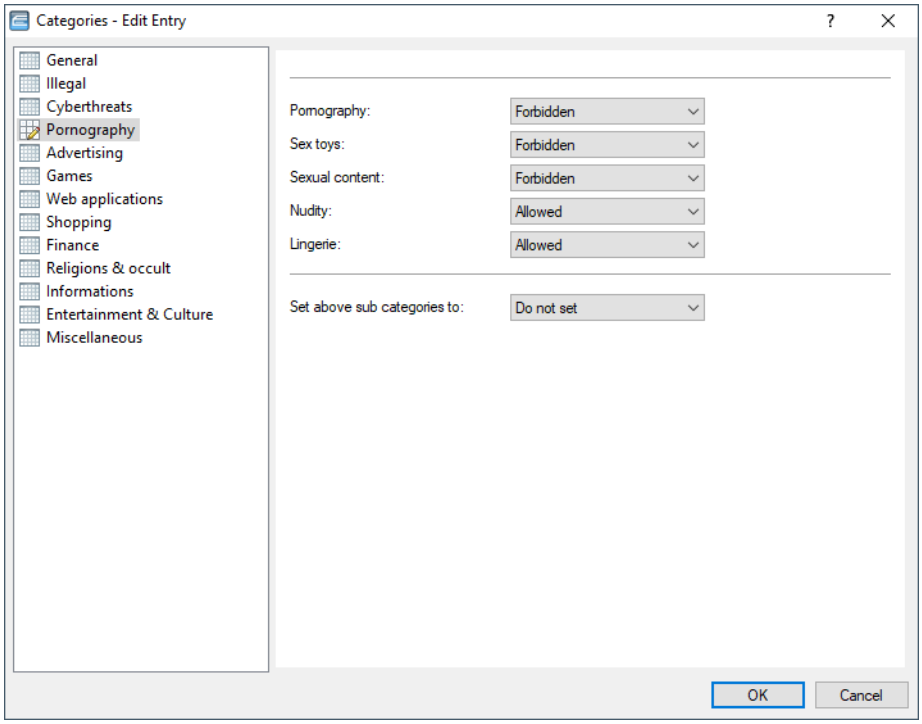
Category settings

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

The following main categories can be configured:

- Illegal
- Cyberthreats
- Pornography
- Advertising
- Games
- Web applications
- Shopping
- Finance
- Religions & occult
- Informations
- Entertainment & Culture

› Miscellaneous



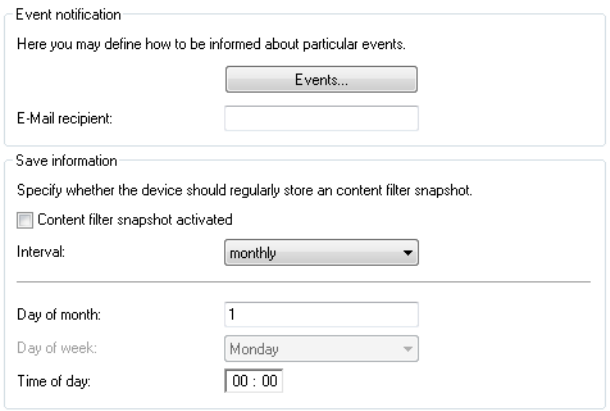
The category profile must then be assigned to a content-filter profile together with a time frame in order to become active.

Possible values:

› Allowed, forbidden, override

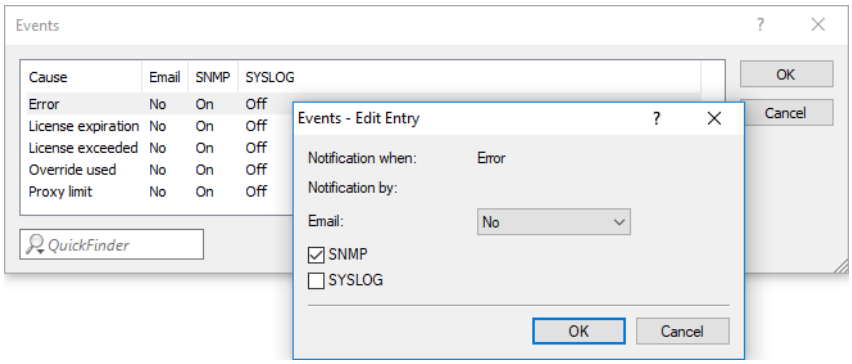
20.11.9 Options for the Content Filter

Under **Content Filter** > **Options** you determine whether you wish to be notified of events and where Content Filter information is to be stored.



Events

This is where you define how you wish to receive notification of specific events. Notification can be made by e-mail, SNMP or SYSLOG. For different event types you can specify whether messages should be output and, if so, how many.



E-mail

Here, you specify if and how e-mail notification takes place:

- **No**

  No e-mail notification is issued for this event.

- **Immediately**

  Notification occurs when the event occurs.

- **Daily**

  The notification occurs once per day.

Notifications can be sent for the following events:

Error

For SYSLOG: Source “System”, priority “Alert”.

Default: SNMP notification

License expiry

For SYSLOG: Source “Admin”, priority “Alert”.

Default: SNMP notification

License exceeded

For SYSLOG: Source “Admin”, priority “Alert”.

Default: SNMP notification

Override applied

For SYSLOG: Source “Router”, priority “Alert”.

Default: SNMP notification

Proxy limit

For SYSLOG: Source “Router”, priority “Info”.

Default: SNMP notification

E-mail recipient

An SMTP client must be defined if you wish to use the e-mail notification function. You can use the client in the device, or another client of your choice.

No e-mail will be sent if no e-mail recipient is specified.

Content Filter snapshot

This is where you can activate the content filter snapshot and determine when and how often it should be taken. The snapshot copies the category statistics table to the last snapshot table, overwriting the old contents of the snapshot table. The category statistics values are then reset to 0.

Interval

Here you decide whether the snapshot should be taken monthly, weekly or daily.

Possible values:

- Monthly
- Weekly
- Daily

Day of month

For monthly snapshots, set the day of the month when the snapshot should be taken. Possible values:

- 1-31

It is advisable to select a number between 1 and 28 in order to ensure that it occurs every month.

Day of week

For weekly snapshots, set the day of the week when the snapshot should be taken. Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Time of day:

If you require a daily snapshot, then enter here the time of day for the snapshot in hours and minutes. Possible values:

- Format HH:MM (default: 00:00)

20.11.10 Additional settings for the Content Filter

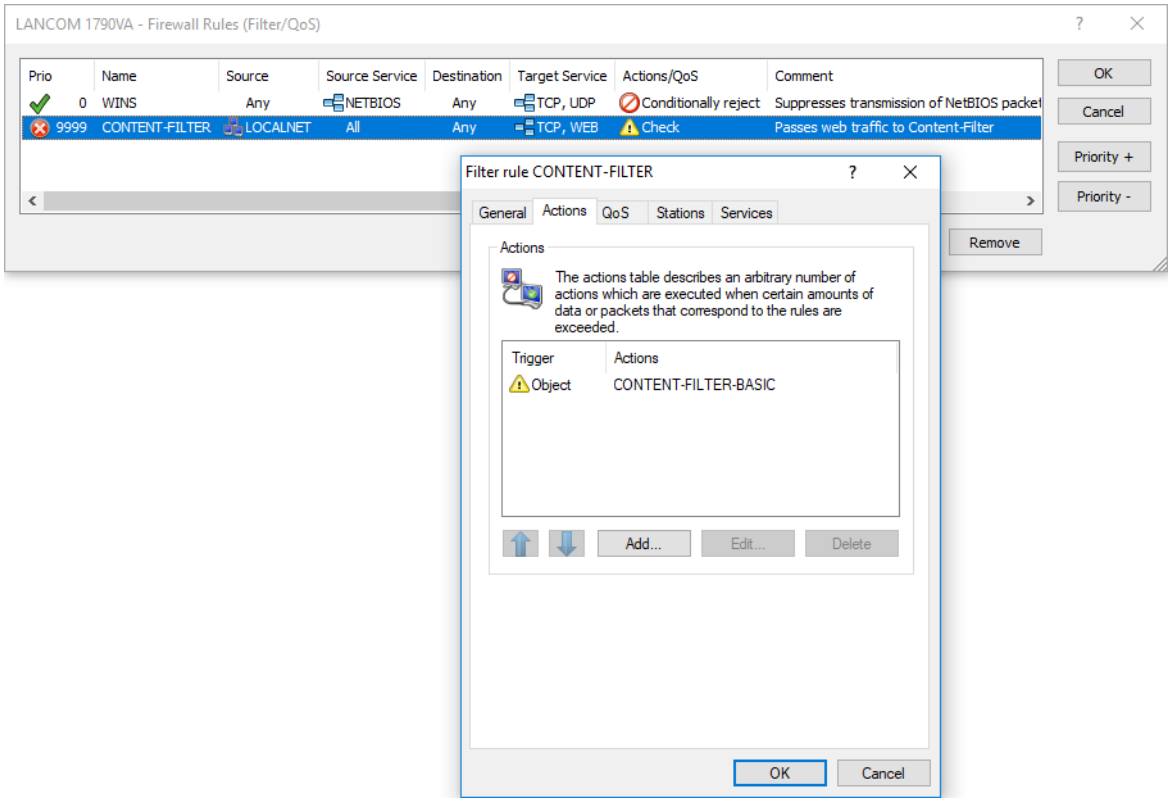
20.11.10.1 Firewall settings for the content filter

The firewall must be activated in order for the Content Filter to function. You can activate the firewall under:

LANconfig: **Firewall/QoS** > **General**

Command line: **Setup** > **IP-Router** > **Firewall**

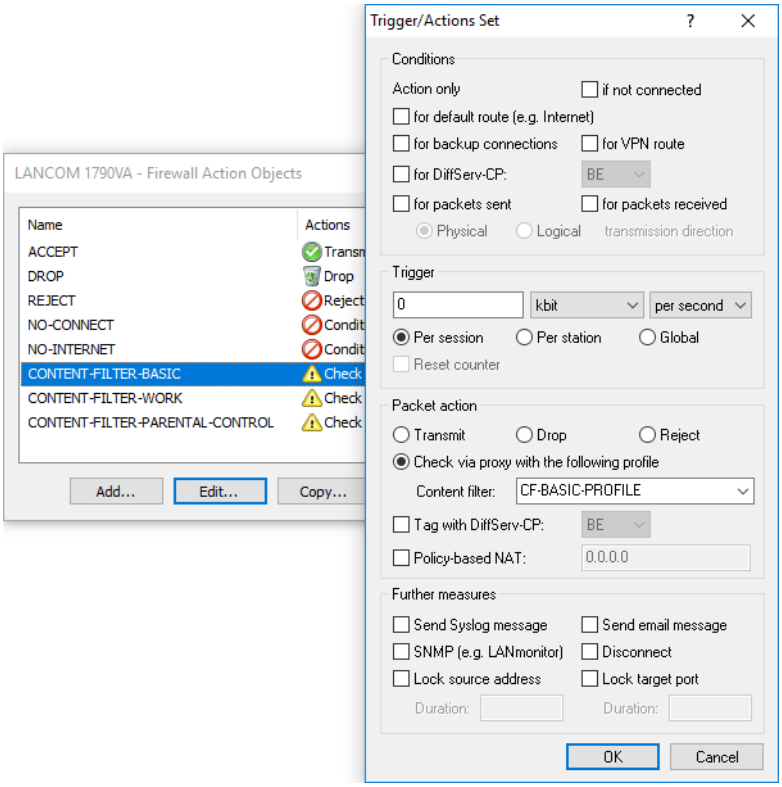
In the default configuration, you will find the firewall rule CONTENT-FILTER that refers to the action object CONTENT-FILTER-BASIC:



The firewall rule should be limited to the target services HTTP and HTTPS so that only outgoing HTTP and HTTPS connections are examined. Without this restriction all packets will be checked by the content filter, which could lead to a loss of system performance.

A content-filter related firewall rule must contain a special action object that uses packet actions to check the data according to a content-filter profile. In the default configuration you will find the action objects CONTENT-FILTER-BASIC,

CONTENT-FILTER-WORK and CONTENT-FILTER-PARENTAL-CONTROL, each of which refer to their corresponding content-filter profile:



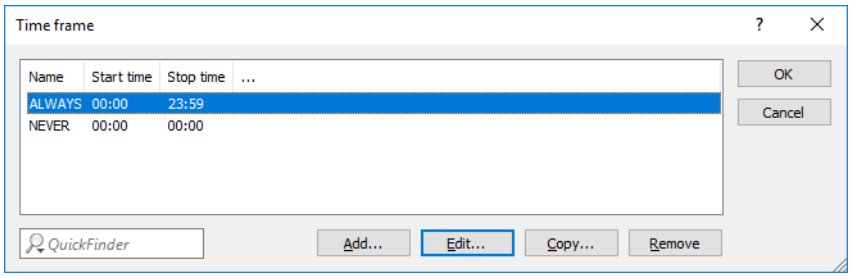
Example: When a web page is accessed, the data packets pass through the firewall and are processed by the rule CONTENT-FILTER. The action object CONTENT-FILTER-BASIC checks the data packets using the content-filter profile CONTENT-FILTER-BASIC.

20.11.10.2 Timeframe

Time frames are used with the Content Filter to define the times when the content-filter profiles apply. One profile may contain several lines with different timeframes. Different lines in a timeframe should complement one another, i.e. if you specify WORKTIME you will should probably specify a timeframe called FREETIME to cover the time outside of working hours.

Time frames can also be used to prevent a WLAN SSID from being broadcast permanently. This can be added to the logical WLAN settings.

The timeframes ALWAYS and NEVER are predefined. You can configure other timeframes under:



LANconfig: **Date & time** > **General** > **Time frame**

Command line: **Setup** > **Time** > **Timeframe**

Name

Enter the name of the time frame for referencing from the content-filter profile or by a WLAN SSID. Several entries with the same name result in a common profile.

Possible values:

› Name of a timeframe

Start

Here you set the start time (time of day) when the selected profile becomes valid.

Possible values:

› Format HH:MM (default: 00:00)

Stop

Here you set the stop time (time of day) when the selected profile ceases to be valid.

Possible values:

› Format HH:MM (default: 23:59)

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

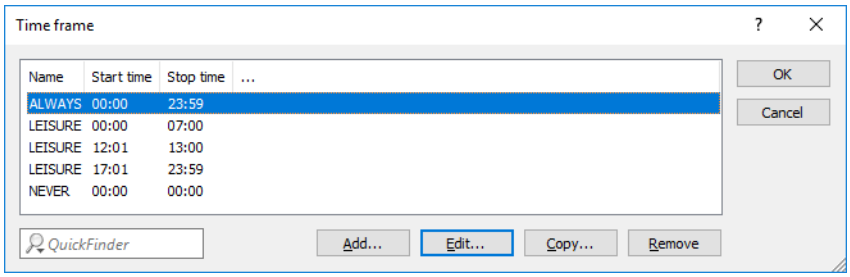
Here you select the weekday on which the timeframe is to be valid.

Possible values:

› Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

The holidays are set under **Date & Time** > **General** > **Public holidays**.

You can form a time schedule with the same name but with different times extending over several lines:



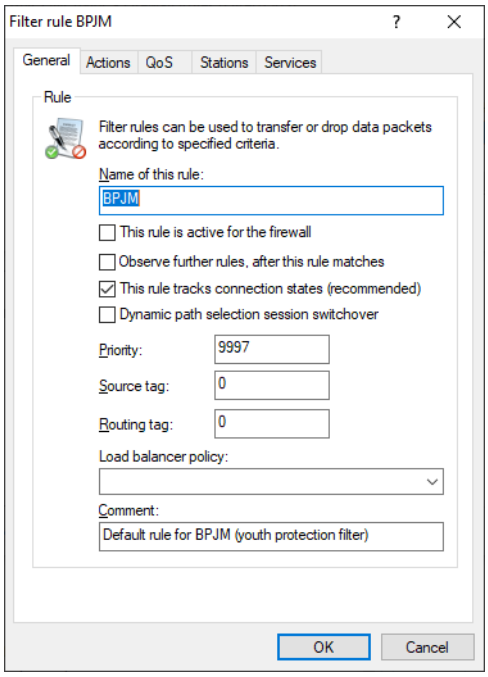
20.12 BPjM module

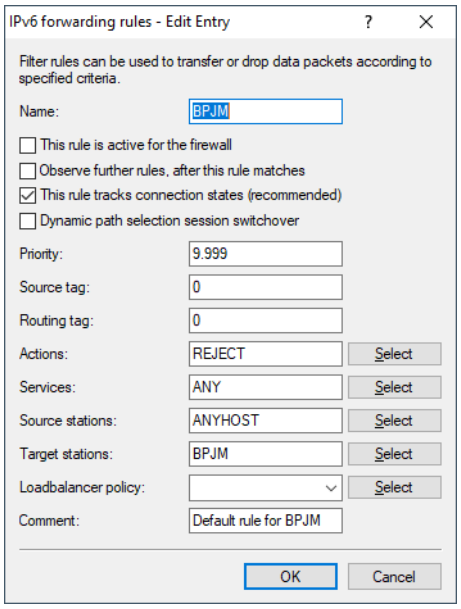
The BPjM module was setup by Germany's Federal Review Board for Media Harmful to Minors (BPjM) and blocks websites that should not be accessible to children and young people. This feature is particularly relevant for schools and educational institutions with underage students. DNS-Domains with content that is officially classified as harmful to minors cannot be accessed by the relevant target group. This list is guaranteed to be automatically updated and extended on a regular basis. The BPjM module blocks DNS-Domains that are listed on the official website of the Federal Review Board for Media Harmful to Minors (BPjM) in Germany. Blocking by category and overrides (allow) are not available.

The BPjM module is available as part of the LANCOM Content Filter option or separately via the LANCOM BPjM Filter software option.

The IPv4 or IPv6 firewalls implement this feature with a default firewall rule that can be activated and configured for each network. For example, it is possible to equip only the students' network with this filter, but exclude other networks from it.

The IPv6 firewall features a new default rule BPJM, which is deactivated by default with the system object "BPJM" as the destination station. A similar rule is available in the IPv4 firewall. The networks to be protected by the BPjM module are specified as source stations.





Further settings can be found in LANconfig under **Miscellaneous Services** > **Services** > **BPjM filter**.



Source address

Source address used by the BPjM module to access the server for BPjM signature updates.

20.12.1 Recommendations for use

If content filters and BPJM filters are to be used together, both rules must be configured with different priorities so that they are run through one after the other.

Likewise, for the first rule, care must be taken to ensure that the item "Observe further rules, after this rule matches" is activated.

In rare cases, the BPJM module may block desired domains because only (DNS) domains and not URL directory levels can be checked due to TLS. In this case, these desired domains can be added to the "BPJM Allow list", e.g. *.example.com.

The LANCOM router must serve as DNS server or DNS forwarder in the network, i.e. clients in the local network must use the router as DNS server. In addition, the direct use of DNS-over-TLS and DNS-over-HTTPS (possibly browser-internal) with external DNS servers by clients must be prevented.

This can be achieved as follows:

- The DHCP server must distribute the router's IP address as the DNS server (set up by default by the Internet Wizard).
- Set up firewall rules that prevent direct use of external DNS servers, for example. by blocking outgoing port 53 (UDP) for clients from the corresponding source network.
- Setting up firewall rules that prevent direct use of external DNS servers supporting DNS-over-TLS, e.g. by blocking outgoing port 853 (TCP) for clients from the corresponding source network.
- Disabling DNS-over-HTTPS (DoH) in the browser.

Notes on synchronizing the firewall's DNS database:

Because the firewall learns its information from client DNS requests, in certain situations the DNS database may not yet be complete. This can happen in the following situations:

- A new firewall rule is added, but the client still has a DNS record cached.
- Shortly after the router reboots and the client still has a DNS record cached.

In these cases, clearing the DNS cache on the client, rebooting the client, or timing out the DNS record on the client will help.

If different DNS names resolve to the same IP address, then they cannot be distinguished. In this case, the first rule that references one of these DNS names always applies. This should not be a problem with large service providers. However, it could occur with small websites hosted by the same provider.

20.12.2 Menu action to delete the BPjM signature definition

You can use the CLI to delete the BPjM signature definition from the router's file system. To do this, execute the command `do /Status/Firewall/BPJM/Delete-Values`.

20.13 TACACS+

20.13.1 Introduction

TACACS+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

TACACS+ is required in order to meet with PCI compliance (Payment Card Industry).

Modern networks with their numerous services and network components present a massive challenge in terms of controlling user access rights. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS): It does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an accept or a reject.



The advanced TACACS+ functions include, among others, the option of requesting user to change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

Please note that LANconfig cannot process all of the messages in the extended login dialog. Should LANconfig reject a login attempt at a device even if the correct data is entered, please use an alternative method of configuration (such as WEBconfig or telnet).

TACACS+ is an alternative AAA server to the widespread RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password only encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable than RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is always informed if the AAA server is unavailable.
- TACACS+ encrypts not only the password like RADIUS but the entire payload data (except for the TACACS+ header). This assures the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. Whereas RADIUS always combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication only, in that only the users are managed but not the permissible commands.

Please note: Even though TACACS+ is used to centrally manage user accounts on an AAA server, you should ensure that you set a secure password for root access to the device. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

20.13.2 Configuring the TACACS+ parameters

The parameters for configuring TACACS+ are to be found under:

Command line: **Setup** > **TACACS+**

Accounting

Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values:

- Activated, deactivated

Default

- Disabled

TACACS+ accounting will only activate if the defined TACACS+ server is available.

Authentication

Following the introduction of authentication via RADIUS, this menu item has been deprecated. Authentication via TACACS+ is now enabled under **Setup** > **Config** > **Authentication**. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server.

TACACS+ authentication will only activate if the defined TACACS+ server is available. Fallback to local users is only possible if a root password has been set for the device. The fallback to local users must be deactivated for devices without a root password. Otherwise a failure of the network connection (TACACS+ server unavailable) would make the device accessible without a password.

Authorization

Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server.

Possible values:

- Activated, deactivated

Default

- Disabled

TACACS+ authorization will only activate if the defined TACACS+ server is available. If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.

Fallback to local users

Should the defined TACACS+ server be unavailable, it is possible to fallback to local user accounts on the device. This allows for access to the device even if the TACACS+ connection should fail, e.g. when deactivating the usage of TACACS+ or for correcting the configuration.

Possible values:

- Allowed, prohibited

Default

- Allowed

The fallback to local user accounts presents a security risk if no root password is set for the device. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

Shared Secret

The password for encrypting the communications between NAS and TACACS+ servers.

Possible values:

- 31 alphanumerical characters

Default

- Blank

The password must be entered identically into the device and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.

SNMP-GET-Requests-Accounting

Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the devices to display information about current connections, etc., or to execute actions such as disconnecting a connection. SNMP can be used to configure devices. For this reason TACACS+ requires authentication for SNMP access requests. Since LANmonitor regularly queries these values, a large

number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request would initiate three sessions with the TACACS+ server.

This parameter allows the regulation of the behavior of devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Entering a read-only community under **Setup** > **SNMP** also enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Possible values:

- only_for_SETUP_tree: With this setting, accounting via TACACS+ server is only required for SNMP access via the setup branch of LCOS.
- All: With this setting, accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- None: With this setting, accounting by TACACS+ server will not be carried out for SNMP accesses.

Default:

- only_for_SETUP_tree

SNMP-GET-Requests-Authorisation

This parameter allows the regulation of the behavior of devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

Possible values:

- only_for_SETUP_tree: With this setting, authorization via TACACS+ server is only required for SNMP access via the setup branch of LCOS.
- All: With this setting, authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- None: With this setting, authorization by TACACS+ server will not be carried out for SNMP accesses.

Default:

- only_for_SETUP_tree

Encryption

Activates or deactivates the encryption of communications between NAS and TACACS+ servers.

Possible values:

- Activated, deactivated

Default

- Activated

We recommend that you do not operate TACACS+ without encryption. If encryption is activated here, the password for encryption entered here must match with the password on the TACACS+ server.

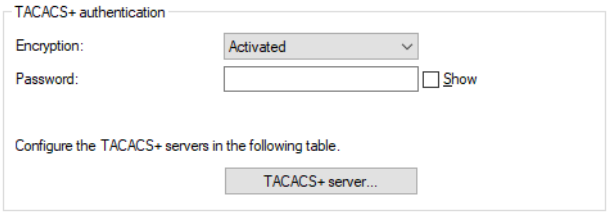
20.13.3 Configuring the TACACS+ server

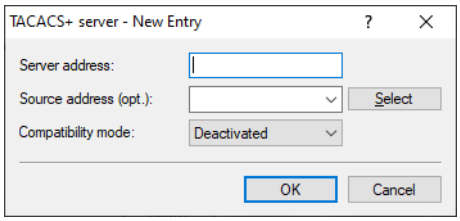
Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server are to be found under:

LANconfig: **Management** > **Authentication** > **TACACS+ authentication** > **TACACS+ server**

Command line: **Setup** > **TACACS+** > **Server**





Server address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Possible values:

› Valid DNS resolvable name, or valid IPv4 or IPv6 address.

Default

› Empty

Source address (opt.)

Optionally you can configure a loopback address here.

As an address, the device accepts the name of the IP networks whose address is to be used, any valid IP address, or the name of a loopback address.

Default

› Empty

Compatibility mode

TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers.

Possible values:

› Activated, deactivated

Default

› Deactivated

20.13.4 Login to the TACACS+ server

Once TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

20.13.4.1 TACACS+ login via LANconfig

Using LANconfig to login to a device with activated TACACS+ authentication is only possible with the user named root. Correspondingly, the user "root" must be configured on the TACACS+ server. To login via LANconfig, enter the password as configured for the user "root" on the TACACS+ server.



Once authenticated by TACACS+, "root" is the only user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the commands "readconfig" and "writeconfig" for the user "root" in order for the user to read the configuration from the device and to upload any changes (*Assigning rights under TACACS+* on page 1679).

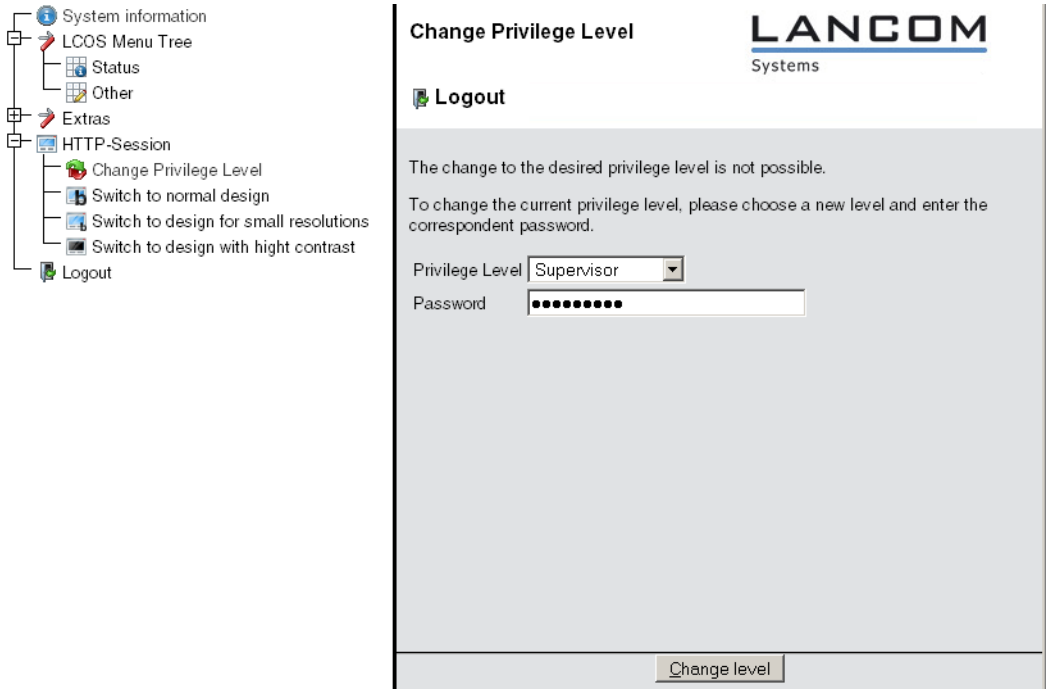
20.13.4.2 TACACS+ login via WEBconfig

Using WEBconfig to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication.



The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user "root") initially have read rights only.

To gain further rights, click on the link **Change privilege level** on the left of the screen.



In this dialog you select the required user rights and enter the corresponding password.

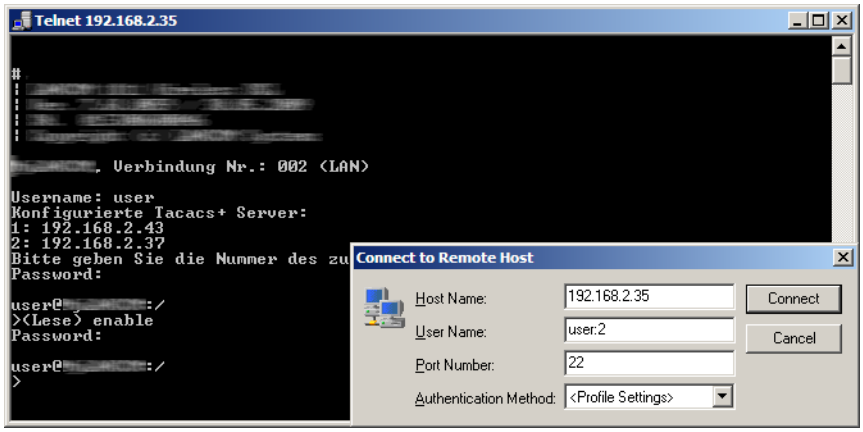
The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration (*Assigning rights under TACACS+* on page 1679).

20.13.4.3 TACACS+ login with telnet or SSH

Using tenet or SSH to login to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server.

When logging in with telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. “user:1” or “user:2”.



After login, all users initially have read-rights only (except for the user "root").

To gain further rights, enter the command `enable` and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

The passwords for individual user rights are configured as “enable” passwords in the TACACS+ server.

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the required commands for each user in order for the user to read and edit the device configuration (*Assigning rights under TACACS+* on page 1679).

20.13.5 Assigning rights under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the "enable" command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights of LCOS are mapped to the TACACS+ privilege levels:

TACACS+ level	LCOS Administrator rights
0	No rights
1	Read-only
3	Read-write
5	Read-only-limited Admin
7	Read-write-limited Admin
9	Read-only Admin
11	Read-write Admin
15	Supervisor (root)

20.13.6 Authorizing functions

If authorization is activated for the device as well as authentication, the TACACS+ server must permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

20.13.6.1 LANconfig

Command	Arguments	Comment
readconfig	None	Read out the entire configuration
writeconfig	None	Write the entire configuration

20.13.6.2 WEBconfig

Command	Arguments	Comment
delRow	SNMP-ID of the table	Delete row
addRow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu

Command	Arguments	Comment
action	SNMP-ID of the action	Execute an action
reboot	None	Restart device
$URL	None	Display a certain URL

When working with WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the LCOS configuration branch of the menu tree. Additionally, the individual parameters which the user may edit must also be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the trace "trace+ tacacs".

20.13.6.3 Telnet/SSH

Command	Arguments	Comment
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding values
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readconfig	None	Read out the entire configuration
readstatus	None	Read-out status menu
writefiash	None	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	None	Write the entire configuration
ll2mdetect	None	Start LL2M detection
ll2mexec	Parameter name	Execute LL2M command
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy

Command	Arguments	Comment
readscript	Parameter name	Read-out script
beginscript	None	Start script
endscript	None	Stop script
flash	Parameter name	Activate/deactivate flash mode

For telnet access, all of the parameters that the user may edit must be enabled. You can view the values sent by telnet to the TACACS+ server with the trace "trace+ tacacs".

You can download the MIB of current devices via WEBconfig (**Extras** > **Get Device SNMP MIB**).

20.13.6.4 SNMP

Command	Arguments	Comment
get	SNMP-ID of the menu item	Read-out value
set	SNMP-ID of the menu item	Set value

20.13.7 Bypassing TACACS+

20.13.7.1 Introduction

TACACS+ enables every change to a network-device configuration to be subject to special authorization. TACACS+ accounting enables each of these steps to be logged. TACACS+ is a requirement for systems used in electronic payment (PCI compliance).

Strict monitoring of this type leads to an increase in traffic to and from the TACACS+ server(s). In large-scale scenarios, the TACACS+ communications caused when using scripts for centralized configuration changes or if CRON commands are run regularly could lead to an overload of the TACACS+ server.

20.13.7.2 Configuration

To avoid overloading the TACACS+ server when carrying out automatic configuration changes, it is possible to exclude CRON, action tables and scripts from the authorization and accounting by TACACS+.

Command line: **Setup** > **TACACS+**

Bypass-Tacacs-for-CRON > Scripts > Action-Table

You can activate or deactivate the bypassing of TACACS+ authorization and TACACS+ accounting for various actions.

Possible values:

- Activated, deactivated.

Default:

- Disabled.

Please observe that this option influences the TACACS+ function for the entire system. Be sure that you restrict the use of CRON, the action tables, and scripts only to an absolutely trustworthy circle of administrators!

20.14 LLDP

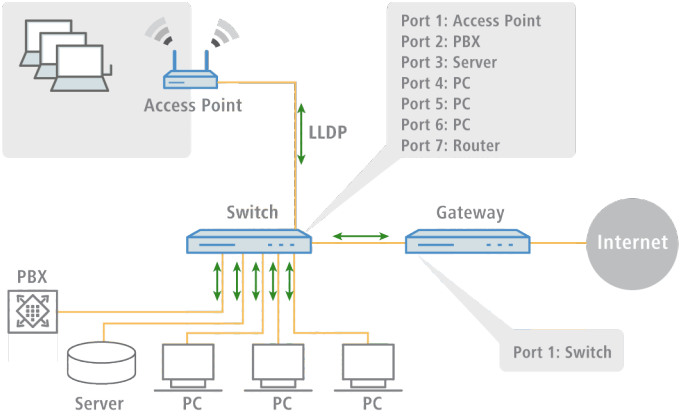
The Link Layer Discovery Protocol (LLDP) provides a simple and reliable way to exchange information between neighboring devices on the network and for determining the topology of networks. LLDP provides discovery functions to identify individual devices and entire network structures using the procedures defined in the IEEE 802.1AB standard. Since the protocol works on Layer 2 (security level) of the OSI layer model and it is, therefore, used for physically addressing devices, its functionality is not limited to logical networks such as IP networks. In principle, LLDP covers all physically accessible devices on the network.

In particular, the vendor-independent LLDP protocol offers many advantages in complex networks:

- It enables the automatic detection of components attached to a network such as routers, switches, and WLAN access points.
- It simplifies the integration of a wide range of different devices, which support the LLDP standard, into an existing network: Using central network management software, and automatic testing and diagnostic processes, the time required for setup, operation and maintenance of a network is reduced.
- The information sent by the individual devices provides an overview of the topology (i.e., structure and arrangement) of the entire network. Central management software provides the administrator with a virtual image of the network, which is automatically updated when there are changes in the topology.
- With the help of management software, the administrator can also easily monitor and manage complex networks. Using this software, he can determine which components and devices are interconnected and can easily locate any faults.
- LLDP can reduce the costs of buying, building or restructuring a network, since companies are no longer dependent on specific manufacturers because of this open standard. Individual network components can be selected based on which one is best for your implementation. This was previously not possible when proprietary protocols were in use.

20.14.1 How it works

LLDP works on a simple principle: The so-called LLDP agent runs on all devices with LLDP support. On the one hand, this software component sends information to all interfaces of the device at regular intervals. This is done using either Unicast or Multicast, depending on the destination addresses, which you can configure as required. On the other hand, the LLDP agent is continuously receiving information from neighboring devices. The transmission and reception of the respective data packets is handled independently from each other.



The data packets being sent and received contain information such as the name and the description of the device, the ID and description of ports, the IP address or MAC address of the device, the specific capabilities of the device (e.g., in terms of switching and routing), VLAN identifiers and vendor-specific details. In this case, LLDP defines basic information that a data packet must always include, as well as optional additional information.

The individual devices store the information received locally in a data structure, the so-called MIB (Management Information Base). An MIB therefore contains data from its own LLDP agent and of the detected, direct neighbor agent.

The information exchange provides a continuing identification of the devices within the network, because the devices normally send packets cyclically (i.e. in configurable intervals). Furthermore, the devices also inform their network neighbors when changes occur on the device or in its network connection.

For the actual device identification process it is crucial that each connection point in the topology is clearly identified as a "Media Service Access Point" (MSAP). An MSAP is composed of a device ID (Chassis ID) and a port identification (Port ID). The unique identification or assignment of devices is therefore based on the fact that each MSAP in the monitored network topology may occur only once.

The Administrator can query and capture the data reported by the devices via a central network management software on his computer, where the query of the individual MIBs is performed using the SNMP protocol. The management software thus documents the entire topology of the network and allows automatic display of this topology along with a graphic representation of the current diagnostic data.

In LANconfig, LLDP is enabled under **Interfaces** > **LAN**.



20.14.2 Structure of LLDP messages

Information is exchanged using specific units of data known as LLDP Data Units (LLDPDU). These data unit consists of TLVs (Type-Length-Values), and each TLV field corresponds to a certain type and has a certain length.

In accordance with the LLDP standard IEEE 802.1AB three TLVs are mandatory at the beginning of an LLDPU in the following order:

- Type 1 = Chassis ID
- Type 2 = Chassis ID
- Type 3 = Time to live

Following these mandatory TLVs, an LLDPDU can include additional, optional TLVs:

- Type 4 = Port description
- Type 5 = System name
- Type 6 = System description
- Type 7 = System capabilities
- Type 8 = Management address

At the end of an LLDPDU the following TLV is mandatory:

- Type 0 = End of LLDPDU

Tabular overview of the TLVs

TLV	Usage	Name	Example	Function
Type 1	Mandatory	Chassis ID	0018.2fa6.b28c	Identifies the device
Type 2	Mandatory	Port ID	Fi-0/12	Identifies the port
Type 3	Mandatory	Time to live	60 sec	Signals to the receiving device how long the received information should remain valid
Type 4	Optional	Port description	GigabitEthernet0/12	Displays details about the port such as the hardware version
Type 5	Optional	System name	PN-I/O 3	Displays the name given to the device by the administrator

TLV	Usage	Name	Example	Function
Type 6	Optional	System description	LCOS software, version 8.9.1 SE	Displays details about the device such as the version of the networking software
Type 7	Optional	System capabilities	Router	Displays the primary function and capabilities of the device.
Type 8	Optional	Management address	192,168.0.1	Shows the IP or MAC address of the device
Type 0	Mandatory	End of LLDPDU	----------	Signals the end of the data unit

20.14.3 Supported operating systems

In principle, LLDP works on all popular systems, provided that LLDP agents or an appropriate software for evaluation of the LLDP packages is available. For Linux there are various open source projects, such as "LLDPD", "Open-LLDP" (with hyphen) or "ladvd", which deploy an LLDP agent.

The project "OpenLLDP" aims to achieve a further dissemination and acceptance of the LLDP protocol (802.1AB). The software supports the transmission and reception of LLDP messages on the Linux, Mac OS X, FreeBSD, and NetBSD platforms. Currently, however, this development seems to be stalled.

Microsoft Windows Vista and Windows 7 contain a proprietary protocol called LLTD (Link Layer Topology Discovery), which is essentially the same functionality as LLDP. On Windows XP, the LLTD component can be installed later as a patch. However, the patch is limited compared to the features implemented in Vista and Windows 7 because the "LLTD Responder" only reports IPv4 addresses, and not IPv6 addresses.

If you want to install LLDP on Windows systems, you can use a shareware called "haneWIN LLDP Agent". Using this, LLDP works on all Windows systems as of Windows 2000, i.e., on both 32-bit and 64-bit systems.

The most widely used free software for evaluation and analysis is Wireshark. The basic version of Wireshark is free of charge and now well-established as a standard. The software supports a wide variety of operating systems and can read and evaluate a wide variety of protocols (including LLDP). However, the focus of the basic version of Wireshark is the analysis of problems within the network. If you need more features (such as the visualization of network traffic in the form of colored graphs), you can purchase add-on modules.

20.15 Sending and receiving SMS text messages

If your device has a 3G/4G WWAN module, is capable of sending and receiving text messages via the Short Message Service (SMS).

In this case the SMS function is mainly used as a messaging and function-enhancing interface for the internal LCOS modules, but also for external instances such as routers, management solutions, accounting systems, and so on. You as a user also have the option to send SMS text messages using the corresponding *function in LANmonitor* or the `smssend` command at the command prompt. LANmonitor also provides you with convenient functions for *managing* sent and received messages.



The sending and receiving of SMS text messages must also be included in the SIM card's contract.

20.15.1 Receiving SMS text messages

Your device uses the ETSI standard TS 127.005 to receive and request these SMS text messages, to store them and, if required, to log the receipt of an SMS to the SYSLOG. The entry in the SYSLOG counts as a "notice" to inform you about

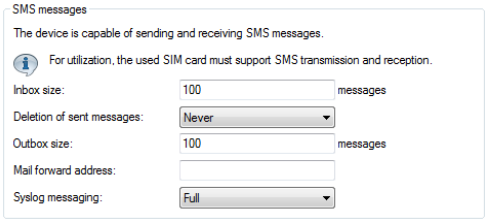
any important messages, such as a notification from an external instance, for example. An instance might be the accounting system of your provider:

If you connect to the Internet via a 3G/4G WWAN module and the contract with your Internet provider includes a volume limit, then depending on the contract your provider will throttle or stop data transfer once this volume limit has been reached. In countries with the appropriate legislation, this also applies when a charging limit for data roaming has been reached. Before the data transfer is throttled or stopped, many providers send an SMS text message informing the customer that the volume limit has been reached. With the corresponding notification settings in the SYSLOG and/or via e-mail, the device can immediately inform you about the reception of the SMS, so that you can respond promptly.

20.15.2 Basic configuration of the SMS module

The following steps show you the basic configuration of the SMS module in a 3G/4G WWAN-enabled device.

1. Start LANconfig and open the configuration dialog for the device.
2. Navigate to the menu item **Log & trace** > **SMS messages**.



3. Under **Inbox size** you set the maximum number of text messages stored in the device inbox.
   If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value `0` disables the limit, i.e. an unlimited number of messages will be stored.
4. The item **Deletion of sent messages** decides how the device handles sent text messages.
   - **Immediately**: Sent messages are not saved.
   - **Never**: Sent messages are saved permanently.
5. Under **Outbox size** you set the maximum number of text messages stored in the device outbox.
   If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value `0` disables the limit, i.e. an unlimited number of messages will be stored.
6. Under **Syslog messaging** you specify if and how the arrival of text messages is logged to the SYSLOG.
   - **No**: Incoming text messages are not logged to SYSLOG.
   - **Only sender/no content**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number.
   - **Full**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number and the message in full.
7. Optional: Under **Mail forwarding address** you specify the e-mail address to which the device is to forward the incoming SMS text messages.

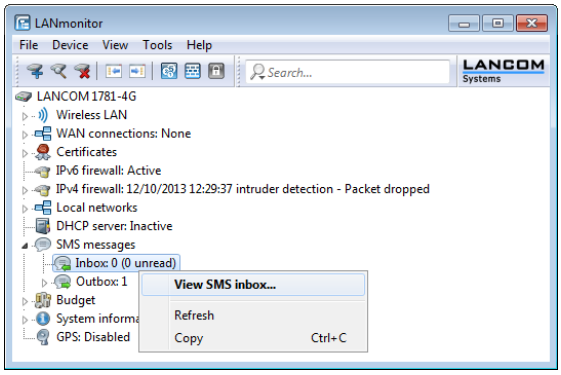
   E-mail routing will only work if a valid SMTP account is configured in the device.
8. Now write the configuration back to the device.

That's it! This concludes the basic configuration of the SMS module.

20.15.3 Managing SMS text messages with LANmonitor

The following section explains shows how you can use LANmonitor to read and delete text messages sent or received by a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages** > **Inbox** or **Outbox**. If there are already text messages on the device, LANmonitor displays the last five received messages under **Inbox** and the last five sent messages under **Outbox**.
2. Open the context menu on the entry and choose **Show SMS inbox** or **Show SMS outbox**.



LANmonitor then displays a window listing all of the sent and received text messages and their status. In the **Inbox** you have the option to delete single or multiple selected messages, or to mark them as read/unread; the Status shows whether they have been read or not (**New** or **Read**). In the **Outbox**, the messages can only be deleted; the Status shows their send status (**Sent** or **Unsent**).

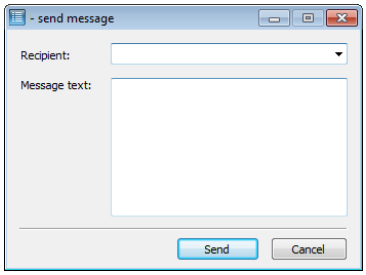
You can manage these messages by using the context menu. To delete all messages in the inbox or outbox, go to the menu bar under **Messages** and select the appropriate action.

You can easily toggle between the inbox and outbox by selecting **View** from the menu bar and selecting the desired option.

20.15.4 Sending SMS text messages with LANmonitor

The following section explains how you can use LANmonitor to send SMS text messages via a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages**.
2. Open the context menu on the entry and select **Send message**.
3. In the Editor window that opens, enter the phone number of the recipient and the message content to be sent. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section *Character set for sending SMS* on page 1687.



4. Click **Send** to send the message via the internal SMS module.

20.15.5 URL placeholder for sending SMS

You have the option of addressing the SMS module as an interface by means of a URL. By integrating predefined placeholders (parameters) into the URL, you can use the device to send SMS text messages by means of an HTTP(S) call. This makes LANCOM cellular routers ideal for use as an SMS gateway.

SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

You use your access credentials to authenticate at the device; just how these are Integrated into the URL is determined by your browser's requirements. The typical notation is `Username:Password@Host`.

Depending on the use case (for example, SMS gateway), we recommended that you create an administrator without access rights (**None**) and with just one function right, **Send SMS**.

Not all Web browsers support the transmission of credentials via the URL. This includes current versions of the Microsoft Internet Explorer, among others. In this case you should use another browser to send SMS via the URL.

The URL call uses the syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&…&oldauth
```

The parameter `oldauth` is **vital**, otherwise none of the available browsers will send the access credentials to the device. In addition, the following placeholders are defined:

`DestinationAddress`

Phone number to which the device should send the SMS. The same conventions apply as for normal telephone calls. Specify the parameters as follows:

```
&DestinationAddress=01511234567
&DestinationAddress=00491511234567
```

`Content`

Content of the text message. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section *Character set for sending SMS* on page 1687.

Spaces and other special characters to be included into an SMS must be sent to the device in the URL-encoded form. For example, spaces are encoded with `%20` and full stops with `%2E`. Specify the parameters as follows:

```
&Content=This%20is%20a%20message%2E
```

Learn more about this topic on the Internet under the keyword "URL encoding" and also at *www.w3schools.com*.

Some browsers perform the URL encoding automatically. Despite this, we recommend that you encode the content yourself to ensure that all of the characters are converted correctly.

20.15.6 Character set for sending SMS

An SMS can contain a maximum of 160 characters (each of 7 bits = 1,120 bits). These are made up of the GSM basic character set (total of 128 characters) as well as selected characters from the extended GSM character set. Although the extended character set allows the use of some additional characters, these take up twice the space and correspondingly reduce the maximum number of characters that the SMS can contain. Characters not implemented in the SMS module are ignored by the device.

The following characters are defined in the **GSM basic character set**:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" in the overview refers to the space character. "LF", "CR" and "ESC" refer to the control characters for the line feed, the carriage return and the escape in the extended GSM character set.

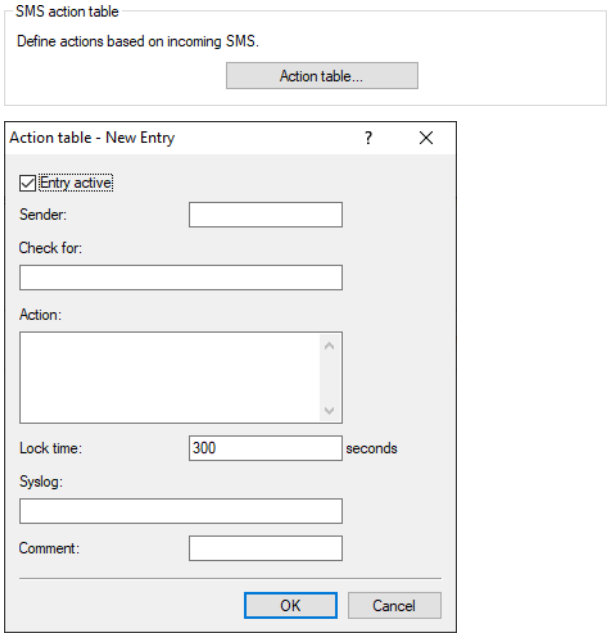
The following characters are implemented from the **extended GSM character set**:

{ | } [ ] ~ ^ \ €

20.15.7 Execute actions on incoming SMS

You can react to incoming SMS with predefined actions. This allows you to respond to an incoming SMS (e.g. data budget used up) by sending your own SMS to the Internet provider, for example to book a new data budget.

In LANconfig you configure this under **Logging/Monitoring** > **SMS messages** > **SMS action table** > **Action table**.



Entry active

Activates or deactivates this table entry.

Sender

Sender address of the incoming SMS, which is the basis for the subsequent action. E.g. 7277 for Deutsche Telekom.

Check for

Content of the incoming SMS to be checked for. For example, `contains=' used up'` in the event of an exhausted data budget. The text that is checked for is case-sensitive!

Action

Defines the action to be executed after checking the specifications under **Sender** and **Check for**. For example, `exec:smssend -d 7277 -t "Speed"` to book a SpeedOn in the Deutsche Telekom network. With `exec` a command is executed on the command line, in this case the command `smssend`.

The possible commands correspond to those of the normal action table, see *Configuring the action table*.

Lock time

Defines the lockout time in seconds, in which the action may not be executed again.

Syslog

Text field for defining the message to be written to the syslog when this action is executed.

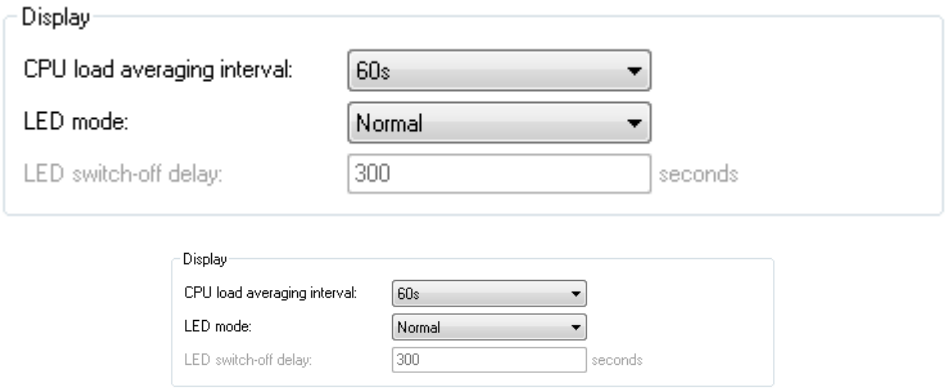
Comment

Comment field.

20.16 Deactivating device LEDs – boot-persistent

To operate an access point as unobtrusively as possible, you can disable the operating and status LEDs on the device. Even after restarting the device, the LEDs stay switched off. You can set up the device so that the LEDs light up briefly for a certain time after a restart, before the device disables them. This is useful for access points that are managed by WLAN controllers, for example to monitor the establishment of the connection to a WLAN controller.

You can set the operating mode of the LEDs in the **Display** section under **Management** > **Advanced**.



The selection list **LED mode** has three options to choose from:

Normal

The LEDs are always enabled, also after rebooting the device.

All off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

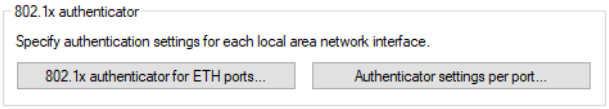
The "LED-Test" function is available despite the LEDs being disabled.

If you change this value and save it within the previously set time, you should restart the timer.

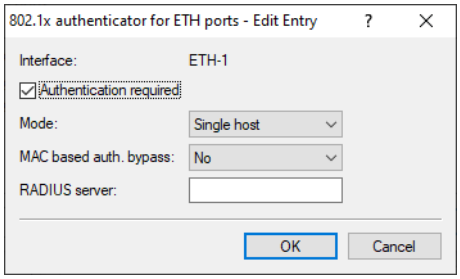
20.17 802.1X authenticator for Ethernet ports

Using the 802.1X authenticator, devices connected to the Ethernet ports of a LANCOM device can be authenticated using 802.1X. This increases security against unauthorized access to the network via Ethernet cables and ports.

In LANconfig you configure the 802.1X authenticator for Ethernet ports under **Interfaces** > **LAN** in the section **802.1x authenticator**.



You perform the configuration in the table **802.1x authenticator for ETH ports**. Each interface is specified here and indicates the existing Ethernet ports.



Authentication required

Use this control to specify whether 802.1X authentication is required for this port.

Mode

Possible values:

Single host

Just one client can authenticate and then operate on this port. If a further client with its own MAC address is detected on this port, the port is reset to the unauthenticated state.

Multiple hosts

Several clients (with different MAC addresses) can operate on this port. Authentication only needs to be performed once. This mode can be used, for example, if a WLAN access point is operated on a port configured in this way and the payload data is not tunneled to a central controller. In this case, data packets from WLAN clients that have their own MAC addresses would also be seen on the Ethernet port configured in this way.

Multiple authentications

Several clients can each perform their own 802.1X authentication on this port.

MAC-based auth. bypass

This specifies whether a failed attempt to start an 802.1X negotiation should be followed by a check of the client's MAC address via RADIUS and a subsequent opening of the port. In this case, the MAC address is transmitted as a RADIUS user name and password in the format "aabbccddeeff". It must also be stored in the RADIUS server in this format.

The MAC address is easy to fake and does not protect against malicious attacks.

In the standard configuration, the 802.1X authenticator will try to start an 802.1X negotiation for 90 seconds before falling back to the MAC address check. This time can be set for each port by changing the command-line parameters **Setup** > **IEEE802.1X** > **Ports** > **Max Req** (default: 3 attempts) and **Setup** > **IEEE802.1X** > **Ports** > **Supp-Timeout** (default: 30 seconds). Alternatively, the mode for **MAC Auth Bypass** can be set to "Immediate". This mode immediately starts a MAC address check without waiting for a timeout.

Possible values:

No

MAC address authentication is not possible.

Yes

MAC address authentication is possible.

Immediately

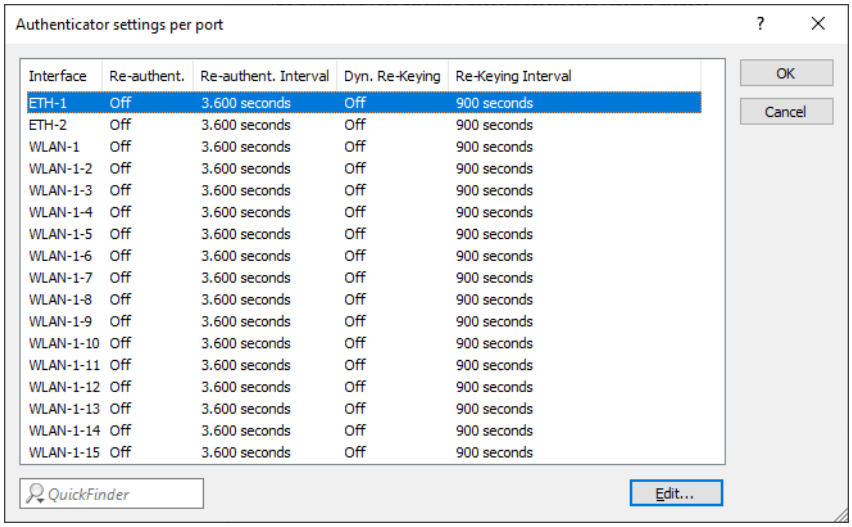
Authentication is immediately performed by MAC address.

RADIUS server

Specifies which RADIUS server is used both for 802.1X and for MAC address validation. To do this, reference one of the entries under **Interfaces** > **802.1X** > **Radius servers** or create a new entry there if necessary.

You configure the format of the MAC address transmitted to the RADIUS server for MAC authentication using the command-line option **Setup** > **LAN** > **IEEE802.1X** > **Username-Attribute-Format**. The individual bytes of the MAC address are represented here as the variables %a to %f. In the default setting specified here, the bytes of the MAC address are output one after the other. In addition to these variables, any of the characters supported by the LCOS can be added. Another commonly used format for the MAC address "aabbcc-ddeeff" (with "-" as separator) can be configured as follows: "%a%b%c-%d%e%f"

In the table **Authenticator settings per port** you set the login information for the local network interfaces.



Interface

Each interface is specified here and indicates the available Ethernet and WLAN interfaces.

Re-authentication required

Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation.

Re-authentication interval

The default value for re-authentication interval for regular re-authentication is 3,600 seconds.

Enable dynamic re-keying

Here you activate the regular generation and transmission of a dynamic WEP key.

Re-keying interval

The default value for the re-keying interval is 900 seconds.

20.18 xDSL Interface

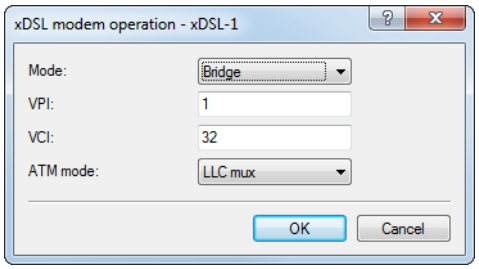
20.18.1 ADSL/VDSL modem operation (bridge mode)

With the ongoing migration of ISDN connections to All-IP, the ISDN connections available at sites are being converted into additional DSL connections. In order to provide this new bandwidth to the whole of the network, the router needs to be connected to the new DSL line. If the DSL connection of the gateway is already in use, a LANCOM VDSL router can be connected upstream as a pure DSL modem. The access and VoIP data continue to be stored in the main gateway. This allows additional DSL connections to be transparently integrated into the existing scenario.

The configuration is conducted as follows:

1. Connect the LANCOM router, which is to operate as a modem, to the VDSL port.
2. Connect the main gateway to the LANCOM modem by means of an Ethernet cable.
3. Under **Interfaces** > **LAN** > **Port table**, assign the LAN interface and the xDSL interface to an unused bridge group.

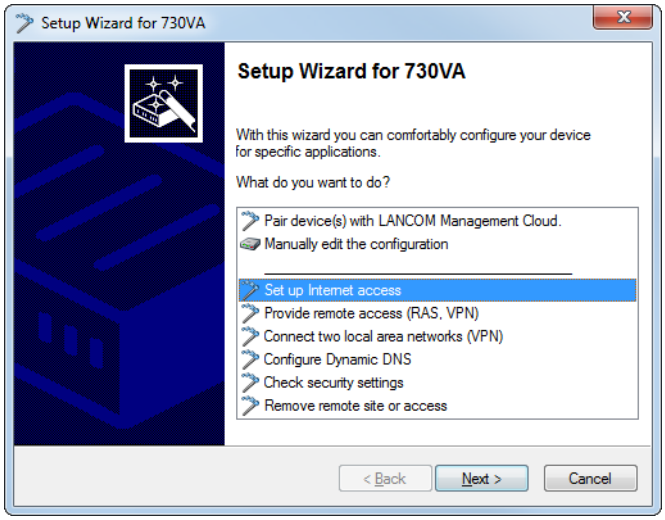
4. Under **Interfaces** > **WAN** > **Interface settings** > **xDSL modem operation**, set the VDSL port to bridge mode. At an ADSL connection, you may need to correct the ATM parameters (Deutsche Telekom: VPI 1, VCI 32, ATM mode LLC-Mux).



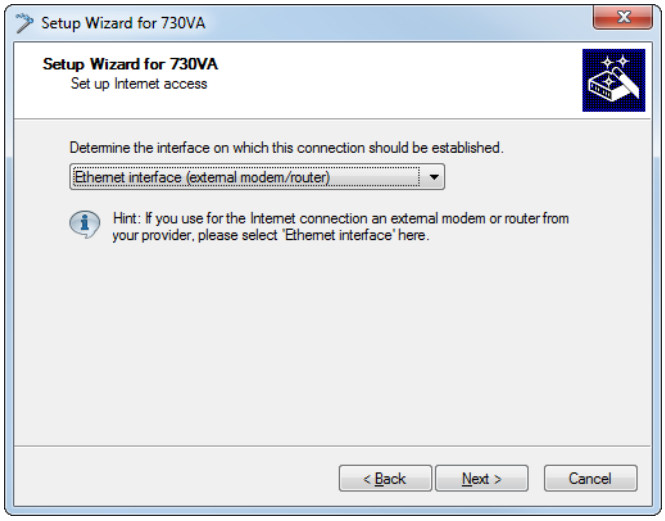
5. Deactivate the DHCP server under **IPv4** > **DHCPv4** > **DHCP networks**.
6. Go to **IPv4** > **General** > **IP networks** to give the router an intranet IP address from an unused range (for example, 192.168.3.254).

Note that the unused bridge group selected above must be selected under **Interface assignment**.

7. Set up the Internet connection on the main gateway using the setup wizard:
   a. Select your device in LANconfig and start the setup wizard "Set up Internet access".



b. Follow the instructions in the setup wizard and select the option that best suits your needs. When you reach the step to set the "Interface for this connection", select the option **Ethernet Interface (external modem/router)**.

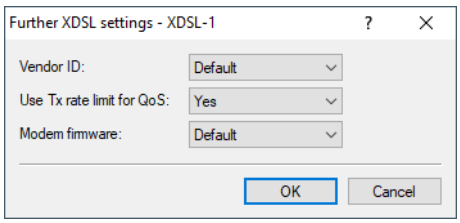


If the LANCOM modem's sync status is to be queried from the network, then go to **Communication** > **Remote sites** > **Remote sites (DSL)** and create a remote site named "Management" with a short hold time of "9999" seconds, layer name "IPOE", and DSL port "1".

In the IP parameter list under **Communication** > **Protocols**, give the remote site "Management" an IP address from the unused range (e.g. 192.168.3.1/24). Finally in the table **IP router** > **Routing** > **IPv4 routing table** add an entry 192.168.3.0/24 to the "Management" remote site with IP masquerading switched off. The modem can now be accessed and queried at the IP address 192.168.3.254.

20.18.2 Further XDSL settings

This table contains further settings for the xDSL.



LANconfig: **Interfaces** > **WAN** > **Further XDSL settings**

Command prompt: **Setup** > **xDSL** > **General**

Interface

Fixed value for this interface: 1 for XDSL-1, 2 for XDSL-2, etc.

Vendor-ID

The code specified by the German Federal Network Agency for LANCOM devices does not work in all countries. In these cases, for example in Switzerland, the alternative identifier must be selected.

Us Tx limit for QoS

This switch changes the use of the sync data rate as the QoS data rate. If activated (default), the sync data rate is used as the QoS data rate. Otherwise the sync data rate is not used and the interface behaves like a DSL interface with regard to the QoS data rate.

Modem firmware

As there is no “best” DSL firmware for every situation, you can switch to another modem firmware available in the LCOS, if necessary.

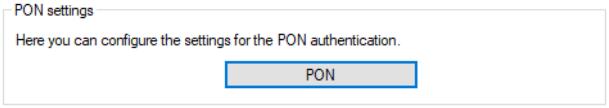
This column is only available for devices with a LCOS that contains an alternative modem firmware.

20.19 GPON support

GPON (Gigabit Passive Optical Network) is an optical transmission standard for fiber optic connections (FTTH). LANCOM offers GPON SFP modules for this purpose, which are available in LANCOM routers with SFP interface. The list of compatible devices can be found in the respective GPON SFP data sheet.

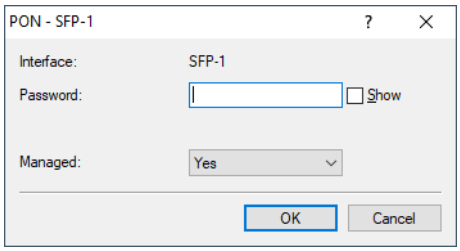
With a GPON module, the LANCOM router can be operated directly on the fiber optic connection of the provider without a separate modem. Please contact your provider if operation without modem and with SFP module is supported. Usually GPON modems are authenticated by serial number and/or GPON password, so operation without provider support is not possible.

As a rule, nothing has to be configured in the device for GPON operation.



LANconfig: **Interfaces** > **WAN** > **PON**

Console: **Setup** > **Interfaces** > **PON**



Interface

Select here the SFP interface in which the PON module is plugged, e.g. SFP-1.

Password

Enter the PON password here if your provider performs password authentication. Other terms for PON password are “ONT installation identifier” or “PLOAM password”. The password consists of either 10 octets in ASCII representation or 20 characters in hexadecimal representation. The password is empty by default.

You can get the PON password for your connection from your Internet provider.

Managed

Configure here if the modem should be managed by the operating system. In this case the system writes the PON password (recommended).

20.20 ACME-Client

As of LCOS 10.80 the Automatic Certificate Management Environment (ACME) client as per *RFC 8555* is supported for Let's Encrypt certificates. *Let's Encrypt* is a free and open certification authority that makes it possible to obtain free SSL/TLS certificates. The certificates can be used for WEBconfig and for the Public Spot.

The prerequisite for using Let's Encrypt is that the device has a publicly resolvable domain name, e.g. DynDNS. For the certificates to be used correctly, the device's WEBconfig must be accessed via its domain name and not the IP address. If WEBconfig is called via the IP address, the certificate check fails because Let's Encrypt certificates are issued for domain names and not IP addresses.

With Let's Encrypt, certificates are issued when a device can prove that it has control of the domain name. For this purpose, Let's Encrypt provides a so-called "challenge" that the device must satisfy. The ACME client in the device performs this process automatically. The ACME client also renews the certificate automatically before a specified certificate expiry period.

A domain name must first be entered into the configuration. The device then automatically submits a certificate request to Let's Encrypt and temporarily opens (for example) the port 443 or 80. Let's Encrypt then checks whether the device and the previously set challenge (e.g. token) can be reached under the specified domain name and port 443 or 80. If this is successful, the certificate is issued. The device renews the certificate automatically before it expires. For this process, the device briefly opens port 80 or 443 for this challenge and closes it again in the second step.

Use of Let's Encrypt is not possible or fails in the following scenarios:

- The device does not have a public IP address
- An upstream firewall blocks access to port 443 or 80 from the Internet

In principle, multiple domain names are also supported in the SAN field (Subject Alternative Name) of the certificate.



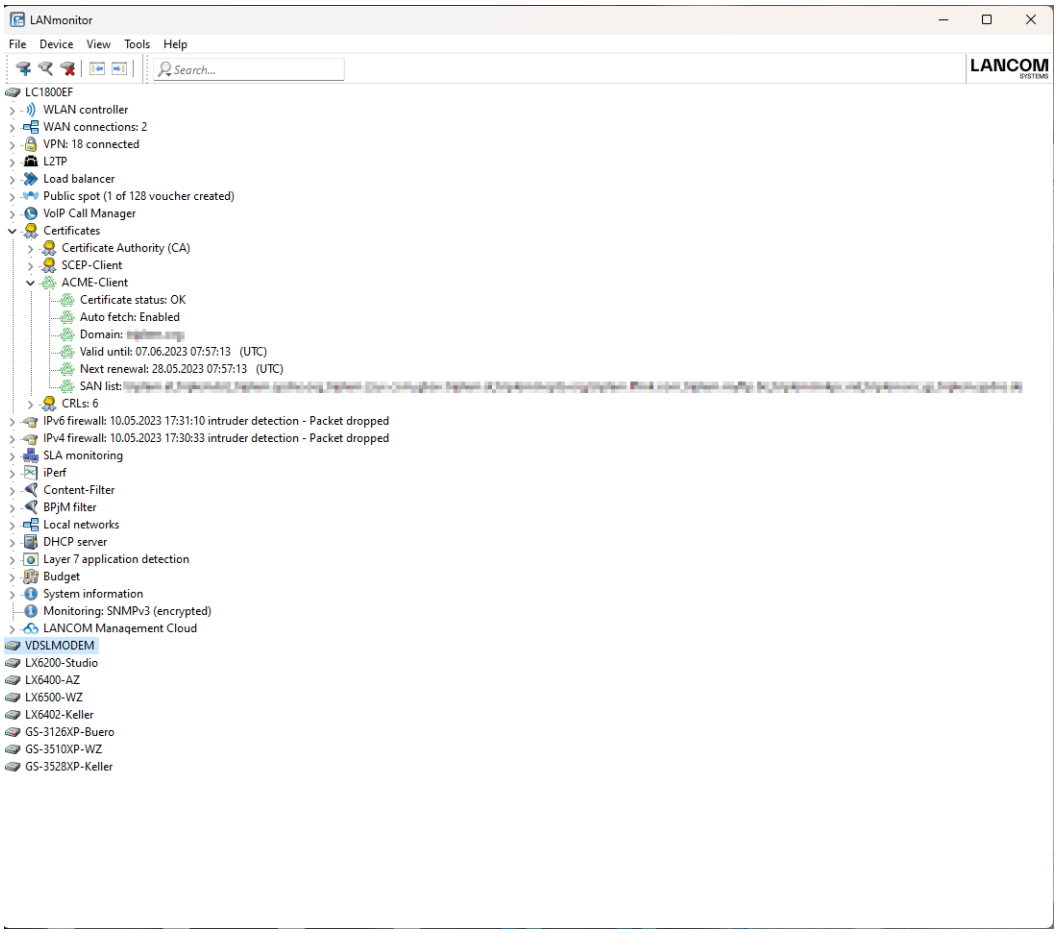
By default, port 443 and the method tls-alpn-01 is used for the ACME challenge. If the method http-01 is to be used on port 80, the LANconfig configuration parameter **General** > **Admin** > **Access settings** > **HTTP access from a WAN interface** must be set to "Automatic".



Please note that it is not possible to use the ACME client with the tls-alpn-01 authorization challenge and simultaneous port forwarding with port 443. The same applies if the ACME client is to be used via the http-01 method for port 80.

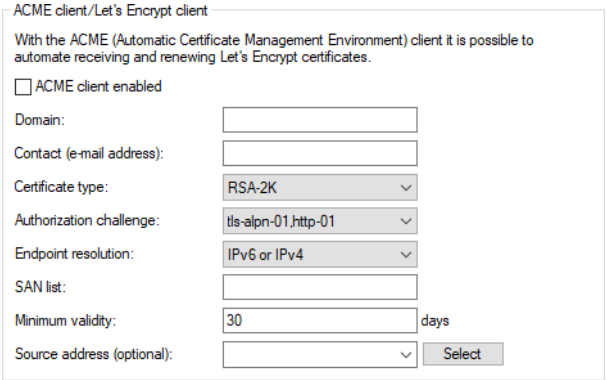
Manual adjustment of the ACME client to any port is not possible according to *RFC 8737* in the protocol.

You can see information about the ACME client in LANmonitor and start or stop a trace with the command line `trace # acme`.



20.20.1 ACME client configuration

In LANconfig, configure the Automatic Certificate Management Environment (ACME) client under **Certificates** > **ACME client**.



ACME client enabled

Activates or deactivates the automatic fetching and renewal of the certificate.

Domain

DNS domain name for which the certificate is to be created, e.g. “test.example.com”

Contact (e-mail address)

Defines the contact information for the certificate request, e.g. the e-mail address “test@example.com”.

Certificate type

Defines the certificate type including key length.

Possible values: RSA-2K, RSA-3K, RSA-4K, ECC-256, ECC-384

Authorization challenge

Specifies the method used to perform the Let's Encrypt authorization challenge. Possible values:

- TLS-alpn-01: Authorization is performed over TLS and port 443
- http-01: Authorization is performed over HTTP and port 80
- http-01,tls-alpn-01: http-01 is preferred over tls-alpn-01
- tls-alpn-01,http-01: tls-alpn-01 is preferred over http-01

Endpoint resolution

Defines the protocol to be used to resolve the endpoint. Possible values:

- IPv4-only
- IPv6-only
- IPv6-or-IPv4

SAN-List

Defines which other domain names should be entered into the SAN field (Subject Alternative Name) of the certificate. This can be a comma-separated list of domain names (without spaces).

Minimum validity

Minimum number of days before expiry for the certificate to be renewed. Default: 30 days

Source address (optional)

References a named loopback address that is used as the sender. If the field is left empty, the router automatically selects an address.

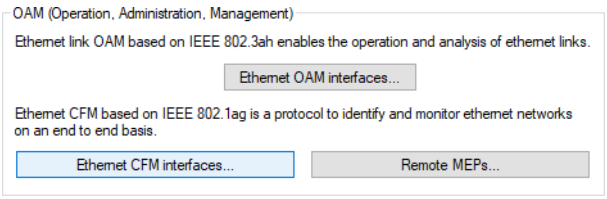
20.21 Operations, Administration, and Management (OAM)

Ethernet OAM according to IEEE 802.3ah is used by ISPs to monitor an Ethernet-based **last mile**, for example, in FTTH or VDSL2 access.

For this purpose, the active side, usually representing the ISP side, regularly transmits OAM packets (OAM Protocol Data Units – OAMPDUs). The passive side, usually representing the CPE side, responds to these OAMPDUs and replies. This verifies the reachability of the other side. This process is called **OAM Discovery**.

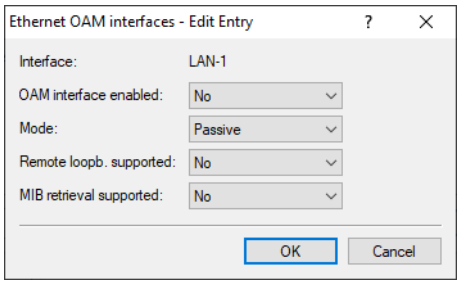
Connectivity Fault Management (CFM) according to IEEE 802.1ag / ITU-T Y.1731 is a collection of protocols and tools for so-called OAM on Layer 2. CFM is used for monitoring and fault analysis in LANs, bridges, or Ethernet-based WANs.

In LANconfig, you can configure OAM under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)**.



20.21.1 Ethernet Link OAM (IEEE 802.3ah)

In LANconfig, configure Ethernet OAM according to IEEE 802.3ah under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Ethernet OAM interfaces**.



Interface

Name of the interface.

OAM interface enabled

Enables/disables OAM on the respective interface.

Mode

Defines the mode (Active/Passive) for the respective interface.

Active

The passive side (usually the CPE side) responds to the OAM packets (OAMPDUs) sent by the sender.

Passive (Default)

The active side (usually the internet provider) sends the OAM packets (OAMPDUs) to the receiver.

Remote loopback supported

Defines whether the device can be placed into loopback mode by the remote side. In loopback mode, the device disables forwarding and sends all received packets back on the interface. The packet is sent back exactly as it was received, with no mirroring of MAC or IP addresses.

MIB retrieval supported

Defines whether the device allows the remote side to retrieve specific status values or counters from the device via packets.

The following two commands are supported on the CLI:

20.21.1.1 Remote-Loopback

With this command, the device sends a Loopback Control OAMPDU to the counterpart, causing the counterpart to enter or exit the loopback mode accordingly. In loopback mode, the counterpart device sets the forwarding mode on this

interface and returns all received packets. The packet is sent back exactly as it was received, without mirroring MAC or IP addresses.

SNMP ID:

2.105.4

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface on which to start or stop the loopback mode. The device sends the message on this interface to place the remote side into loopback mode or to terminate it there.

Possible values from the OAM setup table, e.g., LAN-1, DSL-1, …

[-?]

Displays brief help for the parameters.

<start|stop>

Starts or stops loopback mode.

20.21.1.2 Variable-Read

This command allows the device to send a Variable Request OAMPDU to the remote side. The remote side responds with the value of the requested variable based on the local MIB. This method can be used to read packet counters on the remote side, for example. The remote side must support the feature of reading MIB variables via OAM.

Variables from IEEE 802.3.1 are supported, among others.

Example:

```
> do Variable-Read -i LAN-3 aFramesTransmittedOK

aFramesTransmittedOK = 8444
OK: Action Variable-Read done
```

SNMP ID:

2.105.6

Console path:

Setup > **OAM**

Possible arguments:

-i <interface>

Specifies the interface from which the variable is to be read.

[-?]

Displays brief help for the parameters.

<variable name> [more variable names]

One or more variable names separated by spaces.

20.21.2 Connectivity Fault Management (IEEE 802.1ag / ITU-T Y.1731)

Connectivity Fault Management (CFM) as per IEEE 802.1ag / ITU-T Y.1731 is a collection of protocols and tools for OAM on Layer 2. CFM is used for monitoring and fault analysis in LANs, bridges, or Ethernet-based WANs.

The protocols particularly enable providers or operators and administrators of Ethernet connections to proactively monitor these connections or analyze them in case of faults.

LCOS supports the following functions:

- **Continuity Check Messages (CCM):** Regular status messages are exchanged to monitor the availability of network elements.
- **Loopback:** Loopback messages can be sent and returned by the remote side (ethping / Layer 2). This function is analogous to the ICMP-based Ping on Layer 3. Both Ethernet unicast and multicast addresses are supported.
- **Linktrace:** Linktrace messages can be sent, which are returned by the remote side and responded to by network elements along the path (Layer 2). This function is analogous to the ICMP-based Traceroute on Layer 3.

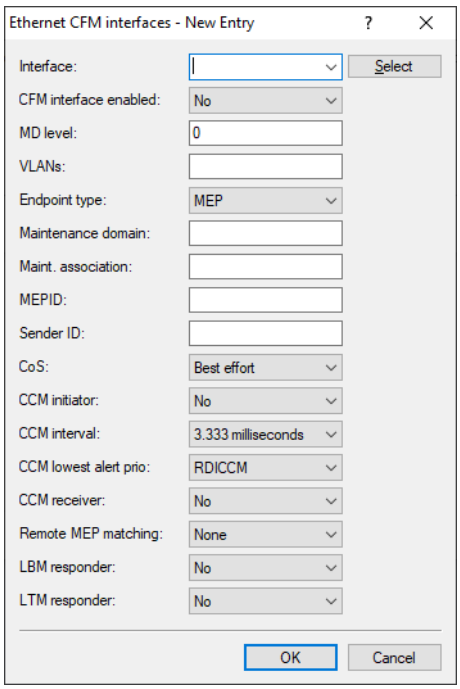
The CCM, Loopback, and Linktrace functions can be used independently, meaning Loopback and Linktrace can be utilized even without regular CCM messages.

Additionally, LCOS supports the following functions from ITU-T Y.1731:

- Reception and status display of ETH-AIS (Alarm Indication Signal)
- Reception and status display of ETH-LCK (Ethernet Locked Signal)
- Reception and processing of ETH-RDI (Remote Defect Indication)

20.21.2.1 Ethernet CFM Interfaces

In LANconfig, configure Ethernet OAM according to IEEE 802.3ah under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Ethernet CFM Interfaces**.



Interface

Specifies the interface where CFM should be enabled. Possible values are LAN interfaces like LAN-1 or WAN interfaces like DSL-1.

CFM interface enabled

Enables or disables CFM on the configured interface.

MD level

Defines the Maintenance Domain Level for this interface.

VLANs

Defines the VLANs on the interface where CFM messages can be sent and received. If left empty, all VLANs are accepted. You can configure either a single VLAN or a comma-separated list of VLANs.

Endpoint type

Defines the CFM endpoint type. Possible values:

MEP (Maintenance Association End Point)

The Maintenance Association End Point represents the boundary of a domain and performs fault detection between the domain boundaries. The MEP creates and sends CFM packets.

MIP (Maintenance Intermediate Point)

The Maintenance Intermediate Point is located within the domain and performs path and fault detection within the domain boundaries. The MIP responds to CFM packets.

Maintenance domain

Specifies the name of the Maintenance Domain (MD).

Maintenance association

Specifies the name of the Maintenance Association (MA).

MEPID

Defines the Maintenance Endpoint ID of the device for this entry (1-8191). This must be unique on each device.

Sender ID

Specifies the optional Sender ID in CFM CCM messages.

CoS

Defines the Class of Service with which CFM CCM (Continuity Check Message) packets are marked. Possible values: Best-Effort (0), Background (1), Excellent-Effort (3), Controlled-Latency (4), Video (5), Voice (6), Network-Control (7).

CCM initiator

Specifies whether the device should send regular CCM (Continuity Check Message) packets.

CCM interval

Defines the interval at which CCM messages are sent by the device. CCM intervals must be consistent between communication partners.

CCM lowest alert prio

Defines the minimum severity level of detected issues required for the MEP to set the RDI (Remote Defect Indication) flag and propagate it in CCM packets. Levels, in ascending severity, include:

RDICCM

A CC frame with the RDI flag set was received from at least one other MEP.

MACstatus (Default)

At least one MEP reported an interface status other than 'up' (e.g., hardware issue), or all MEPs report a port status other than 'up' (e.g., network segment isolated).

RemoteCCM

No CCM frames are being received from at least one configured MEP.

ErrorCCM

Another MEP is using the same MEPID as the local device, or CCM frames are received from an unconfigured MEP (if Matching is not none), or a different CCM interval is being used by another MEP.

XconCCM

CC frames were received from another MEP with a lower MD level, or with a different domain or association.

CCM receiver

Specifies whether the device should process or receive CCM messages.

Remote MEP matching

Defines how the device handles remote MEP presence. Unconfigured remote MEPs can be dynamically learned or treated as an error if a configured remote MEP is not found.

None

Unconfigured MEPs are included in the status table and considered in RDICCM and MACstatus conditions.

Yes

Unconfigured MEPs are included in the status table but not considered in RDICCM and MACstatus conditions. They trigger ErrorCCM.

Strict

Unconfigured MEPs are not included in the status table and not considered in RDICCM and MACstatus conditions. They trigger ErrorCCM.

LBM responder

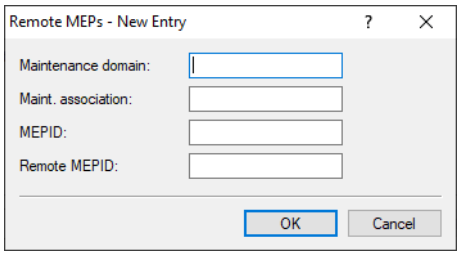
Defines whether the device should respond to CFM Loopback Messages (Ethernet Ping). This feature can be used independently of the CCM operating mode.

LTM responder

Defines whether the device should respond to CFM Linktrace Messages (Ethernet Traceroute). This feature can be used independently of the CCM operating mode.

20.21.2.2 Remote MEPs

In this table, you can optionally define remote MEPs that the device expects on the remote side. In LANconfig, configure these under **Miscellaneous Services** > **Services** > **OAM (Operation, Administration, Management)** > **Remote MEPs**.



Maintenance domain

Defines the name of the Maintenance Domain (MD).

Maintenance association

Defines the name of the Maintenance Association (MA).

MEPID

Defines the Maintenance Endpoint ID of the device for this entry (1-8191). This must be unique on each device.

Remote MEPID

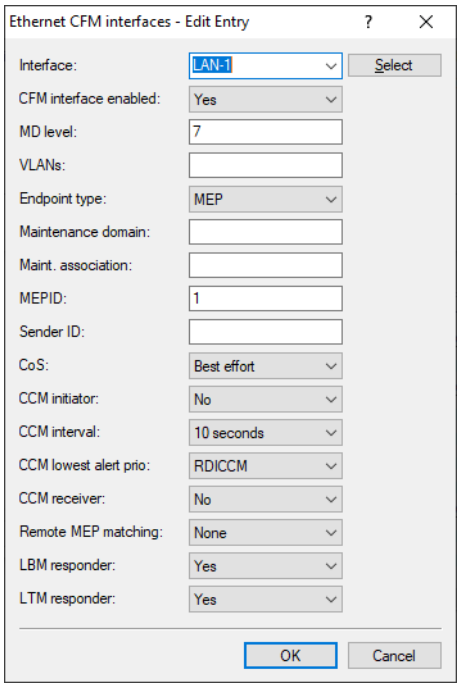
Defines the remote MEPID that is expected for this configuration (1-8191). This must be unique on each device.

20.21.2.3 Commands on the Console

Ethping

```
ethping -i <interface> [-?] [-c count] [-v vlan] [-s size] [-l mdlevel]
<target address>
```

Example: To use CFM Ethernet Ping, a minimal configuration in the Ethernet CFM Interfaces table is required. On the second device, a corresponding configuration is also necessary; however, the MEPID must differ or be unique. In this example, MD-Level 7 is used.




```
root@:/
> ethping -i LAN-1 -l 7 00:a0:57:9c:47:fd
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236825, time=0.130 ms
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236826, time=0.126 ms
    60 Byte Packet from 00:a0:57:9c:47:fd, seq.no=3109236827, time=0.125 ms

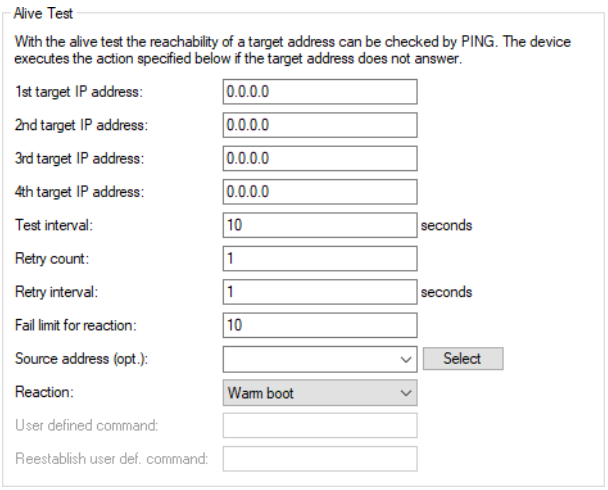
 ---00:a0:57:9c:47:fd ping statistic---
3 Packets transmitted, 3 Packets received, 0% loss
```

Instead of sending the CFM Ethernet Ping to an Ethernet unicast MAC address, the standardized multicast group can also be used. The structure of the multicast address is as follows: 01:80:C2:00:00:3x. Here, x is a value between 0 and 7 and corresponds to the domain level number for the MEP.

20.22 Alive Test

The alive test allows you to check the reachability of IPv4 addresses using ping. If no response is received or if connectivity is restored after being unreachable, the device can perform a configurable action.

In LANconfig, configure the Alive Test under **IPv4** > **General** > **Alive Test**.



Target IP address 1-4

Up to four possible target IPv4 addresses to which the device sends a ping. Only one address needs to be reachable for the Alive Test to be considered successful.

Test interval

The time interval in seconds at which the device sends a ping to the target addresses. If the ping is not answered, the device optionally sends a defined number of retries at specified intervals. With this configuration, the device forms "series" of ping attempts. Only if all these pings are unanswered is the entire series considered unsuccessful.

The product of fail limit and test interval defines the total time that elapses before a restart or the execution of the action.

Choose the test interval to be greater than the product of retry interval and retry count to ensure the desired retries can be performed within the test interval.

Retry count

This value specifies how often the device retries a failed ping to the target address.

Choose this value so that the product of retry interval and retry count is smaller than the chosen test interval to ensure the desired retries can be performed within the test interval.

Retry interval

This value specifies the time interval in which the device retries a failed ping to the target address. If the retry interval is set to 0, the device does not send any retries.

Choose this value so that the product of retry interval and retry count is smaller than the chosen test interval to ensure the desired retries can be performed within the test interval.

Fail limit for reaction

This parameter defines the number of consecutive failed test series before the device restarts or executes the configured action.

The product of this value and the test interval defines the total time that elapses before a restart or the execution of the action.

Source address (opt.)

Assign an optional source address (name of an ARF network, named loopback address, or IP address) to be used for the Alive Test.

Reaction

The action performed by the device if the ping to the target address fails.

Cold boot

The device performs a cold boot.

Warm boot (Default)

The device performs a warm boot.

User-defined command

The device executes a configurable action. Configure this command below.

User-defined command

Enter the action to be performed by the device if the target addresses are unreachable. Any console-executable command can be specified as an action.

This action is only executed if **Reaction** is set to **User-defined command**.

Reestablish user-defined command

Any console-executable command can be specified as a recovery action. This is executed once when the device transitions from the error state of unreachable target addresses to a state where the configured target address is reachable again.

This action is only executed if **Reaction** is set to **User-defined command**.

21 Appendix

21.1 CRON syntax

A CRON job consists of six fields:

```
minute    hour    day of month    month    day of week    command
```

The asterisk '*' serves as a placeholder for all permitted characters.

Here are some examples of performing regular restarts with the use of CRON:

Every day at 13:30h:

```
30        13        *        *        *        restart
```

Every day 30 minutes past each hour:

```
30        *         *        *        *        restart
```

Every 30 minutes every day:

```
*/30      *         *        *        *        restart
```

Every Saturday at 20:15h:

```
15        20        *        *        6        restart
```

Sundays is selected either with '0' or '7'.

At 00:00h on the first day of the month

```
0         0         1        *        *        restart
```

21.2 Factory default active services according to EN 18031 GEC-4

In LCOS, the following network services are active in the factory default state:

Service	Function	Port
SSH	Device management	TCP 22
HTTP	Device management	TCP 80 (automatic redirect to HTTPS)
HTTPS	Device management	TCP 443
LL2M	Device management	Layer 2
LMC	Connection to LANCOM Management Cloud	TCP 443
TFTP	Device search with LANconfig (Sysinfo)	UDP 69
DHCP	DHCP Server	UDP 67
DHCPv6	DHCPv6 Server	UDP 547
DNS	DNS Server	UDP 53
ICMPv6	IPv6 control and diagnostic protocol	– (has no port)

Service	Function	Port
SNMPv3	Device monitoring	UDP 161