LCOS LX 7.20

Menüreferenz

10/2026

ROHDE&SCHWARZ
Make ideas real

Inhalt

1 Einleitung....7
1.1 Bestandteile der Dokumentation....7
1.2 LCOS LX, ein Betriebssystem von R&S®NC....7
1.3 Gültigkeit....8
1.4 Konsole – Zugang....8
1.5 Konsole – Menüstruktur....8
1.6 Konsole – Befehlsübersicht....9
2 Setup....15
2.1 Name....15
2.9 SNMP....15
2.9.1 Send-Traps....15
2.9.21 Port....16
2.9.27 Communities....16
2.9.28 Groups....17
2.9.29 Accesses....19
2.9.30 Views....22
2.9.32 Users....24
2.9.34 Target-Addresses....27
2.9.35 Target-Params....28
2.9.37 Admitted-Protocols....30
2.9.38 Allow-Admins....31
2.9.41 Operating....31
2.11 Config....32
2.11.1 Comment-1....32
2.11.2 Comment-2....32
2.11.3 Comment-3....32
2.11.4 Comment-4....33
2.11.5 Comment-5....33
2.11.6 Comment-6....33
2.11.7 Comment-7....33
2.11.8 Comment-8....34
2.11.9 Location....34
2.11.10 Administrator....34
2.11.11 Config-Aging-Minutes....35
2.11.18 LED-Mode....35
2.11.20 Cron-Table....35
2.11.21 Admins....38
2.11.50 LL2M....39
2.11.51 Tacacs-Plus....41
2.11.52 SSH....44

2.11.90 LED-Off-Seconds....46
2.11.91 LED-Test....46
2.11.99 Root-Hashed....47
2.11.130 PoE-Passthrough....47
2.14 Time....48
2.14.15 Holidays....48
2.14.16 Timeframes....48
2.14.20 Timezone....50
2.14.21 NTP....51
2.20 WLAN....52
2.20.1 Network....53
2.20.2 Country....64
2.20.3 Encryption....65
2.20.4 Band-Steering....73
2.20.5 Client-Isolation-Allowed....80
2.20.8 Radio-Settings....82
2.20.9 Automatic-Environment-Scan-Enabled....89
2.20.10 Automatic-Environment-Scan-Time-Begin....89
2.20.11 Automatic-Environment-Scan-Time-End....90
2.20.12 Hotspot....90
2.20.13 WDS....94
2.20.14 Include-UUID....101
2.20.15 Power-Saving-Mode....102
2.20.16 Include-Devicename....102
2.20.18 Client-Management....103
2.20.19 Client-Management-Mode....105
2.20.20 End2End-Test....106
2.20.133 LEPS....120
2.20.1111 Rate-Selection....123
2.22 Syslog....126
2.22.2 Server....126
2.23 Logging....127
2.23.1 Operating....128
2.23.2 Timer-Seconds....128
2.23.3 Level....128
2.23.4 Target....129
2.23.5 Trace....129
2.23.6 Log-Persistence....130
2.30 RADIUS....130
2.30.3 RADIUS-Server....130
2.30.4 Delete-WLAN-Supplicant-Certificates....133
2.30.11 LAN-Supplicant....133
2.30.12 WLAN-Supplicant....135
2.40 Multicast-Snooping....137

2.40.1 Operating....138
2.45 Bridge....138
2.45.1 DHCP-Snooping....138
2.46 mDNS-Filter....139
2.46.1 Services....140
2.46.2 Services-List....140
2.47 Firewall....141
2.47.1 Rules....142
2.47.2 Host-Groups....144
2.47.3 Log-Actions....145
2.59 WLAN-Management....145
2.59.1 Static-WLC-Configuration....146
2.59.2 Operating....147
2.59.3 Update-Cert-Before....147
2.59.4 Capwap-Port....147
2.60 Power....148
2.60 Dual-PoE-Mode....148
2.61 L2TP....148
2.61.1 Endpoints....149
2.61.2 Ethernet....152
2.62 LAN....153
2.62.1 LACP....153
2.62.2 Ethernet-Ports....155
2.62.3 Spanning-Tree....157
2.70 IP-Configuration....162
2.70.4 Static-Parameters....162
2.70.6 LAN-Interfaces....164
2.70.8 Untagged-VLAN....166
2.99 LBS....167
2.99.1 HTTP-Server....168
2.99.2 Operating....170
2.99.3 LBS-Server-Type....170
2.99.4 BLE-Scan-Type....170
2.99.5 Run-Bluetooth-Scan....171
2.99.6 Delete-CA-Certificate....171
2.99.7 Delete-Scan-Results....171
2.102 LMC....171
2.102.1 Operating....172
2.102.2 Proxy....172
2.102.7 Delete-Certificate....173
2.102.8 DHCP-Client-Auto-Renew....174
2.102.13 Configuration-Via-DHCP....174
2.102.15 LMC-Domain....175
2.102.16 Rollout-Project-ID....175

2.102.17 Rollout-Location-ID....175
2.102.18 Rollout-Device-Role....176
2.102.200 Pairing-Token....176
2.107 Automatic-Firmware-Update....176
2.107.1 Mode....176
2.107.2 Check-Firmware-Now....177
2.107.3 Update-Firmware-Now....177
2.107.4 Cancel-Current-Action....178
2.107.5 Reset-Updater-Config....178
2.107.6 Base-URL....178
2.107.7 Check-Interval....178
2.107.8 Version-Policy....179
2.107.10 Check-Time-Begin....179
2.107.11 Check-Time-End....180
2.107.12 Install-Time-Begin....180
2.107.13 Install-Time-End....180
2.111 IoT....181
2.111.1 USB....181
2.111.88 Wireless-ePaper....182
3 Firmware....190
3.2 Table-Firmsafe....190
3.2.1 Position....190
3.2.2 Status....190
3.8 Switch-Firmware....191
3.10 Boot-count....191
4 Other....192
4.1 Reset-Config....192
4.2 Reboot....192
4.3 Delayed-Reboot....192
4.4 Cancel-Delayed-Reboot....193
4.5 Delete-Support-Info....193
1 Status....194
1.62 Syslog....194
1.62.1 Last-Messages....194

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Hinweis zur Unternehmensbezeichnung: LANCOM Systems heißt seit dem 01.07.2026 **Rohde & Schwarz Networks and Cybersecurity**. Produktinformationen und Kommunikationsmaterialien werden entsprechend unter der neuen Unternehmensbezeichnung geführt.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. Rohde & Schwarz Networks and Cybersecurity haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von Rohde & Schwarz Networks and Cybersecurity gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u. a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS LX) finden Sie über die Kommandozeile mit dem Befehl `show 3rd-party-licenses`. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Wenden Sie sich hierzu via E-Mail an *gpl.rs-nc@rohde-schwarz.com*.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*www.openssl.org*).

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.rohde-schwarz.com/networks-and-cybersecurity

1 Einleitung

1.1 Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

Installation Guide

In dieser Kurzanleitung finden Sie Antworten auf die folgende Fragen:

- Welche Software muss zur Konfiguration installiert werden?
- Wie wird das Gerät angeschlossen?
- Wie kann das Gerät über LANconfig bzw. WEBconfig erreicht werden?
- Wie wird das Gerät der R&S®LANCOM Management Cloud zugeordnet?
- Wie startet man die Setup-Assistenten (z. B. zur Einrichtung des Internetzugangs)?
- Wie wird ein Gerätereset durchgeführt?
- Wo gibt es weitere Informationen und Hilfe?

Hardware-Schnellübersicht

Die Hardware-Schnellübersicht enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Referenzhandbuch

Das Referenzhandbuch geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Die Beschreibungen im Referenzhandbuch orientieren sich überwiegend an der Konfiguration mit LANconfig.

Menü-Referenz

Die vorliegende Menü-Referenz beschreibt alle Parameter von LCOS LX. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte über die Konsole. Zu jedem Parameter werden neben der Beschreibung auch die möglichen Eingabewerte und die Standardbelegung wiedergegeben.

Alle Dokumente, die Ihrem Produkt nicht in gedruckter Form beiliegen, finden Sie als PDF-Datei unter *www.lancom-systems.de/downloads*.

1.2 LCOS LX, ein Betriebssystem von R&S®NC

LCOS LX ist das Betriebssystem für bestimmte R&S®LANCOM Access Points und Teil der R&S®NC Betriebssystem-Familie. Die R&S®NC Betriebssysteme sind die vertrauenswürdige Grundlage für das gesamte R&S®NC Produktportfolio. Jedes Betriebssystem verkörpert die R&S®NC Werte Sicherheit, Zuverlässigkeit und Zukunftsfähigkeit.

- **Für höchste Sicherheit Ihrer Netzwerke**

  wird jedes R&S®NC Betriebssystem in gewohnter Qualität von unseren Entwicklern sorgfältig gepflegt und weiterentwickelt und ist garantiert Backdoor-frei.

- **Sie stehen für größtmögliche Zuverlässigkeit,**

denn über die gesamte Lebenszeit eines Produktes werden regelmäßig Release Updates, Security Updates und Major Releases zur Verfügung gestellt.

› **Als Grundlage maximaler Zukunftsfähigkeit Ihrer Netzwerke**

stehen sie im Zuge der R&S®NC Lifecycle-Richtlinien für alle R&S®NC Produkte kostenlos zur Verfügung, inklusive neuer Major Features.

1.3 Gültigkeit

Die in diesem Handbuch beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt.

1.4 Konsole – Zugang

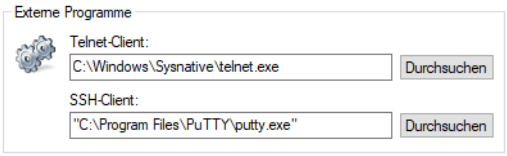
Der Zugang zur LCOS LX-Konsole erfolgt über SSH. Nutzen Sie einen SSH-Client wie z. B. PuTTY, um sich unter Angabe der IP-Adresse des Gerätes mit diesem zu verbinden.

Die Zugangsdaten eines Gerätes im Auslieferungszustand sind:

Benutzername: root

Passwort: <Leer> (es ist kein Passwort gesetzt)

Konfigurieren Sie den von Ihnen präferierten SSH-Client in LANconfig unter **Extras** > **Optionen** > **Extras** > **SSH-Client**:



Anschließend können Sie im Kontextmenü des Gerätes unter **WEBconfig / Konsolen-Sitzung** > **SSH-Sitzung öffnen** eine Konsole öffnen.

1.5 Konsole – Menüstruktur

Das LCOS LX-Kommandozeilen-Interface (die Konsole) ist wie folgt strukturiert:

Status

Enthält die Zustände und Statistiken aller internen Module des Gerätes. Diese sind hier nicht beschrieben, da sich die aufbereitete Visualisierung in WEBconfig empfiehlt. Alternativ können Sie für ihr Gerät die Management Information Base (MIB) herunterladen, welche für die Verwendung mit SNMPv3 die Einträge jeweils mit einer kurzen Beschreibung enthält. Die Geräte-MIB können Sie von *Download-Bereich* herunterladen.

Setup

Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes. Siehe *Setup*.

Sonstiges

Enthält Aktionen wie z. B. für den Reset oder den Reboot. Siehe *Other*.

1.6 Konsole – Befehlsübersicht

Das Kommandozeilen-Interface wird mit den folgenden Befehlen bedient.

Die verfügbaren Befehle sind abhängig vom Funktionsumfang des jeweiligen Gerätes.

Eine Übersicht der möglichen Befehle erhalten Sie ebenfalls, wenn Sie zweimal hintereinander die Tab-Taste drücken. Geben Sie nach dem Befehl die Option `--help` ein, um eine Übersicht möglicher Parameter zu erhalten.

Änderungen an der Konfiguration sind nicht sofort boot-persistent. Sie müssen mit dem Befehl `flash` explizit gespeichert werden.

Tabelle 1: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`add [<Path>]`	Fügt eine Tabellenzeile hinzu.
`beginscript`	Versetzt eine Konsolensitzung in den Skript-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM des Geräts übertragen, sondern zunächst in den Skript-Speicher. Der Modus wird mit dem Befehl `exit` beendet.
`cd <Path>`	Wechselt das aktuelle Menü bzw. Verzeichnis.
`default`	Setzt die Tabelle oder den Wert auf die Defaulteinstellung zurück. Dieses Kommando arbeitet rekursiv. Daher werden alle Werte und Tabellen sowohl im aktuellen als auch in allen darunter liegenden Pfaden zurückgesetzt.
`del <Path> <Index>`	Löscht den Wert oder die Tabellenzeile im mittels `<Path>` referenzierten Zweig des Menübaums. Als `<Index>` geben Sie dabei die Nummer der Zeile an.
`delete`	Synonym zu `del`.
`dir`	Synonym zu `ls`.
`do <Path> [<Parameter>]`	Führt die angegebene Aktion im aktuellen bzw. referenzierten Verzeichnis aus. Sofern die Aktion über zusätzliche Parameter verfügt, lassen sich diese nachfolgend angeben.
`exit`	Beendet die Terminalsitzung.
`flash`	Konfiguration speichern. Änderungen an der Konfiguration sind nicht sofort boot-persistent. Sie müssen mit dem Befehl `flash` explizit gespeichert werden.

Befehl	Beschreibung
`history`	Zeigt eine Liste der letzen ausgeführten Befehle.
`ll2mdetect`	LL2Mdetect erkennt LL2M-fähige Geräte im Netzwerk. Mit diesem Befehl schickt der LL2M-Client eine SYSINFO-Anfrage an den LL2M-Server. Der Server sendet daraufhin seine Systeminformationen wie Hardware, Seriennummer etc. zur Anzeige an den Client zurück. Der LL2Mdetect-Befehl lässt sich mit folgenden Parametern einschränken: **`-a <MAC-Adresse>`** Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse geben Sie in der Form `00a057010203`, `00-a0-57-01-02-03` oder `00:a0:57:01:02:03` an. Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder via `-b` alternativ als Broadcast) an alle LL2M-fähigen Geräte. Einzelne Stellen der MAC-Adresse können mit einem `*` oder `x` als Platzhalter besetzt werden, um Gruppen von MAC-Adressen anzusprechen, z. B. `00-a0-57-xx-xx-xx` für alle Geräte-MAC-Adressen. In einer Befehlszeile mit mehreren Parametern **muss** `-a` der abschließende Parameter sein. Eine andere Reihenfolge ist nicht zulässig. **`-b`** Versendet die LL2Mdetect-Anfrage explizit als Broadcast und nicht als Multicast. **`-f <Version>`** Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein. **`-r <Hardware-Release>`** Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein. **`-s <Serialnumber>`** Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein. **`-v <VLAN-ID>`** Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die

Befehl	Beschreibung
	VLAN-ID des ersten definierten IP-Netzwerks verwendet. **Eine Einschränkung des Befehls auf einen Hardware-Typ (mit dem Parameter "-t") ist bei LCOS LX nicht möglich.** Die Befehlszeile `ll2mdetect -r A` zum Beispiel versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release 'A'. Die Antwort des LL2M-Servers enthält dann die folgenden Angaben: › Name des Gerätes › Gerätetyp › Seriennummer › MAC-Adresse › Hardware-Release › Firmware-Version mit Datum

`ll2mexec`	Mit `ll2mexec` können Befehle an per `ll2mdetect` gefundene Geräte geschickt werden oder interaktive Konsolensessions aufgebaut werden.
	
	Mit diesem Befehl schickt der LL2M-Client ein einzeiliges Kommando zur Ausführung an den LL2M-Server. Mehrere Kommandos lassen sich durch Semikola getrennt in einem LL2M-Befehl kombinieren. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes zur Anzeige an den LL2M-Client übertragen. Der LL2Mexec-Befehl entspricht folgender Syntax:
	`ll2mexec -i <(W)LAN-Interface> <User>[:<Password>]@<MAC-Address>`
	
	Der LL2Mexec-Befehl lässt sich mit folgenden Parametern einschränken:
	
	`-i <(W)LAN-Interface>`
	Versendet den LL2Mexec-Befehl nur über das angegebene (W)LAN-Interface.
	
	`-v <VLAN-ID>`
	Versendet den LL2Mexec-Befehl nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet.
	
	Die Befehlszeile
	`ll2mexec -i ETH1 root@00a057010203 set /setup/name MyDevice`
	
	meldet z.B. den LL2M-Client als 'root' auf dem LL2M-Server mit der MAC-Adresse '00a057010203' an. Da das Passwort weggelassen wurde, sucht das Gerät zunächst nach dem entsprechenden Nutzernamen in der lokalen Datenbank und setzt automatisch das für diesen Nutzer gespeicherte Passwort ein. Wird auch der Nutzername weggelassen, werden die Anmeldedaten des aktuell für die CLI-Sitzung registrierten Nutzers verwendet. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert 'MyDevice'.

`list`	Synonym zu `ls`.

Befehl	Beschreibung
`ls [<Path>]`	Zeigt den Inhalt des aktuellen Verzeichnisses oder des angegebenen Pfades an.
`passwd <Password>`	Ändert das Passwort des aktuellen Benutzerkontos.
`ping [-c count] [-i interval] [-s packetsize] destination`	Sendet einen ICMP echo request an die angegebene IP-Adresse. Mögliche Optionsschalter sind: › `-c count`: Sende `count` Ping-Signale. › `-i interval`: Zeit zwischen den einzelnen Paketen in Sekunden. › `-s packetsize`: Setze Größe der Pakete auf `packetsize` Byte (max. 65500). › `destination`: Adresse oder Hostname des Zielcomputers.
`rm`	Synonym zu `del`.
`set <Index> {Column} <Value>`	Setzt den Wert einer bestimmten Spalte (Column) einer Tabellenzeile auf <Value>.
`set <Path> <Value(s)>`	Setzt den oder die Werte eines bestimmten Pfades auf den oder die angegebenen Werte.
`show diag [<Parameter>]`	Diagnoseinformationen auf der Konsole ausgeben.
`show 3rd-party-licenses`	Die Lizenzinformationen des Gerätes auf der Konsole ausgeben.
`startlmc <Activation Code> [Domain]`	Nachdem Sie in der R&S®LANCOM Management Cloud einen Aktivierungscode erzeugt haben, können Sie dieses Gerät über diesen Code mit der R&S®LANCOM Management Cloud koppeln. Optional können Sie dabei auch eine neue LMC-Domain angeben.
`sysinfo`	Zeigt Systeminformationen an (z. B. Hardware-Release, Softwareversion, MAC-Adresse, Seriennummer etc.).
`trace [--log] [+|-|#|?] <Parameter>`	Startet (`+`) oder stoppt (`-`) einen Trace-Befehl zur Ausgaben von Diagnose-Daten. `#` schaltet zwischen verschiedenen Trace-Ausgaben um und `?` zeigt einen Hilfetext an Über den Parameter `--log` kann die Ausgabe auf „historische“ Informationen aus dem Log eingeschränkt werden.
`writeconfig [noflash]`	Schreibt eine neue Konfiguration in Form einer LCF-Datei in das Gerät. Das System interpretiert alle folgenden Zeilen solange als Konfigurationswerte, bis zwei Leerzeilen auftreten. Dies wird z. B. von Managementsystemen genutzt. Mögliche Optionsschalter sind: › `noflash`: Die übergebene Konfiguration wird nicht persistiert. Dies kann durch das nachträgliche Ausführen des `flash`-Befehls erfolgen.

Legende

› Zeichen- und Klammernregelung:

  › Objekte – hier: dynamische oder situationsabhängige Eingaben – stehen in spitzen Klammern.
  › Runde Klammern gruppieren Befehlsbestandteile zur besseren Übersicht.
  › Vertikale Striche (Pipes) trennen alternative Eingaben.
  › Eckige Klammern beschreiben optionale Schalter.

  Somit sind alle Befehlsbestandteile, die nicht in eckigen Klammern stehen, notwendigen Angaben zuzurechnen.

› `<Path>`:

- Beschreibt den Pfadnamen für ein Menü, eine Tabelle oder einen Parameter, getrennt durch "/".
- `..` bedeutet: eine Ebene höher.
- `.` bedeutet: aktuelle Ebene.

- `<Value>`:
  - Beschreibt einen möglichen Eingabewert.
  - `""` ist ein leerer Eingabewert.

- `<Name>`:
  - Beschreibt eine Zeichensequenz von [0…9] [A…Z] [a…z] [_].
  - Das erste Zeichen darf keine Ziffer sein.
  - Es gibt keine Unterscheidung zwischen Groß- und Kleinschreibung.

- `<Filter>`:
  - Die Ausgaben einiger Kommandos können durch die Angabe eines Filterausdrucks eingeschränkt werden. Die Filterung erfolgt dabei nicht zeilenweise, sondern blockweise abhängig vom jeweiligen Kommando.
  - Ein Filterausdruck beginnt mit einem alleinstehenden '@' und endet entweder am Zeilenende oder an einem alleinstehenden ';', welches das aktuelle Kommando abschließt.
  - Ein Filterausdruck besteht des Weiteren aus einem oder mehreren Suchmustern, die durch Leerzeichen voneinander getrennt sind und denen entweder kein Operator ('Oder'-Muster) oder einer der Operatoren '+' ('Und'- Muster) oder '-' ('Nicht'-Muster) vorangestellt ist.
  - Bei der Ausführung des Kommandos wird ein Informationsblock genau dann ausgegeben, wenn mindestens eines der 'Oder'-Muster, alle 'Und'-Muster und keines der 'Nicht'-Muster passen. Dabei wird die Groß- und Kleinschreibung nicht beachtet.
  - Soll ein Suchmuster Zeichen enthalten, die zur Strukturierung in der Filtersyntax verwendet werden (z. B. Leerzeichen), dann kann das Suchmuster als Ganzes mit "" umschlossen werden. Alternativ kann den speziellen Zeichen ein '\' vorangestellt werden. Wenn ein "" oder ein '\' gesucht werden soll, muss diesem ein '\' vorangestellt werden.

    Es reicht die Eingabe des eindeutigen Wortanfangs.

Erläuterungen zur Adressierung, Schreibweise und Befehlseingabe

- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden, solange sie eindeutig sind. Zum Beispiel kann der Befehl `cd setup` zu `cd se` verkürzt werden. Die Eingabe `cd /s` dagegen ist ungültig, da dieser Eingabe sowohl `cd /Setup` als auch `cd /Status` entspräche.
- Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an.
- Mehrere Werte in einer Tabellenzeile können mit **einem** Befehl verändert werden, z. B. in der Tabelle der WLAN-Netzwerke (`/Setup/WLAN/Network`):
  - `add Guest Guest 1234567890` erstellt ein neues Netzwerk mit dem Namen Guest, der SSID Guest und dem Key 1234567890.

    Die Reihenfolge der Werte muss der Reihenfolge in der Tabelle entsprechen. Werte, die nicht verändert werden sollen, können mit einem * angegeben werden.
  - `set Guest * 0987654321` ändert den Wert Key im Netzwerk Guest. Die SSID wird durch den * unverändert gelassen.

- `set Guest {Key} 1234567890` setzt den Wert Key im Netzwerk Guest. Einzelne Spalten lassen sich durch den Spaltennamen in runden Klammern referenzieren.

- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.

Kommandospezifische Hilfe

- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Optionsschalter aufgerufen wird. Zum Beispiel zeigt der Aufruf `show ?` die Optionen des show-Kommandos an.

2 Setup

In diesem Menü finden Sie die Einstellungen des Gerätes.

Pfad Konsole:

/

2.1 Name

Konfigurieren Sie hier den Gerätenamen. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9 SNMP

Dieses Menü enthält die Konfiguration von SNMP.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *Download-Bereich* herunterladen können.

Pfad Konsole:

Setup

2.9.1 Send-Traps

Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der Tabelle Target-Addresses die Ziele ein, auf denen diese SNMP-Manager installiert sind.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

Yes
No

Default-Wert:

No

2.9.21 Port

Über diesen Parameter legen Sie den Port fest, über den der SNMP-Dienst für externe Programme wie z. B. LANmonitor erreichbar ist.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

0 … 65535

Default-Wert:

161

2.9.27 Communities

SNMP-Agents und SNMP-Manager gehören SNMP-Communities an. Diese Communities fassen bestimmte SNMP-Hosts zu Gruppen zusammen, um diese einerseits einfacher verwalten zu können. Andererseits bieten SNMP-Communities eine eingeschränkte Sicherheit beim Zugriff über SNMP, da ein SNMP-Agent nur SNMP-Anfragen von Teilnehmern akzeptiert, deren Community ihm bekannt ist.

In dieser Tabelle konfigurieren Sie die SNMP-Communities.

Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

Pfad Konsole:

Setup > **SNMP**

2.9.27.1 Name

Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.27.3 Security-Name

Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.27.8 Status

Mit diesem Eintrag aktivieren oder deaktivieren Sie diese SNMP-Community.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

Active
Die Community ist aktiviert.

Inactive
Die Community ist deaktiviert.

Default-Wert:

Active

2.9.28 Groups

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen.

Pfad Konsole:

Setup > **SNMP**

2.9.28.1 Security-Model

SNMPv3 hat das Prinzip des „Security Models“ eingeführt, so dass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3“ zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model“ auszuwählen.

Entsprechend wählen Sie hier ein Security-Modell aus.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

Any

Jedes Modell wird akzeptiert.

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv“.

SNMPv2_C

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv“.

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind die folgenden Sicherheitsstufen möglich:

NoAuthNoPriv

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthNoPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Default-Wert:

SNMPv3_USM

2.9.28.2 Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.9.28.3 Group-Name

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe. Diesen Namen verwenden Sie anschließend bei der Konfiguration der Zugriffsrechte.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.9.28.5 Status

Aktiviert oder deaktiviert diese Gruppenkonfiguration.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.29 Accesses

Diese Tabelle führt die verschiedenen Konfigurationen für Zugriffsrechte, Security-Models und Ansichten zusammen.

Pfad Konsole:

Setup > **SNMP**

2.9.29.1 Group-Name

Wählen Sie hier den Namen einer Gruppe aus, für die diese Zugriffsrechte gelten sollen.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.29.3 Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Any
Jedes Modell wird akzeptiert.
SNMPv1
SNMPv1 wird verwendet.
SNMPv2_C
SNMPv2c wird verwendet.
SNMPv3_USM
SNMPv3 wird verwendet.

Default-Wert:

Any

2.9.29.5 Read-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.29.6 Write-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.29.7 Notify-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Notify-Rechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.29.8 Status

Aktiviert oder deaktiviert diesen Eintrag.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.29.10 Min-Security-Level

Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

AuthPriv

2.9.30 Views

In dieser Tabelle fassen Sie verschiedene Werte oder ganze Zweige der MIB des Gerätes zusammen, die ein Benutzer gemäß seiner Zugriffsrechte einsehen oder verändern kann.

Pfad Konsole:

Setup > **SNMP**

2.9.30.1 View-Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.30.3 OID-Subtree

Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht einschließen soll.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *Download-Bereich* herunterladen können.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.30.4 Type

Bestimmen Sie, ob die nachfolgend angegebenen OID-Teilbäume Bestandteil („Included“) oder kein Bestandteil („Excluded“) der Ansicht sind.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Included

Diese Einstellung gibt MIB-Werten mit aus.

Excluded

Diese Einstellung blockt die Ausgabe von MIB-Werten.

Default-Wert:

Included

2.9.30.6 Status

Aktiviert oder deaktiviert diese Ansicht.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.32 Users

Dieses Menü enthält die Benutzerkonfiguration.

Pfad Konsole:

Setup > **SNMP**

2.9.32.2 Username

Geben Sie hier den SNMPv3 Benutzernamen an.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.9.32.5 Authentication-Protocol

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-96 (Hash-Länge 160 Bits).

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

2.9.32.6 Authentication-Password

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.14 Authentication-Password-Type* geändert wird.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `anything printable`

Default-Wert:

leer

2.9.32.8 Privacy-Protocol

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits).

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits).

AES256

Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

2.9.32.9 Privacy-Password

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.15 Privacy-Password-Type* geändert wird.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

2.9.32.13 Status

Aktiviert oder deaktiviert diesen Benutzer.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.32.14 Authentication-Password-Type

Das Passwort in *2.9.32.6 Authentication-Password* wird immer verschlüsselt abgelegt (Typ „Masterkey“). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext“ ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey“ zurücksetzen.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Plaintext
Masterkey

2.9.32.15 Privacy-Password-Type

Das Passwort in *2.9.32.9 Privacy-Password* wird immer verschlüsselt abgelegt (Typ „Masterkey“). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext“ ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey“ zurücksetzen.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Plaintext
Masterkey

2.9.34 Target-Addresses

In der Liste der Empfängeradressen konfigurieren Sie die Empfänger, an die der SNMP-Agent die SNMP-Traps versendet.

Pfad Konsole:

Setup > **SNMP**

2.9.34.1 Name

Geben Sie hier den Ziel-Adress-Namen an.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.34.3 Transport-Address

Die Transportadresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax <IP-Adresse>:<Port> angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.34.7 Parameters-Name

Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.34.9 Status

Aktiviert oder deaktiviert diese Zieladresse.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.35 Target-Params

In dieser Tabelle konfigurieren Sie, wie der SNMP-Agent die SNMP-Traps behandelt, die er an die Empfänger versendet.

Pfad Konsole:

Setup > **SNMP**

2.9.35.1 Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.35.2 Message-Processing-Model

Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

SNMPv1
SNMPv2c
SNMPv3

Default-Wert:

SNMPv3

2.9.35.3 Security-Model

Legen Sie mit diesem Eintrag das Sicherheitsmodell fest.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default-Wert:

SNMPv3_USM

2.9.35.4 Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.35.5 Security-Level

Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Traps beim Empfänger gelten soll.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Meldung ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

NoAuthNoPriv

2.9.35.7 Status

Aktiviert oder deaktiviert diesen Eintrag.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.37 Admitted-Protocols

Aktivieren Sie hier die SNMP-Versionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

SNMPv1
SNMPv2
SNMPv3

Default-Wert:

SNMPv3

2.9.38 Allow-Admins

Sollen registrierte Administratoren (darunter fällt auch der Benutzer root) auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.9.41 Operating

Dieser Eintrag aktiviert oder deaktiviert SNMP-Traps.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
SNMP-Traps sind ausgeschaltet.

Yes
SNMP-Traps sind eingeschaltet.

Default-Wert:

No

2.11 Config

Enthält die allgemeinen Konfigurationseinstellungen.

Pfad Konsole:

Setup

2.11.1 Comment-1

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.2 Comment-2

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.3 Comment-3

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.4 Comment-4

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.5 Comment-5

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.6 Comment-6

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.7 Comment-7

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.8 Comment-8

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.11.9 Location

Standort des Gerätes. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.11.10 Administrator

Name des Geräte-Administrators. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.11.11 Config-Aging-Minutes

Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine Konfigurations-Verbindung über TCP (z. B. SSH-Verbindung) automatisch beendet wird.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

15

2.11.18 LED-Mode

Bestimmen Sie die LED-Betriebsart.

Konsultieren Sie die Hardwareschnellübersicht des jeweiligen Gerätes für gerätespezifische Details zur LED-Signalisierung.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

On

Die LED(s) des Gerätes sind permanent in Betrieb und signalisieren den Betriebszustand.

Off

Die LED(s) des Gerätes werden nach dem Startvorgang sofort abgeschaltet.

Timed-Off

Die LED(s) des Gerätes werden nach einer konfigurierbaren Zeit (**LED-Off-Seconds**) abgeschaltet.

Default-Wert:

On

2.11.20 Cron-Table

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei jede beliebige Kommandozeilenfunktion. Es können damit also alle Features mit einer zeitlichen Steuerung versehen werden.

Die Funktion der einzelnen Felder entspricht weitestgehend der aus Linux/Unix bekannten Cron-Job-Konfiguration.

Pfad Konsole:

Setup > **Config**

2.11.20.1 Index

Dient der Sortierung mehrerer Cron-Jobs.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

2.11.20.2 Active

Bestimmt, ob der Job ausgeführt wird oder nicht.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

Yes
No

2.11.20.3 Base

Die Zeitbasis bestimmt, ob LCOS LX die zeitliche Steuerung des Befehls auf Grundlage der Echtzeit oder der Systemlaufzeit (entspricht der seit dem Gerätestart vergangenen Zeit) des Gerätes ausführt.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

Real-Time
Operating-Time

2.11.20.4 Minute

Wird die hier angegebene Minute erreicht, wird der Befehl ausgeführt.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 59 (1,2,3 or 0-59 or 1-3,59)`

2.11.20.5 Hour

Wird die hier angegebene Stunde erreicht, wird der Befehl ausgeführt.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 23 (1,2,3 or 0-23 or 1-3,23)`

2.11.20.6 DayOfWeek

Der Befehl wird an den hier per Zahlen angegebenen Wochentagen ausgeführt. Die Ziffern der Wochentage werden dabei durch Kommata voneinander getrennt. 0 entspricht Sonntag, 1 entspricht Montag, …, 6 entspricht Samstag

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 6 (1,2,3 or 0-6 or 1-3,6)`

2.11.20.7 Day

Der Befehl wird an den hier angegebenen Tagen des Monats (von 1 bis 31) ausgeführt.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 1 and 31 (1,2,3 or 1-7 or 1-3,7,8-9)`

2.11.20.8 Month

Der Befehl wird an den hier angegebenen Monaten (von 1 bis 12) ausgeführt.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 1 and 12 (1,2,3 or 1-7 or 1-3,7,8-9)`

2.11.20.9 Command

Der auszuführende CLI-Befehl.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

2.11.20.10 Comment

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.11.21 Admins

Legen Sie für Administratoren in dieser Tabelle an, die gegebenenfalls über eingeschränkte Rechte verfügen.

Der Administrator root hat immer alle Rechte.

Pfad Konsole:

Setup > **Config**

2.11.21.1 Administrator

Anmeldename des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-.`

2.11.21.3 Function-Rights

Aktivieren Sie hier die Funktionsrechte des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

Basic
Admin-Management

2.11.21.5 Rights

Die Rechte des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

None
Admin-RO-Limit
Admin-RW-Limit
Admin-RO
Admin-RW
Supervisor

2.11.21.6 Hashed-Password

Hashwert des Passworts des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.11.50 LL2M

Alle Wege zur Konfiguration eines Geräts setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem Gerät voraus. Egal ob LANconfig, WEBconfig oder SSH – ohne IP-Verbindung können keine Befehle zur Konfiguration an das Gerät übertragen werden. Im Falle

einer Fehlkonfiguration der TCP/IP-Einstellungen oder der VLAN-Parameter kann es vorkommen, dass diese benötigte IP-Verbindung nicht mehr hergestellt werden kann. In diesen Fällen hilft nur ein Reset des Gerätes auf den Auslieferungszustand. Diese Möglichkeit setzt aber den physikalischen Zugriff auf das Gerät voraus, der z. B. bei der verdeckten Montage von Access Points nicht immer gegeben ist oder in größeren Szenarien erheblichen Aufwand darstellen kann.

Um auch ohne IP-Verbindung einen Konfigurationszugriff auf ein Gerät zu ermöglichen, wird das **R&S®NC Layer 2 Management Protokoll (LL2M)** verwendet. Dieses Protokoll benötigt nur eine Verbindung auf Layer 2, also auf dem direkt oder über Layer-2-Switches angebundenen Ethernet, um eine Konfigurationssitzung aufzubauen. LL2M-Verbindungen werden auf LAN- oder WLAN-Verbindungen unterstützt, nicht jedoch über das WAN. Die Verbindungen über LL2M sind passwortgeschützt und gegen Replay-Attacken resistent.

LL2M etabliert dazu eine Client-Server-Struktur: Der LL2M-Client schickt Anfragen oder Befehle an den LL2M-Server, der die Anfragen beantwortet oder die Befehle ausführt. Sowohl der LL2M-Client als auch der LL2M-Server sind im LCOS LX integriert. Die Befehle des LL2M-Clients werden über die Konsole oder die WEBconfig ausgeführt.

Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die Befehle `LL2Mdetect` bzw. `LL2Mexec`. Siehe *1.6 Konsole – Befehlsübersicht*.

Zum Ausführen der Befehle für den LL2M-Client müssen Sie über Root-Rechte auf dem LL2M-Server verfügen.

Access Points vom Typ R&S®LANCOM LW-500 sind nur über LL2M auffind- und konfigurierbar, wenn LL2M-Pakete den Access Point mit einem VLAN-Tag erreichen, welches in der Konfiguration des Access Points enthalten ist (WLAN-SSID-Konfiguration oder Management-VLAN-Konfiguration).

Dieses Menü enthält die Einstellungen für das R&S®NC Layer-2 Management.

Pfad Konsole:

Setup > **Config**

2.11.50.1 Operating

Schaltet den LL2M-Server ein oder aus.

Pfad Konsole:

Setup > **Config** > **LL2M**

Mögliche Werte:

No

LL2M-Server ist ausgeschaltet.

Yes

LL2M-Server ist eingeschaltet.

Default-Wert:

Yes

2.11.50.2 Interfaces

Hier können Sie die Interfaces bzw. Ethernet-Ports angeben, auf denen Sie den LL2M-Server erreichen können. Voreingestellt ist die Erreichbarkeit auf allen Ethernet-Ports. Ein Zugang über WLAN ist nicht vorgesehen.

Pfad Konsole:

Setup > **Config** > **LL2M**

2.11.50.2.1 Port

Portbezeichnung, z.B. ETH1.

Pfad Konsole:

Setup > **Config** > **LL2M** > **Interfaces**

Mögliche Werte:

max. 5 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.11.50.2.2 Active

Schaltet den LL2M-Server für diesen Port ein oder aus.

Pfad Konsole:

Setup > **Config** > **LL2M** > **Interfaces**

Mögliche Werte:

No
Yes

Default-Wert:

Yes

2.11.51 Tacacs-Plus

Konfigurieren Sie hier Authentifizierung, Autorisierung und Accounting (AAA) mittels des TACACS+-Protokolls.

Ist dieses Feature aktiv, werden Admin-Anmeldungen gegen den TACACS+-Server geprüft und angezeigte und geänderte Konfigurationspunkte an den TACACS+-Server zur Freigabe und / oder Logging übertragen.

Die Übertragung der Konfigurationspunkte erfolgt in OID-Darstellung.

Bei aktivem TACACS+-Betrieb ist die WEBconfig des Geräts abgeschaltet.

Pfad Konsole:

Setup > **Config**

2.11.51.1 Operating

Schaltet die Verwendung von TACACS+ ein oder aus.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

No

TACACS+-Betrieb ist ausgeschaltet.

Yes

TACACS+-Betrieb ist eingeschaltet.

Default-Wert:

No

2.11.51.2 Internal-fallback-allowed

Ist diese Option aktiviert, kann bei nicht erreichbaren TACACS+-Servern ein Login mit lokalen Benutzerdaten durchgeführt werden.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

No

Authentifizierungs-Fallback ist ausgeschaltet.

Yes

Authentifizierungs-Fallback ist eingeschaltet.

Default-Wert:

Yes

2.11.51.10 Server-Address

Die IP-Adresse des primären TACACS+-Servers.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

2.11.51.11 Server-Port

Der Port des primären TACACS+-Servers.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

0 … 65535

Default-Wert:

49

2.11.51.12 Server-Secret

Der für die Kommunikation mit dem primären TACACS+-Server verwendete Schlüssel.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

2.11.51.20 Spare-Server-Address

Die IP-Adresse des Backup-TACACS+-Servers.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

2.11.51.21 Spare-Server-Port

Der Port des Backup-TACACS+-Servers.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

0 … 65535

Default-Wert:

49

2.11.51.22 Spare-Server-Secret

Der für die Kommunikation mit dem Backup-TACACS+-Server verwendete Schlüssel.

Pfad Konsole:

Setup > **Config** > **Tacacs-Plus**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

leer

2.11.52 SSH

Konfigurieren Sie hier Einstellungen zu SSH.

Pfad Konsole:

Setup > **Config**

2.11.52.1 RSA-Hostkey-Length

Die Länge des SSH-Hostkeys kann zwischen 2048 Bits und 4096 Bits gewählt werden. Nach der Änderung der Einstellung wird der Hostkey sofort neu generiert.

Pfad Konsole:

Setup > **Config** > **SSH**

Mögliche Werte:

2048 Bits (2048)
4096 Bits (4096)

Default-Wert:

2048 Bits (2048)

2.11.52.5 Keys

Zusätzlich zur interaktiven Authentifizierung mittels Benutzername und Passwort kann auch die Public-Key-Authentifizierung verwendet werden. Diese kann hier konfiguriert werden.

Pfad Konsole:

Setup > **Config** > **SSH**

2.11.52.5.1 CLI-User

Der Benutzer, für den der in Folge eingetragene Public Key gültig sein soll. Dies kann entweder der Benutzer „root“ sein, oder ein optional zusätzlich eingerichteter Administrator (siehe *2.11.21 Admins*).

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.11.52.5.2 Identifier

Der Identifikator wird verwendet, um mehrere Public Keys für den selben CLI-Benutzer verwenden zu können, z. B. wenn für jeden SSH-Client ein eigener Public Key erzeugt wurde, aber der Login im LCOS LX mit dem selben Benutzer-Account erfolgen soll. In diesem Fall wird der selbe CLI-Benutzer eingetragen, aber ein abweichender Identifikator.

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 254 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.11.52.5.3 Algo

Der Algorithmus, mit welchem der Public Key generiert wurde.

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

ssh-rsa
ssh-dss
ssh-ed25519
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
rsa-sha2-256
rsa-sha2-512
sk-ecdsa-sha2-nistp256-openssh
sk-ssh-ed25519-openssh

2.11.52.5.4 Key

Der zu verwendende Public Key.

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 1400 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.11.90 LED-Off-Seconds

Legen Sie eine Zeit in Sekunden nach dem Gerätestart fest, nach der die LED(s) des Gerätes ausgeschaltet werden, wenn der **LED-Mode Timed-Off** eingestellt ist.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

300

2.11.91 LED-Test

Hiermit kann die LED des Gerätes getestet werden, die dann in der entsprechenden Farbe eingeschaltet wird.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

Off
Red
Green
Blue
All
No-Test

Default-Wert:

No-Test

2.11.99 Root-Hashed

Hashwert des Passworts des Administrators root.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.11.130 PoE-Passthrough

Bei Modellen mit PoE-Passthrough-Funktion, wenn der Access Point mit PoE 802.3bt (60W) gespeist wird, kann am zweiten Ethernet-Port ETH2 ein weiteres PoE-Gerät (PD) angeschlossen werden, welches wiederum mit maximal 30W gespeist wird.

Die PoE-Passthrough-Funktion können Sie hier ein- und ausschalten.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

No
Die PoE-Passthrough-Funktion ist ausgeschaltet.

Yes
Die PoE-Passthrough-Funktion ist eingeschaltet.

Default-Wert:

No

2.14 Time

Enthält die allgemeinen Konfigurationseinstellungen zur Zeiteinstellung.

Pfad Konsole:

Setup

2.14.15 Holidays

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

Pfad Konsole:

Setup > **Time**

2.14.15.1 Date

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

Pfad Konsole:

Setup > **Time** > **Holidays**

Mögliche Werte:

max. 10 Zeichen aus `mm/dd/yyyy`

Besondere Werte:

yyyy = 0

Steht für ein beliebiges Jahr.

2.14.16 Timeframes

Zeitrahmen werden verwendet, um einzelne SSIDs anhand eines Zeitplans ein- und auszuschalten. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Fügen Sie den Zeitrahmen bei den logischen WLAN-Einstellungen hinzu, damit er für die entsprechende SSID beachtet wird.

Pfad Konsole:

Setup > **Time**

2.14.16.1 Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er in den logischen WLAN-Einstellungen referenziert wird.

Pfad Konsole:

Setup > **Zeit** > **Zeitrahmen**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.14.16.2 Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM angegeben werden, ab der das gewählte Profil gelten soll.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

max. 5 Zeichen aus `hh:mm`

Default-Wert:

00:00

2.14.16.3 Stop

Hier kann die Endzeit (Tageszeit) im Format HH:MM angegeben werden, bis zu der das gewählte Profil gelten soll.

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

max. 5 Zeichen aus `hh:mm`

Default-Wert:

00:00

2.14.16.4 Weekdays

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

None
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Holiday
Alle in der Tabelle *2.14.15 Holidays* definierten Tage.

2.14.20 Timezone

Konfigurieren Sie die korrekte Zeitzone, in der sich das Gerät befindet.

Pfad Konsole:

Setup > **Time**

Mögliche Werte:

UTC
Europe/Berlin
Europe/Vienna
Europe/Zurich
Europe/London
Europe/Prague
Europe/Warsaw
Europe/Zagreb
Europe/Copenhagen
Europe/Paris
Europe/Helsinki
Europe/Tallinn
Europe/Athens
Europe/Budapest
Europe/Dublin
Europe/Rome
Europe/Riga
Europe/Vilnius
Europe/Luxembourg
Europe/Malta
Europe/Amsterdam
Europe/Nicosia
Europe/Lisbon
Europe/Bucharest
Europe/Bratislava
Europe/Ljubljana
Europe/Madrid
Europe/Stockholm
Europe/Brussels
Europe/Sofia
US/Alaska
US/Pacific
US/Mountain
US/Central
US/Eastern
Pacific/Auckland
Pacific/Honolulu
Australia/Brisbane
Australia/Sydney
Australia/Perth
Australia/Darwin
Australia/Adelaide

Default-Wert:

UTC

2.14.21 NTP

Konfigurieren Sie in diesem Menü einen NTP-Server.

Pfad Konsole:

Setup > **Time**

2.14.21.1 Operating

Aktivieren Sie den konfigurierten NTP-Server.

Pfad Konsole:

Setup > **Time** > **NTP**

Mögliche Werte:

No

Keinen NTP-Server verwenden.

Yes

Der unter **Server** eingestellte NTP-Server wird verwendet, um das Datum und die Zeit zu stellen.

Default-Wert:

No

2.14.21.2 Server

Geben Sie hier die Adresse des zu verwendenden NTP-Servers an.

Pfad Konsole:

Setup > **Time** > **NTP**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.20 WLAN

Konfigurationseinstellungen der WLAN-Parameter.

Pfad Konsole:

Setup

2.20.1 Network

Konfigurieren Sie hier alle generellen Einstellungen rund um die auszustrahlenden WLAN-Netzwerke (SSIDs). Fügen Sie je WLAN-Netzwerk eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

Pfad Konsole:

Setup > **WLAN**

2.20.1.1 Network-Name

Konfigurieren Sie hier einen sprechenden Namen für das WLAN-Netzwerk. Dieser **interne** Name wird verwendet, um die Interface-Konfiguration in weiteren Teilen der Konfiguration zu referenzieren.

Es handelt sich hierbei **nicht** um den SSID-Namen, der z. B. auf den Clients angezeigt wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.20.1.2 SSID-Name

Konfigurieren Sie hier den nach außen sichtbaren SSID-Namen. Dieser Name wird auf den WLAN-Clients angezeigt, wenn nach WLAN-Netzwerken gesucht wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^ _.`

2.20.1.4 Closed-Network

Konfigurieren Sie hier, ob die konfigurierte SSID während der Netzwerksuche durch Clients angezeigt werden soll.

Wenn der SSID-Broadcast unterdrückt wird, dann antwortet der Access Point nicht mehr auf Probe Requests mit leerer SSID. In diesem Fall muss für einen Verbindungsaufbau die SSID explizit am Client eingetragen und konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

SSID anzeigen.

Yes

SSID nicht anzeigen.

2.20.1.10 Max-Stations

Die Zahl gibt an, wieviele Clients gleichzeitig im WLAN-Netzwerk eingebucht sein können, bevor die Anfrage eines weiteren Clients abgewiesen wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 512

Besondere Werte:

0

Der Wert „0“ bedeutet, dass es keine Begrenzung gibt, also unbegrenzt viele Clients gleichzeitig eingebucht sein können (bis zu einer eventuellen Hardware-spezifischen Grenze).

2.20.1.13 Inter-Station-Traffic

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Konfigurieren Sie hier, ob die Kommunikation der WLAN-Clients innerhalb des WLAN-Netzwerks erlaubt sein soll.

Die Kommunikation zwischen den WLAN-Clients wird durch diese Funktion nur innerhalb der SSID auf einem Access Point unterbunden. Soll die Kommunikation auch über mehrere Access Points hinweg unterbunden werden, muss zusätzlich die *2.20.1.14 Client-Isolation* konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Kommunikation der WLAN-Clients untereinander innerhalb des WLAN-Netzwerks ist nicht erlaubt.

Yes

Kommunikation der WLAN-Clients untereinander innerhalb des WLAN-Netzwerks erlaubt.

2.20.1.14 Client-Isolation

Soll die Kommunikation von WLAN-Clients untereinander, bzw. generell zu nicht zulässigen Zielen im Netzwerk unterbunden werden, kann die Client-Isolierung konfiguriert werden.

Hierbei wird jeglicher Datenverkehr ausgehend von WLAN-Clients zu nicht explizit in einer Whitelist erfassten Zielen verboten.

Die Client-Isolierung kann hier je SSID eingeschaltet werden. Geben Sie die erlaubten Ziele unter *2.20.5 Client-Isolation-Allowed* an.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Keine Client-Isolierung.

Yes

Client-Isolierung für dieses Netzwerk aktiv.

2.20.1.16 Min-Client-Strength

Konfigurieren Sie hier die minimale Signalstärke in Prozent, mit der ein Client vom Access Point „gesehen“ werden muss, damit diesem die Anmeldung am WLAN-Netzwerk erlaubt wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 100

Besondere Werte:

0

Der Wert „0“ bedeutet, dass keine minimale Signalstärke vorausgesetzt wird und Clients die Anmeldung immer erlaubt wird.

2.20.1.17 Exclude-From-Client-Management

Nimmt diese SSID gegebenenfalls vom Band Steering aus.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Band Steering mit dieser SSID durchführen.

Yes

SSID vom Band Steering ausnehmen.

2.20.1.18 Timeframe

Geben Sie hier den Namen eines *Zeitrahmens* an, über den diese SSID zeitgesteuert an- bzw. abgeschaltet wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.20.1.19 Hotspot

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.20.1.20 Summaric-Tx-Limit-Kbit/s

Hier können Sie eine WLAN Bandbreiten-Begrenzung einstellen, die für das gesamte WLAN-Netzwerk dient. Alle darin angemeldeten Clients können Daten insgesamt nur mit der hier konfigurierten Übertragungsrate empfangen. Die Angabe der Übertragungsrichtung versteht sich aus Sicht des Access Points, „Tx“ bedeutet hier also die Übertragungsrate, mit der der Access Point Daten an den Client sendet. Diese Einstellung beeinflusst also die Download-Rate am Client.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bedeutet, dass keine Begrenzung aktiv ist.

2.20.1.21 Summaric-Rx-Limit-Kbit/s

Hier können Sie eine WLAN Bandbreiten-Begrenzung einstellen, die für das gesamte WLAN-Netzwerk dient. Alle darin angemeldeten Clients können Daten insgesamt nur mit der hier konfigurierten Übertragungsrate senden. Die Angabe der Übertragungsrichtung versteht sich aus Sicht des Access Points, „Rx“ bedeutet hier also die Übertragungsrate, mit der die Clients Daten an den Access Point senden. Diese Einstellung beeinflusst also die Upload-Rate am Client.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bedeutet, dass keine Begrenzung aktiv ist.

2.20.1.25 Block-Multicast

Hiermit können Multicasts, die von WLAN-Clients gesendet oder von diesen empfangen werden, blockiert werden. Es kann nach IPv4 und IPv6 unterschieden werden.

ICMPv6-Pakete werden nicht geblockt, damit der IPv6-Adressbezug weiterhin funktioniert.

Dieses Feature wird vom LW-500 nicht unterstützt.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Keine Multicasts blockieren.

IPv4-only

Nur IPv4-Multicasts blockieren.

IPv6-only

Nur IPv6-Multicasts blockieren.

Both

Sowohl IPv4- als auch IPv6-Multicasts blockieren.

Default-Wert:

No

2.20.1.26 Client-Tx-Limit-Kbit/s

Begrenzen Sie hier die von WLAN-Clients genutzte Bandbreite in Senderichtung.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.1.27 Client-Rx-Limit-Kbit/s

Begrenzen Sie hier die von WLAN-Clients genutzte Bandbreite in Empfangsrichtung.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.1.28 ARP-Handling

Clients im WLAN, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der „ARP-Behandlung“ übernimmt der Access Point diese Aufgabe und beantwortet die ARP-Anfragen an Stelle der Stationen im Stromsparmodus. In großen Netzen wird hierdurch ebenfalls die Mediumszeit effizienter genutzt, da ARP-Anfragen und -Antworten nicht mehr an den WLAN-Client gesendet werden müssen, sondern schon stellvertretend vom Access Point beantwortet werden.

Der LCOS LX Access Point ermittelt die Zuordnung zwischen IP-Adresse und MAC-Adresse aus den DHCP-Nachrichten, die entweder zwischen WLAN-Client und DHCP-Server ausgetauscht werden oder es werden ARP-Request der verbundenen WLAN-Clients, sog.gratuitous ARP-Request oder ARP-Replys ausgewertet. Ist die Zuordnung bekannt, werden ARP-Anfragen durch den Access Point beantwortet und nicht mehr an den Client weitergeleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „An“ ARP-Anfragen trotzdem in das WLAN geleitet.

Konnte keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermittelt werden, werden in der Betriebsart „Strikt“ ARP-Anfragen nicht in das WLAN geleitet. Dies bedeutet zum Beispiel, dass zu WLAN-Clients mit festen IP-Adressen (kein DHCP) keine Verbindung vom LAN aus initiiert werden kann. In diesem Fall sollte dieses Feature nicht verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

Off

Die ARP-Behandlung ausgeschaltet. ARP-Anfragen werden immer in das WLAN geleitet.

On

Die ARP-Behandlung ist eingeschaltet. Wenn der Access Point keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermitteln konnte, werden ARP-Anfragen in das WLAN weitergeleitet.

Strict

Die ARP-Behandlung eingeschaltet. Wenn der Access Point keine Zuordnung zwischen IP-Adresse und MAC-Adresse ermitteln konnte, werden ARP-Anfragen nicht in das WLAN weitergeleitet.

Default-Wert:

Off

2.20.1.29 Multicast-To-Unicast

Konfigurieren Sie einzeln je WLAN-Netzwerk ob und wie eine Konvertierung von Multicasts in Unicasts vorgenommen werden soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

None
Conversion

Die Multicasts werden in Unicasts umgewandelt (Layer-2-Unicast auf dem WLAN-Layer mit Unicast-MAC-Adresse als Ziel). Dies entspricht dem Verhalten im LCOS.

Encapsulation

Die Multicasts werden in Unicast-Aggregate gekapselt (A-MSDU mit Unicast-MAC-Adresse als Ziel, die einen einzelnen Layer-2-Multicast beinhaltet). Diese Variante sollte zum Einsatz kommen, wenn Ziel-Anwendungen die Ziel-MAC-Adresse überprüfen. Es ist aber zu beachten, dass Aggregate nicht von 802.11a/b/g-Clients unterstützt werden.

2.20.1.30 Bridge

Wird bei WLC-Betrieb intern verwendet bzw. bei Verwendung von L2TP muss hier das L2TP-Interface eingetragen werden,

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

br-lan
WLC-Tunnel-1 … WLC-Tunnel-32
L2TP-Tunnel-1 … L2TP-Tunnel-16

2.20.1.32 WDS-Link

Hier können Sie festlegen, dass bestimmte SSIDs über WDS-Verbindungen übertragen werden. Referenzieren Sie dazu hier einen Eintrag aus *2.20.13.1.1 Link-Name*.

Soll ein Repeater-Betrieb realisiert werden, muss diese Konfiguration ebenso auf dem entfernten via WDS angebundenen Access Point dupliziert werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.1.34 U-APSD

Beim Automatic Power Save Delivery (APSD) handelt es sich um eine Erweiterung des Standards IEEE 802.11e. APSD wird in zwei Varianten angeboten:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

Die beiden Verfahren unterscheiden sich u. a. in der Nutzung der Übertragungskanäle. R&S®NC Access Points und Wireless Router unterstützen U-APSD, auf dem auch das Verfahren WMM Power Save oder kurz WMM-PS basiert. U-APSD ermöglicht für WLAN-Geräte eine deutliche Stromeinsparung. Ein besonders großer Bedarf für diese Funktion entsteht durch die immer stärkere Nutzung von WLAN-fähigen Telefonen (Voice over WLAN – VoWLAN).

Mit der Aktivierung des U-APSD für ein WLAN können die WLAN-Geräte im Gesprächsbetrieb in einen „Schlummer-Modus“ wechseln, während sie auf das nächste Datenpaket warten. Die VoIP-Datenübertragung erfolgt in einem festen zeitlichen Raster – die WLAN-Geräte synchronisieren ihre aktiven Phasen mit diesem Zyklus, so dass sie rechtzeitig vor dem Empfang des nächsten Pakets wieder bereit sind. Der Stromverbrauch wird dadurch deutlich reduziert, die Gesprächszeit der Akkus wird merklich erhöht.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No
Unscheduled APSD abgeschaltet.

Yes
Unscheduled APSD eingeschaltet.

Default-Wert:

Yes

2.20.1.35 RRM

Der Standard IEEE 802.11k beschreibt einen Weg, WLAN-Clients über potentielle Roaming-Ziele, also weitere Access Points in Reichweite mit derselben SSID, zu informieren (Radio Resource Measurement). Diese Information an den Client erfolgt durch den im Standard definierten „Neighbour Report“.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Radio Resource Measurement abgeschaltet.

Yes

Radio Resource Measurement eingeschaltet.

2.20.1.36 DTIM-Period

Die DTIM-Periode kann per SSID konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

1 … 255

Default-Wert:

1

2.20.1.42 MLO-Mode

Mit Multi Link Operation (MLO) können Wi-Fi 7-fähige WLAN-Clients mehrere Assoziationen gleichzeitig mit demselben Access Point verwalten. Dies erhöht den Datendurchsatz und reduziert die Latenz.

Bei WLAN-Clients mit nur einem Funkmodul (Radio) kann besonders schnell zwischen den qualitativ besseren Frequenzbändern gewechselt werden. Dies sorgt vor allem in Funkumgebungen mit hoher Signaldichte für weniger Verbindungsabbrüche und eine stabilere WLAN-Konnektivität.

WLAN-Clients mit mehreren Funkmodulen (Radios) können mehrere Frequenzbänder gleichzeitig nutzen, um den Datendurchsatz zu maximieren.



Für einen standardkonformen Wi-Fi 7- und Multi Link Operation-Betrieb sind bestimmte Verschlüsselungseinstellungen zwingend erforderlich:

- Der WPA-Sitzungsschlüsseltyp muss AES-GCMP-256 enthalten
- Der Group-Mgmt-Cipher muss BIP-GMAC-256 sein
- Die SAE/OWE-DH-Gruppen müssen DH-19, DH-20 und DH-21 umfassen
- Protected Management Frames (IEEE 802.11w) müssen aktiviert sein
- Beacon-Schutz (Beacon Protection) muss aktiviert sein

Zur einfachen Anwendung dieser Einstellungen ist ab LCOS LX 7.10 das zusätzliche Verschlüsselungsprofil „P-PSK-WiFi7“ in der Konfiguration enthalten und kann verwendet werden.

Da einige dieser Einstellungen zu Kompatibilitätsproblemen mit bestehenden (Legacy-)Clients führen können, empfehlen wir, eine separate SSID für Wi-Fi 7, MLO und die oben genannten Verschlüsselungseinstellungen einzurichten und ausschließlich mit Wi-Fi 7-Clients zu verwenden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

Auto

MLO wird für alle Wi-Fi 7 / IEEE 802.11be-fähigen Radios, auf denen die SSID ausgestrahlt wird, aktiviert.

Single-Link

Jedes Wi-Fi 7 / IEEE 802.11be-fähige Radio wird zu einem eigenständigen MLD (Multi Link Device). Es wird hier also die MLO-„Infrastruktur“ verwendet, aber die Radios bleiben getrennt. Die Verwendung dieses Modus kann bei Kompatibilitätsproblemen sinnvoll sein.

Disabled

MLO kommt nicht zum Einsatz. Die Radios werden nicht als MLD konfiguriert.

2.20.1.43 Client-Mgmt-Profile

Wählen Sie hier eines der Client-Management-Profile aus *2.20.18.2 Profiles* aus.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.1.100 Key

Konfigurieren Sie hier den Pre-shared Key (PSK), der für das WLAN-Netzwerk verwendet wird.

Dieser Eintrag kommt nur dann zum Tragen, wenn ein Verschlüsselungsprofil ausgewählt wird, welches WPA(2)-PSK oder WEP verwendet (WEP ist unsicher und wird lediglich aus Gründen der Abwärtskompatibilität unterstützt. R&S®NC empfiehlt jedoch ausdrücklich,

WPA2 oder WPA3 zu verwenden). Wird 802.1X verwendet, hat der Eintrag keine Auswirkung, das Feld kann dann leer gelassen werden.

Bei Verwendung der Verschlüsselungsmethode WEP müssen die folgenden Einschränkungen beachtet werden:

- WEP-40-Bits / WEP-40-Bits-802.1X – 5 beliebige Zeichen aus dem erlaubten Zeichensatz ODER 10 HEX Zeichen
- WEP-104-Bits / WEP-104-Bits-802.1X – 13 beliebige Zeichen aus dem erlaubten Zeichensatz ODER 26 HEX Zeichen
- WEP-128-Bits / WEP-128-Bits-802.1X – 16 beliebige Zeichen aus dem erlaubten Zeichensatz ODER 32 HEX Zeichen

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.1.101 Radios

Konfigurieren Sie hier, auf welchen WLAN-Radios bzw. -Frequenzen die SSID ausgestrahlt werden soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

2.4GHz+5GHz
Die SSID wird auf den Frequenzen 2,4 GHz und 5 GHz ausgestrahlt.

2.4GHz
Die SSID wird nur auf der Frequenz 2,4 GHz ausgestrahlt.

5GHz
Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

none
Die SSID wird nicht ausgestrahlt. Dies kann als genereller Ein- / Aus-Schalter für die SSID verwendet werden.

2.20.1.102 Encryption-Profile

Konfigurieren Sie hier ein Verschlüsselungs-Profil aus den in **Setup** > **WLAN** > **Encryption** vorhandenen, welches definiert, welches Authentisierungs- und Verschlüsselungsverfahren für die SSID zum Tragen kommen soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

2.20.1.103 Idle-Timeout

Dies ist die Zeit in Sekunden, nach der ein Client getrennt wird, wenn der Access Point keine Pakete mehr von ihm empfangen hat. Jeglicher Datenverkehr des Clients setzt diesen Timeout wieder zurück.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

2.20.1.200 VLAN-ID

Mit dieser VLAN-ID werden Datenpakete, die aus dem WLAN an das LAN gerichtet sind, getaggt. Ebenso werden Pakete, die mit dieser VLAN-ID vom LAN kommen und an das WLAN gerichtet sind, wieder ent-taggt.

Diese Betriebsart entspricht dem normalerweise als „Access“ bekannten Tagging-Modus, da davon ausgegangen wird, dass WLAN-Clients Daten normalerweise untagged übertragen. Der Tagging-Modus ist nicht anpassbar.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.20.2 Country

Konfigurieren Sie hier, in welchem Land das Gerät betrieben wird. Abhängig davon werden automatisch die passenden regulatorischen Begrenzungen eingestellt.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Australia
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech-Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
New-Zealand
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United-Kingdom
United-States
Europe

2.20.3 Encryption

Konfigurieren Sie hier alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke. Standardmäßig sind bereits einige Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden.

Pfad Konsole:

Setup > **WLAN**

2.20.3.1 Profile-Name

Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.2 Encryption

Konfigurieren Sie hier, ob das WLAN-Netzwerk verschlüsselt sein soll oder keine Verschlüsselung verwendet werden soll (Open Network).

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

Keine Verschlüsselung verwenden.

Yes

Verschlüsselung verwenden.

2.20.3.4 Method

Konfigurieren Sie hier die Verschlüsselungsmethode.

Das Verfahren WEP bietet heutzutage keinerlei Vertraulichkeit mehr und sollte nur eingesetzt werden, um Legacy-Clients einzubinden, die kein neueres Sicherheitsverfahren unterstützen. In diesem Fall empfiehlt es sich, die WEP-Clients in einem eigenen VLAN vom Rest der WLAN-Infrastruktur zu isolieren.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

WEP-40-Bits

WEP mit Schlüssellänge 40 Bit

WEP-104-Bits

WEP mit Schlüssellänge 104 Bit

WEP-128-Bits

WEP mit Schlüssellänge 128 Bit

WEP-40-Bits-802.1X

WEP mit Schlüssellänge 40 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-104-Bits-802.1X

WEP mit Schlüssellänge 104 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-128-Bits-802.1X

WEP mit Schlüssellänge 128 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

802.11i-WPA-PSK

WPA(2) mit Pre-Shared-Key

802.11i-WPA-802.1X-192-Bits

WPA(2) mit 802.1X und 192 Bit Schlüssellänge

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

Enhanced-Open

Hotspots werden bisher hauptsächlich unverschlüsselt betrieben, wodurch auf der Funkschnittstelle keinerlei Vertraulichkeit der übertragenen Daten gegeben ist. Auch die verbreitete Praxis, einen Hotspot mit WPA2-PSK abzusichern und den gemeinsamen Schlüssel etwa durch einen Aushang bekannt zu machen, bietet nur eingeschränkte Sicherheit. Da WPA2-PSK keine Perfect Forward Secrecy bietet, kann ein Angreifer, dem dieser Schlüssel bekannt ist, nachträglich damit abgesicherten Datenverkehr entschlüsseln. Das Enhanced Open-Verfahren kann verwendet werden, um diese Risiken zu minimieren. Es bietet verschlüsselte Kommunikation für alle Clients, die dieses Verfahren unterstützen, so dass nicht jeder in der gleichen Funkzelle alles einfach mitlesen kann. Es bleibt das Risiko einer Man-in-the-Middle-Attacke, aber im Vergleich zu einem unverschlüsselten offenen Hotspot ist es ein deutlich geringeres Risiko. Es muss nur die Verschlüsselungsmethode eingestellt werden. Mehr ist nicht notwendig, um die Kommunikation mit Clients, welche dieses Verfahren unterstützen, zu verschlüsseln.

2.20.3.9 WPA-Version

Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden **802.11i-WPA-PSK** und **802.11i-WPA-802.1X** verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

WPA1

Die WPA-Version 1 wird exklusiv verwendet.

WPA2

Die WPA-Version 2 wird exklusiv verwendet.

WPA3

Die WPA-Version 3 wird exklusiv verwendet.

WPA1/2

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 1 oder 2 verwendet.

WPA2/3

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 2 oder 3 verwendet.

2.20.3.11 WPA-Rekeying-Cycle

Ein 48 Bit langer Initialization Vector (IV) erschwerte bei WEP die Berechnung des Schlüssels für Angreifer. WPA führte darüber hinaus die Verwendung eines neuen Schlüssels für jedes Datenpaket ein (Per-Packet Key Mixing und Re-Keying). Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels würde erst nach 16 Millionen Paketen erfolgen. In stark genutzten WLANs also erst nach einigen Stunden. Um die Wiederholung des echten Schlüssels zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen.

Konfigurieren Sie hier die Zeit in Sekunden, nach der der Access Point bei Verwendung einer WPA-Version einen Austausch der verwendeten Schlüssel durchführt.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 32 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bedeutet, dass kein Wechsel der Schlüssel durchgeführt wird.

2.20.3.12 WPA1-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

2.20.3.13 WPA2-3-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 2 bzw.3 angeboten werden sollen. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Für maximale Kompatibilität mit Legacy-Clients sollte die alleinige Einstellung „AES-CCMP-128“ verwendet werden. Beachten Sie, dass ein standardkonformer IEEE 802.11be-Betrieb die Verwendung von AES-GCMP-256 vorsieht. Erfahrungsgemäß unterstützen aktuelle Wi-Fi 7-Clients aber auch andere Verschlüsselungsverfahren wie AES-CCMP-128, bzw. Kombinationen daraus. Dies ist insbesondere bei Betrieb von gemischten SSIDs für Wi-Fi 7- und älteren Clients zu beachten, die in der Regel nur AES-CCMP-128 unterstützen. Verwenden Sie im Zweifelsfall eine separate SSID für Wi-Fi 7 mitsamt der passenden Verschlüsselungseinstellungen.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird angeboten.

AES-CCMP-128

Dieses Verfahren des Advanced Encryption Standard (AES) wird angeboten.

AES-CCMP-256

Dieses Verfahren des Advanced Encryption Standard (AES) wird angeboten.

AES-GCMP-128

Dieses Verfahren des Advanced Encryption Standard (AES) wird angeboten.

AES-GCMP-256

Dieses Verfahren des Advanced Encryption Standard (AES) wird angeboten.

Default-Wert:

AES-CCMP-128

2.20.3.14 Prot.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann

diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf „Mandatory (Obligatorisch)“ gesetzt angenommen. Bei WPA2 ist diese Option optional.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No
PMF nicht verwenden.

optional
PMF anbieten. Der Client entscheidet, ob diese verwendet werden.

mandatory
PMF verwenden.

2.20.3.15 Prot.-Beacons

Der Standard IEEE 802.11be (Wi-Fi 7) schreibt die Verwendung von Beacon Protection vor. Dies kann hier konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No
Beacon Protection abgeschaltet.

Yes
Beacon Protection eingeschaltet.

Auto
Dieser Modus schaltet die Beacon Protection automatisch für alle Radios an, die IEEE 802.11be unterstützen. Zur Erhöhung der Kompatibilität mit Legacy-Clients kann es erforderlich sein, die Beacon Protection abzuschalten.

Default-Wert:

Auto

2.20.3.16 Pre-Authentication

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2/802.1X unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1X-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1X-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.
- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

Prä-Authentifizierung nicht durchführen.

Yes

Prä-Authentifizierung durchführen.

2.20.3.17 OKC

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

OKC ist aktiviert.

Yes

OKC ist nicht aktiviert.

2.20.3.19 WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r.

Standard+Fast-Roaming

Kombination aus Standard und Fast Roaming

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am Access Point anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als Standard aktiviert ist.

2.20.3.20 PMK-IAPP-Secret

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Stellen Sie daher sicher, dass diese Passphrase auf allen Access Points, zwischen denen mittels Fast Roaming geroamt werden soll, identisch ist.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.21 RADIUS-Server-Profile

Konfigurieren Sie hier das RADIUS-Serverprofil, welches bei der Verwendung von 802.1X zum Einsatz kommt. Bei der Verwendung von PSK-basierten Verschlüsselungsmethoden ist hier keine Eingabe erforderlich.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.26 SAE/OWE-Groups

Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen als Bitmaske, auf deren Basis die Protokollpartner einen Schlüssel für den Datenaustausch erstellen. Die vorhandenen Gruppen nutzen elliptische Kurven.

Das bei WPA3 verwendete Authentisierungsverfahrens SAE (Simultaneous Authentication of Equals) nutzt diese Verfahren zusammen mit AES zur Erzeugung eines kryptographisch starken Schlüssels.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

DH-19

Bit 0x80000 (524288) – 256-bit random ECP group

DH-20

Bit 0x100000 (1048576) – 384-bit random ECP group

DH-21

Bit 0x200000 (2097152) – 521-bit random ECP group

Default-Wert:

DH-19

2.20.4 Band-Steering

Konfigurieren Sie hier die Einstellungen zum Band Steering. Mittels Band Steering können Clients vom überlaufenen 2,4-GHz-Frequenzband auf das 5-GHz-Frequenzband gelenkt werden, sodass für den einzelnen Client mehr Bandbreite zur Verfügung steht und die Benutzererfahrung verbessert wird. LCOS LX bietet die Möglichkeit, Clients mittels des 802.11v-Standards auf das jeweils für sie optimale Frequenzband zu leiten. Auch Clients, die den 802.11v-Standard nicht unterstützen, können durch eine gezielte Verzögerung von Probe Responses oder gezielte Trennung vom WLAN auf das 5-GHz-Band geleitet werden.

Pfad Konsole:

Setup > **WLAN**

2.20.4.1 Active-Profile

Wählen Sie hier das Profil, welches die Einstellungen für das Band-Steering-Modul festlegt.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering**

Mögliche Werte:

P-DEFAULT
Steering erfolgt anhand der Mediumsauslastung und der erkannten Intereferenz auf dem aktuellen Kanal und erfolgt bevorzugt mittels 802.11v. Unterstützt der Client kein 802.11v, wird das Steering mittels einer gezielten Disassoziierung des Clients durchgeführt. Das Steering erfolgt sowohl vor der Assoziierung, als auch, bei Bedarf, während der Client bereits assoziiert ist. Dies ist das empfohlene Profil.

P-LEGACY
Steering erfolgt vor der Assoziierung des Clients durch gezielte Zurückhaltung von Probe Responses. Es wird unabhängig von der Auslastung immer das 5-GHz-Band bevorzugt.

P-DISABLED
Es wird keinerlei Steering durchgeführt. Der Client entscheidet autark, welches Frequenzband er wählt.

<Custom>
Neben den vorgegebenen Profilen können Sie auch in **Profiles** selbst erstellte Profile einstellen.

Default-Wert:

P-DEFAULT

2.20.4.2 Profiles

Passen Sie hier die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

Pfad Konsole:
Setup > **WLAN** > **Band-Steering**

2.20.4.2.1 Profile-Name

Der Name des Profils.

Pfad Konsole:
Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:
max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.2.2 Operating

Steuert, ob das Band Steering für dieses Profil aktiv ist.

Pfad Konsole:
Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

No
Band Steering ist nicht aktiv.

Yes
Band Steering ist aktiv.

2.20.4.2.3 Steering-Min-PHY-Signal

Legt die Client-Signalstärke (in dB) fest, ab der ein Steering des Clients durchgeführt wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.2.4 Upgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen erreichen potentiell ein Steering des Clients auf das 5-GHz-Band erfolgen soll.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.2.5 Upgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die mindestens erreicht sein muss, damit der Client für ein Steering auf das 5-GHz-Band in Betracht gezogen wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.2.6 Downgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen Erreichen potentiell ein Steering des Clients auf das 2,4-GHz-Band erfolgen soll.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.2.7 Downgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die unterschritten sein muss, damit der Client für ein Steering auf das 2,4-GHz-Band in Betracht gezogen wird.

Für ein Steering auf 2,4 GHz (Downgrade) muss sowohl die hier konfigurierte Signalstärke unterschritten sein, als auch der Grenzwert aus **Downgrade-TX-Rate-Threshold** erreicht werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.2.8 2.4GHz-Sub-Profile

Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.2.9 5GHz-Sub-Profile

Konfigurieren Sie hier, welches 5-GHz-Unterprofil zur Anwendung kommt.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.3 2.4GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 2,4-GHz-Unterprofile.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering**

2.20.4.3.1 Profile-Name

Der Profilname des 2,4-GHz-Unterprofils.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.3.2 Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.3.3 Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.3.4 Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 2,4-GHz-Kanal als ausgelastet angenommen wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.3.5 Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.3.6 Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 2,4-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

2.20.4.3.7 Delay-Probe-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die erreicht sein muss, damit Probe Responses an den Client zum Zwecke des Steerings zurückgehalten werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.3.8 Delay-Probe-Time-Window

Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Delay-Probe-Min-Request-Count** konfiguriert wurde, damit diese beantwortet werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.3.9 Delay-Probe-Min-Request-Count

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Delay-Probe-Time-Window** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.4 5GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 5-GHz-Unterprofile.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering**

2.20.4.4.1 Profile-Name

Der Profilname des 5-GHz-Unterprofils.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.4.2 Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.4.3 Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.20.4.4.4 Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 5-GHz-Kanal als ausgelastet angenommen wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.4.5 Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.4.6 Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 5-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

Pfad Konsole:

Setup > **WLAN** > **Band-Steering** > **5GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

2.20.5 Client-Isolation-Allowed

Konfigurieren Sie hier die erlaubten Ziele für die Client-Isoliserung. Siehe auch *2.20.1.14 Client-Isolation*.

Pfad Konsole:

Setup > **WLAN**

2.20.5.1 Network-Name

Wählen Sie hier das Netzwerk / die SSID, für die der Eintrag gelten soll. Erfassen Sie dann wahlweise eine Ziel-IP-Adresse (*2.20.5.2 IP-Network*) oder Ziel-MAC-Adresse (*2.20.5.3 MAC-Address*).

In Hotspot-Szenarien bietet es sich an, die MAC-Adresse des Gateways hier zu erlauben, um den Internetzugang sicherzustellen. Die Angabe dessen IP-Adresse ist nicht ausreichend, da in diesem Szenario die Ziel-IP-Adresse die eines Ziels im Internet ist.

Das Feature ermittelt die passende Gateway-Adresse automatisch aus einer DHCP-Verhandlung zwischen einem WLAN-Client und DHCP-Server. In Roaming-Szenarien wird beim Roaming allerdings üblicherweise keine erneute DHCP-Verhandlung durchgeführt, so dass in solchen Szenarien das explizite Whitelisting des Gateways erforderlich ist.

Pfad Konsole:

Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.5.2 IP-Network

Erlaubte Ziel-IP-Adresse für dieses Netzwerk.

Pfad Konsole:

Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 19 Zeichen einer IPv4-Adresse `a.b.c.d/xx`

2.20.5.3 MAC-Address

Erlaubte Ziel-MAC-Adresse für dieses Netzwerk.

Pfad Konsole:

Setup > **WLAN** > **Client-Isolation-Allowed**

Mögliche Werte:

max. 17 Zeichen einer MAC-Adresse `xx:xx:xx:xx:xx:xx`

2.20.8 Radio-Settings

Konfigurieren Sie hier alle Einstellungen rund um die physikalischen Radio-Parameter. Standardmäßig ist für jedes physikalisch vorhandene WLAN-Radio ein Eintrag in der Tabelle enthalten, der bei Bedarf modifiziert werden kann.

Pfad Konsole:

Setup > **WLAN**

2.20.8.1 Ifc

Der interne Name des WLAN-Radios. Dieser kann nicht verändert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

2.20.8.3 5GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 5-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

11an-mixed
Es werden die Modi 802.11a und 802.11n verwendet.

11anac-mixed
Es werden die Modi 802.11a, 802.11n und 802.11ac verwendet.

11nac-mixed
Es werden die Modi 802.11n und 802.11ac verwendet.

11ac-only
Es wird nur der Modus 802.11ac verwendet.

11anacax-mixed
Es werden die Modi 802.11a, 802.11n, 802.11ac und 802.11ax (Wi-Fi 6) verwendet.

11anacaxbe-mixed
Es werden die Modi 802.11a, 802.11n, 802.11ac, 802.11ax (Wi-Fi 6) und 802.11be (Wi-Fi 7) verwendet.

Auto
Es werden alle vom Gerät unterstützten Modi verwendet.

2.20.8.6 Radio-Band

Konfigurieren Sie hier, ob dieses Radio-Modul im 2,4-GHz-, 5-GHz- oder 6 GHz-Spektrum arbeitet.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

2.4GHz
Das Radio-Modul arbeitet im 2,4-GHz-Spektrum.

5GHz
Das Radio-Modul arbeitet im 5-GHz-Spektrum.

6GHz
Das Radio-Modul arbeitet im 6-GHz-Spektrum.

2.20.8.7 Sub-Band

Konfigurieren Sie hier, welche Sub-Bänder im 5-GHz-Modus verwendet werden.

Die WLAN-Kanäle 120, 124 und 128 werden nicht verwendet, da diese Kanäle durch den Primärnutzer RADAR verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

Band-1
Es wird nur das Sub-Band 1 verwendet. Dies entspricht den WLAN-Kanälen 36, 40, 44, 48, 52, 56, 60 und 64.

Band-2
Es wird nur das Sub-Band 2 verwendet. Dies entspricht den WLAN-Kanälen 100, 104, 108, 112, 116, 132, 136 und 140.

Band-1+2
Es werden die Sub-Bänder 1 und 2 verwendet.

Band-5
Die Bezeichnung Band-5 orientiert sich an der U-NII-Nomenklatur der FCC und entspricht dem Band U-NII-5. In der EU ist im Rahmen des 6 GHz-Bands lediglich der Frequenzbereich 5.925–6.425 MHz für WLAN freigegeben (was Band-5, bzw. U-NII-5 entspricht).

2.20.8.8 Channel

Konfigurieren Sie hier den Kanal, auf dem das WLAN-Radio arbeiten soll.

Im 5-GHz-Betrieb stellt der hier eingestellte Kanal einen bevorzugten Kanal dar. Da im 5-GHz-Band Dynamic Frequency Selection (DFS) vorgeschrieben ist, kann die Verwendung des bevorzugten Kanals allerdings nicht garantiert werden.

Im 6 GHz-Band können in LCOS LX folgende Kanäle konfiguriert werden:

1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93

Hierbei handelt es sich um 20 MHz breite Kanäle. Wird eine höhere Kanalbreite als 20 MHz gewählt (Standardeinstellung für das 6 GHz-Band: 160 MHz) wird der hier eingestellte Kanal zum Primärkanal des dann verwendeten breiteren Kanals. Auf diese Weise kann der Primärkanal ebenfalls frei innerhalb eines >20 MHz breiten Kanals gewählt werden – dazu muss lediglich der gewünschte 20 MHz-Kanal eingetragen werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bewirkt die automatische Auswahl eines geeigneten Kanals.

Bei der automatischen Kanalwahl erfolgt im laufenden Betrieb keine Änderung des Kanals. Der Kanal wird lediglich beim Start des WLAN-Moduls gewählt.

2.20.8.9 2.4GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 2,4-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt.

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

11bg-mixed
Es werden die Modi 802.11b und 802.11g verwendet.

11g-only
Es wird nur der Modus 802.11g verwendet.

11bgn-mixed
Es werden die Modi 802.11b, 802.11g und 802.11n verwendet.

11gn-mixed
Es werden die Modi 802.11g und 802.11n verwendet.

11bgnax-mixed
Es werden die Modi 802.11b, 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

11gnax-mixed
Es werden die Modi 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

Auto

Es werden alle vom Gerät unterstützen Modi außer 802.11b unterstützt.

2.20.8.13 Channel-List

Konfigurieren Sie hier eine kommaseparierte Liste von weiteren WLAN-Kanälen. Im Rahmen der automatischen Kanalwahl wird ein Kanal aus dieser Liste ausgewählt, anstatt aus allen unterstützten WLAN-Kanälen.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.8.17 Antenna-Mask

Die Einstellungen zur Antennenmaske haben nur Geräte mit externen bzw. abnehmbaren Antennen.

Diese Einstellung hilft bei der Verwendung von WLAN-Antennen mit vom Access Point abweichender Anzahl an Streams (z. B. Antenne mit zwei Streams, verbunden mit einem Access Point mit vier Streams). Hiermit können die nicht mit einer Antenne verbundenen Ports auf Seiten des Access Points deaktiviert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

All (0x0)

Wenn kein Bit dieser Maske gesetzt ist, dann sind alle Antennen aktiv.

Antenna-1 (0x1)

Bit 1 steuert Antenne 1.

Antenna-2 (0x2)

Bit 2 steuert Antenne 2.

Antenna-3 (0x4)

Bit 3 steuert Antenne 3.

Antenna-4 (0x8)

Bit 4 steuert Antenne 4.

Default-Wert:

All (0x0)

2.20.8.19 6GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 6-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

11ax
Es wird der Modus 802.11ax (Wi-Fi 6) verwendet.

11axbe-mixed
Es werden die Modi 802.11ax (Wi-Fi 6) und 802.11be (Wi-Fi 7) verwendet.

Auto
Es werden alle vom Gerät unterstützten Modi verwendet.

2.20.8.24 Max.-Channel-Bandwidth

Konfigurieren Sie hier die maximal erlaubte Kanalbandbreite.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

20MHz
Die Kanalbandbreite beträgt immer 20 MHz.

40MHz
Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 40 MHz, kann aber auch auf 20 MHz zurückfallen.

80MHz
Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 80 MHz, kann aber auch auf 40 MHz oder 20 MHz zurückfallen.

160MHz
Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 160 MHz, kann aber auch auf 80 MHz, 40 MHz oder 20 MHz zurückfallen.

320MHz
Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 320 MHz, kann aber auch auf 160 MHz, 80 MHz, 40 MHz oder 20 MHz zurückfallen.

Auto
Für ein 2,4-GHz-Radio wird immer die Kanalbandbreite 20 MHz verwendet. Für ein 5-GHz-Radio wird die maximal mögliche Kanalbandbreite (bis zu 80 MHz) verwendet. Für ein 6-GHz-Radio wird die maximal mögliche Kanalbandbreite (bis zu 160 MHz) verwendet.

2.20.8.29 Exclude-DFS-Channels

Konfigurieren Sie hier, ob im 5-GHz-Band Kanäle verwendet werden sollen, für die Dynamic Frequency Selection (DFS) vorgeschrieben ist.

Werden diese Kanäle hierüber ausgeschlossen, stehen im 5-GHz-Band noch die Kanäle 36, 40, 44 und 48 zur Verfügung. Da für diese kein DFS vorgeschrieben ist, können diese Kanäle bei aktivierter Option **Exclude-DFS-Channels** im Radio-Channel und in der **Channel-List** fest konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

No

Für DFS reservierte Kanäle verwenden.

Yes

Für DFS reservierte Kanäle nicht verwenden.

2.20.8.33 Power-Setting

Diese Einstellung regelt, ob die maximal erlaubte und von der Hardware des Access Point realisierbare Sendeleistung verwendet wird („Automatic“) oder ob im manuellen Modus („Manual“) die gewünschte Ziel-Sendeleistung vorgegeben werden kann. Dies erfolgt unter *2.20.8.34 EIRP* in dBm.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

Automatic

Maximal erlaubte und von der Hardware des Access Point realisierbare Sendeleistung verwenden.

Manual

Unter *2.20.8.34 EIRP* in dBm angegebene Ziel-Sendeleistung verwenden.

Ist die Hardware des Access Points nicht in der Lage, die gewünschte Sendeleistung einzustellen, wird automatisch der maximal mögliche Wert eingestellt.

In keinem Fall wird der Access Point die regulatorischen Limits für die Sendeleistung überschreiten. Diese werden automatisch immer beachtet, unabhängig von der hier vorgenommenen Konfiguration.

Default-Wert:

Automatic

2.20.8.34 EIRP

Abhängig von der Einstellung in *2.20.8.33 Power-Setting* stellen Sie hier die verwendete Sendeleistung in dBm ein.

Ist die Hardware des Access Points nicht in der Lage, die gewünschte Sendeleistung einzustellen, wird automatisch der maximal mögliche Wert eingestellt.

In keinem Fall wird der Access Point die regulatorischen Limits für die Sendeleistung überschreiten. Diese werden automatisch immer beachtet, unabhängig von der hier vorgenommenen Konfiguration.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

2.20.8.35 Include-Weather-Radar-Channels

Die vom Wetterradar verwendeten Kanäle 120, 124 und 128 im Frequenzbereich 5,6 bis 5,65 MHz werden bei der automatischen Kanalwahl berücksichtigt. Wird einer der Kanäle verwendet, erhöht sich die DFS-Scan-Zeit (CAC-Time) von 1 auf 10 Minuten. Während des Scans ist das 5 GHz-Radio nicht für WLAN-Clients erreichbar.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

Yes

Für Wetterradar reservierte Kanäle verwenden.

No

Für Wetterradar reservierte Kanäle nicht verwenden.

2.20.8.36 Max.-Distance

Geben Sie hier die Distanz zur am weitesten entfernten WLAN-Station ein (z. B. zu einem WDS-Partner).

Anhand dieser Einstellung wird der interne Timeout für WLAN-ACK-Pakete so weit erhöht, dass Pakete von einer weit entfernten Station noch verarbeitet werden können. Default ist 1 Kilometer.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

Default-Wert:

1

2.20.8.37 Channel-Selection

In Netzwerken, die ohne manuelle WLAN-Kanalplanung oder ARC 2.0 betrieben werden, kommt eine automatische Kanalwahl zum Einsatz, die den WLAN-Kanal anhand von Qualitätskriterien wie Kanallast, Störungen und weiteren SSIDs auf diesem Kanal bewertet. Wenn in einem solchen Netzwerk alle Access Points zeitgleich gestartet werden, z. B. nach einem Stromausfall, kann es vorkommen, dass die Kanal-Qualitätsbewertung auf allen Access Points zum selben Ergebnis kommt und somit viele Access Points auf demselben Kanal arbeiten, was je nach Szenario nicht wünschenswert ist. Mit der zufallsbasierten WLAN-Kanalwahl kann die Kanalwahl nach Neustart zufallsbasiert erfolgen, so dass in größeren Netzen eine möglichst gleichmäßige Verteilung mit geringer Mehrfachbelegung eines Kanals stattfindet.

R&S®NC empfiehlt, eine Kanalplanung LMC-gestützt mittels ARC 2.0 durchzuführen, oder eine manuelle Planung anhand einer Ausleuchtung (Site Survey) durchzuführen.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

Auto
Automatische Kanawahl.

Random
Zufallsbasierte WLAN-Kanalwahl.

2.20.9 Automatic-Environment-Scan-Enabled

Dieser Eintrag wird durch die R&S®LANCOM Management Cloud gesetzt, welche diesen Umgebungsscan benötigt. Die Ergebnisse sind nur durch die R&S®LANCOM Management Cloud lesbar.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Yes
Automatischer Umgebungsscan wird durchgeführt.

No
Automatischer Umgebungsscan wird nicht durchgeführt.

2.20.10 Automatic-Environment-Scan-Time-Begin

Startzeit für das Zeitfenster, in dem der automaische Umgebungsscan durchgeführt wird.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Uhrzeit im Format `hh:mm`

2.20.11 Automatic-Environment-Scan-Time-End

Stoppzeit für das Zeitfenster, in dem der automaische Umgebungsscan durchgeführt wird.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Uhrzeit im Format `hh:mm`

2.20.12 Hotspot

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN**

2.20.12.1 Hotspots

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot**

2.20.12.1.1 Name

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.12.1.2 URL

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

max. 256 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.12.1.3 Revision-ID

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

max. 36 Zeichen aus `UUID`

2.20.12.1.4 Private-Network

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

No
Yes

2.20.12.1.5 DHCP-Range-Start

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

max. 32 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.20.12.1.6 DHCP-Range-End

Dieses ist ein von der R&S®LANCOM Management Cloud verwalteter interner Wert des Cloud-managed Hotspot-Feature, der nicht verändert werden darf.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Hotspots**

Mögliche Werte:

max. 32 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.20.12.2 Walled-Garden

Walled Garden ermöglicht die Definition von IP-Adressen oder Hostnamen, die für noch nicht angemeldete Hotspot-Clients erreichbar sein sollen. Typischerweise sind dies Hosts, auf denen weitere Ressourcen, die von der Landingpage benötigt werden, bereitgestellt werden (z. B. Grafiken, Fonts, oder auch ganze Drittanbieter-Login-Dienste).

Zur Konfiguration des Walled Garden gehen Sie folgendermaßen vor:

1. Legen Sie einen Cloud-managed Hotspot in der R&S®LANCOM Management Cloud an.
2. Als nächstes ermitteln Sie den Namen dieses Cloud-managed Hotspot aus der Tabelle unter **Setup** > **WLAN** > **Hotspot** > **Hotspots**.
3. Legen Sie nun in dieser Tabelle einen oder mehrere Einträge an, die in „Hotspot“ den Namen der Hotspot-Konfiguration und in „Hostname“ den freizuschaltenden Host oder IP-Adresse beinhalten. Die Angabe von Wildcards wie z. B. „*.lancom.de“ ist möglich.
4. Soll ein Walled Garden-Host nur in dem Fall ohne Anmeldung erreichbar sein, wenn die R&S®LANCOM Management Cloud nicht erreichbar ist, dann kann zusätzlich je Eintrag der Schalter „LMC-unreachable-only“ gesetzt werden.
5. Speichern Sie anschließend die Konfiguration mittels des Befehls „flash“.

DNS-Anfragen nicht angemeldeter Clients im Hotspot-Netz werden analysiert und die aufgelösten IP-Adressen im Hintergrund zwischengespeichert, um die Angabe von Wildcards zu unterstützen.

Zur Vereinfachung bietet es sich an, diese Konfigurationsschritte in der R&S®LANCOM Management Cloud durch ein Add-in durchzuführen.

Pfad Konsole:

Setup > **WLAN** > **Hotspot**

2.20.12.2.1 Hotspot

Name des Hotspots.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.20.12.2.2 Hostname

Geben Sie hier den freizuschaltenden Host oder dessen IP-Adresse an. Die Angabe von Wildcards wie z. B. „*.lancom.de“ ist möglich.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9].-*`

2.20.12.2.3 LMC-unreachable-only

Soll ein Walled-Garden-Host nur in dem Fall ohne Anmeldung erreichbar sein, wenn die R&S®LANCOM Management Cloud nicht erreichbar ist, dann kann zusätzlich dieser Schalter auf „Yes“ gesetzt werden.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Mögliche Werte:

No
Yes

2.20.12.3 Allowed-Targets

In Netzen, die als Cloud-managed Hotspot betrieben wird, ist prinzipiell der Datenverkehr in RFC1918-Netze verboten. Dies betrifft die folgenden Netze:

- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12

Mit diesem Feature kann der Datenverkehr in diese Netze oder zu einzelnen Hosts selektiv erlaubt werden.

In der R&S®LANCOM Management Cloud ist ein Add-in erforderlich.

Pfad Konsole:

Setup > **WLAN** > **Hotspot**

2.20.12.3.1 Hotspot

Name des Hotspots.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.12.3.1 IP-Network

Erlaubtes IPv4-Netz für diesen Hotspot.

Pfad Konsole:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

Mögliche Werte:

max. 19 Zeichen aus `IPv4-Adresse: a.b.c.d/xx`

2.20.13 WDS

Mittels des Wireless Distribution System (WDS) lassen sich Punkt-zu-Punkt-WLAN-Verbindungen zwischen Access Points aufbauen. Diese Verbindungen dienen als kabelloser Backhaul und ermöglichen so die Anbindung von abgesetzt betriebenen Access Points an den Rest des Netzwerks. So lässt sich beispielsweise die WLAN-Abdeckung auch in Bereichen sicher stellen, in denen keine Ethernet-Anbindung von Access Points möglich ist.

Die beteiligten Access Points können wahlweise ihrerseits SSIDs für die WLAN-Client-Anbindung anbieten („Repeater“-Betrieb) oder die kabellose Backhaul-Verbindung mit ihrem Ethernet-Port verbinden (Wireless Bridge).

Pfad Konsole:

Setup > **WLAN**

2.20.13.1 Links

Konfigurieren Sie in dieser Tabelle alle generellen Einstellungen rund um die auszustrahlenden WLAN-Netzwerke (SSIDs). Fügen Sie je WLAN-Netzwerk eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

Pfad Konsole:

Setup > **WLAN** > **WDS**

2.20.13.1.1 Link-Name

Der Name der Verbindung. Wird für die weitere Referenzierung in der Gerätekonfiguration verwendet.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.13.1.2 SSID-Name

Der Name der speziellen SSID, die für die WDS-Verbindung verwendet wird. Dieser Name muss auf beiden Seiten der Verbindung übereinstimmen.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.13.1.3 Mode

Im Rahmen einer WDS-Verbindung gibt es drei Rollen: Access Point, Client, Legacy Client. Der als Client konfigurierte Partner sucht anhand der oben konfigurierten SSID einen als Access Point konfigurierten Partner und initiiert die Verbindung. Der als Legacy-Client konfigurierte Access Point kann sich in die SSID eines beliebigen Access Points einbuchen.

Im Rahmen eines Punkt-zu-Multipunkt-Szenarios können sich mehrere Clients zu einem Access Point verbinden.

Die Menge aus regulären konfigurierten SSIDs für die Client-Anbindung sowie konfigurierten WDS-Verbindungen kann die Menge an insgesamt durch das jeweilige Gerätemodell unterstützen SSIDs nicht überschreiten – es wird sozusagen dasselbe „SSID-Budget“ verwendet.

Es können beliebig viele WDS-Verbindungen im Access Point-Modus betrieben werden (bis zur Ausschöpfung der o. g. Menge an technisch maximal möglichen SSIDs des Gerätemodells. Es kann jedoch nur eine WDS-Verbindung im Station-Modus je Gerät betrieben werden. Verbindungen im Access Point-Modus und Station-Modus (von letzterer nur eine) können gleichzeitig auf demselben Gerät betrieben werden.

Beachten Sie, dass für ein Punkt-zu-Multipunkt-Szenario in der Regel eine einzelne Verbindung im AP-Modus auf dem „Verteilerknoten“ ausreichend ist.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

Access-Point
Station

2.20.13.1.4 Radio

Das Frequenzband, welches für die WDS-Verbindung genutzt werden soll. Aus Kapazitätsgründen empfiehlt sich die Verwendung von 5 GHz oder 6 GHz (je nach Hardware-Fähigkeiten des verwendeten Gerätemodells).

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

2.4GHz
Die SSID wird nur auf der Frequenz 2,4 GHz ausgestrahlt.

5GHz
Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

6GHz
Die SSID wird nur auf der Frequenz 6 GHz ausgestrahlt.

2.20.13.1.5 Encryption-Profile

Das Verschlüsselungsprofil, welches für die WDS-Verbindung verwendet werden soll.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.13.1.6 Encryption-Key

Der WPA-PSK, welcher für die WDS-Verbindung verwendet wird. Bei der Verwendung eines Verschlüsselungsprofils mit 802.1X, kann dieses Feld leer bleiben.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.13.1.8 Additional-VLANs

Im Rahmen der WLAN-Konfiguration ist es möglich, einzelne SSIDs mit WDS-Verbindungen zu verknüpfen. Diese werden dann gebridget über die WDS-Verbindung zur Verfügung gestellt. Sollen zusätzliche, z. B. über Ethernet transportierte VLANs ebenfalls übertragen werden, können diese hier eingetragen werden (kommaseparierte Liste von VLAN-IDs [0-4095]).

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[0-9],`

2.20.13.1.9 LCOS-Client-Bridge-Support

Wird der LCOS LX-Access Point im Client-Modus mit einem LCOS-Access Point im Basisstations-Modus verbunden, können hierfür weiterhin 4-Adress-Frames verwendet werden, was die Übertragung von VLANs oder MAC-Adressen ermöglicht. Dieser Modus kann nicht verwendet werden, wenn der LCOS LX-Access Point im Basisstations-Modus betrieben wird und ein LCOS-Access Point im Client-Modus an diesem eingebucht wird.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

No
Yes

Default-Wert:

Yes

2.20.13.1.10 Additional-Untagged-VLAN

Nicht-VLAN-getaggte Pakete werden über die WDS-Verbindung übertragen.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

No
Nicht-VLAN-getaggte Pakete werden nicht über die WDS-Verbindung übertragen.

Yes
Nicht-VLAN-getaggte Pakete werden über die WDS-Verbindung übertragen.

Default-Wert:

Yes

2.20.13.1.11 Roaming-Profile

Hier können Sie ein Roaming-Profil eintragen, wenn der Access Point sich im Client oder Legacy-Client Modus befindet.

Konfigurieren Sie optional ein Verschlüsselungsprofil.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil.

Erstellen Sie bei Bedarf ein Roamingprofil.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Links**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.13.2 Encryption

Konfigurieren Sie in dieser Tabelle alle Einstellungen rund um die Verschlüsselung und Authentisierung des Wireless Distribution Systems.

Für WDS-Verbindungen empfehlen wir, ausschließlich WPA3 zu verwenden um höchste Sicherheit zu garantieren.

Pfad Konsole:

Setup > **WLAN** > **WDS**

2.20.13.2.1 Profile-Name

Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.2.2 Method

Konfigurieren Sie hier die Verschlüsselungsmethode.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

802.11i-WPA-PSK
WPA(2/3) mit Pre-Shared-Key

2.20.13.2.3 WPA-Version

Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden **802.11i-WPA-PSK** und **802.11i-WPA-802.1X** verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

WPA1
Die WPA-Version 1 wird exklusiv verwendet.

WPA2
Die WPA-Version 2 wird exklusiv verwendet.

WPA3
Die WPA-Version 3 wird exklusiv verwendet.

WPA1/2
Abhängig von den Fähigkeiten des Clients wird die WPA-Version 1 oder 2 verwendet.

WPA2/3
Abhängig von den Fähigkeiten des Clients wird die WPA-Version 2 oder 3 verwendet.

2.20.13.2.4 WPA1-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

TKIP
Die TKIP-Verschlüsselung wird verwendet.

AES
Die AES-Verschlüsselung wird verwendet.

TKIP/AES
Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

2.20.13.2.5 WPA2-3-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 bzw. 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

2.20.13.2.6 RADIUS-Client-Profile

Geben Sie hier ggf. ein RADIUS-Clientprofil an.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Encryption**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.13.3 Roaming

Konfigurieren Sie hier die Einstellungen für das Roaming-Profil.

Pfad Konsole:

Setup > **WLAN** > **WDS**

2.20.13.3.1 Profile-Name

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später in der WDS-Verbindung angeben.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.13.3.2 Signal-Strength-Threshold

Tragen Sie hier den Schwellenwert ein, ab welchem sich das Scan-Intervall des Access Points verändern soll. Werte von 0 bis 100 geben einen Prozentwert an. Werte von -100 bis 0 sind in dbm.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

max. 4 Zeichen aus `-[0-9]`

2.20.13.3.3 Good-Signal-Scan-Interval

Befindet sich die Signalstärke oberhalb des Grenzwertes, wird in dieser Zeit in Sekunden ein Scan durchgeführt, um zu prüfen, ob ein besserer Access Point zum Verbinden vorhanden wird.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

0 … 4.294.967.295 Sekunden

2.20.13.3.4 Bad-Signal-Scan-Interval

Fällt die Signalstärke auf den angegebenen Grenzwert, wird direkt ein Scan ausgelöst, um nach einem besseren Access Point zu suchen. Ist kein besserer Access Point vorhanden, wird in der angegebenen Zeit in Sekunden weiter gesucht, bis eine Verbindung zu einem Access Point mit einer besseren Signalstärke verbunden werden konnte oder sich das Signal mit dem verbundenen Access Point wieder verbessert hat.

Pfad Konsole:

Setup > **WLAN** > **WDS** > **Roaming**

Mögliche Werte:

0 … 4.294.967.295 Sekunden

2.20.14 Include-UUID

Konfiguriert, ob ein Access Point seine UUID überträgt. Die LANCOM UUID dient u. a. als Ekahau-Erweiterung zur Zusammenfassung mehrerer SSIDs zu einem Access Point.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

No
UUID nicht übertragen.

Yes
UUID übertragen.

Default-Wert:

No

2.20.15 Power-Saving-Mode

Wird der WLAN-Energiesparmodus aktiviert, reduziert der Access Points die Anzahl der aktiven WLAN-Streams je Radio auf 1, sofern kein Client eingebucht ist. Sobald mindestens ein Client mit dem Radio verbunden ist, wird die Anzahl der aktiven Streams wieder auf das für dieses Radio mögliche Maximum erhöht.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

No

WLAN-Energiesparmodus aus.

Yes

WLAN-Energiesparmodus an.

Default-Wert:

No

2.20.16 Include-Devicename

Konfiguriert, ob ein Access Point seinen Gerätenamen überträgt. Zur Unterstützung von WLAN-Ausleuchtungs-Tools kann der Gerätename des Access Points in Beacons eingefügt werden. Der Name ist für alle Radios eines Multi-Radio-Access Points identisch, so dass eine namentliche Zuordnung der einzelnen Radios zu einem Access Point möglich wird.

Der Gerätename wird als Vendor-spezifisches Info-Element wie folgt kodiert:

```
Tag: Vendor Specific: LANCOM Systems GmbH
  Tag Number: Vendor Specific (221)
    # 1 Byte (static value)
  Tag length: 13
    # 1 Byte (static length)
      # In this case: 3 Bytes OUI + 1 Byte LCS Subtype + 2 Bytes LCS Version + 7 Bytes LCS Devicename
  OUI: 00:a0:57 (LANCOM Systems GmbH)
    # 3 Bytes (static value)
  Vendor Specific OUI Type: 8
    # 1 Byte (static length)
      # LCS Subtype: 8 == Devicename
  Vendor Specific Data: 080100544553542d4150
    # Wireshark output comprising 1 Byte "Vendor Specific OUI Type" (0x08)
    # In this case: 9 Bytes
      # 2 Bytes (static value)
        # LCS Version: 1 (little-endian)
      # In this case: 7 Bytes
        # ASCII encoded String
          # In this case: 0x544553542d4150 == TEST-AP
```

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

No
Gerätenamen nicht übertragen.

Yes
Gerätenamen übertragen.

Default-Wert:

No

2.20.18 Client-Management

Konfifurieren Sie hier das Client Management.

Pfad Konsole:
Setup > **WLAN**

2.20.18.2 Profiles

Definieren Sie hier Konfigurationsprofile für das Client-Management. Die Profile können in der Netzwerktabelle ausgewählt werden.

Pfad Konsole:
Setup > **WLAN** > **Client-Management**

2.20.18.2.1 Profile-Name

Name dieses Profils.

Pfad Konsole:
Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:
max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.18.2.2 RRM

Aktivieren Sie hier die Verwendung von RRM.

Pfad Konsole:
Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No
Yes

2.20.18.2.3 BTM

Aktivieren Sie hier die Verwendung von WNM/BTM.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No
Yes

2.20.18.2.4 Neighbor-Load-Threshold

Der prozentuale Wert, bis zu dem APs ausgelastet sein dürfen, um noch als Roaming-Ziele in Frage zu kommen. 100% entsprechen dabei aktuell 80 eingebuchten Clients, es wird nicht zwischen verschiedenen AP-Modellen unterschieden. Der Wert wird für RRM und WNM/BTM verwendet.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

0 … 100

2.20.18.3 Radio-Settings

Definieren Sie hier die Radio-Einstellungen des Client-Managements.

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

2.20.18.3.1 Ifc

Die WLAN-Schnittstelle, für die die folgenden Einstellungen gültig sind.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

max. 9 Zeichen aus `WLAN-1,WLAN-1-2,...`

2.20.18.3.2 BTM-Load-Threshold

Wenn die Last dieser WLAN-Schnittstelle des APs den Grenzwert überschreitet, sendet der AP BTM-Requests an eingebuchte Clients, um diese auf andere APs zu steuern.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

0 … 100

2.20.18.3.3 BTM-Load-Min-Delta

Dies ist ein dynamischer Schwellenwert: er ist relativ zur eigenen Last dieses APs. Der hier konfigurierte Wert stellt die minimale Lastdifferenz gegenüber unserer eigenen Last dar: Nur Nachbar-APs, deren Last mindestens um BTM-Last-min.-Delta niedriger ist als unsere eigene Last, werden an Clients empfohlen. Alle anderen werden als „nicht verwenden“ markiert. Beispiel: BTM-Last-Grenzwert beträgt 80, BTM-Last-min.-Delta ist 10. Angenommen, unsere eigene Last liegt bei 85 – wir haben den Schwellenwert damit überschritten und versuchen, Clients über BTM-Anfragen an Nachbar-APs zu verlagern. Mit dem Min-Delta von 10 werden jedoch nur APs an Clients empfohlen, deren Last mindestens 10 Punkte niedriger ist als unsere eigene. In diesem Beispiel werden daher alle Nachbar-APs mit einer Last von 75 oder höher als „nicht verwenden“ markiert. (Hinweis: Der statische Schwellenwert aus der Profiltabelle gilt weiterhin unabhängig davon.)

Dieses „Min-Delta“ dient der Erzeugung einer Hysterese, um zu verhindern, dass zwei Nachbar-APs mit hoher Last – jeweils nahe ihrem eigenen Schwellenwert – Clients ständig zwischen ihnen hin und her wechseln lassen.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

0 … 100

2.20.19 Client-Management-Mode

Entscheiden Sie hier, ob Client-Management, reines Band-Steering oder keins der Features genutzt werden soll.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Client-Management
Band-Steering
Off

2.20.20 End2End-Test

Mit dem WLAN End-to-End-Test lässt sich die Verfügbarkeit und Leistungsfähigkeit eines WLANs aus Sicht eines Endgeräts überprüfen – ganz ohne zusätzliches Testgerät vor Ort. Dazu wird ein vorhandener R&S®LANCOM Access Point vorübergehend in den Client-Modus versetzt und führt definierte Tests entlang des gesamten Verbindungswegs vom WLAN bis ins Internet aus.

Der Test erkennt unter anderem Probleme bei der WLAN-Authentifizierung, der IP-Adressvergabe per DHCP, der Namensauflösung über DNS, der Anmeldung an einem Captive Portal sowie bei Ping- und HTTP-Verbindungen. Die Testprofile können an die jeweilige Netzwerkumgebung angepasst werden. Nicht benötigte Tests lassen sich dabei aus dem Profil entfernen – beispielsweise der Captive-Portal-Test, wenn kein Hotspot betrieben wird.

Ein Testlauf kann bei Bedarf manuell durch einen Administrator gestartet oder über die interne Cron-Tabelle regelmäßig geplant werden. Die Ergebnisse werden in den entsprechenden Logtabellen gespeichert und zusätzlich an den Gerätesyslog weitergegeben. Von dort können sie beispielsweise an externe SIEM-Systeme weitergeleitet werden.

Während der Testausführung arbeitet der Access Point im Client-Modus. Dadurch steht er vorübergehend nicht für den normalen WLAN-Betrieb zur Verfügung und verbundene Clients werden getrennt. Nach Abschluss des Testlaufs wechselt der Access Point automatisch zurück in den normalen Betriebsmodus und nimmt die Versorgung der WLAN-Clients wieder auf.

Die Tests werden in einer festgelegten Reihenfolge ausgeführt:

1. WLAN-Verbindung
2. Netzwerkverbindung einschließlich DHCPv4, DHCPv6 und SLAAC
3. DNS-Auflösung
4. Captive Portal
5. Ping
6. HTTP-Verbindung

Diese Reihenfolge kann nicht verändert werden, da die einzelnen Prüfungen aufeinander aufbauen. Eine WLAN-Verbindung ist beispielsweise die Voraussetzung für die Netzwerkkommunikation, eine gültige IP-Adresse wird für DNS-Abfragen benötigt, und ein HTTP-Test ist gegebenenfalls erst nach erfolgreicher Anmeldung am Captive Portal möglich.

Pfad Konsole:

Setup > **WLAN**

2.20.20.1 Test-Profiles

In diesem Menü werden Testläufe zusammengestellt. Ein Testlauf besteht aus mehreren Einzeltests, die gemeinsam ausgeführt werden.

Für jedes Testprofil muss mindestens ein Test der Kategorie **WLAN-Verbindung** konfiguriert werden. Weitere Einzeltests können optional hinzugefügt werden – abhängig davon, welche Prüfungen ausgeführt werden sollen.

Bleibt die **WLAN-Authentifizierung** leer, wird eine offene WLAN-Verbindung ohne Verschlüsselung verwendet. Die SSID muss in diesem Fall ein offenes Netzwerk bereitstellen.

Statische IPv4- oder IPv6-Parameter können leer bleiben, wenn im jeweiligen **IPvX-Modus** keine statischen Parameter ausgewählt wurden.

Pro Testprofil können mehrere Einzeltests derselben Kategorie ausgeführt werden. Hierzu werden die entsprechenden Tests durch Kommas getrennt angegeben.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.1.1 Profile-Name

Der Name dieses Testprofils.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.2 WLAN-Connection

Wählen Sie eine der vorhandenen WLAN-Verbindungen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.3 WLAN-Authenticationn

Wählen Sie eine der vorhandenen WLAN-Authentifizierungen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.4 IPv4-Mode

Wählen Sie entweder DHCP oder statisch.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

DHCP
static

2.20.20.1.5 IPv6-Mode

Wählen Sie entweder Router Advertisement, DHCPv6, statisch oder Aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

Router-Advertisement
DHCPv6
static
Off

2.20.20.1.6 IPv4-Static-Parameters

Wählen Sie ggf. die statischen IPv4-Parameter aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.7 IPv6-Static-Parameters

Wählen Sie ggf. die statischen IPv6-Parameter aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.1.8 DNS-Targets

Wählen Sie eines der vorhandenen DNS-Ziele.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.20.1.9 Ping-Targets

Wählen Sie eines der vorhandenen Ping-Ziele.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.20.1.10 Captive-Portal-Login

Wählen Sie eines der vorhandenen Captive-Portal-Logins.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.20.1.11 HTTP-Targets

Wählen Sie eines der vorhandenen HTTP-Ziele.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.20.2 WLAN-Connection

Legen Sie fest, mit welcher SSID die Verbindung hergestellt und die Tests ausgeführt werden sollen.

Optional kann eine bestimmte BSSID angegeben werden, wenn die Verbindung gezielt zu einem bestimmten Access Point hergestellt werden soll. Wird keine BSSID konfiguriert, wählt der Test automatisch einen Access Point mit der angegebenen SSID aus. Dabei wird der Access Point mit der besten Signalstärke bevorzugt.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.2.1 WLAN-Connection-Name

Geben Sie dieser Verbindung einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.2.2 SSID-Name

Die SSID für die Tests.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.20.2.3 BSSID

Optionale BSSID für die Tests.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

max. 17 Zeichen aus `mac address (xx:xx:xx:xx:xx:xx)`

2.20.20.2.4 Radio-Band

Das Radio-Band für diese Verbindung.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

2.4GHz
5GHz
6GHz

2.20.20.3 WLAN-Authentication

Der WLAN E2E-Test unterstützt sowohl die Authentifizierung per PSK als auch per IEEE 802.1X mit den üblichen Optionen auf Client-Seite.

Für die Verwendung von IEEE 802.1X muss zuvor ein passendes Supplicant-Profil konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.3.1 WLAN-Authentication-Name

Geben Sie dieser WLAN-Authentifizierung einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.3.2 Encryption-Key

Geben Sie den PSK an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.20.3.3 Method

Wählen Sie die Methode der WLAN-Authentifizierung aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

802.11i-WPA-PSK
802.11i-WPA-802.1X
Enhanced-Open
802.11i-WPA-802.1X-192-Bits

2.20.20.3.4 WPA-Version

Wählen Sie die WPA-Version aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

WPA1
WPA2
WPA1/2
WPA3
WPA2/3

2.20.20.3.5 Session-Keytypes

Wählen Sie den Typ des Sitzungsschlüssels aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

TKIP
AES
TKIP/AES

2.20.20.3.6 802.1X-Client-Profile

Wählen Sie ein IEEE 802.1X-Clientprofil aus.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.4 IP-Static-Parameters

Wenn für den Test eine statische IP-Konfiguration verwendet werden soll, tragen Sie die entsprechenden IP-Parameter in dieser Tabelle ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.4.1 IP-Static-Parameters-Name

Geben Sie dieser statischen IP-Konfiguration einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.4.2 IP-Address

Tragen sie die IP-Adresse ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.4.3 IP-Gateway

Tragen sie den IP-Gateway ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.4.4 Primary-IP-DNS

Tragen sie die IP-Adresse des primären DNS-Servers ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.4.5 Secondary-IP-DNS

Tragen sie die IP-Adresse des sekundären DNS-Servers ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.5 DNS-Targets

Hier können Sie den DNS-Test konfigurieren. Im Feld **Expected-Response** können Sie durch das Präfix „A:“ oder „AAAA:“ festlegen, dass ein bestimmter A- bzw. AAAA-Record erwartet wird.

Mehrere Records können als kommagetrennte Liste angegeben werden. Der Test gilt als erfolgreich, sobald einer der konfigurierten Records mit der empfangenen Antwort übereinstimmt.

Bleibt das Feld **Expected-Response** leer, gilt jeder empfangene A- oder AAAA-Record als erfolgreiche Antwort.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.5.1 DNS-Targets-Name

Geben Sie diesen DNS-Zielen einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.5.2 DNS-Target-Hostname

Geben Sie die Hostnamen an, die getestet werden sollen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9].-`

2.20.20.5.3 Expected-Response

Geben Sie die für diesen Test erwartete Antwort ein.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.20.6 Ping-Targets

Hier können Sie den Ping-/ICMP-Test konfigurieren. Die Felder Ping- und Fehler-Anzahl sind mit den gezeigten Standardwerten vorbelegt und können bei Bedarf angepasst werden.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.6.1 Ping-Targets-Name

Geben Sie diesen Ping-Zielen einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.6.2 Ping-Target-Hostname

Geben Sie den Hostnamen an, der getestet werden sollen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9].-:%`

2.20.20.6.3 Ping-Count

Geben Sie die Ping-Anzahl an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

10

2.20.20.6.4 Fail-Count

Geben Sie die Fehler-Anzahl an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

2

2.20.20.7 Captive-Portal-Logins

Wenn das zu testende Netzwerk durch ein Captive Portal geschützt ist, können Sie die erforderlichen Anmeldeparameter hier konfigurieren.

Der E2E-Test ruft zunächst die konfigurierte Test-URL auf, um zu prüfen, ob das Captive Portal eine Weiterleitung durchführt. Wird eine Weiterleitung erkannt, erstellt der Test eine HTTP-POST-Anfrage mit den Einträgen aus der Tabelle Captive-Portal-Login-Daten und sendet diese an die im Feld Formular-Aktion angegebene URL.

Anschließend wird die Test-URL erneut aufgerufen. Erfolgt nun keine Weiterleitung mehr, gilt die Anmeldung als erfolgreich und der Test wird bestanden.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.7.1 Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.7.2 Type

Hier kann entweder „Login“ oder „Logout“ ausgewählt werden.

Je nach Captive Portal kann es sinnvoll sein, den Benutzer nach Abschluss des Tests wieder abzumelden. Dadurch lassen sich beispielsweise Ressourcen auf dem Captive-Portal-Gateway schonen oder erneute Anmeldungen mit denselben Zugangsdaten bei späteren Testläufen ermöglichen.

Legen Sie hierzu einen zusätzlichen Eintrag mit dem Typ „Logout“ an. Konfigurieren Sie dabei die **Formular-Aktion** so, dass sie die Abmeldeaktion des Captive Portals ausführt. Die URL für die Abmeldung kann sich von der URL des Anmeldeformulars unterscheiden. Analysieren Sie hierzu den HTML-Code des jeweiligen Portals.

Viele moderne Captive Portals mit Click-through-Anmeldung bieten jedoch keine Abmeldefunktion. Die Benutzersitzung wird in diesem Fall erst nach einem Timeout beendet. Ein regelmäßig in kurzen Abständen ausgeführter Captive-Portal-Test kann dann möglicherweise erfolgreich sein, ohne die Anmeldung tatsächlich zu prüfen, da die MAC-Adresse des testenden Access Points noch im Captive Portal zwischengespeichert ist.

Wenn Sie das Captive Portal selbst verwalten, kann eine spezielle Testfunktion sinnvoll sein. Beispielsweise könnte ein verstecktes Formular im HTML-Code eine dedizierte Testsitzung starten, die bereits nach kurzer Zeit automatisch abläuft.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

Login
Logout

2.20.20.7.3 Test-URL

Dies ist die URL, die der E2E-Test aufruft, um festzustellen, ob das Captive Portal eine Weiterleitung durchführt. Sie kann auf jede URL zeigen, die zuverlässig mit einem HTTP-Statuscode aus dem Bereich „200“ antwortet. Idealerweise wird eine URL verwendet, die mit „200“ oder „204“ antwortet.

Das Feld ist standardmäßig leer, da keine URL eines externen Drittanbieters fest vorgegeben werden kann. Es muss daher eine geeignete URL konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.7.4 Form-Action

Dies ist die URL, an die die Anmeldedaten per HTTP POST übertragen werden. Beim klassischen LCOS-Public Spot kann dies beispielsweise eine URL wie die Folgende sein:

```
https://pspot.lancom.de:443/authen/login/
```

Bleibt dieses Feld leer, verwendet der E2E-Test automatisch die URL, zu der das Captive Portal beim ersten Aufruf der Success-URL weitergeleitet hat. Bei R&S®LANCOM Management Cloud-basierten Hotspots funktioniert die Anmeldung dadurch in der Regel ohne zusätzliche Konfiguration dieser URL.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.8 HTTP-Targets

In dieser Tabelle können Sie eine HTTP-Verbindung testen. Der E2E-Test ruft die konfigurierte **HTTP-Ziel-URL** ab und vergleicht den empfangenen HTTP-Statuscode mit dem im Feld **Expected-Response** angegebenen Wert.

Der HTTP-Test kann zusätzlich als Geschwindigkeitstest verwendet werden, wenn über die HTTP-Ziel-URL eine ausreichend große Datei heruntergeladen werden kann. Damit eine aussagekräftige Durchsatzmessung möglich ist, sollte in diesem Fall auch **Maximale Größe (Bytes)** konfiguriert werden. Wird kein Maximalwert angegeben, wird die Datei vollständig heruntergeladen.

Der gemessene Durchsatz wird in den Testergebnissen immer angezeigt. Aussagekräftig ist dieser Wert jedoch nur, wenn eine ausreichend große Datei heruntergeladen wird und der TCP-/HTTP-Download eine realistische Übertragungsgeschwindigkeit erreichen kann.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.8.1 HTTP-Targets-Name

Geben Sie diesen HTTP-Zielen einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.8.2 HTTP-Target-URL

Geben Sie die URL an, die getestet werden soll.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.20.20.8.3 Expected-Response

Geben Sie die erwartete Antwort an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.20.8.4 Max-Size-Bytes

Optionale Größenbeschränkung.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 20 Zeichen aus `[0-9]`

2.20.20.9 Captive-Portal-Login-Data

In dieser Tabelle werden die Formularelemente konfiguriert, die für eine Anmeldung oder Abmeldung per HTTP POST an das Captive Portal übertragen werden.

Bei einem klassischen, auf LCOS basierenden Public Spot können die Formulardaten beispielsweise wie folgt aussehen:

Attribut	Wert
AGB	checked
password	geheim
userid	rsnc

Wenn zusätzlich die Logout-Funktion verwendet wird, müssen in dieser Tabelle auch die entsprechenden Attribute für den Logout-Test hinterlegt werden.

Bei sehr einfachen Portalseiten, die beispielsweise nur ein einziges Formularattribut – etwa eine Schaltfläche für den Click-through-Login – enthalten, versucht der E2E-Test, dieses Attribut automatisch per POST zu übertragen. In diesem Fall ist keine zusätzliche Konfiguration in dieser Tabelle erforderlich. Dies funktioniert derzeit beispielsweise beim One-Button-Login des R&S®LANCOM Management Cloud-Hotspots.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.20.9.1 Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.20.9.2 Attribute

Geben Sie hier die benötigten Attribue an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.20.9.3 Value

Geben Sie hier die Werte zu den konfigurierten Attribuen an.

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.20.20.20 Run-Tests

Mit dieser Aktion starten Sie die Tests.

Beispiel: `do Run-Tests`

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

2.20.133 LEPS

Mit R&S®NC Enhanced Passphrase Security (LEPS) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen. Alternativ lässt sich auch ein MAC-Adress-Filter realisieren.

Pfad Konsole:

Setup > **WLAN**

2.20.133.1 Operating

Schaltet LEPS ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.20.133.2 Profiles

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

2.20.133.2.1 Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.20.133.2.2 Network-Name

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-Profil gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-Profil verbunden sind.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

2.20.133.2.3 Mac-List

Hier können Sie angeben, ob und wie die MAC-Adressen ürberprüft werden sollen.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

Disabled
Die MAC-Adresse wird für die LEPS-Anmeldung nicht beachtet. Eine ggf. gesetzte benutzerspezifische Passphrase wird hingegen geprüft.

Whitelist
Nur die Clients werden zugelassen, deren MAC-Adresse bekannt ist.

Blacklist
Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

2.20.133.2.4 VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

0 … 4095

2.20.133.3 Users

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

2.20.133.3.1 Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.133.3.2 Profile

Wählen Sie hier das Profil aus, für das der LEPS-Benutzer gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID anmelden, mit der sie über das LEPS-Profil verbunden sind.

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Users**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.133.3.3 WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-Benutzer sich am WLAN anmelden soll.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

max 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.20.133.3.4 VLAN

Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch am LEPS-Benutzer ein VLAN konfiguriert, gilt die am LEPS-Benutzer konfigurierte VLAN-ID.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

0 … 4095

2.20.133.3.7 MAC-Address

Optionale Angabe einer MAC-Adresse für einen MAC-Filter. Abhängig von der Einstellung im Profil wird dieser Eintrag nicht beachtet oder es können sich dann nur die in dieser Tabelle aufgeführten Clientgeräte anmelden (Whitelist). Mittels Blacklist funktioniert der MAC-Filter genau anders herum – die angegebenen MAC-Adressen können sich nicht anmelden.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

MAC-Adresse im Format `xx:xx:xx:xx:xx:xx`

2.20.1111 Rate-Selection

Zur Verringerung der Mediumslast kann es hilfreich sein, die Broad- und Multicast-Datenrate zu erhöhen. Broad- und Multicasts werden normalerweise mit der niedrigst möglichen Rate versendet, um auch weit entfernte Clients zu erreichen; allerdings belegen sie somit ein hohes Maß an Mediumszeit. Eine Anpassung bietet sich vor allem in großen Netzen mit einer hohen Access Point-Dichte an. In dieser Tabelle können Sie die Raten für die WLAN-Netzwerke festlegen.

Pfad Konsole:

Setup > **WLAN**

2.20.1111.1 Network-Name

Das Netzwerk bzw. die SSID, für die die hier konfigurierten Raten gelten sollen. Der Name muss einem Namen der in *2.20.1 Network* eingerichteten Netzwerke entsprechen.

Pfad Konsole:

Setup > **WLAN** > **Rate-Selection**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.1111.23 Broadcast-Rate

Die für das Senden von Broadcasts zu verwendende Rate.

Wird als Broadcast-Rate 6 Mbit/s, 12 Mbit/s oder 24 Mbit/s ausgewählt, wird diese Rate ebenfalls für das Senden von Beacons verwendet.

Andere Raten als diese haben nur Einfluss auf Broadcast-Pakete und verändern nicht die Beacon-Rate.

Pfad Konsole:

Setup > **WLAN** > **Rate-Selection**

Mögliche Werte:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default-Wert:

default

2.20.1111.24 Multicast-Rate

Die für das Senden von Multicasts zu verwendende Rate.

Pfad Konsole:

Setup > **WLAN** > **Rate-Selection**

Mögliche Werte:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default-Wert:

default

2.20.1111.25 Beacon-Rate

Die Datenrate, mit der WLAN-Beacons ausgesendet werden. In High-Density-Szenarien ist es empfehlenswert, diese Datenrate zu erhöhen, um Airtime zu sparen.

Pfad Konsole:

Setup > **WLAN** > **Rate-Selection**

Mögliche Werte:

default
6Mbps
12Mbps
24Mbps

Default-Wert:

default

2.20.1111.101 Radioband

Das Band, für das die konfigurierten Raten gelten sollen. Hiermit kann weiter auf ein bestimmtes Band eingeschränkt werden.

Pfad Konsole:

Setup > **WLAN** > **Rate-Selection**

Mögliche Werte:

2.4GHz+5GHz
2.4GHz
5GHz
none

Default-Wert:

2.4GHz+5GHz

2.22 Syslog

Zu Diagnosezwecken kann das Syslog eines LCOS LX-basierten Gerätes an einen externen Syslog-Server gesendet werden.

Hier finden Sie die Einstellungen dafür.

Pfad Konsole:

Setup

2.22.2 Server

Konfigurieren Sie in dieser Tabelle einen oder mehrere Syslog-Server. Die Nachrichten können via TCP oder UDP versandt werden.

Beachten Sie, dass Syslog-Nachrichten unverschlüsselt sind und ggf. sensible Informationen über Ihr Netzwerk beinhalten können. Sie sollten daher nur über ein sicheres Netz zu Diagnosezwecken übertragen werden.

Pfad Konsole:

Setup > **Syslog**

2.22.2.1 Name

Name des externen Syslog-Servers.

Pfad Konsole:

Setup > **Syslog** > **Server**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.22.2.7 IP-Address

IP-Adresse des externen Syslog-Servers.

64 chars from IPv4 or IPv6 address

Pfad Konsole:

Setup > **Syslog** > **Server**

Mögliche Werte:

max. 64 Zeichen aus `IPv4- oder IPv6-Adresse`

2.22.2.8 Port

Port des externen Syslog-Servers.

Pfad Konsole:

Setup > **Syslog** > **Server**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

514

2.22.2.9 Protocol

Protokoll (TCP/UDP), mit dem der externe Syslog-Server angesprochen wird.

Pfad Konsole:

Setup > **Syslog** > **Server**

Mögliche Werte:

TCP
UDP

Default-Wert:

TCP

2.23 Logging

Hier finden Sie die Einstellungen zum Logging.

Pfad Konsole:

Setup

2.23.1 Operating

Aktiviert das Tracesystem während des Bootvorgangs.

Wenn in der Tabelle *2.23.5 Trace* kein Eintrag vorgenommen wurde, dann beendet sich das Tracesystem automatisch.

Pfad Konsole:

Setup > **Logging**

Mögliche Werte:

Yes

Tracesystem aktiviert.

No

Tracesystem nicht aktiviert.

Default-Wert:

No

2.23.2 Timer-Seconds

Gibt die Sekunden an, wielange das System aktiviert bleibt. Empfehlenswert ist ein Wert zwischen 60 und 120 Sekunden, da der lxcd erfahrungsgemäß solange braucht, bis aktiviert wird.

Pfad Konsole:

Setup > **Logging**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Besondere Werte:

0

Keine Zeitbeschänkung.

2.23.3 Level

Hier wird angegeben, welches Log-Level aktivert werden soll. Dabei schließt ein höheres Level alle darunter liegenden Levels automatisch mit ein. Also würde der Level Debug die Level Error, Warning und Info ebenfalls aktivieren.

Pfad Konsole:

Setup > **Logging**

Mögliche Werte:

Info

Level 0 - Info-Meldungen

Warning
Level 1 - Warnungen
Error
Level 2 - Fehler-Meldungen
Debug
Level 3 - Debug-Meldungen
Guru
Level 4 - Meldungen für Entwickler

Default-Wert:

Info

2.23.4 Target

Dieser Wert gibt an, wohin die Trace-Daten geschrieben werden. Wenn Syslog gewählt wird, wird das aktivierte Tracesystem die Nachrichten ins Syslog schreiben.

Pfad Konsole:
Setup > **Logging**

Mögliche Werte:

Syslog
Trace-Daten werden ins Syslog geschrieben. Mit Remote-Syslog wäre hier ein Remote-Tracing möglich.
Devlog
Trace-Daten werden in /proc/lxlog geschrieben. Dieses Logg wird mit dem „Support Information“-System exportiert.

2.23.5 Trace

Diese Tabelle beinhaltet die Namen der Traces, deren Trace-Daten geschrieben werden sollen. Eine Übersicht der möglichen Namen erhalten Sie über den CLI-Befehl `trace ?`.

Pfad Konsole:
Setup > **Logging**

2.23.5.1 Name

Ein Name in der Tabelle der Traces, deren Trace-Daten geschrieben werden sollen. Eine Übersicht der möglichen Namen erhalten Sie über den CLI-Befehl `trace ?`.

Pfad Konsole:
Setup > **Logging** > **Trace**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]:*-_`

Default-Wert:

leer

2.23.6 Log-Persistence

Hierüber kann das letzte lxlog nach dem Booten persistiert werden. Bei Aktivierung wird somit /tmp/lxlog_latest.gz nach /config/lxbootlog.gz kopiert.

Pfad Konsole:

Setup > **Logging**

Mögliche Werte:

Yes
No

Default-Wert:

No

2.30 RADIUS

Konfigurationseinstellungen der Parameter für RADIUS und IEEE 802.1X.

Pfad Konsole:

Setup

2.30.3 RADIUS-Server

Konfigurieren Sie hier die Einstellungen für RADIUS-Server-Profile zur Verwendung mit WLAN-Netzwerken, die 802.1X als Authentisierungsverfahren verwenden.

Pfad Konsole:

Setup > **RADIUS**

2.30.3.1 Name

Wählen Sie hier einen sprechenden Namen für das RADIUS-Server-Profil. Dieser interne Name wird verwendet, um das RADIUS-Server-Profil in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.3 Port

Wählen Sie hier den (UDP)-Port, der verwendet wird, um den RADIUS-Server zu kontaktieren.

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

0 … 65535

2.30.3.4 Secret

Konfigurieren Sie hier das Secret, mit welchem der Datenverkehr zwischen dem Gerät und dem RADIUS-Server verschlüsselt wird. Dieses Secret muss ebenfalls auf dem RADIUS-Server hinterlegt sein.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.5 Backup

Konfigurieren Sie hier ein Backup-Profil, welches verwendet wird, wenn der RADIUS-Server im hier konfigurierten Profil nicht erreichbar ist.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.8 Server-IP-Address

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Server erreichbar ist.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `IPv4- oder IPv6-Adresse`

2.30.3.9 Accounting-Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Accounting-Server zu kontaktieren.

Normalerweise ist dies der Port 1813 (RADIUS Accounting).

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

0 … 65535

2.30.3.14 Accounting-IP-Address

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Accounting-Server erreichbar ist.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `IPv4- oder IPv6-Adresse`

2.30.3.15 MAC-Check

Statt einen Benutzernamen über den RADIUS-Server zu authentifizieren, kann dies auch mit einer MAC-Adresse geschehen.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

No

Keine Überprüfung anhand der MAC-Adresse.

Yes

Die Berechtigungen der Clients am RADIUS-Server über die MAC-Adresse überprüfen.

2.30.3.16 Fallback-Dynamic-VLAN-ID

Wenn von einem RADIUS-Server keine VLAN-ID für einen WLAN-Client übermittelt wird, so wird die hier vergebene VLAN-ID verwendet.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass die vom RADIUS-Server mitgesendete VLAN-ID verwendet wird.

2.30.3.17 Require-Message-Authenticator

Mit dieser Option lässt sich festlegen, ob das Vorhandensein eines Message-Authenticators in RADIUS-Nachrichten zwingend gefordert wird. Ist dies der Fall, werden Nachrichten ohne Message-Authenticator nicht bearbeitet und verworfen.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Werte:

No

Message-Authenticator in RADIUS-Nachrichten nicht notwendig.

Yes

Message-Authenticator in RADIUS-Nachrichten muss vorhanden sein.

2.30.4 Delete-WLAN-Supplicant-Certificates

Mit dieser Aktion löschen Sie alle vorhandenen Zertifikate der WLAN-Supplicants.

Pfad Konsole:

Setup > **RADIUS** > **RADIUS-Server**

Mögliche Argumente:

keine

2.30.11 LAN-Supplicant

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät LAN-seitig an einer mit 802.1X gesicherten Switch-Infrastruktur zu authentifizieren.

Pfad Konsole:

Setup > **RADIUS**

2.30.11.1 Interface-Name

Der Name der LAN-Schnittstelle. Aktuell gibt es nur die Schnittstelle INTRANET, daher kann diese nicht geändert werden.

Pfad Konsole:

Setup > **RADIUS** > **LAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.30.11.2 Method

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

Pfad Konsole:

Setup > **RADIUS** > **LAN-Supplicant**

Mögliche Werte:

none
MD5
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

2.30.11.3 Username

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

Pfad Konsole:

Setup > **RADIUS** > **LAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.30.11.4 Password

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Pfad Konsole:

Setup > **RADIUS** > **LAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.30.12 WLAN-Supplicant

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät WLAN-seitig an einer mit 802.1X gesicherten Infrastruktur zu authentifizieren.

Pfad Konsole:

Setup > **RADIUS**

2.30.12.1 Profile-Name

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.30.12.2 Method

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von TLS ist das Hochladen eines Zertifikates notwendig.

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

none
MD5
TLS
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

2.30.12.3 Username

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.30.12.4 Password

Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.30.12.5 Certificate

Sie können das RADIUS-Server Zertifikat automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren.

Pfad Konsole:

Setup > **RADIUS** > **WLAN-Supplicant**

Mögliche Werte:

Auto-accept
Zertifikat automatisch annehmen.

Container

Hochgeladenes Zertifikat prüfen.

2.40 Multicast-Snooping

Alle Geräte mit WLAN-Schnittstellen verfügen über eine „LAN-Bridge“, die für die Übertragung der Daten zwischen den Ethernet-Ports und den WLAN-Schnittstellen sorgen. Die LAN-Bridge arbeitet dabei in vielen Aspekten wie ein Switch. Die zentrale Aufgabe eines Switches besteht darin, Pakete nur an den Port weiterzuleiten, an dem der Empfänger angeschlossen ist. Dazu bildet der Switch automatisch aus den eingehenden Datenpaketen eine Tabelle, in der die Absender-MAC-Adressen den Ports zugeordnet werden.

Wenn eine Ziel-Adresse eines eingehenden Pakets in dieser Tabelle gefunden wird, kann der Switch das Paket gezielt an den richtigen Port weiterleiten. Wird die Ziel-Adresse nicht gefunden, so leitet der Switch das Paket an alle Ports weiter. D. h. ein Switch kann ein Paket nur dann zielgerichtet weiterleiten, wenn die Zieladresse schon einmal als Absenderadresse eines Pakets über einen bestimmten Port bei ihm eingegangen ist. Broadcast- oder Multicast-Pakete können aber niemals als Absenderadresse in einem Paket eingetragen sein, darum werden diese Pakete immer auf alle Ports „geflutet“.

Während dieses Verhalten für Broadcasts die richtige Aktion ist, da Broadcasts schließlich alle möglichen Empfänger erreichen sollen, ist es für Multicasts nicht unbedingt die gewünschte Lösung. Multicasts richten sich in der Regel an eine bestimmte Gruppe von Empfängern in einem Netzwerk, nicht aber an alle.

Videostreams werden z. B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.

Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im Gerät wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das „überflüssige“ Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber gerade in WLAN-Netzwerken zu Performance-Problemen. Dort kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, da Multicasts im WLAN – genau wie Broadcasts – mit der niedrigst möglichen Übertragungsrate gesendet werden, damit diese von jedem WLAN-Teilnehmer empfangen werden können.

Mit dem Internet Group Management Protocol (IGMP) für IPv4 sowie Multicast Listener Discovery (MLD) für IPv6 stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP nutzt dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).

Das Multicast-Snooping macht sich diese Nachrichten zunutze, um zu entscheiden, an welchen Port (also auch, an welche WLAN SSID) Multicasts gesendet werden müssen.

Pfad Konsole:

Setup

2.40.1 Operating

Schalten Sie Multicast-Snooping ein oder aus.

Pfad Konsole:

Setup > **Multicast-Snooping**

Mögliche Werte:

No

Multicast-Snooping ausgeschaltet.

Yes

Multicast-Snooping eingeschaltet.

2.45 Bridge

Pfad Konsole:

Setup

2.45.1 DHCP-Snooping

Der Access Point kann DHCP-Paketen, die durchgeleitet werden, die Circuit-ID und / oder Remote-ID hinzufügen. Der DHCP-Server kann abhängig von dieser Information Entscheidungen treffen, z. B. bestimmte IP-Adressen vergeben.

Pfad Konsole:

Setup > **Bridge**

2.45.1.1 Port

Hier kann der WLAN-Netzwerkname oder ein LAN-Port (je nach Gerätemodell ETHx oder LANx) konfiguriert werden, auf dem DHCP-Requests ergänzt werden sollen.

Die Bezeichner der LAN-Ports sind in der CLI-Tabelle **Status** > **LAN** > **Ports** einsehbar.

Pfad Konsole:

Setup > **Bridge** > **DHCP-Snooping**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.45.1.2 Circuit-ID

Hier kann die Circuit-ID (Option 82) unter Verwendung dieser Platzhalter konfiguriert werden:

- %i: Fügt den Namen der Schnittstelle ein, über die der Relay-Agent die DHCP-Anfrage empfangen hat.
- %n: Fügt den Namen des DHCP-Relay-Agents ein, wie er unter **Setup** > **Name** angegeben ist.
- %s: Fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable eine leere Zeichenkette.
- %r: Fügt die systemweite MAC-Adresse ein.
- %%: Fügt ein Prozentzeichen ein.

Pfad Konsole:

Setup > **Bridge** > **DHCP-Snooping**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.45.1.3 Remote-ID

Hier kann die Remote-ID unter Verwendung dieser Platzhalter konfiguriert werden:

- %i: Fügt den Namen der Schnittstelle ein, über die der Relay-Agent die DHCP-Anfrage empfangen hat.
- %n: Fügt den Namen des DHCP-Relay-Agents ein, wie er unter **Setup** > **Name** angegeben ist.
- %s: Fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable eine leere Zeichenkette.
- %r: Fügt die systemweite MAC-Adresse ein.
- %%: Fügt ein Prozentzeichen ein.

Pfad Konsole:

Setup > **Bridge** > **DHCP-Snooping**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.46 mDNS-Filter

mDNS (Multicast DNS) wird zur einfachen Diensterkennung im (W)LAN verwendet. Prominente Anwendungen, die darauf basieren, sind Bonjour / AirPlay und Google Cast.

Da mDNS-Anfragen als Multicast versendet werden, muss das Versenden auf WLAN-Ebene mit der kleinsten erlaubten Datenrate erfolgen, wodurch je nach Aufkommen an mDNS-Anfragen sehr viel Airtime belegt wird. Mittels des mDNS-Filter lassen sich Anfragen an definierbare mDNS-Dienste selektiv erlauben, die über das WLAN weitergeleitet werden sollen.

Pfad Konsole:

Setup

2.46.1 Services

Die Services-Tabelle enthält standardmäßig die gängigsten mDNS-basierten Dienste, kann aber auch manuell erweitert werden.

Pfad Konsole:

Setup > **mDNS-Filter**

2.46.1.1 Name

Der Name eines Dienstes.

Pfad Konsole:

Setup > **mDNS-Filter** > **Services**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.46.1.2 Service-Type

Der Typ dieses Dienstes.

Pfad Konsole:

Setup > **mDNS-Filter** > **Services**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.46.1.3 Comment

Kommentar zu diesem Eintrag.

Pfad Konsole:

Setup > **mDNS-Filter** > **Services**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.46.2 Services-List

Konfigurieren Sie hier Filter auf Basis der Dienste aus der Services-Tabelle.

Die Dienst-Liste arbeitet als Whitelist: Ist die Liste nicht befüllt, sind alle mDNS-Dienste erlaubt. Enthält die Liste Einträge, sind nur die erlaubten Dienste erlaubt. Alle weiteren Dienste werden gefiltert.

Pfad Konsole:

Setup > **mDNS-Filter**

2.46.2.1 Network-Name

Hier kann der WLAN-Netzwerkname konfiguriert werden, für den der Filter gelten soll.

Pfad Konsole:

Setup > **mDNS-Filter** > **Services-List**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.46.2.2 Services

Hier kann ein oder mehrere der in der Services-Tabelle definierten mDNS-basierten Dienste hinzugefügt werden, für welche Anfragen weitergeleitet werden sollen.

Pfad Konsole:

Setup > **mDNS-Filter** > **Services-List**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.47 Firewall

Mit der Firewall kann Datenverkehr von und zu WLAN-Netzen auf IP-Ebene gefiltert werden. Es ist eine Deny-All-Strategie (jeglicher Verkehr wird verboten, bis auf konfigurierte Ausnahmen) oder eine Allow-All-Strategie (jeglicher Verkehr wird erlaubt, nur Ausnahmen werden verboten) möglich. Es können neben IP-Adressen auch Hostnamen / DNS-Namen als Ziel verwendet werden. Die Firewall liest dazu jegliche DNS-Anfragen von Clients im betroffenen WLAN-Netzwerk mit und speichert die aufgelösten IP-Adressen bis zum Erreichen der TTL (time-to-live) in einem internen Zwischenspeicher. Versucht ein Client anschließend die Verbindung zu einer so ermittelten IP-Adresse aufzubauen, kann diese - je nach Konfiguration - blockiert oder erlaubt werden.

Das „mitlesen“ Der DNS-Anfragen ist nur bei unverschlüsseltem DNS möglich. Verwendet der Client verschlüsselte Verfahren wie z. B. DoT (DNS-over-TLS) oder DoH (DNS-over-HTTPS), können die DNS-Anfragen nicht inspiziert werden. In diesem Fall kann es sich anbieten, diese DNS-Verfahren ebenfalls mittels der Firewall zu blockieren. Für DoT kann eine Sperre erfolgen, indem der dafür verwendete Port 853 gesperrt wird. DoH verwendet den regulären HTTPS-Port 443 und kann daher nicht generell blockiert werden;

allerdings erfolgt die Auflösung der DoH-Server in der Regel initial über reguläres DNS, so dass populäre DoH-Server-Domains unter Angabe ihres Namens mit der Firewall blockiert werden können.

Eine lückenlose Blockade von DoH ist prinzipbedingt nicht möglich; steht im Vordergrund, dass jeglicher unkontrollierter Traffic unterbunden werden muss, empfiehlt sich daher eine Deny-All-Strategie zu konfigurieren und erlaubte Dienste explizit freizuschalten.

Beim Roaming eines Client zwischen APs stellen die Applikationen des Clients normalerweise nicht als Reaktion darauf neue DNS-Anfragen. Dies erfolgt i.d.R. erst nach Ablauf der TTL (time-to-live). Die Firewall des AP, auf den geroamt wird, kann also keine DNS-Anfragen analysieren und die aufgelösten IP-Adressen lernen und daher den Datenverkehr des Clients eigentlich nicht blockieren.Um dies trotzdem zu ermöglichen, wird der DNS-Cache der Firewall zwischen APs, welche mit der oder den selben SSIDs konfiguriert sind, via IAPP übertragen und synchron gehalten. Dadurch erzeugen alle zusammengehörigen APs des Netzwerks das selbe effektive Firewall-Regelwerk und können den Datenverkehr basierend auf den IP-Adressen filtern, die ein beliebiger AP im Netzwerk aus den DNS-Anfragen des Clients ermittelt hat. Der aktuelle DNS-Cache lässt sich auf dem AP mittels des CLI-Befehls `ls /Status/DNS/Snooping-Results` einsehen.

Beachten Sie, dass lediglich der (flüchtige) DNS Cache synchronisiert wird. Die Konfiguration des AP, bestehend aus Host-Gruppen und Filter-Regeln, wird nicht synchronisiert und muss separat für alle APs identisch gehalten werden.

Pfad Konsole:

Setup

2.47.1 Rules

Konfigurieren Sie hier die Firewall-Regeln.

Pfad Konsole:

Setup > **Firewall**

2.47.1.1 Enabled

Hier wird gesteuert, ob die Regel für die Firewall aktiv ist.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

No

Regel nicht aktiv.

Yes

Regel aktiv.

2.47.1.2 Priority

Priorität der Regel. Regeln mit niedrigeren Werten werden vor Regeln mit höheren Werten verarbeitet.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

2.47.1.3 Network

Das WLAN-Netzwerk, für das die Regel aktiv ist.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.47.1.4 Host-Group

Eine oder mehrere zuvor konfigurierte Host-Gruppen, auf die als Ziel der Regel geprüft wird.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.47.1.5 Protocol

Konfiguriert, ob die Regel nur für TCP, UDP, oder jeglichen Traffic zutrifft.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

Any
TCP
UDP

2.47.1.6 Port

Wird als Protokoll TCP oder UDP eingetragen, kann hier zusätzlich eine Portnummer als Filter-Kriterium hinterlegt werden.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

0 … 65535

2.47.1.7 Action

Konfiguriert, ob bei Zutreffen der Regel die Verbindung erlaubt oder verworfen wird.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

Accept
Drop

2.47.1.99 Comment

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

2.47.2 Host-Groups

Konfigurieren Sie hier Hostnamen oder IP-Adressen, die später in den Firewall-Regeln verwendet werden.

Pfad Konsole:

Setup > **Firewall**

2.47.2.1 Name

Name der Gruppe.

Pfad Konsole:

Setup > **Firewall** > **Host-Groups**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.47.2.2 Hostnames

Ein oder mehrere IP-Adressen oder Hostnamen, kommasepariert. Es kann das Wildcard-Zeichen * für beliebige Zeichen an dieser Stelle verwendet werden.

Die Syntax der Wildcard-Ausdrücke ist mit der der App-Definitionen des LCOS kompatibel.

Pfad Konsole:

Setup > **Firewall** > **Host-Groups**

Mögliche Werte:

max. 255 Zeichen aus `comma separated list of IP addresses, networks or hostnames (with wildcards)`

2.47.3 Log-Actions

Wird eine Firewall-Regel durchlaufen, wird dazu ein Eintrag im Syslog erzeugt.

Je nach Datenaufkommen kann hierfür viel CPU-Leistung benötigt werden und sehr viele Syslog-Nachrichten erzeugt werden.

Pfad Konsole:

Setup > **Firewall**

Mögliche Werte:

No

Keinen Eintrag schreiben.

Yes

Eintrag schreiben.

2.59 WLAN-Management

LCOS LX-basierte Access Points können von einem R&S®NC WLAN-Controller (WLC) verwaltet werden. Wie bei LCOS-basierten Access Points kommt hierzu das Protokoll CAPWAP zum Einsatz.

Voraussetzung ist ein R&S®NC WLAN-Controller mit LCOS-Version 10.40 oder höher.

Im Auslieferungszustand suchen LCOS LX-basierte Access Points im lokalen Netzwerk nach einem WLAN-Controller. Ebenso wird unter dem DNS-Namen „WLC-Address“ versucht, einen WLAN-Controller zu erreichen.

Wurde der Access Point in die Verwaltung durch einen WLC aufgenommen, wird dieser Access Point nicht weiter versuchen, die R&S®LANCOM Management Cloud zu kontaktieren.

Auf diese Weise ist eine Zero-Touch-Inbetriebnahme möglich, bei der keine weitere Konfiguration des Access Points notwendig ist. In besonderen Fällen kann es dennoch erforderlich sein, eine manuelle Konfiguration vorzunehmen. Dies ist in der Gerätekonfiguration hier möglich.

Pfad Konsole:

Setup

2.59.1 Static-WLC-Configuration

Konfiguriert benutzerdefinierte WLAN-Controller. Dies kann notwendig sein, wenn ein WLC nicht über das lokale Netzwerk (z. B. bei gerouteten Verbindungen) gefunden wird und auch der DNS-Name „WLC-Address“ nicht verwendet werden kann, um dem Access Point die Adresse des WLCs mitzuteilen.

Pfad Konsole:

Setup > **WLAN-Management**

2.59.1.1 IP-Address

Geben Sie die IP-Adresse oder den DNS-Namen eines WLAN-Controllers an.

Pfad Konsole:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Mögliche Werte:

max. 44 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.59.1.2 Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen.

Pfad Konsole:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Mögliche Werte:

0 … 65535

Default-Wert:

1027

2.59.2 Operating

Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.

Für den Stand-Alone-Betrieb empfiehlt es sich, diese Option abzuschalten.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

No

Die Suche nach einem WLC ist ausgeschaltet.

Yes

Es wird aktiv nach einem WLC gesucht.

Default-Wert:

Yes

2.59.3 Update-Cert-Before

Konfiguriert, wie viele Tage vor dem Ablaufdatum das Gerätezertifikat erneuert wird, mit dem sich der Access Point am WLC authentifiziert.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

30

2.59.4 Capwap-Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen. Der Standardwert von 1027 ist der Standardport des CAPWAP-Protokolls. R&S®NC WLCs verwenden standardmäßig ebenfalls diesen Port.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

0 … 65535

Default-Wert:

1027

2.60 Power

In diesem Menü finden Sie Einstellungen zum Power-Management.

Pfad Konsole:

Setup

2.60 Dual-PoE-Mode

Stellen Sie hier den Betriebsmodus des Access Points ein, wenn dieser Dual PoE unterstützt. Bei Dual PoE können beide Ethernet-Ports als PoE-Eingang verwendet werden.

Pfad Konsole:

Setup > **Power**

Mögliche Werte:

Hitless-Failover

Ermöglicht den unterbrechungsfreien Weiterbetrieb des Access Point in dem Fall, dass an einem von beiden Ethernet-Ports die PoE-Versorgung wegfällt. Der Access Point wird nicht neu starten. Für diesen Modus ist es erforderlich, dass an beiden Ethernet-Ports dieselbe PoE-Leistung bereitgestellt wird.

Im Falle des R&S®NC LX-7500 ist für einen uneingeschränkten Betrieb IEEE 802.3bt (Klasse 6 / 51W) erforderlich.

Load-Balancing

Der Access Point bezieht seine Leistung gleichzeitig via PoE aus beiden Ethernet-Ports. In der Regel ist die aus beiden Ports bezogene Leistung ähnlich hoch, dies wird allerdings letztendlich von der anliegenden Spannung beeinflusst und ist daher von Switch / PoE-Injektor und / oder Verkabelung abhängig.

Dies ermöglicht den uneingeschränkten Betrieb des R&S®NC LX-7500 mit 2x IEEE 802.3at (Klasse 4 / 25,5W).

2.61 L2TP

LCOS LX unterstützt das Layer 2 Tunneling Protocol (L2TP) in Version 3. Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden.

Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Datentypen

L2TP verwendet zwei Typen von Daten:

Steuerdaten

Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

Nutzdaten

Die Nutzdaten kapseln die Ethernet-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

Pfad Konsole:

Setup

2.61.1 Endpoints

In dieser Tabelle werden die grundsätzlichen Einstellungen zur Konfiguration eines L2TP-Tunnels vorgenommen.

Sollen RAS-Verbindungen ohne Konfiguration in einem Gerät über RADIUS authentifiziert werden, muss in dieser Tabelle ein Default-Eintrag mit folgenden Werten angelegt werden:

- **Tunnel-Id**: DEFAULT
- **Auth-Peer**: Yes
- **Hide**: No

Alle anderen Werte müssen leer bleiben. Wird **Auth-Peer** im DEFAULT-Eintrag auf „No“ gesetzt, werden alle Hosts ungeprüft angenommen und nur die PPP-Sessions authentifiziert.

Pfad Konsole:

Setup > **L2TP**

2.61.1.1 Tunnel-Id

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

2.61.1.2 IP-Address

Die IP-Adresse des Tunnel-Endpunkts. Anstelle einer IP-Adresse (IPv4 oder IPv6) kann auch ein FQDN angegeben werden.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

2.61.1.3 Port

Der zu nutzende UDP-Port.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

0 … 65535

Default-Wert:

1701

2.61.1.4 Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge **Tunnel-Id** und **Hostname** überkreuz übereinstimmen.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.]*``

2.61.1.5 Password

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.]*``

2.61.1.6 Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

No

Gegenstelle muss nicht authentifiziert werden.

Yes

Gegenstelle muss authentifiziert werden.

Default-Wert:

No

2.61.1.7 Hide

Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

No

Tunnelaushandlung wird nicht verschleiert.

Yes

Tunnelaushandlung wird verschleiert.

Default-Wert:

No

2.61.1.8 Operating

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

Pfad Konsole:

Setup > **L2TP** > **Endpoints**

Mögliche Werte:

Nein

L2TP-Endpunkt ist inaktiv.

Ja

L2TP-Endpunkt ist aktiv.

Default-Wert:

Ja

2.61.2 Ethernet

In dieser Tabelle verknüpfen Sie L2TPv3-Endpunkte mit einem WLAN-Netzwerk.

Pfad Konsole:

Setup > **L2TP**

2.61.2.1 L2TP-Endpoint

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts (*2.61.1.1 Tunnel-Id*). Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen“. Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

2.61.2.2 Remote-End

Konfigurieren Sie hier den Namen, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet werden soll. Je Ethernet-Tunnel muss dieser Name also auf aufbauender und annehmender Seite gleich lauten.

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.]*`

2.61.2.3 Interface-Name

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16
16 virtuelle L2TP-Ethernet-Schnittstellen

2.61.2.4 MTU

Diese Einstellung passt die MTU eines L2TP-Ethernet-Tunnels auf den angegebenen Wert an, z. B. bei Verbindung des Tunnels über Netzwerke mit kleinerer MTU hinweg.

Pfad Konsole:

Setup > **L2TP** > **Ethernet**

Mögliche Werte:

68 … 1500

Default-Wert:

1500

2.62 LAN

Hier finden Sie die Einstellungen, welche die LAN-Anbindung des Access Points betreffen.

Pfad Konsole:

Setup

2.62.1 LACP

Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von LAN-Ports zu einem virtuellen Link. Physikalische Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

Pfad Konsole:

Setup > **LAN**

2.62.1.1 Name

Dieser Parameter zeigt die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

max. 9 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

BUNDLE-0

2.62.1.2 Operating

Über diesen Parameter aktivieren oder deaktivieren Sie die Schnittstellen-Bündelung.

Wenn Sie die Bündelung aktivieren, fasst das Gerät die gewählten Geräte-Schnittstellen unter einer gemeinsamen logischen Bündel-Schnittstelle zusammen. Im deaktivierten Zustand bleiben die in der dazugehörigen Tabelle ausgewählten Schnittstellen als eigenständige Schnittstellen nutzbar.

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

No
Yes

2.62.1.3 Priority

Tragen Sie hier die LACP-System-Priorität ein.

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

Vielfache von 4096 `max. 6 Zeichen aus[0-9]`

Default-Wert:

65535

2.62.1.4 Distribution-Policy

Zur Verteilung der Netzwerkpakete auf die verschiedenen gebündelten Schnittstellen steht eine Vielzahl von Möglichkeiten bereit. Folgende Merkmale werden jeweils zur Verteilung herangezogen:

layer2

MAC-Adressen

layer2+3

Eine Kombination aus MAC-Adressen und IP-Adressen

layer3+4

IP-Adressen und TCP/UDP-Ports

encap2+3

Wie layer2+3. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

encap3+4

Wie layer3+4. Es wird aber versucht, diese Informationen im Falle von gekapselten Protokollen aus dem inneren Protokoll zu erlangen

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

layer2
layer2+3
layer3+4
encap2+3
encap3+4

Default-Wert:

layer3+4

2.62.1.5 Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt.

Pfad Konsole:

Setup > **LAN** > **LACP**

Mögliche Werte:

max. 16 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default-Wert:

ETH1,ETH2

2.62.2 Ethernet-Ports

Hier sind Einstellungen zu den Ethernet-Schnittstellen zu finden, zum Beispiel die Geschwindigkeit oder die Aktivierung von Energy Efficient Ethernet / IEEE 802.3az.

Pfad Konsole:

Setup > **LAN**

2.62.2.1 Port

Konfigurieren Sie hier den Ethernet-Port, für den diese Einstellungen gelten sollen.

Pfad Konsole:

Setup > **LAN** > **Ethernet-Ports**

Mögliche Werte:

max. 10 Zeichen aus LAN-Port `ETHx|LANx`

2.62.2.2 Advertised-Rates

Konfigurieren Sie hier die angekündigten Raten für diesen Ethernet-Port.

Pfad Konsole:

Setup > **LAN** > **Ethernet-Ports**

Mögliche Werte:

auto
100HDX
100FDX
1000FDX

Default-Wert:

auto

2.62.2.3 Power-Saving

Über diesen Parameter aktivieren oder deaktivieren Sie Energy Efficient Ethernet / IEEE 802.3az für diesen Ethernet-Port.

Pfad Konsole:

Setup > **LAN** > **Ethernet-Ports**

Mögliche Werte:

No
Yes

2.62.3 Spanning-Tree

Dieses Menü enthält die Einstellungen des Spanning-Tree-Protokolls.

Pfad Konsole:

Setup > **LAN**

2.62.3.1 Operating

Hier können Sie die Unterstützung für Spanning-Tree ein- und ausschalten. Bei ausgeschaltetem Spanning-Tree verschickt der Router keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete weiter, anstatt sie selber zu verarbeiten.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

No
Yes

2.62.3.2 Port-Data

In dieser Tabelle kann man weitere Spanning-Tree-Parameter pro Port einstellen.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

2.62.3.2.1 Port-Data

Der Name der LAN-Schnittstelle.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Mögliche Werte:

max. 64 Zeichen aus LAN-Port `ETHx|LANx`

2.62.3.2.2 Priority

Legt die Priorität des Ports fest. Bei mehreren möglichen Netzwerkpfaden mit gleichem Pfadkosten entscheidet die Priorität, welcher Port verwendet wird. Bei Gleichheit der Priorität wird der Port mit der kleineren Nummer ausgewählt.

Aus Gründen der Kompatibilität zu RSTP darf dieser Wert nur in Schritten von 16 verändert werden, da bei RSTP nur die oberen 4 Bit dieses 16-Bit-Wertes genutzt werden. Niedrigere Werte bringen eine höhere Priorität.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Mögliche Werte:

0
16
32
48
64
80
96
112
128
144
160
176
192
208
224
240

Default-Wert:

128

2.62.3.2.3 Edge-Port

Kennzeichnet den Port als Edge-Port, an dem keine weitere Bridge, sondern nur Endgeräte wie Workstations oder Server angeschlossen sind. Edge-Ports wechseln sofort in den Forwarding-Zustand.

Edge-Ports werden weiterhin vom RSTP überwacht. Werden an einem solchen Port BPDU entdeckt, verliert der Port den Status als Edge-Port.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.62.3.2.4 Path-Cost-Override

Mit diesem Parameter wird die Priorität von gleichwertigen Pfaden gesteuert. Der hier eingestellte Wert wird anstelle der berechneten Pfadkosten für die Auswahl verwendet.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree** > **Port-Data**

Mögliche Werte:

0 … 4294967295

Besondere Werte:

0

Dieser Wert schaltet die Pfadkosten-Beeinflussung aus.

2.62.3.3 Bridge-Priority

Legt die Priorität der Bridge im LAN fest. Damit kann man beeinflussen, welche Bridge vom Spanning-Tree-Protokoll bevorzugt zur Root-Bridge gemacht wird.

Aus Gründen der Kompatibilität zu RSTP sollte dieser Wert nur in Schritten von 4096 verändert werden, da bei RSTP die unteren 12 Bit dieses 16-Bit-Wertes für andere Zwecke verwendet werden.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

0
4096
8192
12288
16384
20480
24576
28672
32768
36864
40960
45056
49152
53248
57344
61440

Default-Wert:

32768

2.62.3.4 Protocol-Version

Hier kann das Protokoll gewählt werden. Je nach Wahl wird entweder das Classic- oder das Rapid-Protokoll verwendet, welches in der IEEE 802.1D-1998 chapter 8 bzw. in der IEEE 802.1D-2004 chapter 17 definiert ist.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

Classic

Verwendet die Verfahren des klassischen STP zur Bestimmung der Netzwerktopologie.

Rapid

Verwendet die Verfahren des RSTP zur Bestimmung der Netzwerktopologie.

RSTP ist kompatibel zu STP. Wenn Komponenten im Netzwerk verwendet werden, die nur das klassische STP unterstützen, werden auch bei Aktivierung von RSTP die Verfahren von STP verwendet.

2.62.3.5 Forward-Delay

Diese Zeit (in Sekunden) legt fest, wieviel Zeit mindestens vergehen muss, bevor ein Spanning-Tree-Port den Zustand (Listening, Learning, Forwarding) wechseln darf.

Bei Verwendung des RSTP hat die Weiterleitungs-Verzögerung oft keine Auswirkung, da das RSTP selbst über geeignete Mechanismen verfügt, um den schnellen Wechsel in den Forwarding-Zustand auszulösen.

Eine Modifikation dieses Zeitwertes wird nur bei genauer Kenntnis des Spanning-Tree-Protokolls empfohlen. Eine Anpassung kann sinnvoll sein, um Reaktionszeiten auf Topologieveränderungen zu optimieren oder eine stabile Funktion in Netzen mit sehr vielen „Bridge-Hops“ zu erreichen.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

15

2.62.3.6 Hello-Time

Dieser Parameter (in Sekunden) legt fest, in welchen Intervallen ein als Root-Bridge ausgewähltes Gerät Spanning-Tree-Informationen ins LAN schickt.

Eine Modifikation dieses Zeitwertes wird nur bei genauer Kenntnis des Spanning-Tree-Protokolls empfohlen. Eine Anpassung kann sinnvoll sein, um Reaktionszeiten auf Topologieveränderungen zu optimieren oder eine stabile Funktion in Netzen mit sehr vielen „Bridge-Hops“ zu erreichen.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

2

2.62.3.7 Max-Age

Dieser Wert bestimmt die Zeit (in Sekunden), nach der eine Bridge über Spanning-Tree empfangene Nachrichten als „veraltet“ verwirft. Dieser Parameter bestimmt, wie schnell der Spanning-Tree-Algorithmus auf Änderungen z. B. durch ausgefallene Bridges reagiert.

Eine Modifikation dieses Zeitwertes wird nur bei genauer Kenntnis des Spanning-Tree-Protokolls empfohlen. Eine Anpassung kann sinnvoll sein, um Reaktionszeiten auf Topologieveränderungen zu optimieren oder eine stabile Funktion in Netzen mit sehr vielen „Bridge-Hops“ zu erreichen.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

20

2.62.3.8 Transmit-Hold-Count

Anzahl der BPDUs, die bei RSTP gesendet werden dürfen, bevor eine Sekunde Pause eingelegt wird.

Bei Verwendung des klassischen STP hat die Sende-Verzögerung keine Auswirkung.

Pfad Konsole:

Setup > **LAN** > **Spanning-Tree**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

6

2.70 IP-Configuration

Parameter für die IP-Konfiguration des Gerätes.

Pfad Konsole:

Setup

2.70.4 Static-Parameters

Einstellungen rund um die IP- und Netzwerkkonfiguration, die zum Tragen kommen, wenn Sie statische IP-Adressen verwenden möchten.

Sämtliche in dieser Tabelle vorgenommenen Einstellungen kommen nur zum Tragen, wenn Sie für das entsprechende LAN-Interface die IPv4- oder IPv6-Adressquelle **static** gewählt haben. Ansonsten werden alle notwendigen Informationen z. B. via DHCP bezogen, sodass in dieser Tabelle keinerlei Konfiguration notwendig ist.

Pfad Konsole:

Setup > **IP-Configuration**

2.70.4.1 Interface-Name

Tragen Sie hier den Namen des Interface ein, auf das sich die weiteren hier vorgenommenen Einstellungen beziehen sollen.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.70.4.2 IPv4-Gateway

Konfigurieren Sie hier das IPv4-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.3 IPv6-Gateway

Konfigurieren Sie hier das IPv6-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.4.4 Primary-IPv4-DNS

Konfigurieren Sie hier den primären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.5 Secondary-IPv4-DNS

Konfigurieren Sie hier den sekundären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.6 Primary-IPv6-DNS

Konfigurieren Sie hier den primären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.4.7 Secondary-IPv6-DNS

Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.6 LAN-Interfaces

Legen Sie hier grundsätzliche Konfigurationsoptionen rund um die eigenen IP-Einstellungen und den Netzwerkzugriff des Gerätes fest.

Pfad Konsole:

Setup > **IP-Configuration**

2.70.6.1 Interface-Name

Vergeben Sie hier einen sprechenden Namen für das Interface. Dieser Name wird verwendet, um die Interface-Konfiguration in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.70.6.2 Interface-ID

Der interne Bezeichner für das Interface. Dieser kann nicht geändert werden.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

2.70.6.3 VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.70.6.4 IPv4-Address-Source

Wählen Sie hier, woher die IPv4-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

DHCP

Die IP-Adresse wird via DHCP bezogen.

static

Es wird die statisch konfigurierte IP-Adresse für das Interface verwendet.

2.70.6.5 IPv6-Address-Source

Wählen Sie hier, woher die IPv6-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

Router-Advertisement

Die IPv6-Adresse wird aus Router-Advertisements abgeleitet, die vom Gerät auf dem jeweiligen Interface empfangen werden.

Ist im Router-Advertisement das Other- und / oder Managed-Flag gesetzt, werden zusätzliche Konfigurationsoptionen via DHCPv6 bezogen – auch, wenn als Adressquelle **Router-Advertisement** eingestellt ist.

DHCPv6

Die IPv6-Adresse wird per DHCPv6 bezogen.

static

Es wird die statisch konfigurierte IPv6-Adresse für das Interface verwendet.

2.70.6.6 Static-IPv4-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv4-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 19 Zeichen aus `IPv4-Adresse: a.b.c.d/xx`

2.70.6.7 Static-IPv6-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv6-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d/64`

2.70.6.9 Comment

Legen Sie hier einen beliebigen Kommentar zur Interface-Konfiguration ab.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

2.70.8 Untagged-VLAN

Besitzt ein Gerät mehr als einen Ethernet-Port, können die weiteren Ethernet-Ports optional mit einen Untag-VLAN konfiguriert werden. Das Untag-VLAN wird ohne VLAN-Tag auf dem weiteren

LAN-Port verwendet und dient z.B. dazu, weitere Netzwerkgeräte in das Netzwerk einzubinden, die ihrerseits nicht VLAN-fähig sind. Der weitere Ethernet-Port agiert somit als Access-Port. Die Untag-Ports und deren VLAN-TAG werden in dieser Tabelle angegeben.

Pfad Konsole:

Setup > **IP-Configuration**

2.70.8.1 Port

Geben Sie einen Port für Untag-VLAN an.

Pfad Konsole:

Setup > **IP-Configuration** > **Untagged-VLAN**

Mögliche Werte:

ETH1
ETH2
…

2.70.8.2 VLAN

Geben Sie eine VLAN-ID für Untag-VLAN an.

Pfad Konsole:

Setup > **IP-Configuration** > **Untagged-VLAN**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.99 LBS

Die R&S®NC Access Points können als LBS-Client mit einem LBS-Server zusammen arbeiten. Dann melden Sie an den LBS-Server alle verbundenen Clients, sodass der LBS-Server entsprechend diesen Clients ortsbasierte Dienste anbieten kann. Unterstützt wird ab LCOS LX 5.30 eine HTTP-Schnittstelle.

Mittels der HTTP-Schnittstelle können Access Points LBS-Daten direkt an einen frei konfigurierbaren HTTP-Endpunkt senden. Da die Daten im JSON-Format vorliegen, wird eine einfache Verarbeitung auf der Empfängerseite sichergestellt.

Pfad Konsole:

Setup

2.99.1 HTTP-Server

Hier konfigurieren Sie die HTTP-Endpunkte für die LBS-Daten.

Pfad Konsole:

Setup > **LBS**

2.99.1.1 URL

Konfigurieren Sie hier die URL des HTTP-Endpunkts.

Es werden HTTP und HTTPS unterstützt. Bei der Verwendung von HTTPS muss zusätzlich ein CA-Zertifikat zur Überprüfung des Servers auf das Gerät hochgeladen werden. Dies kann über WEBconfig erfolgen.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

max. 251 Zeichen aus `URL mit http oder https`

2.99.1.3 Secret

Das Secret (Schlüssel) wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.99.1.4 Data-Sources

Konfigurieren Sie hier, welche Arten von LBS-Daten gesendet werden sollen. Aktuell ist nur BLE verfügbar.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

BLE

2.99.1.5 BLE-Measurements-Fields

Konfigurieren Sie hier im Detail, welche Messfelder bzw. vom Access Point ermittelten Daten in den Nachrichten an den HTTP-Endpunkt enthalten sein sollen. Es empfiehlt sich, diese auf den tatsächlich benötigten Umfang anzupassen, um das Datenaufkommen gering zu halten.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

None
BLE-Address-Type-Transmit
BLE-Advertising-Data-Transmit
BLE-Name-Transmit
BLE-RSSI-Transmit
BLE-Scan-Response-Data-Transmit

2.99.1.6 Buffering-Timeout

Nachdem die konfigurierte Zeit (in Sekunden) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

Werden sowohl dieser Wert als auch *2.99.1.6 Buffer-Size* auf 0 gesetzt, werden die Nachrichten so rasch wie möglich an den Server gesendet.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bedeutet, dass keine Begrenzung aktiv ist.

2.99.1.6 Buffer-Size

Nachdem die konfigurierte Datenmenge (in Bytes) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

Werden sowohl dieser Wert als auch *2.99.1.6 Buffering-Timeout* auf 0 gesetzt, werden die Nachrichten so rasch wie möglich an den Server gesendet.

Pfad Konsole:

Setup > **LBS** > **HTTP-Server**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0“ bedeutet, dass keine Begrenzung aktiv ist.

2.99.2 Operating

Schalten Sie das BLE-Radio hier ein, damit fortlaufend Daten über die BLE-Umgebung erhoben werden.

Pfad Konsole:

Setup > **LBS**

Mögliche Werte:

No

BLE-Radio ausgeschaltet.

Yes

BLE-Radio eingeschaltet.

Default-Wert:

No

2.99.3 LBS-Server-Type

Konfigurieren Sie hier den LBS-Server-Typ. Aktuell wird nur die HTTP-API mit Datenpaketen im JSON-Format unterstützt.

Pfad Konsole:

Setup > **LBS**

Mögliche Werte:

HTTP-JSON

2.99.4 BLE-Scan-Type

Wählen Sie hier zwischen einem passiven und aktiven Scan. Der BLE-Name sowie eine Scan-Response kann nur im aktiven Scan erhoben werden. Beachten Sie, dass BLE-Clients ggf. durch das Beantworten der Scan-Anfragen erhöhten Stromverbrauch zeigen können.

Pfad Konsole:

Setup > **LBS**

Mögliche Werte:

Passive
Active

2.99.5 Run-Bluetooth-Scan

Mit dieser Aktion können Sie einen Bluetooth-Scan ausführen.

Beispiel: `do Run-Bluetooth-Scan`

Pfad Konsole:

Setup > **LBS**

2.99.6 Delete-CA-Certificate

Mit dieser Aktion können Sie das für die Kommunikation mit einem HTTPS-Server verwendete Zertifikat löschen.

Beispiel: `do Delete-CA-Certificate`

Pfad Konsole:

Setup > **LBS**

2.99.7 Delete-Scan-Results

Mit dieser Aktion können Sie die Werte des letzten Bluetooth-Scans löschen.

Beispiel: `do Delete-Scan-Results`

Pfad Konsole:

Setup > **LBS**

2.102 LMC

Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die R&S®LANCOM Management Cloud (LMC).

Pfad Konsole:

Setup

2.102.1 Operating

Legen Sie fest, ob das Gerät über die LMC verwaltet werden soll.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Das Gerät stellt keine Verbindung zur LMC her.

Yes

Das Gerät wird von der LMC verwaltet.

Default-Wert:

Yes

2.102.2 Proxy

Soll die Verbindung vom Gerät zur LMC über einen HTTP-Proxy-Server aufgenommen werden, kann dieser hier konfiguriert werden. Sobald eine Proxy-URL eingetragen ist, wird die LMC-Verbindung immer über den Proxy-Server aufgenommen.

Ist zusätzlich der Schalter *2.102.2.4 Tunnel* aktiviert, wird eine transparenter Tunnel über den Proxy-Server mittels der HTTP CONNECT-Methode verwendet. Der Proxy-Server muss dies unterstützen. Ist der Schalter nicht aktiviert, werden einzelne HTTP-Requests über den Proxy weitergeleitet.

Pfad Konsole:

Setup > **LMC**

2.102.2.1 URL

Soll die Verbindung vom Gerät zur LMC über einen HTTP-Proxy-Server aufgenommen werden, kann dieser hier konfiguriert werden. Sobald eine Proxy-URL eingetragen ist, wird die LMC-Verbindung immer über den Proxy-Server aufgenommen.

Pfad Konsole:

Setup > **LMC** > **Proxy**

Mögliche Werte:

max. 256 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

2.102.2.2 Username

Benutzername zur Verwendung mit einem HTTP-Proxy-Server.

Pfad Konsole:

Setup > **LMC** > **Proxy**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.102.2.3 Password

Passwort für den Benutzer zur Verwendung mit einem HTTP-Proxy-Server.

Pfad Konsole:

Setup > **LMC** > **Proxy**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

2.102.2.4 Tunnel

Falls eine Proxy-URL angegeben wurde und dieser Schalter aktiviert wird, dann wird ein transparenter Tunnel über den Proxy-Server mittels der HTTP CONNECT-Methode verwendet. Der Proxy-Server muss dies unterstützen. Ist der Schalter nicht aktiviert, werden einzelne HTTP-Requests über den Proxy weitergeleitet.

Pfad Konsole:

Setup > **LMC** > **Proxy**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.102.7 Delete-Certificate

Mit dieser Aktion löschen Sie das LMC-Zertifikat.

Pfad Konsole:

Setup > **LMC**

Mögliche Argumente:

keine

2.102.8 DHCP-Client-Auto-Renew

Mit diesem Parameter legen Sie das Verhalten des Gerätes fest, wenn sich die DHCP-Einstellungen des Netzes ändern und der LMC-Client keine Verbindung zur LMC aufbauen kann.

Kann der LMC-Client die konfigurierte LMC nicht erreichen, hat sich wahrscheinlich der IP-Adressbereich des Netzes geändert. Geräte, die als DHCP-Client konfiguriert sind, behalten jedoch die zuvor zugewiesene IP-Adresse, bis deren DHCP-Lease-Time abgelaufen ist. Durch Aktivieren dieses Parameters fordert das Gerät unabhängig von der verbleibenden DHCP-Lease-Time die DHCP-Adresse erneut an (DHCP-Renew).

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies keinen DHCP-Renew aus.

Yes

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies einen DHCP-Renew aus. Ist das DHCP-Renew nicht erfolgreich, wird der DHCP-Prozess komplett neu angestoßen. Das Gerät versucht dann, eine IP-Adresse von einem beliebigen DHCP-Server zu erhalten, um die Verbindung zur LMC wiederherzustellen.

Default-Wert:

No

2.102.13 Configuration-Via-DHCP

Legen Sie fest, ob die LMC-Domain von einem DHCP-Server bezogen werden soll.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Die LMC-Domain wird nicht von einem DHCP-Server bezogen. Es wird der im Feld **LMC-Domain** konfigurierte Wert genommen.

Yes

Die LMC-Domain wird von einem DHCP-Server bezogen.



Um die LMC-Domain von einem DHCP-Server bereitzustellen, konfigurieren Sie am DHCP-Server innerhalb der DHCP-Option 43 die Sub-Option 18 mit

der LMC-Domain. Weitere Informationen zur Konfiguration der LMC Parameter finden Sie im LCOS-Referenzhandbuch im Abschnitt „Auslieferung der LMC-Domain durch den LCOS-DHCP-Server“.

Default-Wert:

No

2.102.15 LMC-Domain

Geben Sie hier den Domain-Namen der LMC an. Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der Public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen („Private Cloud“ oder „on premise installation“), tragen Sie bitte die entsprechende LMC-Domain ein.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.16 Rollout-Project-ID

Geben Sie hier die Projekt-ID dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.17 Rollout-Location-ID

Geben Sie hier den Standort dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.18 Rollout-Device-Role

Geben Sie hier die Rolle dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.102.200 Pairing-Token

Geben Sie hier den Aktivierungscode an, den Sie zum Koppeln mit der LMC erzeugt haben.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 36 Zeichen aus `^[1-9A-NP-Z-]{24,47}$|^$|^\*$|^-$`

2.107 Automatic-Firmware-Update

Der R&S®NC Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen R&S®NC Geräten ohne weiteren Benutzereingriff (unattended). R&S®NC Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Der R&S®NC Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den R&S®NC Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im R&S®NC Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle R&S®NC Geräte signiert. Der R&S®NC Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

Pfad Konsole:

Setup

2.107.1 Mode

Stellen Sie hier den Betriebsmodus des R&S®NC Auto Updaters ein.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

manual

Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.

Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check

Der Auto Updater prüft regelmäßig beim R&S®NC Update-Server auf neue Updates. Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS LX-Menübaum und via Syslog signalisiert. Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check-and-update

Der Auto Updater prüft regelmäßig beim R&S®NC Update-Server auf neue Updates. Der Update-Server ermittelt anhand der Versions-Policy das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater. Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

Default-Wert:

check-and-update

2.107.2 Check-Firmware-Now

Dieser Befehl veranlasst das Gerät, zu prüfen, ob auf dem R&S®NC Update-Server eine neuere Firmware vorhanden ist.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.3 Update-Firmware-Now

Dieser Befehl veranlasst das Gerät, die neueste Firmware vom R&S®NC Update-Server herunterzuladen und zu installieren.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.4 Cancel-Current-Action

Dieser Befehl veranlasst das Gerät, die aktuelle laufende Aktion des Auto Updaters abzubrechen. Dies bezieht sich sowohl auf manuell gestartete als auch auf geplant ausgeführte Aktionen.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.5 Reset-Updater-Config

Dieser Befehl setzt die auf den Auto Updater bezogenen bootpersistenten Konfigurationsdateien zurück. Dies schließt die lokale Blacklist ein, die Firmware-Versionen enthält, mit denen ein automatisches Update fehlgeschlagen ist.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.6 Base-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

max. 252 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default-Wert:

https://update.lancom-systems.de

2.107.7 Check-Interval

Der Auto Updater bestimmmt beim ersten Start einen zufälligen Zeitraum innerhalb eines Tages oder einer Woche, an dem die Prüfung durchgeführt wird. Das eigentliche Update soll dann im nächsten Zeitraum zwischen 2-4 Uhr (Voreinstellung) durchgeführt werden.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

daily
weekly

Default-Wert:

daily

2.107.8 Version-Policy

Stellen Sie hier die Versionsrichtlinie des R&S®NC Auto Updaters ein. Diese steuert, welche Firmware-Versionen einem Gerät zum Update angeboten werden.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

latest

Releaseübergreifend immer die neueste Version. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber auch auf 5.00 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

current

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber nicht auf 5.00 Rel.

security-updates-only

Innerhalb eines Releases das neueste SU. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 SU1 aktualisiert, aber nicht auf 4.00 RU2.

latest-without-REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 4.00 ist installiert; es wird auf 5.00 RU1 aktualisiert, aber nicht auf 5.00 REL.

Default-Wert:

security-updates-only

2.107.10 Check-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

2.107.11 Check-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

2.107.12 Install-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

2

2.107.13 Install-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

4

2.111 IoT

Einstellungen für vom LCOS LX unterstützte IoT-Technologien wie z. B. Wireless ePaper und Bluetooth Low Energy.

Pfad Konsole:

Setup

2.111.1 USB

Konfigurieren Sie hier die Einstellungen für den USB-Ethernet-Support.

Pfad Konsole:

Setup > **IoT**

2.111.1.1 CDC-EEM-Support

Konfigurieren Sie hier die Einstellungen des Protokolls CDC-EEM für den USB-Ethernet-Support.

Pfad Konsole:

Setup > **IoT** > **USB**

2.111.1.1.1 Operating

Schalten Sie den USB-Ethernet-Support hier ein oder aus.

Pfad Konsole:

Setup > **IoT** > **USB** > **CDC-EEM-Support**

Mögliche Werte:

No
USB-Ethernet-Support ausgeschaltet.

Yes
USB-Ethernet-Support eingeschaltet.

Default-Wert:

No

2.111.1.1.2 VLAN-ID

Optionale Angabe einer VLAN-ID.

Pfad Konsole:

Setup > **IoT** > **USB** > **CDC-EEM-Support**

Mögliche Werte:

0 … 4095

2.111.88 Wireless-ePaper

Konfigurieren Sie hier die Einstellungen für das Wireless ePaper-Modul.

Pfad Konsole:

Setup > **IoT**

2.111.88.1 Operating

Aktivieren Sie hiermit die Wireless ePaper Funktion des Access Point.

Der Server muss für den Verbindungstyp ThinAP2.0/TCP konfiguriert sein. Weitere Informationen finden Sie in der *R&S®NC Support Knowledge Base*. Der Legacy-Verbindungsmodus via UDP wird von LCOS LX nicht unterstützt.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

No

Die Wireless ePaper Funktion ist nicht aktiviert.

Yes

Die Wireless ePaper Funktion ist aktiviert.

Default-Wert:

No

2.111.88.2 Channel

Konfigurieren Sie den Funkkanal, der für die Ansteuerung der Wireless ePaper Displays verwendet werden soll.

Je nach verwendetem Funkkanal kann die Serververbindung eines Displays bis zu 30 Minuten (Kanäle 3, 5, 8, 9, 10) oder bis zu 120 Minuten (Kanäle 0, 1, 2, 4, 6, 7) dauern. Wählen Sie daher bevorzugt aus Kanäle 3, 5, 8, 9, 10, da diese häufiger von den Wireless ePaper Displays gescannt werden und es keine Interferenzen mit den häufig verwendeten WLAN-Kanälen 1, 6 und 11 gibt.

Wählen Sie nicht für zwei Access Points in einem Bereich denselben Kanal aus. Dies verursacht Interferenzen und hindert Displays daran, dem Netzwerk beizutreten. Derselbe Kanal darf nur auf zwei Access Points eingerichtet werden, wenn sichergestellt ist, dass sich jedes Display nur in Reichweite eines dieser Access Points befindet.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz

Default-Wert:

2404MHz

2.111.88.3 Server-Address

IP-Adresse des Wireless ePaper Servers.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9].-:%`

2.111.88.4 Server-Port

Der TCP-Zielport, welcher für die Kommunikation zum Server verwendet werden soll.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

0 … 65535

Default-Wert:

7354

2.111.88.5 Protocol

Das für die Kommunikation zum Server verwendete Protokoll.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

ThinAP2.0/TLS

Default-Wert:

ThinAP2.0/TLS

2.111.88.6 Server-Authentication

Optional kann der Access Point bei der Verbindungsaufnahme mit dem Wireless-ePaper-Server dessen Server-Zertifikat überprüfen. Wird diese Option aktiviert, ist zusätzlich ein entsprechendes CA-Zertifikat (bzw. Zertifikatskette) im PEM-Format über die WEBconfig auf den Access Point zu laden.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.111.88.7 Server-Hostname-Verification

In Zusammenhang mit der Option *2.111.88.6 Server-Authentication* steuert diese Einstellung, ob überprüft wird, dass der im Zertifikat angegebene „Common Name“ mit dem Hostnamen des angesprochenen Wireless ePaper Servers übereinstimmt.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.111.88.10 Use-Separate-IP-Interface

Mit dieser Funktion lässt sich eine separate IP / VLAN-Schnittstelle für den Wireless-ePaper-Client des Access Point festlegen. So kann die Verbindung zum ePaper-Server oder der Vusion Cloud über ein separates Interface, statt über die standardmäßige Management-IP / VLAN-Schnittstelle, aufgebaut werden.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

Mögliche Werte:

No

Die separate IP-Schnittstelle für Wireless ePaper ist nicht aktiviert.

Yes

Die separate IP-Schnittstelle für Wireless ePaper ist aktiviert. Konfigurieren Sie diese unter *2.111.88.20 IP-Interface* und *2.111.88.30 Static-IP-Parameters*.

Default-Wert:

No

2.111.88.20 IP-Interface

Konfigurieren Sie hier das separate IP-Interface für die Verbindung zum ePaper-Server oder der Vusion Cloud.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.20.1 Interface-Name

Das Interface ist hier immer „Wireless-ePaper“. Auf dieses beziehen sich die weiteren hier vorgenommenen Einstellungen.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET|Wireless-ePaper`

Default-Wert:

Wireless-ePaper

2.111.88.20.2 Interface-ID

Der interne Bezeichner für das Interface. Dieser kann nicht geändert werden.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

max. 16 Zeichen aus `br-lan|epaper`

Default-Wert:

ePaper

2.111.88.20.3 VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

2 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.111.88.20.4 IPv4-Address-Source

Wählen Sie hier, woher die IPv4-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

DHCP

Die IP-Adresse wird via DHCP bezogen.

static

Es wird die statisch konfigurierte IP-Adresse für das Interface verwendet.

2.111.88.20.5 IPv6-Address-Source

Wählen Sie hier, woher die IPv6-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

Router-Advertisement

Die IPv6-Adresse wird aus Router-Advertisements abgeleitet, die vom Gerät auf dem jeweiligen Interface empfangen werden.

Ist im Router-Advertisement das Other- und / oder Managed-Flag gesetzt, werden zusätzliche Konfigurationsoptionen via DHCPv6 bezogen – auch, wenn als Adressquelle **Router-Advertisement** eingestellt ist.

DHCPv6

Die IPv6-Adresse wird per DHCPv6 bezogen.

static

Es wird die statisch konfigurierte IPv6-Adresse für das Interface verwendet.

2.111.88.20.6 Static-IPv4-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv4-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

max. 19 Zeichen aus `IPv4-Adresse: a.b.c.d/xx`

2.111.88.20.7 Static-IPv6-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv6-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d/64`

2.111.88.30 Static-IP-Parameters

Konfigurieren Sie hier weitere Einstellungen rund um die IP- und Netzwerkkonfiguration, die zum Tragen kommen, wenn Sie statische IP-Adressen verwenden möchten.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper**

2.111.88.30.1 Interface-Name

Das Interface ist hier immer „Wireless-ePaper“. Auf dieses beziehen sich die weiteren hier vorgenommenen Einstellungen.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET|Wireless-ePaper`

Default-Wert:

Wireless-ePaper

2.111.88.30.2 IPv4-Gateway

Konfigurieren Sie hier das IPv4-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.111.88.30.3 IPv6-Gateway

Konfigurieren Sie hier das IPv6-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.111.88.30.4 Primary-IPv4-DNS

Konfigurieren Sie hier den primären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.111.88.30.5 Secondary-IPv4-DNS

Konfigurieren Sie hier den sekundären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.111.88.30.6 Primary-IPv6-DNS

Konfigurieren Sie hier den primären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.111.88.30.7 Secondary-IPv6-DNS

Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

3 Firmware

In diesem Menü finden Sie die Aktionen und Einstellmöglichkeiten zur Verwaltung der Geräte-Firmware.

Pfad Konsole:

/

3.2 Table-Firmsafe

In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2) und die Angabe des Zustandes (aktiv oder inaktiv).

Pfad Konsole:

Firmware

3.2.1 Position

Position im Speicherbereich für den aktuellen Eintrag.

Pfad Konsole:

Firmware > **Table-Firmsafe**

3.2.2 Status

Status des aktuellen Eintrags.

Pfad Konsole:

Firmware > **Table-Firmsafe**

Mögliche Werte:

active

Diese Firmware wird derzeit vom Gerät verwendet.

inactive

Diese Firmware befindet sich im Wartezustand und kann aktiviert werden.

3.8 Switch-Firmware

Hier schalten Sie via Kommandozeile die aktive Firmware um in den inaktiven Zustand. Entsprechend wird die alternative, nicht aktive Firmware in den aktiven Zustand geschaltet.

Das Gerät startet automatisch neu und verwendet sogleich die alternative Firmware. Durch nochmaliges Umschalten stellen Sie den Ausgangszustand wieder her.

Pfad Konsole:

Firmware

Mögliche Werte:

`do Switch-Firmware`

Firmware umschalten und Gerät neu starten

3.10 Boot-count

Speichert die Anzahl der mit der aktuellen Firmware durchgeführten Neustarts des Gerätes.

Pfad Konsole:

Firmware

4 Other

In diesem Menü finden Sie zusätzliche Funktionen aus dem LCOS LX-Menübaum.

Pfad Konsole:

/

4.1 Reset-Config

Mit dieser Aktion können Sie die Konfiguration zurücksetzen.

Beispiel: `do Reset-Config`

Pfad Konsole:

Other

4.2 Reboot

Mit dieser Aktion starten Sie das Gerät neu.

Beispiel: `do Reboot`

Pfad Konsole:

Other

4.3 Delayed-Reboot

Mit dieser Aktion starten Sie das Gerät verzögert neu. Die Verzögerung wird als Parameter in Sekunden angegeben.

Beispiel: `do Delayed-Reboot 30`

Pfad Konsole:

Other

4.4 Cancel-Delayed-Reboot

Mit dieser Aktion brechen Sie einen mit `do Delayed-Reboot` eingeleiteten verzögerten Neustart innerhalb der Verzögerungszeit ab.

Beispiel: `do Cancel-Delayed-Reboot`

Pfad Konsole:

Other

4.5 Delete-Support-Info

Mit dieser Aktion löschen Sie das persistente Bootlog und nach einem Absturz angelegte Coredumps.

Beispiel: `do Delete-Support-Info`

Pfad Konsole:

Other

1 Status

In diesem Menü finden Sie einige Statusinformationen.

Pfad Konsole:

/

1.62 Syslog

In diesem Menü finden Sie einige Statusinformationen zum Syslog.

Pfad Konsole:

Status

1.62.1 Last-Messages

In dieser Tabelle finden Sie die Nachrichten des Syslog. Beispiel:

```
Id Time           Priority  Message                                                LMC-Message-ID
===-------------------------------------------------------------------------------------------------
0  1786102398625  err       "lxcron[6204]: Service temporarily not available"  5c9f6e94-e39a-...
1  1786102399918  notice    "mcastds: Entering evloopRun"                      4276b3ac-bfc9-...
2  1786102403656  err       "lxcron[7226]: Service temporarily not available"  38b0a6cc-e95b-...
```

Pfad Konsole:

Status > **Syslog**

1.62.1.1 Id

ID einer Syslog-Nachricht.

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

1.62.1.2 Time

Zeitstempel einer Syslog-Nachricht.

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 20 Zeichen aus `[0-9]`

1.62.1.3 Priority

Stufe einer Syslog-Nachricht.

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

1.62.1.4 Message

Text einer Syslog-Nachricht.

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

1.62.1.5 LMC-Message-ID

LMC-Message-ID einer Syslog-Nachricht.

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`