LCOS 10.94

R&S®LANCOM 1650E

Secure Internet access over Gigabit Ethernet

Small and medium-sized businesses often need secure and reliable access to the Internet as well as allowing mobile employees or branch offices to connect to the company headquarters. With the R&S®LANCOM 1650E and excellent R&S®LANCOM IPSec and WireGuard VPN, you can easily connect your sites. The connection to any DSL, cable, and fiber-optic modems offers the maximum flexibility with regard to the Internet lines available at the site. The SD-WAN functions of the branch router in combination with the R&S®LANCOM Management Cloud (R&S®LMC) not only simplify your network management, but also accelerate and automate the administration, monitoring, and rollout of your network components.

- Secure SD-WAN – centralized cloud management with secure network separation, automated provisioning, and intelligent path control
- Flexible connection of external modems via Gigabit Ethernet
- 3 integrated VPN channels
- Network virtualization with 2 networks on one device (ARF)
- Extended protection with the content filter of the R&S®LANCOM Security Essentials Option

R&S®LANCOM 1650E

WAN connectivity via Gigabit Ethernet

The Internet Access Router enables flexible connection of external provider modems via Gigabit Ethernet, offering maximum independence with regard to the Internet connections available at the site.

Reliable, intelligent site connectivity with Secure SD-WAN

Secure SD-WAN enables centrally managed and secure networking of all sites. In combination with the R&S®LANCOM Management Cloud (R&S®LMC), it allows company-wide security and access policies to be implemented, while rollouts, configurations, and updates are automated and accelerated. Encrypted Auto VPNs, High Scalability and Advanced Mesh VPNs, Dynamic Path Selection, as well as active/active WAN with load balancing ensure resilient, fail-safe connections.

Multi-layered security – automatically integrated

A SPI firewall is integrated into the LCOS operating system ex works (Built-in Security). Secure network segmentation is provided via ARF and VLAN, while PQ-PSKs protect against "store-now-decrypt-later" attacks and prepare for quantum resistance.

Encrypted communication via VPN

The gateway enables secure Internet connections for mobile employees, home offices, and locations via 3 integrated VPN channels (IPsec and WireGuard).

Individually upgradeable security with content filter

The R&S®LANCOM Security Essentials Option enhances the router with a cloud-based web and content filter that protects against phishing, ransomware, and malicious websites. Thanks to its unlimited number of users, the option is ideally suited for growing networks.

R&S®LANCOM 1650E

Layer 2 features	
VLAN	4.096 IDs based on IEEE 802.1q, dynamic assignment
Multicast	IGMP-Snooping, MLD-Snooping
Protocols	ARP-Lookup, LLDP, ARP, Proxy ARP, BOOTP, DHCP
Layer 3 features	
Firewall	Stateful inspection firewall including paket filtering, extended port forwarding, N:N IP address mapping, paket tagging, support for DNS targets, user-defined rules and notifications
Quality of Service	Traffic shaping, bandwidth reservation, DiffServ/TOS, packetsize control, layer-2-in-layer-3 tagging, support for 8 QoS queues (6 free configurable)
Security	Intrusion Prevention, IP spoofing, access control lists, Denial of Service protection, detailed settings for handling reassembly, session-recovery, PING, stealth mode and AUTH port, URL blocker, password protection, programmable reset button
PPP authentication mechanisms	PAP, CHAP, MS-CHAP, and MS-CHAPv2
High availability / redundancy	VRRP (Virtual Router Redundancy Protocol)
Router	IPv4-, IPv6-, IPv4/IPv6 dual stack
SD-WAN Application Routing	SD-WAN Application Routing in connection with the R&S®LANCOM Management Cloud
SD-WAN dynamic path selection	SD-WAN dynamic path selection in connection with the R&S®LANCOM Management Cloud
SD-WAN Zero Touch Deployment	Zero touch commissioning of the device in conjunction with the R&S®LANCOM Management Cloud
Router virtualization	ARF (Advanced Routing and Forwarding) up to separate processing of 2 contexts
IPv4 services	HTTP and HTTPS server for configuration by web interface, DNS client, DNS server, DNS relay, DNS proxy, dynamic DNS client, DHCP client, DHCP relay and DHCP server including autodetection, NTP client, SNTP server, policy-based routing, Bonjour-Proxy, RADIUS
IPv6 services	HTTP and HTTPS server for configuration by web interface, DHCPv6 client, DHCPv6 server, DHCPv6 relay, DNS client, DNS server, dynamic DNS client, NTP client, SNTP server, Bonjour-Proxy, RADIUS
Dynamic routing protocols	RIPv2
IPv4 protocols	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (server), RADIUS, RADSEC (secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
IPv6 protocols	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, Syslog, SNMPv1,v2c,v3, MLDv2, NPTv6 (NAT66), VRRPv3
WAN operating mode	VDSL, ADSL1, ADSL2 or ADSL2+ additional with external DSL modem at an ETH port
WAN protocols	PPPoE, Multi-PPPoE, GRE, EoGRE, PPTP (PAC or PNS), L2TPv2 (LAC or LNS), L2TPv3 with Ethernet-Pseudowire and IPoE (using DHCP or no DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IP(v6)oE (autokonfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT
Security	
Intrusion Prevention	Monitoring and blocking of login attempts and port scans
IP spoofing	Source IP address check on all interfaces: only IP addresses belonging to the defined IP networks are allowed
Access control lists	Filtering of IP or MAC addresses and preset protocols for configuration access
Denial of Service protection	Protection from fragmentation errors and SYN flooding
General	Detailed settings for handling reassembly, PING, stealth mode and AUTH port
Password protection	Password-protected configuration access can be set for each interface
Two-factor authentication	Two-factor authentication (2FA) for local device management via WEBconfig, SSH or Telnet with external Authenticator application

R&S®LANCOM 1650E

Security	
Alerts	Alerts via e-mail, SNMP traps and SYSLOG
Authentication mechanisms	PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanism
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
High availability / redundancy	
VRRP	VRRP (Virtual Router Redundancy Protocol VRRPv2 and VRRPv3) for backup in case of failure of a device or remote station.
FirmSafe	For completely safe software upgrades thanks to two stored firmware versions, incl. test mode for firmware updates
Load balancing	Static and dynamic load balancing over up to 2 WAN connections. Channel bundling with Multilink PPP (if supported by network operator)
VPN redundancy	Backup of VPN connections across different hierarchy levels, e.g. in case of failure of a central VPN concentrator and re-routing to multiple distributed remote sites. Any number of VPN remote sites can be defined (the tunnel limit applies only to active connections). Up to 32 alternative remote stations, each with its own routing tag, can be defined per VPN connection. Automatic selection may be sequential, or dependant on the last connection, or random (VPN load balancing)
Line monitoring	Line monitoring with LCP echo monitoring, dead-peer detection and up to 4 addresses for end-to-end monitoring with ICMP polling
VPN	
IPSec over HTTPS	Enables IPsec VPN based on TCP (at port 443 like HTTPS) which can go through firewalls in networks where e. g. port 500 for IKE is blocked. Suitable for client-to-site connections and site-to-site connections. IPSec over HTTPS is based on the NCP VPN Path Finder technology
Number of VPN tunnels	Max. number of concurrent active WireGuard or IPSec, PPTP (MPPE) and L2TPv2 tunnels: 3. Unlimited configurable connections.
Hardware accelerator	Integrated hardware accelerator for 3DES/AES encryption and decryption
Realtime clock	Integrated, buffered realtime clock to save the date and time during power failure. Assures timely validation of certificates in any case
Random number generator	Generates real random numbers in hardware, e. g. for improved key generation for certificates immediately after switching-on
1-Click-VPN Client assistant	One click function in LANconfig to create VPN client connections, incl. automatic profile creation for the R&S®LANCOM Advanced VPN Client
1-Click-VPN Site-to-Site	Creation of VPN connections between R&S®LANCOM routers via drag and drop in LANconfig
IKE, IKEv2	IPSec key exchange with Preshared Key or certificate (RSA signature, ECDSA-Signature, digital signature)
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL. Secure Key Storage protects a private key (PKCS#12) from theft.
Certificate rollout	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) per certificate hierarchy
Certificate revocation lists (CRL)	CRL retrieval via HTTP per certificate hierarchy
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs
XAUTH	XAUTH client for registering R&S®LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at R&S®LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token
RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single configuration entry
Proadaptive VPN	Automated configuration and dynamic creation of all necessary VPN and routing entries based on a default entry for site-to-site connections.
Algorithms	3DES (168 bit), AES-CBC and -GCM (128, 192 or 256 bit), RSA (1024-4096 bit), ECDSA (P-256-, P-384-, P-521-curves) and Chacha20-Poly 1305. OpenSSL implementation with FIPS-140 certified algorithms. MD-5, SHA-1, SHA-256, SHA-384 or SHA-512 hashes
Post-quantum security	Post-quantum Preshared Keys (PPK) for IKEv2

R&S®LANCOM 1650E

VPN	
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
MOBIKE	IKEv2 VPN clients can seamlessly switch between different networks (e.g. from WLAN to mobile radio) without having to re-establish the VPN tunnel
WireGuard	Support of WireGuard
R&S®LANCOM Dynamic VPN	Enables VPN connections from or to dynamic IP addresses. The IP address is communicated via the ICMP or UDP protocol in encrypted form. Dynamic dial-in for remote sites via connection template
Dynamic DNS	Enables the registration of IP addresses with a Dynamic DNS provider in the case that fixed IP addresses are not used for the VPN connection
Specific DNS forwarding	DNS forwarding according to DNS domain, e.g. internal names are translated by proprietary DNS servers in the VPN. External names are translated by Internet DNS servers
Split DNS	Allows the selective forwarding of traffic for IKEv2 depending on the addressed DNS domain.
IPv4 VPN	Connecting private IPv4 networks
IPv4 VPN over IPv6 WAN	Use of IPv4 VPN over IPv6 WAN connections
IPv6 VPN	Connecting private IPv6 networks
IPv6 VPN over IPv4 WAN	Use of IPv6 VPN over IPv4 WAN connections
Radius	RADIUS authorization and accounting, outsourcing of VPN configurations in external RADIUS server in IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Transmission of multiple, securely separated networks within a VPN tunnel
Advanced Mesh VPN	On demand dynamic VPN tunnel establishment between branches
Performance	
Routing-Performance	Data regarding the overall routing performance can be found inside the R&S®NC tech paper "Routing-Performance" here.
VoIP	
SIP ALG	The SIP ALG (Application Layer Gateway) acts as a proxy for SIP communication. For SIP calls the ALG opens the necessary ports for the corresponding media packets. Automatic address translation (STUN is no longer needed).
Interfaces	
WAN: Ethernet	10/100/1000 Mbps Gigabit Ethernet
Ethernet ports	3 individual 10/100/1000 Mbps Ethernet ports; up to 3 ports can be operated as additional WAN ports with load balancing. Ethernet ports can be electrically disabled within LCOS configuration. The ports support energy saving according to IEEE 802.3az
Port configuration	Each Ethernet port can be freely configured (LAN, DMZ, WAN, monitor port, off). LAN ports can be operated as a switch or separately. Additionally, external DSL modems or termination routers can be operated as a WAN port with load balancing and policy-based routing. DMZ ports can be operated with their own IP address range without NAT
USB 2.0 host port	USB 2.0 hi-speed host port for connecting USB printers (USB print server), USB data storage (FAT file system); bi-directional data exchange is possible
Serial interface	Serial configuration interface / COM port (USB-C): 9,600 - 115,000 baud.
Management and monitoring	
Management	R&S®LANCOM Management Cloud, LANconfig, WEBconfig, R&S®LANCOM Layer 2 management (emergency management)
Management functions	Alternative boot configuration, voluntary automatic updates for LCMS and LCOS, individual access and function rights up to 16 administrators, RADIUS and RADSEC user management, remote access (WAN or (W)LAN, access rights (read/write) adjustable seperately), SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, access rights via TACACS+, scripting, timed control of all parameters and actions through cron job
FirmSafe	Two stored firmware versions, incl. test mode for firmware updates

R&S®LANCOM 1650E

Management and monitoring	
automatic firmware update	configurable automatic checking and installation of firmware updates
Monitoring	R&S®LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring functions	Device SYSLOG, SNMPv1,v2c,v3 incl. SNMP-TRAPS, extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, internal logging buffer for firewall events
Monitoring statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter, accounting information exportable via LANmonitor and SYSLOG
IPerf	IPerf is a tool for measurements of the bandwidth on IP networks (integrated client and server)
SLA-Monitor (ICMP)	Performance monitoring of connections
Netflow	Export of information about incoming and outgoing IP traffic
SD-LAN	SD-LAN – automatic LAN configuration via the R&S®LANCOM Management Cloud
SD-WAN	SD-WAN – automatic WAN configuration via the R&S®LANCOM Management Cloud
Hardware	
Weight	0,99 lbs (450 g)
Environment	Temperature range 0–40°C; humidity 0–95%; non-condensing
Housing	Robust synthetic housing, rear connectors, ready for wall mounting, Kensington lock; 210 x 45 x 140 mm (W x H x D)
Fans	None; fanless design without rotating parts, high MTBF
waste heat (max.)	48 BTU/h
Power consumption (max./idle)	12 watt / 6 watt
Declarations of conformity*	
Europe/EFTA	CE
Country of Origin	Made in Germany
***) Note**	The full text of the specific Declaration of Conformity is available here
Scope of delivery	
Manual	Quick Installation Guide (DE/EN)
Cable	1 Ethernet cable, 3 m
Power supply unit	External power adapter (230 V), NEST 12 V/2.0 A DC, coaxial power connector 2.1/5.5 mm, temperature range from -5 to +45° C, R&S®LANCOM item no. 111303 (EU)
Support	
Warranty extension	Free warranty extension up to 3 years (replacement service for defects) Find details here. The service and support conditions valid as of July 1, 2026, available at rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-and-Support-Conditions-20260701.pdf, apply.
Security updates	Up to 2 years after End of Sale of the device (but min. 3 years, see Link), can be extended by purchasing R&S®NC Support products
Software updates	Regular free updates including new features as part of the R&S®NC Lifecycle Management (Link)
Information on the EU Data Act	For details on product data and data on connected services, please refer to: Link
Manufacturer support	Available with R&S®NC products such as Support Access (for R&S®NC Community Partners only), Direct, or Premium
R&S®NC Support Access	Exclusively forR&S®NC Community partners: Personal manufacturer support (best effort) and security updates for the device, valid for all service categories, term-based (starting at the beginning of each quarter) for 1, 3, or 5 years (item no. 10804, 10805, or 10806)

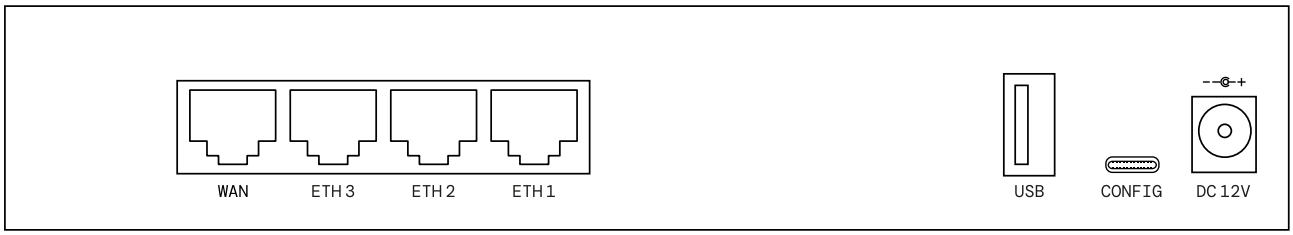
R&S®LANCOM 1650E

Support	
R&S®NC Replacement Basic S	Security updates until EOL (min. 5 years) and 5 years replacement service with shipment of the replacement device within 5 days after arrival of the defective device (8/5/5Days), item no. 10720
R&S®NC Replacement Advanced S	Security updates until EOL (min. 5 years) and 5 years NBD advance replacement with delivery of the replacement device within one business day (8/5/NBD), item no. 10730
R&S®NC Support Direct 24/7 S	Direct, prioritized 10/5 manufacturer support incl. 24/7 emergency hotline and security updates for the device, guaranteed first response times (SLA) of max. 30 minutes for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years (item no. 10752, 10753 or 10754)
R&S®NC Support Direct Advanced 24/7 S	Direct, prioritized 10/5 manufacturer support incl. 24/7 emergency hotline and security updates for the device, NBD advance replacement with delivery of the device on the next business day (24/7/NBD), guaranteed first response times (SLA) of max. 30 minutes for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years (item no. 10776, 10777 or 10778)
R&S®NC Support Direct 10/5 S	Direct, prioritized 10/5 manufacturer support and security updates for the device, guaranteed first response times (SLA) of max. 2 hours for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years.(item no. 10740, 10741 or 10742)
R&S®NC Support Direct Advanced 10/5 S	Direct, prioritized 10/5 manufacturer support and security updates for the device, NBD advance replacement with delivery of the device on the next business day (10/5/NBD), guaranteed first response times (SLA) of max. 2 hours for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years.(item no. 10764, 10765 or 10766)
Software	
Lifecycle Management	After discontinuation (End of Sale), the device is subject to the R&S®NC Lifecycle Management. Details can be found at: Link
IT Security made in Germany	The development and quality assurance take place in Germany in accordance with high security standards. The „IT Security made in Germany" quality label of the German IT Security Association attests to the level of security achieved.
Options	
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 1-Year (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62168
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 3-Years (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62169
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 5-Years (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62170
R&S®LANCOM BPjM Filter	R&S®LANCOM BPjM Filter Option, 5 years subscription, item no. 61418
R&S®LANCOM All-IP Lizenz Option	Upgrade option for the operation of the R&S®LANCOM routers with All-IP connections, support of PBX systems and telephony devices as well as voice & fax services, incl. Voice Call Manager, item no. 61419
R&S®LANCOM VoIP +10 Option	Upgrade for R&S®LANCOM VoIP router with 10 additional internal VoIP numbers (additionally up to 40) and 10 external SIP lines (additionally up to 55) item no. 61423
R&S®LANCOM Management Cloud	
R&S®LANCOM Management Cloud	R&S®LMC-A-1Y License (1 Year), enables the management of one category A device for one year via the R&S®LANCOM Management Cloud, item no. 50100
R&S®LANCOM Management Cloud	R&S®LMC-A-3Y License (3 Years), enables the management of one category A device for three years via the R&S®LANCOM Management Cloud, item no. 50101
R&S®LANCOM Management Cloud	R&S®LMC-A-5Y License (5 Years), enables the management of one category A device for five years via the R&S®LANCOM Management Cloud, item no. 50102
Accessories	
VPN Client Software	R&S®LANCOM Advanced VPN Client for Windows - single license, item no. 61600
VPN Client Software	R&S®LANCOM Advanced VPN Client for Mac OS X, single license, item no. 61606

LCOS 10.94

R&S®LANCOM 1650E

Item number(s)	
R&S®LANCOM 1650E (EU)	62163



Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions. 09/2026

ROHDE&SCHWARZ
Make ideas real