LCOS LX 7.12

Referenzhandbuch

10/2025

LANCOM SYSTEMS

Inhalt

Copyright

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@lancom.de*.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

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

Menüreferenz

Die Menüreferenz 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 LANCOM

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

- **Für höchste Sicherheit Ihrer Netzwerke**

  wird jedes LANCOM 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 LANCOM Lifecycle-Richtlinien für alle LANCOM 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.

2 Bedienung

2.1 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines Gerätes einstellen. LANconfig benötigt einen Konfigurationsrechner mit einem aktuellem Windows-Betriebssystem. Weitere Informationen finden Sie in den Kapiteln *LANconfig – Geräte konfigurieren* auf Seite 7 und *Features über LANconfig konfigurieren* auf Seite 21.
- **WEBconfig** – Weitere Informationen finden Sie in den Kapiteln *WEBconfig – Geräte überwachen und konfigurieren* auf Seite 8 und *Features über WEBconfig konfigurieren* auf Seite 104.
- **Konsole** – alternativ zu LANconfig können Sie auch über SSH eine Konsole auf dem Gerät öffnen und darüber auf das Kommandozeileninterface zugreifen. Über den TCP-Port 22 ist der Zugriff auf das Gerät über ein SSH-Programm wie z. B. PuTTY möglich.
- **LANCOM Management Cloud** – die hyper-integrierte Lösung für die automatisierte Steuerung Ihres Netzwerks.

Die Standard-Zugangsdaten für alle Konfigurationswege lauten:

- Benutzer: root
- Passwort: <Leer> (es ist kein Passwort gesetzt)

Um die Sicherheit zu gewährleisten, werden Sie beim ersten Zugriff über WEBconfig aufgefordert, das Passwort zu ändern.

Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen.

2.1.1 LANconfig – Geräte konfigurieren

Von der komfortablen Inbetriebnahme eines Einzelplatzgerätes mit den einfach zu bedienenden Installationsassistenten bis zum ganzheitlichen Management mit Firmware- und Konfigurationsverteilung größerer Installationen reicht das Anwendungsspektrum von LANconfig.

Basisfunktionen

- Automatisches Erkennen von neuen, unkonfigurierten Geräten
- (Fern-)Konfiguration von Geräten über IP-Adresse, URL oder über die serielle Schnittstelle
- Integration von Telnet-, SSH-, HTTPS- und TFTP-Konfiguration
- Kontext-basiertes Hilfesystem zu den Konfigurations-Parametern
- In allen Installationsschritten bieten die Assistenten angepasste Eingabemasken
- Einrichtung von Backup-Verbindungen

Management von größeren Installationen

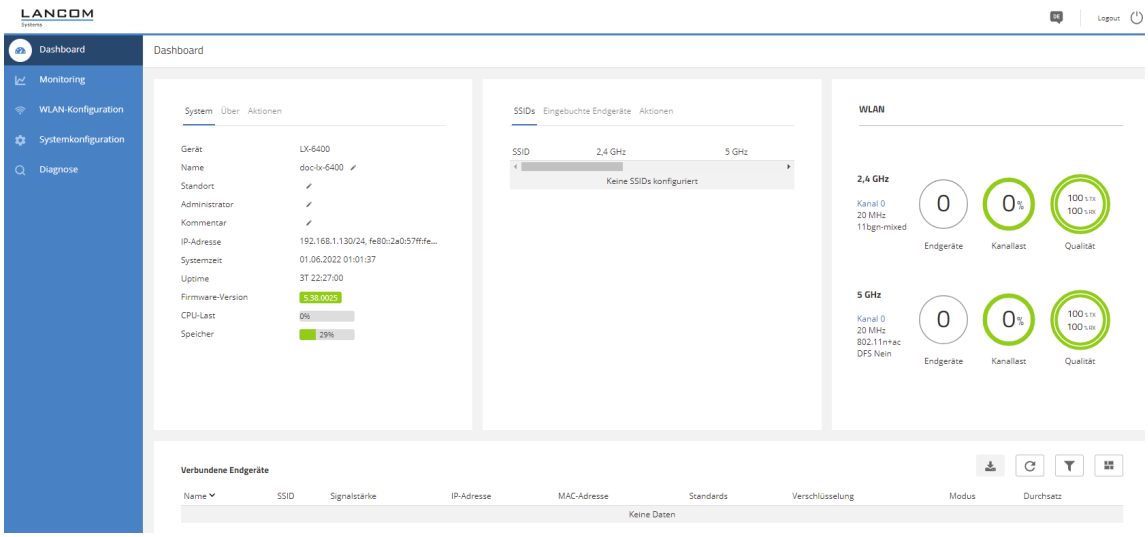
- Gruppenbildung
- Zentrale Firmware-Verteilung
- Simultankonfiguration mehrerer Geräte
- Verteilen von Konfigurations-Scripten
- WLAN-Gruppenkonfiguration
- Logging aller Aktionen
- Erstellung von neuen „Offline"-Konfigurationen für alle Geräte und sowohl LCOS als auch LCOS LX-Versionen

2.1.2 WEBconfig – Geräte überwachen und konfigurieren

Mittels WEBconfig konfigurieren Sie Einzelgeräte oder überwachen diese im laufenden Betrieb. Sie erreichen die WEBconfig über HTTP und HTTPS. Im Falle von HTTP erfolgt automatisch eine Umleitung auf eine verschlüsselte HTTPS-Verbindung.

Da die WEBconfig mit einem selbst-signierten SSL-Zertifikat arbeitet, muss dieses einmalig (pro Gerät) im Browser als Ausnahme hinzugefügt werden.

Im Folgenden eine Übersicht über die wesentlichen Bestandteile der WEBconfig, die Sie jeweils im linken Bereich in der **Sidebar** auswählen können.



Dashboard

Über das Dashboard werden Ihnen Statusinformationen des Gerätes im laufenden Betrieb angezeigt.

- System – grundsätzliche Informationen zum Gerät, z. B. der Gerätename und die Firmware-Version.
- WLAN – Informationen zur Auslastung der vom Gerät betriebenen WLAN-Kanäle.
- Verbundene Stationen – zeigt alle aktuell mit dem Gerät verbundenen WLAN-Stationen.
- Nachbarschaft – Überblick über die WLAN-Umgebung, insbesondere die in der Umgebung aktiven WLAN Access Points und WLAN-Router.
- Monitoring – Graphen zur zeitlichen Visualisierung des WLAN-Durchsatzes, des LAN-Durchsatzes, der Anzahl der WLAN-Stationen sowie der Kanalauslastung.

Konfiguration

- Systemkonfiguration – Konfiguration grundsätzlicher Parameter Ihres Gerätes, z. B. den Gerätenamen oder die IP-Einstellungen zum Management des Gerätes.

› WLAN – Die WLAN-Konfiguration wurde mit dem Ziel entworfen, den Nutzer für die am häufigsten verwendeten Konfigurationsarbeiten zu unterstützen und die mühevolle Konfiguration kleiner Details unnötig zu machen. Gleichzeitig ist aber weiterhin die Konfiguration davon abweichender Szenarien möglich.

Logs

In diesem Bereich wird das Syslog des Gerätes ausgegeben.

2.1.3 Konsole – Befehlsübersicht

Das Kommandozeilen-Interface wird mit den folgenden Befehlen bedient. Eine Übersicht der möglichen Konfigurationsparameter und Aktionen finden Sie in der LCOS LX-Menüreferenz.

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.
`history`	Zeigt eine Liste der letzen ausgeführten Befehle.

Befehl	Beschreibung
`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. **`-t <Hardware-Type>`** Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein. **`-v <VLAN-ID>`** Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID

Befehl	Beschreibung
	angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet. 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`.
`ls [<Path>]`	Zeigt den Inhalt des aktuellen Verzeichnisses oder des angegebenen Pfades an.
`passwd <Password>`	Ändert das Passwort des aktuellen Benutzerkontos.

Befehl	Beschreibung
`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 LANCOM Management Cloud einen Aktivierungscode erzeugt haben, können Sie dieses Gerät über diesen Code mit der 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. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Diagnose* auf Seite 150.
`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.

3 Feature-Beschreibungen

Im Folgenden finden Sie Beschreibungen zu einigen ausgewählten WLAN-Features.

3.1 WLC Layer-3-Tunnel

Beim Layer-3-Tunneling handelt es sich um eine erweiterte Nutzung des CAPWAP-Protokolls (Control and Provisioning of Wireless Access Points), welches von WLAN-Controllern (WLC) zum Management von WLAN Access Points genutzt wird. Es ermöglicht, die Daten des WLANs zentral über den WLAN-Controller in das LAN einzuspeisen, indem es einen direkten Datentunnel zwischen WLAN-Controller und Access Point erstellt. Zur Konfiguration ist im logischen Netzwerkprofil des WLC die Einstellung **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)** > **SSID verbinden mit** auf eine der angebotenen WLC-Tunnel-Schnittstellen einzustellen. Der Datenverkehr der jeweiligen SSID wird nun an die jeweilige WLC-Tunnel-Schnittstelle des WLC geleitet. Die WLC-Tunnel-Schnittstelle kann nun für ein ARF-Netz oder in der LAN-Bridge des WLC weiter verwendet werden.

Layer-3-Tunneling ist ideal für Umgebungen, in denen unmanaged Switches eingesetzt werden oder keine weitergehende VLAN-Konfiguration der Switches möglich ist. So können Datentunnel ganz einfach und mit extrem geringem Zeitaufwand aufgebaut werden, ohne, dass eine VLAN-Infrastruktur zwischen WLAN-Controller und Access Point benötigt wird, um den Datenverkehr einzelner SSIDs voneinander zu isolieren. Eine VLAN-Infrastruktur wird erst beim Übergang vom WLAN-Controller in die lokalen Netzwerke benötigt, da die Daten der einzelnen SSIDs im Layer-3-Tunnel zwischen Access Point und WLAN-Controller transportiert werden. Alternativ kann der WLAN-Controller in seiner Funktion als Router die über den Tunnel angelieferten Daten auch in andere IP-Netze oder auch in das Internet routen.

Die Nutzung dieser Funktion erfordert seitens der LANCOM WLAN-Controller die Betriebssystem-Version LCOS 10.42 RU3 oder höher.

3.2 Band Steering

Der Standard IEEE 802.11 enthält kaum Kriterien, nach denen ein WLAN-Client den Access Point für eine Verbindung auswählen sollte. Zwar gibt es allgemeine Richtlinien, wonach z. B. ein Access Point mit höherem RSSI-Wert (d. h. der empfangenen Signalstärke) zu bevorzugen ist. Doch in der Praxis beachten WLAN-Clients weder die oben angesprochenen Definitionen noch die allgemeinen Richtlinien konsequent. Wird eine SSID in sowohl 2,4 GHz als auch 5 GHz ausgestrahlt, besteht im Normalfall keine Möglichkeit auf die Entscheidung des Clients, welches Frequenzband er bevorzugt, Einfluss zu nehmen.

Die gezielte Zuweisung von WLAN-Clients, das sog. „Client Steering", basiert auf dem Prinzip, dass viele Clients die verfügbaren Access Points durch einen aktiven Scan-Vorgang ermitteln. Aktives Scannen bedeutet hier, dass ein Client Test-Anforderungspakete (Probe Requests) versendet, welche die Netzwerkkennung enthalten, zu der ein Client eine Verbindung aufbauen soll. Access Points mit der entsprechenden Kennung versenden daraufhin eine Test-Antwort und ermöglichen es dem Client auf diese Weise, eine Liste mit verfügbaren Access Points zu erstellen. Die Tatsache, dass die weitaus meisten WLAN-Clients sich nur mit solchen Access Points verbinden, von denen sie eine Test-Antwort (Probe Response) erhalten haben, kann zur Steuerung des Auswahlverhaltens (und somit zur gezielten Zuweisung) eingesetzt werden.

Für die gezielte Zuweisung gibt es mehrere, zum Teil sehr fortgeschrittene Kriterien. Eines dieser Kriterien betrifft die verwendeten Funkfrequenzbereiche, in denen Clients kommunizieren. So erwartet man von modernen Dual-Band-WLAN-Clients immer häufiger, dass diese den 5-GHz-Frequenzbereich gegenüber dem inzwischen überfüllten

2,4-GHz-Bereich bevorzugen. Weist man einem WLAN-Client ganz gezielt ein bestimmtes Frequenzband bzw. einen bestimmten Frequenzbereich zu, spricht man von Band Steering.

Die Liste mit den ermittelten (bzw. „gesehenen") Clients enthält alle Clients, von denen der Access Point ein Test-Anforderungspaket empfangen hat. Zusammen mit der Funkfrequenz, auf der der WLAN-Client die Test-Anforderung gesendet hat, bildet diese Liste eine der Entscheidungsgrundlagen für den Access Point, die betreffende Anforderung zu beantworten oder nicht.

Weitere Kriterien für eine solche Entscheidungsfindung hängen mit den gemeldeten Kennungen der Clients und der Konfiguration der Geräte zusammen: So kann es z. B. vorkommen, dass auf dem bevorzugten Frequenzband weniger SSIDs gemeldet werden als auf dem weniger bevorzugten. Ebenso kann eine zu geringe Sendestärke beim Melden der SSIDs dazu führen, dass der Client auf dem bevorzugten Frequenzband keine Test-Antwort erhält. Für den letzteren Fall sollte man sicherstellen, dass der Access Point Test-Antworten auf dem weniger bevorzugten Frequenzband nicht durch den Steuerungsmechanismus unterdrückt.

Sie können das Band-Steering des Access Points im LANconfig unter **Wireless-LAN** > **Client-Management** konfigurieren.

3.3 Fast Roaming

Zusammen mit der Authentifizierung nach dem Standard IEEE 802.1X und dem Schlüsselmanagement nach dem Standard IEEE 802.11i bieten moderne WLAN-Installationen ein hohes Maß an Sicherheit und Vertraulichkeit der übertragenen Daten. Allerdings erfordern diese Standards die Übertragung zusätzlicher Datenpakete während der Verbindungsverhandlung sowie zusätzliche Rechenleistung auf Client- und Serverseite.

IEEE 802.11 benötigte ursprünglich zum Aufbau einer Datenverbindung zwischen WLAN-Client und Accesss Point lediglich bis zu sechs Datenpakete. Die Standard-Erweiterung IEEE 802.11i besserte Schwachstellen bei der WEP-Verschlüsselung aus, verlängerte dabei jedoch den Anmeldeprozess je nach Authentifizierungsmethode um ein Vielfaches.

Diese verlängerte Anmeldezeit des WLAN-Clients am Accesss Point ist für nicht zeitkritische Anwendungen ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem Accesss Point zum nächsten, ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel. Als Beispiel seien hier Voice-over-IP (VoIP) oder die Anwendung in industriellen Echtzeit-Umgebungen genannt. Roaming bedeutet in diesem Zusammenhang, dass die Netzwerkverbindung ohne Abbruch von einem Access Point auf den anderen übergeht.

Methoden wie Pairwise Master Key Caching (PMK Caching), Pre-Authentication, Opportunistic Key Caching (OKC) sowie der Einsatz von zentralen WLAN-Controllern (WLC) zur Schlüsselverwaltung verbessern die Zeit für die Schlüsselaushandlung zwischen WLAN-Client und Accesss Point bei der Anmeldung. Allerdings reicht das immer noch nicht aus, die vergleichsweise lange Zeit für die Schlüsselverhandlung zwischen WLAN-Client und Accesss Point auf ein brauchbares Maß zu begrenzen.

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim Accesss Point zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim Accesss Point. Beim Roaming von einem Accesss Point zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen Accesss Point reservieren. Die dafür notwendigen zusätzlichen Management-Frames erhöhen die Anmeldezeit jedoch wieder deutlich.

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem Accesss Point zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am Access Point wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Wie beim Opportunistic Key Caching (OKC) existiert eine zentrale Schlüssel-Verwaltung, sinnvollerweise in Form eines WLCs, der die angeschlossenen Accesss Points mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der Accesss Point IEEE 802.11r beherrscht.

Die vom WLC verwalteten Accesss Points senden als Kennung das sogenannte „Mobility Domain Information Element (MDIE)" aus, das den WLAN-Clients im Empfangsbereich u. a. mitteilt, welcher „Mobility Group" der Accesss Point

angehört. Anhand dieser Gruppenkennung erkennt der WLAN-Client, ob er derselben Domain angehört und sich somit ohne Verzögerung anmelden kann. Diese Mobility Domain hat der WLAN-Client während der ersten Anmeldung an einem Accesss Point mitgeteilt bekommen.

Die Domain-Kennung sowie spezielle, bei der Erstanmeldung generierte und an alle verwalteten Accesss Points übertragenen Schlüssel verringern die Verhandlungsschritte bei der Neuanmeldung bei einem Accesss Point auf die angestrebten vier bis sechs Schritte.

Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen Accesss Point einen neuen PMK aushandeln. Dieser ist auch auf dem Accesss Point gültig, mit dem sich der WLAN-Client im Anschluss verbinden möchte.

Zusätzlich ermöglicht IEEE 802.11r in Form eines „Resource Requests" die Reservierung von zusätzlicher Bandbreite auf dem neuen Accesss Point, ohne dass weitere Datenpakete wie bei IEEE 802.11e die Anmeldung unnötig verlängern.

Ältere WLAN-Clients haben möglicherweise Probleme damit, eine Verbindung zu einer SSID mit aktiviertem 802.11r aufzubauen. Daher ist hier der Einsatz zweier SSIDs ratsam: eine SSID für ältere Clients ohne 802.11r-Unterstützung und eine weitere SSID mit aktiviertem 802.11r für Clients mit 802.11r-Unterstützung.

Das Fast-Roaming lässt sich in LANconfig einstellen unter **Wireless-LAN** > **Allgemein** > **Verschlüsselung** > **WPA2-Key-Management**.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Fast Roaming über Inter Access Point Protocol (IAPP)

Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. 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. Beim Wechsel eines Clients zu einem anderen Access Point informiert (Handover Request) der übernehmende Access Point den ehemals bedienenden Access Point. Der ehemalige Access Point löscht daraufhin den Client aus seiner Stationstabelle. Im Handover Request ist die MAC-Adresse des Clients enthalten, sodasss im LAN vorhandene Geräte über das neue Routing informiert werden und ihre Zuordnungstabelle aktualisieren können.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **Wireless-LAN** > **Allgemein** > **Verschlüsselung** > **PMK-IAPP-Secret**.

Beachten Sie bitte, dass es für die Verwendung von Fast Roaming über IAPP erforderlich ist, in den Verschlüsselungs-Einstellungen unter WPA2-Key-Management die Option Fast Roaming auszuwählen.

3.4 LANCOM Enhanced Passphrase Security (LEPS)

Mit LANCOM Enhanced Passphrase Security (LEPS) kann eine Menge von Passphrasen konfiguriert werden, die dann den einzelnen Benutzern, Gruppen oder MAC-Adressen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden" will, aber die Geräte nicht selber konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Preshared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Da LEPS ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Die Unsicherheit von globalen Passphrasen wird durch LEPS grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase „verloren geht" oder ein

Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

Zusätzlich zu Passphrasen für Benutzer lassen sich auch MAC-Adressen **individuelle** Passphrasen zuordnen – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt dann die Anmeldung am Access Point.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

Im Vergleich zu LEPS für Benutzer ist der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

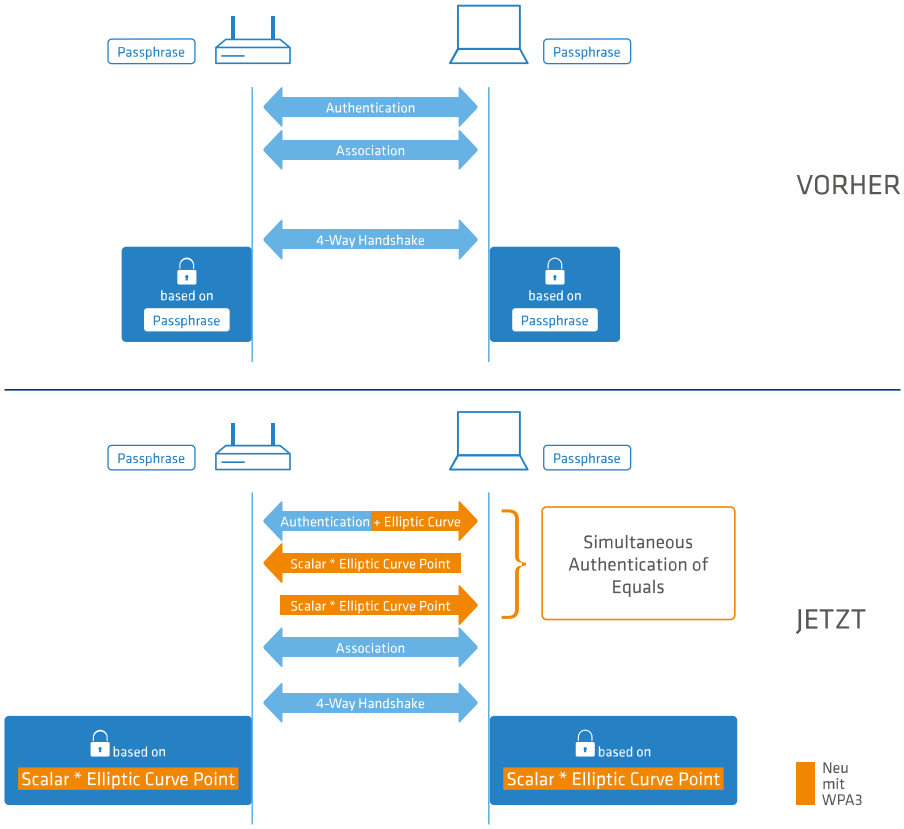
Aus technischen Gründen ist LEPS für Benutzeraccounts, für die eine Passphrase vergeben ist, aber keine MAC-Adresse, nicht mit Fast Roaming kompatibel.

3.5 WPA3 (Wi-Fi Protected Access 3)

Der 2018 eingeführte WPA3-Standard der Wi-Fi-Alliance bietet gegenüber dem bereits 2004 eingeführten Vorgängerstandard WPA2 eine verbesserte Sicherheit durch eine Kombination verschiedener aktueller Sicherheitsverfahren. Wie WPA2 existiert auch WPA3 in den Ausprägungen WPA3-Personal und WPA3-Enterprise.

WPA3-Personal bietet durch die Verwendung des Authentisierungsverfahrens Simultaneous Authentication of Equals (SAE) eine Methode, die lediglich ein Passwort für die Authentifizierung voraussetzt und dennoch Brute-Force- und Wörterbuch-Attacken ins Leere laufen lässt. Zudem bietet dieses Verfahren erstmalig Forward Secrecy – dies bedeutet,

dass in der Vergangenheit mitgeschnittener, WPA3-gesicherter Datenverkehr auch später nicht mehr entschlüsselt werden kann, wenn der Angreifer Kenntnis des Pre-Shared Keys erlangt.



Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA) Suite B-Kryptographie verwendet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

In beiden Varianten ist nun die Verwendung von Protected Management Frames (PMF) nach IEEE 802.11w verpflichtend. PMF verhindern, dass Angreifer durch Deassoziieren mittels gefälschter Management Frames und Belauschen der Wiederanmeldung Material bekommen, um das WLAN-Passwort zu errechnen.

3.5.1 WPA3-Personal

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Personal unterstützen; die Authentisierung wird mit dieser Konfiguration nur noch über Simultaneous Authentication of Equals (SAE) zugelassen. Ebenfalls wird für diese SSID nun die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

3.5.2 WPA3-Enterprise

WPA3-Enterprise ändert oder ersetzt die in WPA2-Enterprise definierten Protokolle nicht grundlegend. Stattdessen definiert es Richtlinien, um eine größere Konsistenz bei der Anwendung dieser Protokolle zu gewährleisten und die gewünschte Sicherheit zu gewährleisten.

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Enterprise unterstützen. Für diese SSID wird die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

Suite B-Kryptographie

Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA)-Suite-B-Kryptographie eingeschaltet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Es wird die Verwendung der folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Der im LCOS integrierte RADIUS-Server unterstützt die hier genannen Cipher-Suiten.

4 Features über LANconfig konfigurieren

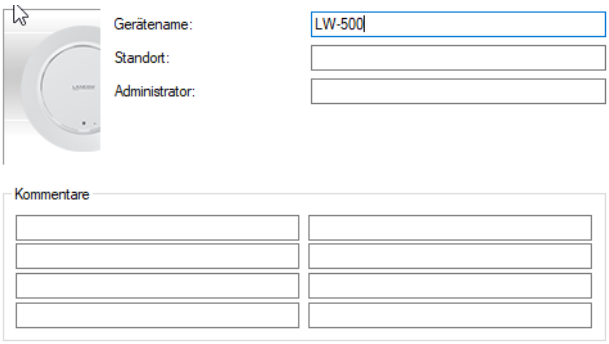
Im Folgenden werden alle Einstellungsmöglichkeiten in LANconfig erläutert. Diese sind abhängig vom Gerät, sodass nicht immer alle aufgeführten Optionen zur Verfügung stehen.

4.1 Management

Im Abschnitt **Management** finden Sie allgemeine Einstellungen zum Gerät.

4.1.1 Allgemein

Die beschreibenden Einstellungen zum Gerät finden Sie unter **Management** > **Allgemein**.



Name

Konfigurieren Sie hier den Gerätenamen.

Standort

Konfigurieren Sie hier den Gerätestandort.

Administrator

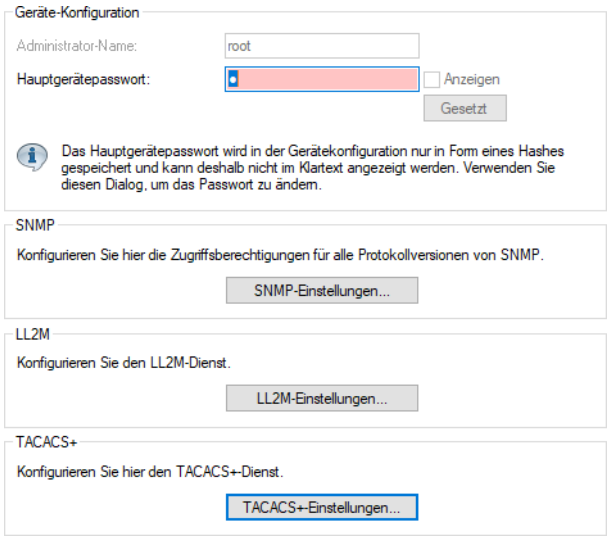
Konfigurieren Sie hier den Namen des Geräte-Administrators.

Kommentare

Verwenden Sie die Kommentarfelder zum Eintragen beliebiger Kommentare zur Gerätekonfiguration.

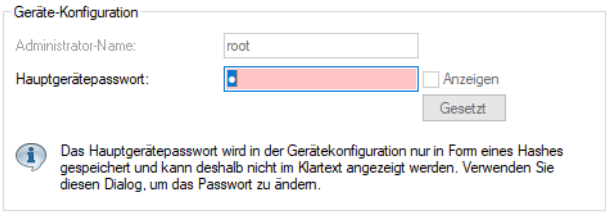
4.1.2 Admin

Die Einstellungen, um das Hauptgerätepasswort des Gerätes und die Einstellungen für SNMP zu ändern, finden Sie unter **Management** > **Admin**.



4.1.2.1 Hauptgerätepasswort

Die Einstellungen, um das Hauptgerätepasswort des Gerätes zu ändern, finden Sie unter **Management** > **Admin** > **Geräte-Konfiguration**.



Administrator-Name

Konfigurieren Sie hier den Anmeldenamen des Geräte-Administrators. Abhängig vom Gerät kann dieser Name fest vorgegeben sein und wird dann hier nur angezeigt.

Hauptgerätepasswort

Konfigurieren Sie hier das Hauptgerätepasswort. Dieses wird abhängig vom Gerät auf diesem nur als Hashwert gespeichert, sodass die Anzeige im Klartext nicht immer möglich ist.

Wenn Sie ein neues Passwort eingeben, dann erscheint ein Feld, um das geänderte Passwort erneut einzugeben. Da die Eingabe nicht angezeigt wird, dient dies zur Verifikation Ihrer Eingabe. Alternativ aktivieren Sie die Option **Anzeigen**. Danach wird Ihre Eingabe normal angezeigt. Falls ihr Bildschirm während der Eingabe einsehbar ist, dann raten wir von dieser Option ab.

4.1.2.2 Simple Network Management Protocol (SNMP)

Das Simple Network Management Protocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netzwerk von einer zentralen Instanz aus. Seit der ersten Veröffentlichung von SNMPv1 im Jahr 1988 entwickelte es sich im Laufe der Zeit über die Version SNMPv2 bis zur Version SNMPv3 weiter, um einer immer komplexeren Netzwerk-Infrastruktur sowie gesteigerten Ansprüchen an Sicherheit, Flexibilität und Komfort gerecht zu werden.

Mit Hilfe des Protokolls SNMP (Simple Network Management Protocol) werden höchste Ansprüche, wie das simple Management und Monitoring eines Netzwerks erfüllt. Es ermöglicht die frühzeitige Erkennung von Problemen und Störungen in einem Netzwerk und unterstützt bei deren Beseitigung. Das Simple Network Management Protocol ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus und regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Dadurch lassen sich Parameter wie der Zustand des Gerätes, CPU-Auslastung, Temperatur eines Geräts, Verbindungsstatus, Störungen, etc. z. B. über LANmonitor überwachen und auswerten. Der Administrator wird aktiv bei der Netzwerkverwaltung unterstützt und kann Probleme frühzeitig in seinem Monitoringsystem erkennen. Die neueste Version des Protokolls SNMPv3 ermöglicht im Gegensatz zu den Vorgängerversionen SNMPv1 und SNMPv2 eine verschlüsselte Datenkommunikation zwischen Netzwerk und Managementsystem und bietet damit einen entscheidenden Sicherheitsfaktor. Die integrierte Nutzerverwaltung bietet zusätzlich, dank verschiedener Benutzer-Accounts, eine Authentifizierung für die optimale Zugriffskontrolle bei Konfigurationen. So lassen sich Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern und das Netzwerk ist optimal geschützt.

SNMP-Komponenten

Die typische SNMP-Architektur besteht aus drei Komponenten:

SNMP-Manager

Der SNMP-Manager sendet SNMP-Anfragen an den SNMP-Agent und wertet dessen SNMP-Antworten aus. Als solche SNMP-Manager fungieren z. B. LANconfig und LANmonitor. Da LCOS LX-Geräte sich an die Standards von SNMPv1, SNMPv2 und SNMPv3 halten, ist auch der Einsatz einer alternativen SNMP-Verwaltungs- und Management-Software möglich.

SNMP-Agent

Der SNMP-Agent ist ein Modul, das auf dem verwalteten Gerät aktiviert ist. Er nimmt die Anfragen des SNMP-Managers entgegen, sammelt entsprechend der Anfrage die Zustandsdaten des Geräts aus dessen MIB und sendet diese Daten als „SNMP Response" zurück an den SNMP-Manager. Je nach Konfiguration sendet der SNMP-Agent bei bestimmten Zustandsänderungen im verwalteten Gerät auch eigenständig einen sogenannten „SNMP Trap" an den SNMP-Manager. Die Benachrichtigung in Form einer SYSLOG-Meldung oder einer E-Mail an den Administrator des Geräts ist ebenfalls möglich.

Verwaltetes Gerät

Die Zustände dieses Gerätes finden sich in seiner Management Information Base (MIB). Auf Anfrage des SNMP-Agenten liest das Gerät die entsprechenden Daten aus und gibt sie an den SNMP-Agenten zurück.

Die Übertragung von SNMP-Requests und SNMP-Responses zwischen SNMP-Manager und SNMP-Agent erfolgt standardmäßig im User Datagram Procol (UDP) über den Port 161. Die Übertragung von SNMP-Traps erfolgt standardmäßig im UDP über Port 162.

SNMP-Versionen

Die Unterschiede zwischen den verschiedenen SNMP-Versionen lassen sich wie folgt zusammenfassen:

SNMPv1

Die Version 1 startete in 1988 und galt lange Zeit als De-Facto-Standard für Netzwerk-Management. Die Authentifizierung des SNMP-Managers am SNMP-Agent erfolgt bei SNMPv1 über einen Community-String, der in beiden Komponenten identisch sein muss. Diese Sicherheit ist allerdings stark eingeschränkt, da die Übertragung des Community-Strings im Klartext erfolgt. Nicht zuletzt die gesteigerten Anforderungen an eine sichere Netzwerk-Kommunikation machten eine Überarbeitung der Version 1 notwendig.

SNMPv2

In die Version 2 flossen seit 1993 hauptsächlich Verbesserungen im Komfortbereich ein. Mehrere Zwischenschritte und wieder verworfene Konzepte führten letztendlich zur Version SNMPv2c. Diese Version ermöglicht die komfortable Abfrage von großen Datenmengen über einen `GetBulkRequest`-Befehl und

die Kommunikation von SNMP-Managern untereinander. Der Austausch des Community-Strings erfolgt allerdings wie bei der Version 1 weiterhin im Klartext.

SNMPv3

Die Version 3 erfüllt schließlich ab 1999 die mittlerweile dringend notwendigen Sicherheitsanforderungen. U. a. erfolgt die Kommunikation verschlüsselt, und auch die Kommunikationspartner müssen sich zuvor authentifizieren und autorisieren. Darüber hinaus ist der SNMP-Aufbau modularer geworden, so dass z. B. Modernisierungen bei Verschlüsselungstechnologien in SNMPv3 einfließen können, ohne den Standard komplett neu gestalten zu müssen.

LCOS LX unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

4.1.2.2.1 SNMPv3-Grundlagen

Die Protokoll-Struktur von SNMP hat sich in der Version 3 grundlegend geändert. SNMPv3 ist in mehrere Module mit klar definierten Interfaces aufgeteilt, die untereinander kommunizieren. Die drei wichtigsten Elemente in SNMPv3 sind „Message Processing and Dispatch (MPD)", „User-based Security Model (USM)" und „View-based Access Control Mechanism (VACM)".

MPD

Das MPD-Modul ist verantwortlich für die Verarbeitung (processing) und die Weiterbeförderung (dispatch) der ein- und ausgehenden SNMP-Meldungen.

USM

Das USM-Modul verwaltet Sicherheitsfunktionen, die die Authentifizierung der Nutzer sowie die Verschlüsselung und Integrität der Daten sicherstellen. 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.

VACM

Der VACM stellt sicher, dass der Sender einer SNMP-Anfrage berechtigt ist, die angefragte Information zu erhalten. Die entsprechenden Zugriffsberechtigungen finden sich in den folgenden Einstellungen und Parametern:

SNMPv3-Views

„SNMPv3-Views" fassen Inhalte, Statusmeldungen und Aktionen der Management Information Base (MIB) zusammen, die eine SNMP-Anfrage mit entsprechenden Zugriffsrechten erhalten bzw. ausführen darf. Diese Ansichten können einzelne Werte, aber auch komplette Pfade der MIB sein. Die Angabe dieser Inhalte erfolgt anhand der jeweiligen OIDs der MIB-Einträge.

Auf diese Weise erhält der Sender einer SNMP-Anfrage auch nach erfolgreicher Authentifizierung nur Zugriff auf die Daten, für die er gemäß SNMPv3-Views die Zugriffsrechte besitzt.

SNMPv3-Groups

„SNMPv3-Groups" fassen Nutzer mit gleichen Zugriffsrechten in einer jeweiligen Gruppe zusammen.

Security-Levels

„Security Levels" bestimmen die Sicherheitsstufe für den Austausch von SNMP-Nachrichten. Die folgenden Stufen sind auswählbar:

NoAuth-NoPriv

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.

Auth-NoPriv

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

Auth-Priv

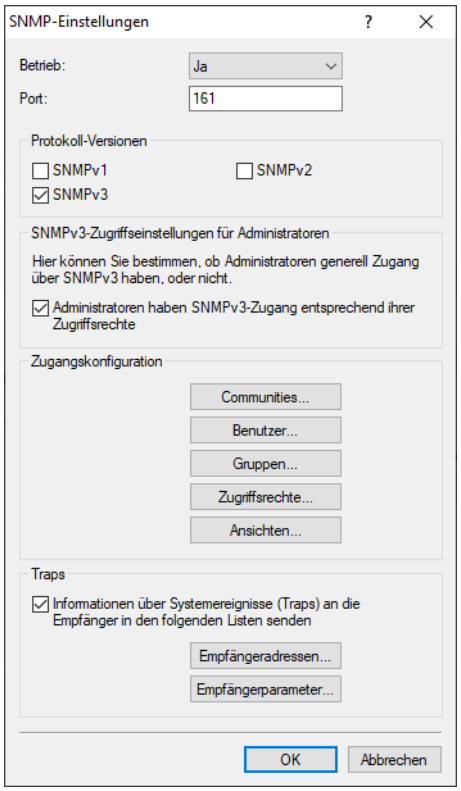
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Kontext

Der „Kontext" ist dafür vorgesehen, die einzelnen SNMP-Entities voneinander zu unterscheiden.

4.1.2.2.2 SNMP konfigurieren

Die SNMP-Einstellungen des Gerätes finden Sie unter **Management** > **Admin** > **SNMP** > **SNMP-Einstellungen**.



Betrieb

Aktivieren Sie SNMP für die im Folgenden angegebenen SNMP-Protokollversionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

Port

Passen Sie ggfs. den Port für SNMP an. Default: 161

Protokoll-Versionen

SNMPv1

Aktiviert SNMPv1.

SNMPv2

Aktiviert SNMPv2c.

SNMPv3

Aktiviert SNMPv3.

SNMPv3-Zugriffseinstellungen für Administratoren

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Zugangskonfiguration

SNMP-Communities

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten „Community", welche die Bedeutung eines Passworts bzw. Zugangsschlüssels inne hat. Die Authentifizierung kann hierbei wahlweise

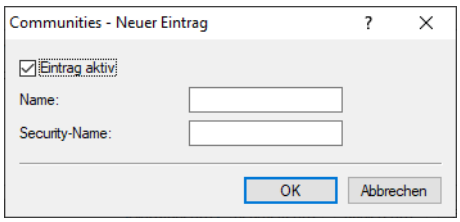
- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff),
- oder eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen.

Eine Communitiy fasst somit 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.

Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig eigene Communities zu definieren.

Diese Konfiguration ist nur für die SNMP-Versionen v1 und v2c relevant.



Eintrag aktiv

Aktiviert oder deaktiviert diese SNMP-Community.

Name

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

Security-Name

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

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

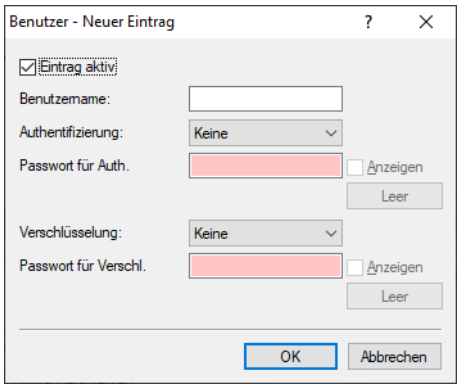
Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community.

Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Benutzer

Neben den am Gerät registrierten Administratoren ist der Zugriff auch für einzelne Nutzer möglich. Hier konfigurieren Sie die Einstellungen für Authentifizierung und Verschlüsselung für diese Anwender bei Nutzung von SNMPv3.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Benutzer.

Benutzername

Vergeben Sie hier einen aussagekräftigen Namen für diesen Benutzer.

Authentifizierung

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss. Zur Verfügung stehen die folgenden Verfahren:

Keine

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 (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).

Passwort für Authentifizierung

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Verschlüsselung

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll. Zur Verfügung stehen die folgenden Verfahren:

Keine

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

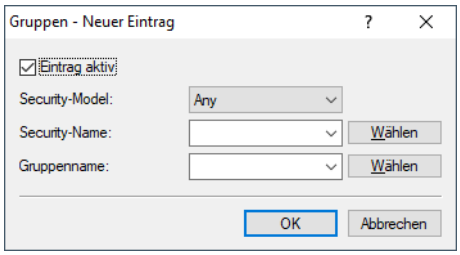
Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Passwort für Verschlüsselung

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Gruppen

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen. Als Standardeintrag ist die Konfiguration für den SNMP-Zugriff über den LANmonitor bereits voreingestellt.



Eintrag aktiv

Aktiviert oder deaktiviert diese Gruppe.

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 einen der folgenden Einträge aus:

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 „Keine Authentifizierung und keine Verschlüsselung".

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 „Keine Authentifizierung und keine Verschlüsselung".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind Sicherheitsstufen möglich, die bei den **Zugriffsrechten** aktiviert werden.

Security-Name

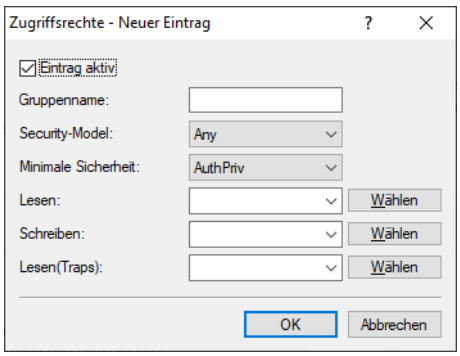
Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Gruppenname

Wählen Sie hier eine Gruppe aus, die Sie unter **Zugriffsrechte** definiert haben.

Zugriffsrechte

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Gruppenname

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe.

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Minimale Sicherheit

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

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

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

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Lesen

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Schreiben

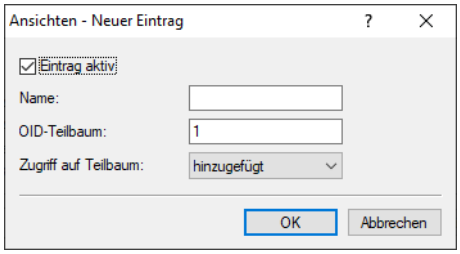
Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Lesen (Traps)

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte für Traps erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Ansichten

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



Eintrag aktiv

Aktiviert oder deaktiviert diese Ansicht.

Name

Vergeben Sie hier einen aussagekräftigen Namen für die Ansicht.

OID-Teilbaum

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

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

Zugriff auf Teilbaum

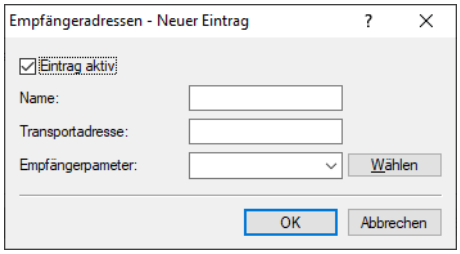
Bestimmen Sie, ob die angegebenen OID-Teilbäume Bestandteil („hinzugefügt“) oder kein Bestandteil („entfernt“) der Ansicht sind.

Traps

Wenn Sie die Option **Informationen über Systemereignisse (Traps) an die Empfänger in den folgenden Listen senden** aktivieren, dann bekommen die unter **Empfängeradressen** und **Empfängerparameter** konfigurierten Empfänger entsprechende Informationen.

Empfängeradressen

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Transportadresse

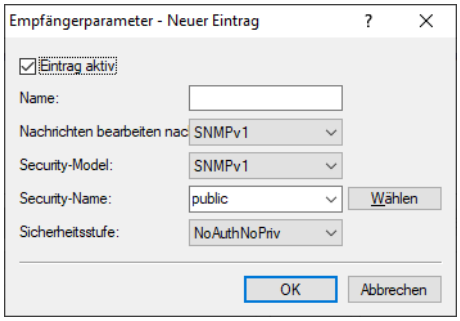
Konfigurieren Sie hier die Adresse des Empfängers. Diese Adresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax „<IP-Adresse>:<Port>" angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Empfängerparameter

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

Empfängerparameter

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Nachrichten bearbeiten nach

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

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, sodass 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 auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

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. Dies kann ausschließlich zusammen mit SNMP-Benutzern gewählt werden. Die effektive mögliche Sicherheitsstufe hängt von den gewählten Authentifizierungs- und Verschlüsselungsmethoden des Benutzers ab.

Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Sicherheitsstufe

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

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

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

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

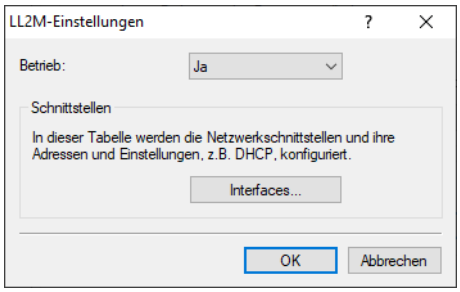
Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

4.1.2.3 LL2M

Die LL2M-Einstellungen des Gerätes finden Sie unter **Management** > **Admin** > **LL2M** > **LL2M-Einstellungen**.



Betrieb

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 der Zugriff über die serielle Konfigurationsschnittstelle, die allerdings nicht bei allen Geräten verfügbar ist oder ein Reset des Gerätes auf den Auslieferungszustand. Beide Möglichkeiten setzen 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 **LANCOM 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.

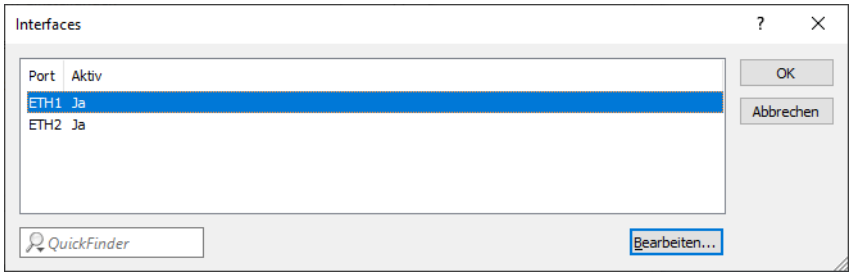
Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die Befehle `LL2Mdetect` bzw. `LL2Mexec`. Siehe *Konsole – Befehlsübersicht* auf Seite 9

Aktivieren Sie hier LL2M.

Access Points vom Typ 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).

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.



4.1.2.4 TACACS+

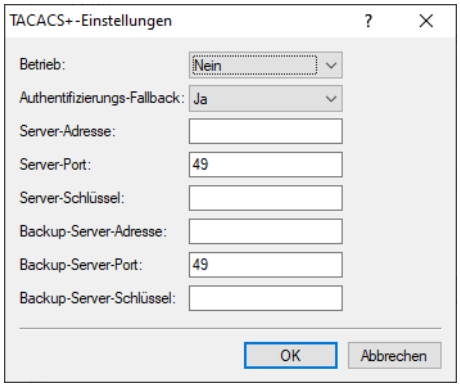
Konfigurieren Sie hier Authentifizierung, Autorisierung und Accounting (AAA) mittels des TACACS+-Protokolls.

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.

Die TACACS+-Einstellungen des Gerätes finden Sie unter **Management** > **Admin** > **TACACS+** > **TACACS+-Einstellungen**.



Betrieb

Schaltet die Verwendung von TACACS+ ein oder aus.

Authentifizierungs-Fallback

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

Server-Adresse

Die IP-Adresse des primären TACACS+-Servers.

Server-Port

Der Port des primären TACACS+-Servers.

Server-Schlüssel

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

Backup-Server-Adresse

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

Backup-Server-Port

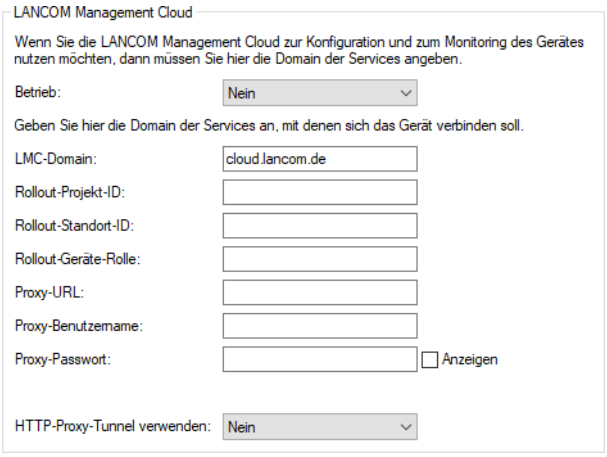
Der Port des Backup-TACACS+-Servers.

Backup-Server-Schlüssel

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

4.1.3 LMC

Die Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud (LMC) finden Sie unter **Management** > **LMC**.



Betrieb

Legen Sie fest, ob das Gerät über die LMC verwaltet werden soll.

Nein

Das Gerät stellt keine Verbindung zur LMC her.

Ja

Das Gerät wird von der LMC verwaltet.

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.

Rollout-Projekt-ID

Geben Sie hier die Projekt-ID dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Rollout-Standort-ID

Geben Sie hier den Standort dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Rollout-Geräte-Rolle

Geben Sie hier die Rolle dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Proxy-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.

Proxy-Benutzername

Benutzername zur Verwendung mit einem HTTP-Proxy-Server.

Proxy-Passwort

Passwort für den Benutzer zur Verwendung mit einem HTTP-Proxy-Server.

Wiederholen

Wiederholung des Passworts für den Benutzer zur Verwendung mit einem HTTP-Proxy-Server.

HTTP-Proxy-Tunnel verwenden

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.

4.1.4 Erweitert

Hier finden Sie die Einstellungen für die LED-Funktionalität, die Möglichkeit, das Syslog an externe Server zu senden und Einstellungen zu SSH.

4.1.4.1 LED

Hier finden Sie die Einstellungen für die LED-Funktionalität. Diese sind unter **Management** > **Erweitert**.

Bei Geräten, die für volle Funktionalität (z. B. Aktivierung aller WLAN-Streams) PoE 802.3bt benötigen, wird über eine dauerhaft gelb leuchtende Power-LED signalisiert, dass eine unzureichende Stromversorgung vorliegt.

LED-Mode

Wählen Sie zwischen den LED-Betriebsarten:

Ein

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

Aus

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

Verzögert aus

Die LED(s) des Gerätes werden nach einer konfigurierbaren Zeit abgeschaltet.

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

LED-Ausschalt-Verzögerung

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

4.1.4.2 PoE-Passthrough

Hier finden Sie die Einstellungen für PoE-Passthrough. Diese sind unter **Management** > **Erweitert**.

PoE-Passthrough

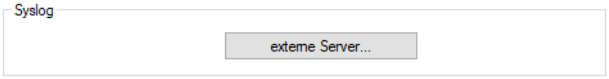
Bei Modellen mit PoE-Passthrough-Funktion, wenn der Access Point mit PoE 802.3bt (60W) gespeist wird, kann am zweiten Ethernet-Port ETH2 ein weiteres PoE-Gerät (PD) angeschlossen werden, welches wiederum mit maximal 30W gespeist wird.

Die PoE-Passthrough-Funktion können Sie hier ein- und ausschalten. Im Auslieferungszustand ist sie deaktiviert. Der LANmonitor und die WEBconfig stellen weitere Statusinformationen bereit.

4.1.4.3 Syslog

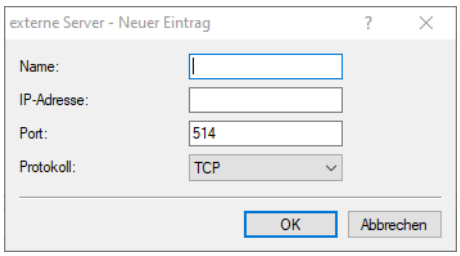
Zu Diagnosezwecken kann das Syslog eines LCOS LX-basierten Gerätes an einen externen Syslog-Server gesendet werden.

Die Einstellungen hierzu finden Sie unter **Management** > **Erweitert** > **Syslog**.



Konfigurieren Sie unter **externe Server** 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.



Name

Name des externen Syslog-Servers.

IP-Adresse

IP-Adresse des externen Syslog-Servers.

Port

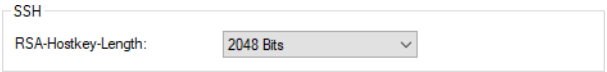
Port des externen Syslog-Servers.

Protokoll

Protokoll (TCP/UDP), mit dem der externe Syslog-Server angesprochen wird.

4.1.4.4 SSH

Unter **Management** > **Erweitert** finden Sie die Einstellungen für die SSH-Funktionalität.



RSA-Hostkey-Length

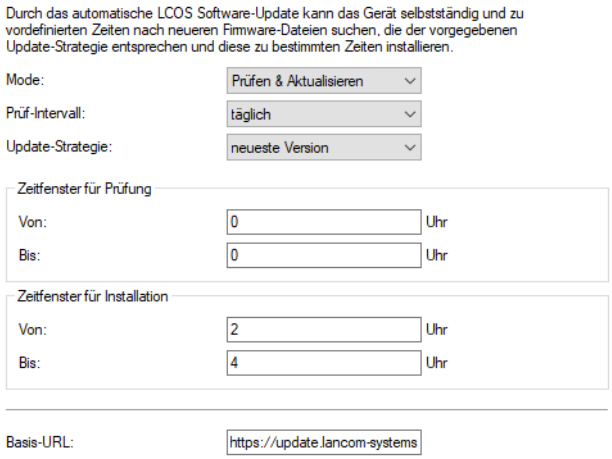
Die Länge des SSH-Hostkeys kann zwischen 2048 Bits und 4096 Bits gewählt werden. Nach der Änderung der Einstellung wird der Hostkey sofort neu generiert.

4.1.5 Software-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff. LANCOM 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 LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

Die Konfiguration des LANCOM Auto Updaters finden Sie in LANconfig unter **Management** > **Software-Update**.



Mode

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** 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.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

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

Manuell

- 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

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

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste Version ohne REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 REL.

Zeitfenster für Prüfung

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 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.

Zeitfenster für Installation

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

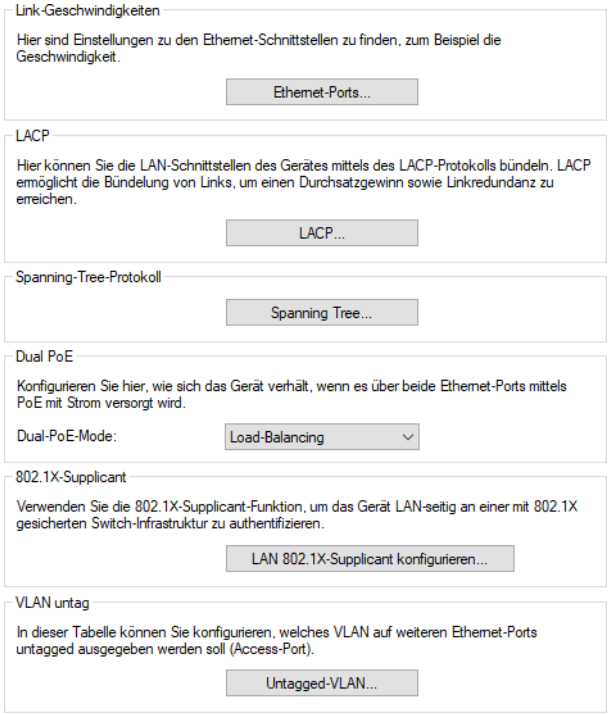
Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

4.2 Schnittstellen

Im Abschnitt **Schnittstellen** finden Sie Einstellungen zu den Schnittstellen des Gerätes.

4.2.1 Port-Einstellungen

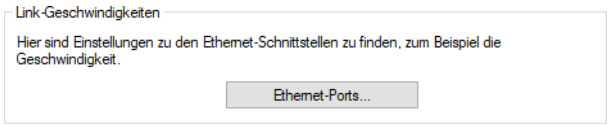
Die Einstellungen zur Konfiguration der Ethernet-Ports des Gerätes finden Sie unter **Schnittstellen** > **Port-Einstellungen**.

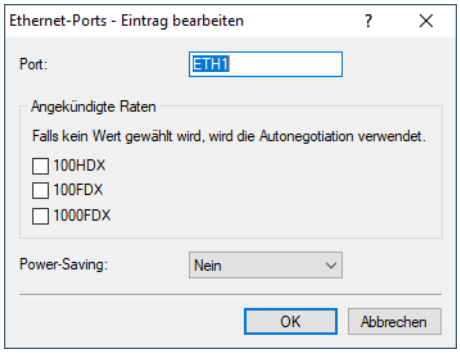


4.2.1.1 Link-Geschwindigkeiten

Hier sind Einstellungen zu den Ethernet-Schnittstellen zu finden, zum Beispiel die Geschwindigkeit oder die Aktivierung von Energy Efficient Ethernet / IEEE 802.3az.

LANconfig: **Schnittstellen** > **Port-Einstellungen** > **Link-Geschwindigkeiten** > **Ethernet-Ports**





Port

Konfigurieren Sie hier den Ethernet-Port, für den diese Einstellungen gelten sollen.

Angekündigte Raten

Konfigurieren Sie hier die angekündigten Raten für diesen Ethernet-Port. Falls kein Wert gewählt wird, dann wird die Autonegotiation verwendet.

Power-Saving

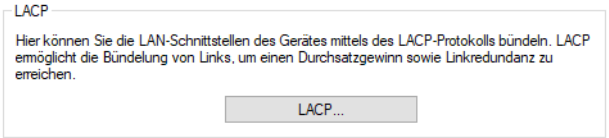
Über diesen Parameter aktivieren oder deaktivieren Sie Energy Efficient Ethernet / IEEE 802.3az für diesen Ethernet-Port.

4.2.1.2 Link Aggregation (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.

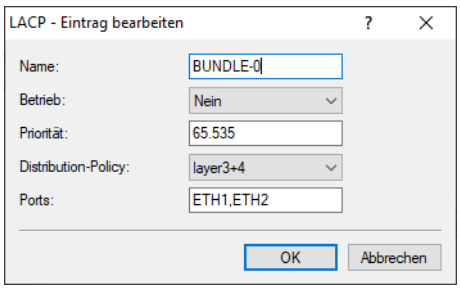
Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

LANconfig: **Schnittstellen** > **Port-Einstellungen** > **LACP**



4.2.1.2.1 LACP (Link Aggregation Control Protocol)

Über **LACP** konfigurieren Sie das Link Aggregation Control Protocol.



Name

Die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

Betrieb

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.

Priorität

Tragen Sie hier die LACP-System-Priorität ein. Der Standardwert ist 65.535.

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

Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt. Default: ETH1,ETH2

4.2.1.3 Spanning Tree Protokoll

In Netzwerken mit mehreren Switches und Bridges können zwischen zwei angeschlossenen Netzwerkteilnehmern durchaus mehrere physikalische Verbindungen bestehen. Diese redundanten Datenwege sind auch durchaus erwünscht, da sie bei Ausfall einzelner Netzstränge alternative Wege zum Ziel anbieten können. Auf der anderen Seite kann es durch diese

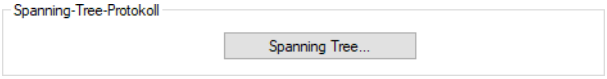
Mehrfachverbindungen zu unerwünschten Schleifen (Loops) oder zu mehrfach empfangenen Frames kommen. Beide Effekte stören den reibungslosen Datenverkehr im Netz.

Insbesondere bei Verwendung von Access Points des Typs LANCOM LX-7500 für Hitless Failover ist die Verwendung des (Rapid) Spanning Tree Protokolls ((R)STP) unerlässlich, um eine Redundanz nicht nur in der Stromversorgung, sondern auch bei der Datenübertragung herzustellen und die Entstehung einer Schleife zu unterbinden.

Alternativ kann auch LACP in Zusammenhang mit Hitless Failover verwendet werden. Hier ist je nach Access Point-Modell die Link-Geschwindigkeit und Umschaltgeschwindigkeit zu beachten.

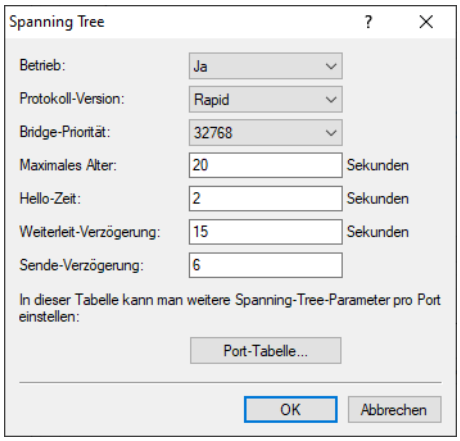
Standardmäßig ist RSTP beim LANCOM LX-7500 eingeschaltet, um out-of-the-box einen Betrieb mit beiden Ethernet-Verbindungen zu ermöglichen. Grundsätzlich wird das Spanning-Tree-Protokoll von allen Acccess Points mit mindestens zwei Ethernet-Ports unterstützt.

LANconfig: **Schnittstellen** > **Port-Einstellungen** > **Spanning-Tree-Protokoll**



4.2.1.3.1 Spanning Tree Protokoll konfigurieren

Über **Spanning Tree** konfigurieren Sie das Spanning-Tree-Protokoll.



Betrieb

Bei ausgeschaltetem Spanning Tree verschickt ein Gerät keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete durch, anstatt sie selber zu verarbeiten.

Protokoll-Version

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.

Bridge-Priorität

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.

Maximales Alter

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.

Hello-Zeit

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.

Weiterleit-Verzögerung

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.

Sende-Verzögerung

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.

Port-Tabelle

In der Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte separat eingestellt werden.

Priorität

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 gewählt, der weiter oben in der Liste steht.

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.

Als Edge-Port kennzeichnen

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.

Pfadkosten-Beeinflussung

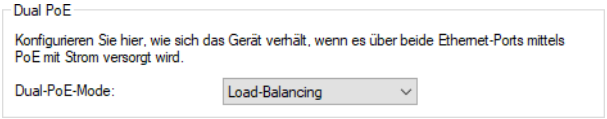
Mit diesem Parameter wird die Priorität von gleichwertigen Pfaden gesteuert. Der hier eingestellte Wert wird anstelle der berechneten Pfadkosten für die Auswahl verwendet. Die Voreinstellung 0 schaltet die Pfadkosten-Beeinflussung aus.

4.2.1.4 Dual PoE

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.

Der Access Point LANCOM LX-7500 unterstützt Dual PoE – beide Ethernet-Ports können als PoE-Eingang verwendet werden. Im Werkszustand ist der LANCOM LX-7500 für Load-Balancing vorkonfiguriert.

LANconfig: **Schnittstellen** > **Port-Einstellungen** > **Dual PoE** > **Dual-PoE-Mode**



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 LANCOM 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 LANCOM LX-7500 mit 2x IEEE 802.3at (Klasse 4 / 25,5W).

Monitoring auf der CLI

Die Einstellung bzw. der aktuelle Status lassen sich über die CLI unter **Status** > **Hardware-Info** > **Power** > **Failover-Status** (1.47.42.10) abfragen. Folgende Status sind möglich:

Disabled

Der Access Point ist nicht für Hitless Failover konfiguriert, sondern für Load Balancing.

Ready

Der Access Point ist für Hitless Failover konfiguriert, die PoE-Versorgung erfolgt über beide Ports. Der Failover-Fall ist nicht eingetreten.

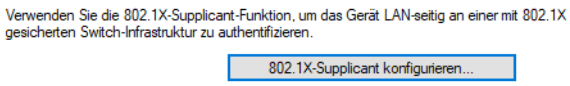
Engaged

Der Access Point ist für Hitless Failover konfiguriert, die Versorgung über einen von beiden Ports ist ausgefallen. Der Failover-Fall ist eingetreten.

Die Statusinformationen werden im LANmonitor bei den Systeminformationen des Access Points angezeigt.

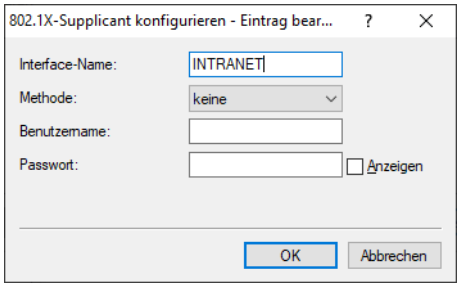
4.2.1.5 802.1X-Supplicant

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. Diese sind unter **Schnittstellen** > **Port-Einstellungen** > **802.1X-Supplicant**.



4.2.1.5.1 802.1X-Supplicant konfigurieren

Die 802.1X-Supplicant-Funktionalität konfigurieren Sie unter **Schnittstellen** > **Port-Einstellungen** > **802.1X-Supplicant** > **LAN 802.1X-Supplicant konfigurieren**.



Interface-Name

Der Name der LAN-Schnittstelle. Aktuell gibt es nur die Schnittstelle INTRANET, daher kann diese nicht geändert werden.

Methode

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

Benutzername

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

Passwort

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Die Unterstützung für eine Anmeldung mittels Client-Zertifikaten folgt in einer zukünftigen LCOS LX-Version.

4.2.2 Layer-3-Ethernet-Tunnel mit L2TPv3

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

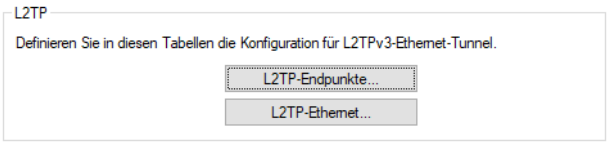
Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

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.

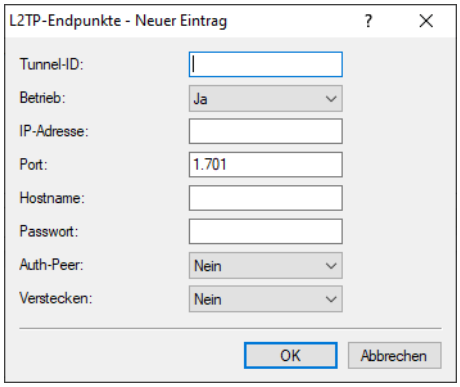
Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

LANconfig: **Schnittstellen** > **L2TP**



4.2.2.1 L2TP-Endpunkte

Über **L2TP-Endpunkte** konfigurieren Sie die L2TP-Endpunkte für die L2TPv3-Tunnel. Damit nehmen Sie die Tunnel-Konfiguration für die Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt vor.



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.

Betrieb

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts.

Port

Der zu nutzende UDP-Port. Default: 1701

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.

Passwort

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

Verstecken

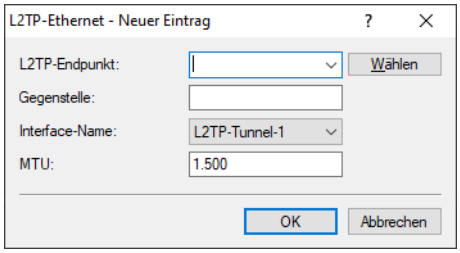
Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

Verbinden Sie anschließend ein konfiguriertes WLAN-Netzwerk mit der virtuellen L2TP-Ethernet-Schnittstelle.

Wechseln Sie dazu zu **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** und setzen Sie im gewünschten Eintrag die Einstellung **Bridge** auf die soeben konfigurierte virtuelle L2TP-Ethernet-Schnittstelle.

4.2.2.2 L2TP-Ethernet

Über **L2TP-Ethernet** konfigurieren Sie den L2TPv3-Tunnel zwischen einem WLAN-Netzwerk und einem L2TP-Endpunkt.



L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut.

Gegenstelle

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.

Interface-Name

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

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. Mögliche Werte: 68-1500

4.2.3 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.

LANconfig: **Schnittstellen** > **Multicast Snooping**

Betrieb

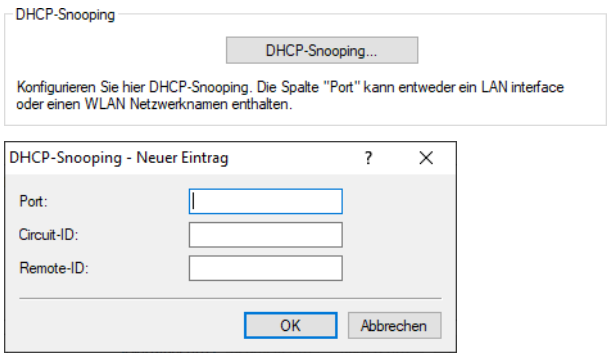
Schalten Sie Multicast-Snooping ein oder aus.

Zusätzlich ist optional eine Konvertierung von Multicast-Datenströmen in Unicast möglich. Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert. Die Pakete werden zwar je Client dupliziert, können aber, da es sich nun um Unicasts handeln, mit der für diesen Client höchstmöglichen Datenrate übertragen werden. Auch wenn die Pakete nun dupliziert werden, wird durch die viel schnellere Übertragung in den meisten Szenarien insgesamt deutlich weniger Airtime verbraucht, die dann für andere Übertragungen zur Verfügung steht. Siehe *Multicast-zu-Unicast* auf Seite 61.

4.2.4 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.

LANconfig: **Schnittstellen** > **DHCP-Snooping**



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.

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.

Remote-ID

Hier kann die Remote-ID unter Verwendung dieser Platzhalter konfiguriert werden:

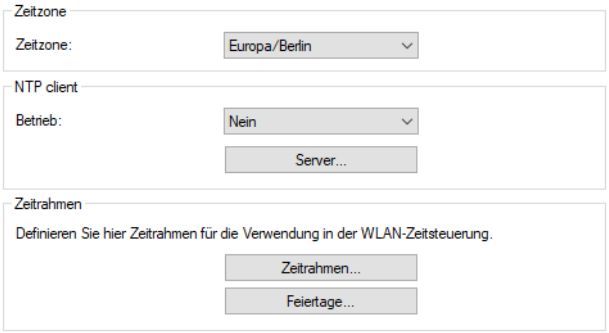
- %i: Fügt den Namen der Schnittstelle ein, über die der Relay-Agent die DHCP-Anfrage empfangen hat.
- %n: Fügt den Namen des DHCP-Relay-Agents ein, wie er unter **Setup** > **Name** angegeben ist.
- %s: Fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable eine leere Zeichenkette.
- %r: Fügt die systemweite MAC-Adresse ein.
- %%: Fügt ein Prozentzeichen ein.

4.3 Datum / Zeit

Im Abschnitt **Datum / Zeit** finden Sie die entsprechenden Einstellungen des Gerätes.

4.3.1 Konfiguration

Die Einstellungen des Gerätes zu Datum und Uhrzeit finden Sie unter **Datum / Zeit** > **Konfiguration**.



Zeitzone

Geben Sie die korrekte Zeitzone an.

NTP Client

Über das Network Time Protocol (NTP) kann das Gerät sich die aktuelle Zeit von einem öffentlich zugänglichen Zeit-Server im Internet (NTP-Server mit „Open Access"-Policy, in Deutschland z. B. von der Physikalisch-Technischen Bundesanstalt) beziehen. LANCOM Router können ebenfalls als NTP-Server arbeiten, so dass nicht jedes Gerät auf einen externen NTP-Server zugreifen muss.

Betrieb

Ja

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

Nein

Keinen NTP-Server verwenden.

Server

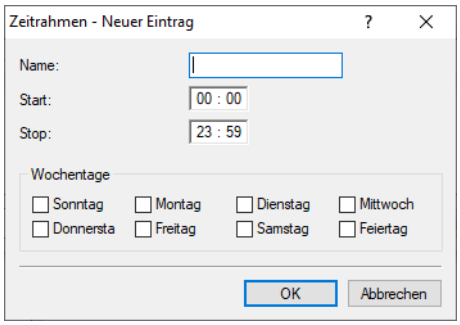
Wählen Sie hier aus den vorgegebenen NTP-Servern aus oder geben Sie die Adresse des zu verwendenden NTP-Servers an.

4.3.1.1 Zeitrahmen

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.

Beispielhaft sind hier bereits mehrere Zeitrahmen angelegt, die eine Konfiguration für einen Unterrichtstag an einer Schule zeigen sollen. Es existieren zwei Zeitrahmen mit dem identischen Namen „Unterricht" – aber mit unterschiedlicher Start- und Stoppzeit, um zwischen diesen beiden Zeitrahmen eine 45-minütige Pause realisieren zu können. Diese ist wiederum in dem Zeitrahmen „Pause" definiert. Zeitrahmen können auf bestimmte Wochentage eingeschränkt werden. Feiertage, sofern sie in der *Feiertage-Tabelle* hinterlegt wurden, werden ebenfalls beachtet. Sommer / Winterzeit wird ebenfalls anhand der eingestellten Zeitzone beachtet.

Voreingestellt sind die Zeitrahmen ALWAYS und NEVER. Weitere Zeitrahmen können Sie in LANconfig konfigurieren unter **Datum/Zeit** > **Konfiguration** > **Zeitrahmen**. Im gleichen Bereich finden Sie auch die Möglichkeit, für die Zeitrahmen Feiertage vorzugeben.



Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Startzeit

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stoppzeit

Hier kann die Stoppzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein 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.

Wochentage

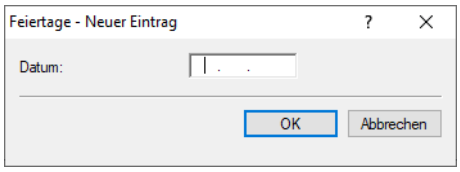
Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

Feiertage

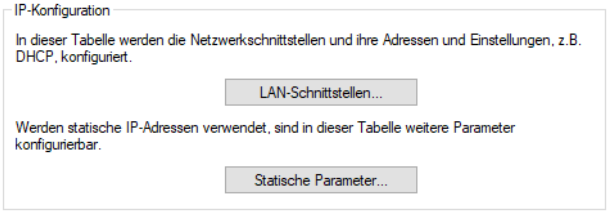


Geben Sie hier die Feiertage an, die in Zeitrahmen berücksichtigt werden sollen.

Das Jahr 0 steht für ein beliebiges Jahr.

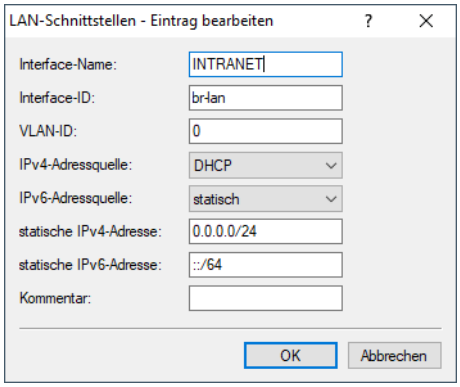
4.4 IP-Konfiguration

Die Einstellungen für die IP-Konfiguration Ihres Gerätes finden Sie unter **IP-Konfiguration** > **Konfiguration**.



4.4.1 LAN-Schnittstellen

Bearbeiten Sie unter **IP-Konfiguration** > **Konfiguration** > **LAN-Schnittstellen** grundsätzliche Konfigurationsoptionen rund um die eigenen IP-Einstellungen und den Netzwerkzugriff des Gerätes.



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.

Interface-ID

Der interne Bezeichner für das Interface.

VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll. Der Standardwert „0" bedeutet, dass kein VLAN verwendet wird.

IPv4-Adressquelle

Wählen Sie hier, woher die IPv4-Adresse des Interface bezogen werden soll:

DHCP

Die IP-Adresse wird via DHCP bezogen.

Statisch

Es wird die statisch konfigurierte IP-Adresse für das Interface verwendet.

IPv6-Adressquelle

Wählen Sie hier, woher die IPv6-Adresse des Interface bezogen werden soll:

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.

Statisch

Es wird die statisch konfigurierte IPv6-Adresse für das Interface verwendet.

Statische IPv4-Adresse

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv4-Adressquelle **Statisch** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).

Statische IPv6-Adresse

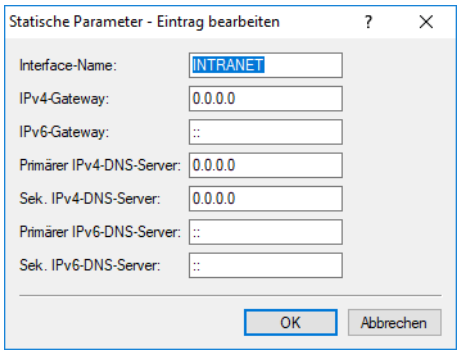
Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv6-Adressquelle **Statisch** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Kommentar

Legen Sie hier einen beliebigen Kommentar zur Interface-Konfiguration ab.

4.4.2 Statische Parameter

Bearbeiten Sie unter **IP-Konfiguration** > **Konfiguration** > **Statische Parameter** weitere 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 **Statisch** gewählt haben. Ansonsten werden alle notwendigen Informationen z. B. via DHCP bezogen, sodass in dieser Tabelle keinerlei Konfiguration notwendig ist.

Interface-Name

Tragen Sie hier den Namen des Interface ein, auf das sich die weiteren hier vorgenommenen Einstellungen beziehen sollen.

IPv4-Gateway

Konfigurieren Sie hier das IPv4-Gateway für das referenzierte Interface.

IPv6-Gateway

Konfigurieren Sie hier das IPv6-Gateway für das referenzierte Interface.

Primärer IPv4-DNS-Server

Konfigurieren Sie hier den primären IPv4-DNS-Server für das referenzierte Interface.

Sekundärer IPv4-DNS-Server

Konfigurieren Sie hier den sekundären IPv4-DNS-Server für das referenzierte Interface.

Primärer IPv6-DNS-Server

Konfigurieren Sie hier den primären IPv6-DNS-Server für das referenzierte Interface.

Sekundärer IPv6-DNS-Server

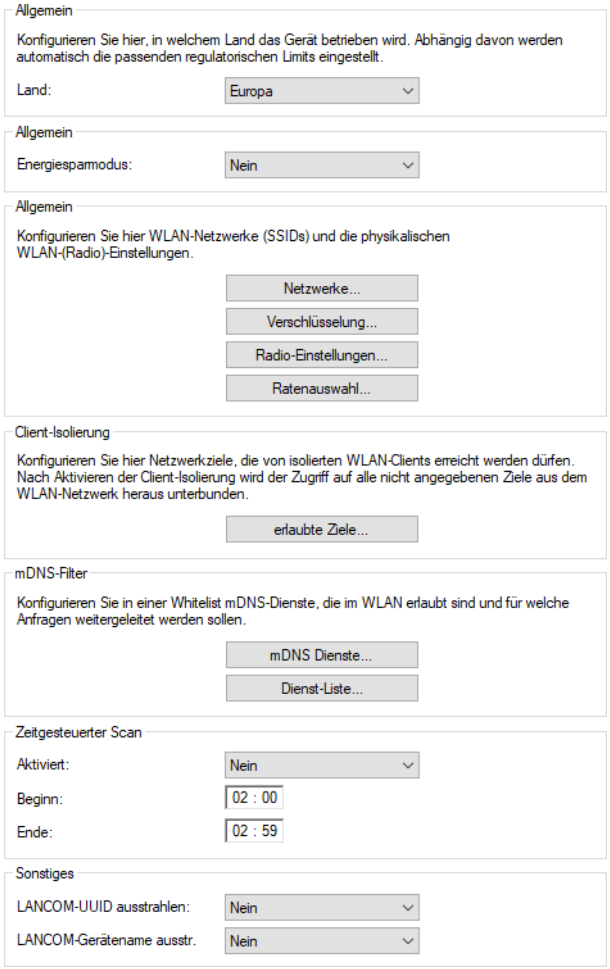
Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

4.5 Wireless-LAN

Im Abschnitt **Wireless-LAN** finden Sie alle Einstellungen rund um das Ausstrahlen von WLAN-Netzwerken.

4.5.1 WLAN-Netzwerke

Die Einstellungen für WLAN-Netzwerke Ihres Gerätes finden Sie unter **Wireless-LAN** > **WLAN-Netzwerke**.



Allgemein

Land

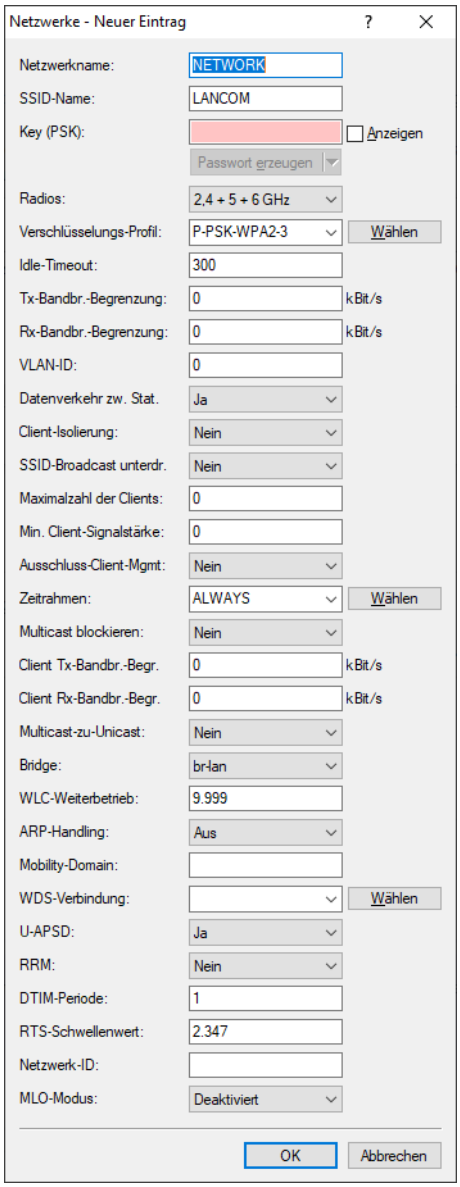
Konfigurieren Sie hier, in welchem Land das Gerät betrieben wird. Abhängig davon werden automatisch die passenden regulatorischen Begrenzungen eingestellt.

Energiesparmodus

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.

4.5.1.1 Netzwerke

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** 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.



Netzwerkname

Wählen 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. Dieser wird im nächsten Schritt konfiguriert.

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.

Key (PSK)

Konfigurieren Sie hier den Pre-shared Key (PSK), der für das WLAN-Netzwerk verwendet wird. Wenn Sie **Anzeigen** auswählen, dann können Sie über **Passwort erzeugen** ein zufällig erzeugtes Passwort erstellen. Über den Pfeil daneben können Sie die Stärke, Länge und einige Einstellungen zu verwendeten Zeichen des erzeugten Pre-shared Key einstellen.

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. LANCOM Systems GmbH 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

Radios

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

2,4 GHz

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

5 GHz

Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

6 GHz

Die SSID wird nur auf der Frequenz 6 GHz ausgestrahlt.

„Kombinationen“

Die SSID wird auf den angegenemem Frequenzen ausgestrahlt.

keiner

Die SSID wird nicht ausgestrahlt. Dies kann als genereller Ein- / Aus-Schalter für die SSID verwendet werden.

Verschlüsselungs-Profil

Wählen Sie hier ein Verschlüsselungs-Profil, welches definiert, welches Authentisierungs- und Verschlüsselungsverfahren für die SSID zum Tragen kommen soll.

Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können ausgewählt werden:

P-NONE

Keine Verschlüsselung, die SSID ist offen.

P-PSK-WPA2

Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WiFi7

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.

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.

Tx-Bandbreiten-Begrenzung

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

Rx-Bandbreiten-Begrenzung

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

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.

Datenverkehr zwischen Stationen

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.

Client-Isolierung

Die Client-Isolierung kann hier je SSID eingeschaltet werden. Siehe auch *#unique_63/unique_63_Connect_42_ci-0*.

SSID-Broadcast unterdrücken

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.

Maximalzahl der Clients

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

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

Minimale Client-Signalstärke

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.

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

Ausschluss-Client-Management

Nimmt diese SSID gegebenenfalls vom Band Steering aus.

Zeitrahmen

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

Multicast blockieren

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.

Client Tx-Bandbr.-Begr.

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

Client Rx-Bandbr.-Begr.

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

Multicast-zu-Unicast

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

Nein

Keine Konvertierung durchführen.

Konvertiere zu Unicast

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.

Kapsele in Unicast-Aggregat

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.

Damit das Feature funktioniert, ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren. Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

Bridge

Wird bei WLC-Betrieb intern verwendet bzw. bei Verwendung von *Layer-3-Ethernet-Tunnel mit L2TPv3* auf Seite 47 muss hier das L2TP-Interface eingetragen werden,

WLC-Weiterbetrieb

Dieser Wert wird bei Betrieb mit einem WLAN-Controller von diesem geschrieben.

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.

Aus

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

An

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.

Strikt

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.

WDS-Verbindung

Hier können Sie festlegen, dass bestimmte SSIDs über WDS-Verbindungen übertragen werden. Referenzieren Sie dazu hier einen Eintrag aus *Verbindungen* auf Seite 79.

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

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. LANCOM 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.

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". Aktivieren Sie hier diese Option.

DTIM-Periode

Die DTIM-Periode kann per SSID konfiguriert werden.

MLO-Modus

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.

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.

Deaktiviert

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

4.5.1.2 Verschlüsselung

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke. Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-NONE

Keine Verschlüsselung, die SSID ist offen.

P-PSK-WPA2

Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

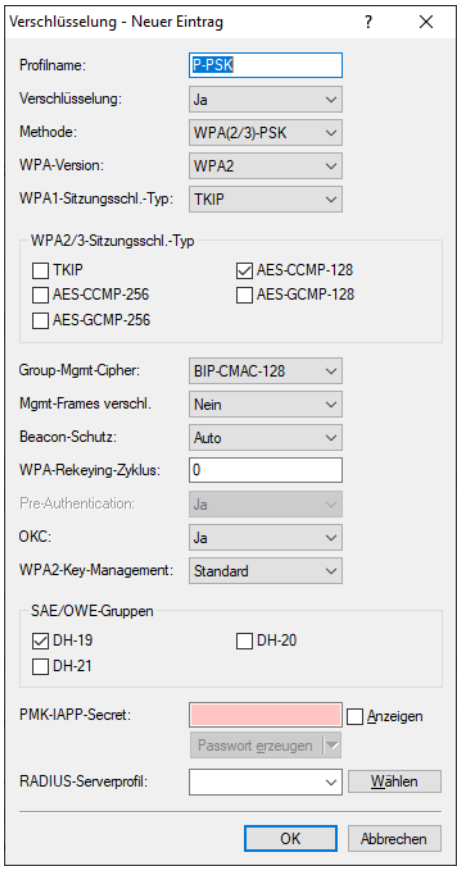
Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WiFi7

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.



Profilname

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

Verschlüsselung

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

Methode

Konfigurieren Sie hier die Verschlüsselungsmethode. Folgende Methoden stehen zur Auswahl:

WPA

- WPA(2/3)-PSK: WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal
- WPA(2/3)-802.1X: WPA2 und / oder WPA3 mit 802.1X, auch bekannt als WPA-Enterprise

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

WEP

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.

- 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.

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.

Clients, welche die Verschlüsselungs-Methode **Enhanced-Open** nicht unterstützen, können sich nicht mit dem WLAN verbinden.

WPA-Version

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode. Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden WPA(2)-PSK und WPA(2)-802.1X verwendet werden. Folgende Versionen stehen zur Auswahl:

- 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.

WPA1-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

WPA2/3-Sitzungsschlüssel-Typ

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

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.

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

Group-Mgmt-Cipher

Konfigurieren Sie hier die Group Management Cipher.

Management-Frames verschlüsseln

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.

Beacon-Schutz

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

Der ab Werk ausgewählte Modus „Auto" 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.

WPA-Rekeying-Zyklus

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.

In der Standardeinstellung ist der Wert auf „0" eingestellt, so dass keine vorzeitige Aushandlung des Schlüssels erfolgt.

Pre-Authentication

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

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen Access Points, um sich ggf. mit einem von ihnen neu verbinden zu können. Access Points, 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 Access Point über das Infrastruktur-Netzwerk an, das die Access Points 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 Access Point sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue Access Point 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 Access Point verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

OKC (Opportunistic Key Caching)

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

Authentifizierung von WLAN-Clients über EAP und 802.1X ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation Anwendung. Der Nachteil der Authentifizierung über 802.1X ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und Access Point sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der Access Point Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen Access Points im WLAN-Netzwerk verarbeiten muss.

Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLAN-Controller (WLC) oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access Point in der Erwartung, dass dieser OKC aktiviert hat (deshalb „opportunistisch"). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1X-Authentifizierung aus.

Ein LANCOM Access Point kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

In von der LANCOM Management Cloud (LMC) verwalteten Netzen oder Netzen aus Standalone-Access-Points werden die PMKs über das IAPP-Protokoll übertragen. In LMC-verwalteten Netzen wird das IAPP automatisch konfiguriert. Sorgen Sie in Netzen aus Standalone-Access-Points dafür, dass das PMK-IAPP-Secret auf allen Access Points des Netzwerks konfiguriert und identisch ist.

WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll. 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. Siehe auch *Fast Roaming* auf Seite 16.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

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.

SAE/OWE-Gruppen

Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen, 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.

DH-19

256-bit random ECP group

DH-20

384-bit random ECP group

DH-21

521-bit random ECP group

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.

RADIUS-Serverprofil

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. Die Profile erzeugen Sie unter *RADIUS* auf Seite 84.

Hinweis zur WLAN-Verschlüsselung im 6 GHz-Band

Da im 6 GHz-Band aufgrund des für WLAN vollkommen neuen Frequenzbandes keine Abwärtskompatibilität mit alten Clients notwendig ist, werden veraltete Sicherheitsverfahren nicht unterstützt. Konkret bedeutet dies:

- ausschließliche Verwendung von WPA3 für verschlüsselte Netze. Dementsprechend ist auch kein Transition-Modus bzw. gemischter Modus wie WPA2/3 möglich.
- Verwendung von Enhanced Open für „offene" Netze (die dadurch dennoch eine Verschlüsselung der übertragenen Daten bieten). Offene, unverschlüsselt betriebene SSIDs sind nicht mehr möglich!
- Protected Management Frames müssen verpflichtend genutzt werden

Die o. g. Bedingungen können in der LCOS LX-Konfiguration gesetzt werden. Ist die explizite Konfiguration nicht gewünscht oder möglich (z. B. beim gemischten Betrieb derselben SSID auf mehreren Bändern, was ein häufiger Anwendungsfall ist), werden folgende Anpassungen von LCOS LX dynamisch vorgenommen, sobald eine SSID auf dem 6 GHz-Band verwendet werden soll:

- WPA-Versionen <3 werden automatisch auf WPA3 angepasst
- Enhanced-Open wird für offene Netzwerke aktiviert
- Protected Management Frames wird aktiviert

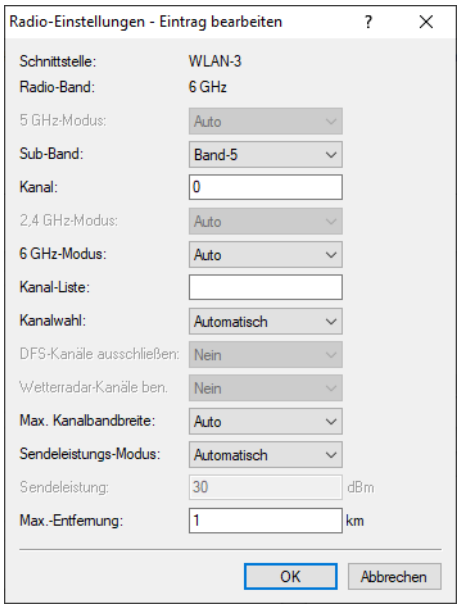
Hierdurch ist es möglich, bestehende Verschlüsselungsprofile weiter zu verwenden und eine gemeinsame Konfiguration für eine SSID, die zusätzlich auf 6 GHz ausgestrahlt werden soll, zu verwenden. Diese Einstellungen werden dynamisch im Betrieb angepasst, die im Gerät hinterlegte Konfiguration wird also nicht verändert.

4.5.1.3 Radio-Einstellungen

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** 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.

Auf kompatiblen Access Points enthält diese Tabelle einen zusätzlichen Eintrag „WLAN-3" zur Konfiguration des 6 GHz-WLAN-Radios.

Wie bei den 2,4 GHz- und 5 GHz-Radios ist das Frequenzband nicht veränderbar. Das Radio WLAN-3 unterstützt nur das 6 GHz-Band.



Schnittstelle

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

Radio-Band

Zeigt an, ob diese Schnittstelle im 2,4-GHz-, 5-GHz- oder 6-GHz-Frequenzbereich arbeitet.

5 GHz-Modus

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:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

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.

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

Sub-Band

Konfigurieren Sie hier, welche Sub-Bänder im 5-GHz-Modus verwendet werden. Folgende Sub-Bänder stehen zur Auswahl:

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 wird sowohl das Sub-Band 1, als auch das Sub-Band 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).

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

Kanal

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

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.

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.

2,4 GHz-Modus

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. Folgende Modi stehen zur Auswahl:

Auto

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

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.

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

6 GHz-Modus

Konfigurieren Sie hier, in welchem Modus das 6-GHz-Radio betrieben werden soll. Folgende Modi stehen zur Auswahl:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

802.11ax

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

11axbe-mixed

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

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

Kanal-Liste

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.

Kanalwahl

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.

LANCOM empfiehlt, eine Kanalplanung LMC-gestützt mittels ARC 2.0 durchzuführen, oder eine manuelle Planung anhand einer Ausleuchtung (Site Survey) durchzuführen.

DFS-Kanäle ausschließen

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 **DFS-Kanäle ausschließen** im Radio-Kanal und in der **Kanal-Liste** fest konfiguriert werden.

Wetterradar-Kanäle benutzen

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.

Max. Kanalbandbreite

Konfigurieren Sie hier die maximal erlaubte Kanalbandbreite. Folgende Einstellungen stehen zur Auswahl:

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 maximal mögliche Kanalbandbreite (bis zu 320 MHz) verwendet. Auf Wunsch kann die Kanalbandbreite hier über einen der anderen Werte weiter eingeschränkt werden.

20 MHz

Die Kanalbandbreite beträgt immer 20 MHz.

40 MHz

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

80 MHz

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

160 MHz

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

320 MHz

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.

Antennen-Gewinn

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist eine Dämpfung der Leistung auf den zulässigen Wert erforderlich. Hier wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Bei einer AirLancer Extender O-18a-Antenne mit einem Gewinn von 18 dBi wird bei einer Kabellänge von 4 m Länge mit einer Dämpfung 1 dB/m ein Antennen-Gewinn von 18 - 4 = 14 eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter

Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.

Nur bei Geräten mit externen Antennen verfügbar.

Antennen-Maske

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.

Sendeleistungs-Modus

Diese Einstellung regelt, ob die maximal erlaubte und von der Hardware des Access Point realisierbare Sendeleistung verwendet wird („Automatisch") oder ob im manuellen Modus („Manuell") die gewünschte Ziel-Sendeleistung vorgegeben werden kann. Dies erfolgt im Feld **Sendeleistung** in dBm.

Sendeleistung

Abhängig von der Einstellung im Feld **Sendeleistungs-Modus** stellen Sie hier die 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.

Max. Entfernung

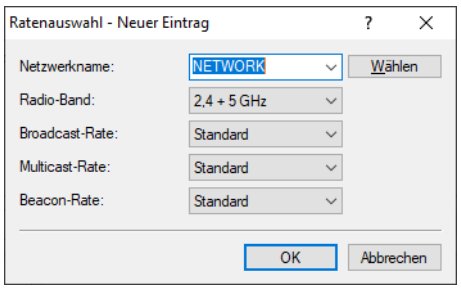
Geben Sie hier die Distanz zur am weitesten entfernten WLAN-Station ein (z. B. zu einem WDS-Partner).

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.

4.5.1.4 Ratenauswahl

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.

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Ratenauswahl** die Broad- und Multicast-Datenrate.



Netzwerkname

Das Netzwerk bzw. die SSID, für die die hier konfigurierten Raten gelten sollen. Der Name muss einem Namen der in *Netzwerke* auf Seite 58 eingerichteten Netzwerke entsprechen.

Radio-Band

Das Band, für das die konfigurierten Raten gelten sollen. Hiermit kann weiter auf ein bestimmtes Band eingeschränkt werden.

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.

Multicast-Rate

Die für das Senden von Multicasts zu verwendende Rate.

Beacon-Rate

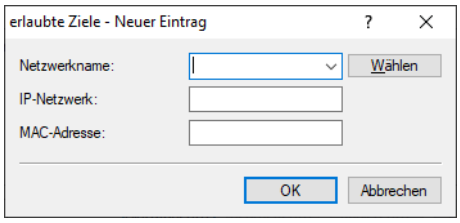
Die Datenrate, mit der WLAN-Beacons ausgesendet werden. In High-Density-Szenarien ist es empfehlenswert, diese Datenrate zu erhöhen, um Airtime zu sparen.

4.5.1.5 Client-Isolierung

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 je SSID eingeschaltet werden. Konfigurieren Sie dies unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** > **Client-Isolierung**. Konfigurieren Sie anschließend die erlaubten Ziele unter **Wireless-LAN** > **WLAN-Netzwerke** > **erlaubte Ziele**.



Netzwerkname

Wählen Sie hier das Netzwerk / die SSID, für die der Eintrag gelten soll. Erfassen Sie dann wahlweise eine Ziel-IP-Adresse oder Ziel-MAC-Adresse.

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.

IP-Netzwerk

Erlaubte Ziel-IP-Adresse für dieses Netzwerk.

MAC-Adresse

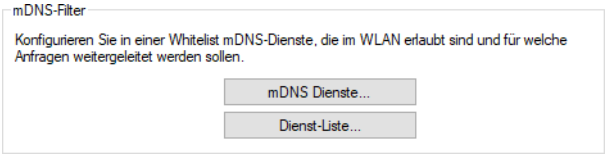
Erlaubte Ziel-MAC-Adresse für dieses Netzwerk.

4.5.1.6 mDNS-Filter

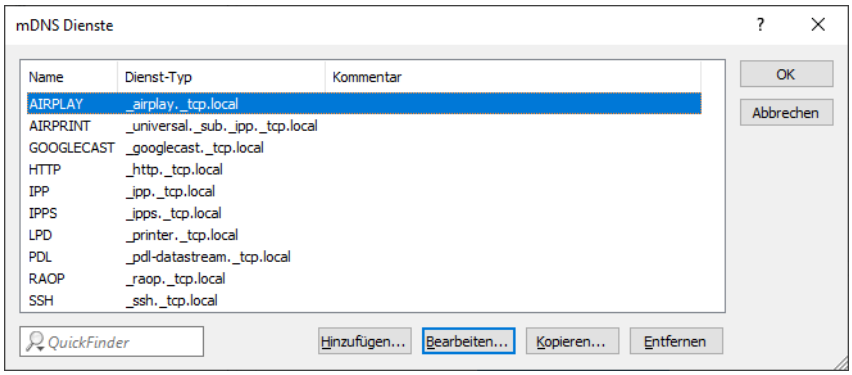
mDNS (Multicast DNS) wird zur einfachen Diensterkennung im (W)LAN verwendet. Prominente Anwendungen, die darauf basieren, sind Bonjour / AirPlay und Google Cast.

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.

Den mDNS-Filter konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **mDNS-Filter**.



mDNS-Dienste enthält standardmäßig die gängigsten mDNS-basierten Dienste, kann aber auch manuell erweitert werden.



Name

Der Name eines Dienstes.

Dienst-Typ

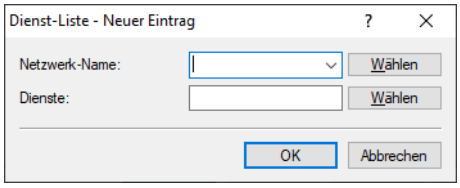
Der Typ dieses Dienstes.

Kommentar

Kommentar zu diesem Eintrag.

Konfigurieren Sie in der **Dienst-Liste** Filter auf Basis der Dienste aus der Tabelle **mDNS-Dienste**.

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.



Netzwerk-Name

Hier kann der WLAN-Netzwerkname konfiguriert werden, für den der Filter gelten soll.

Dienste

Hier kann ein oder mehrere der in der Services-Tabelle definierten mDNS-basierten Dienste hinzugefügt werden, für welche Anfragen weitergeleitet werden sollen.

4.5.1.7 Sonstiges

LANCOM-UUID ausstrahlen

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.

LANCOM-Gerätename ausstrahlen

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
```

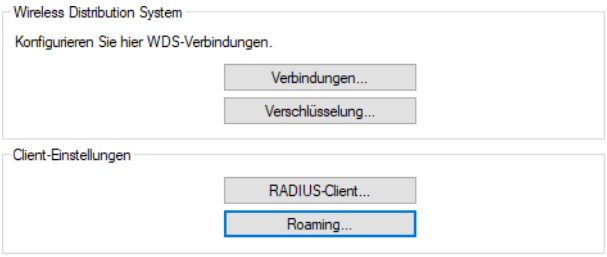
4.5.2 Wireless Distribution System (WDS) / Punkt-zu-Punkt-Verbindungen

Mittels des 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).

Mit LCOS LX 6.10 ist der WDS-Betrieb über eine Strecke von maximal 300 Metern validiert.

Die Einstellungen für WDS Ihres Gerätes finden Sie unter **Wireless-LAN** > **WDS**.



Übertragung von WLAN-Netzwerken

Im Rahmen der WLAN-Konfiguration können Sie festlegen, dass bestimmte SSIDs über WDS-Verbindungen übertragen werden. Dies erfolgt unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** im Auswahlfeld **WDS-Verbindung**.

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

Radio-Einstellungen

Die allgemeinen Radio-Einstellungen, die für den Access Point vorgenommen wurden, gelten auch für WDS-Verbindungen (insbesondere die Einstellung des WLAN-Kanals). Nehmen Sie diese wie gewohnt unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** vor.

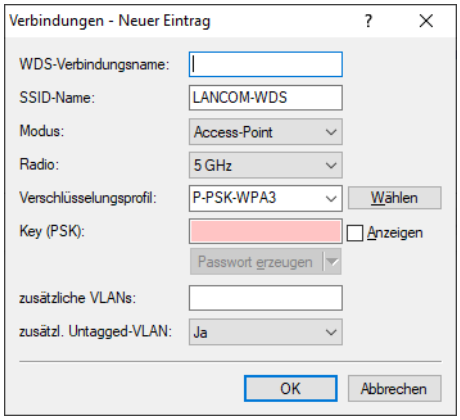
Achten Sie insbesondere darauf, dass eine eventuelle Kanalvorgabe oder Einschränkung auf bestimmte Unterbänder auf beiden Seiten der WDS-Verbindung übereinstimmt, damit die Verbindung aufgebaut werden kann. Alternativ kann auf beiden Seiten die automatische Kanalwahl verwendet werden. In diesem Fall sucht die Station über alle erlaubten Kanäle, bis der WDS-Partner gefunden wird.

Client-Modus für flexible Einbindung von Ethernet-fähigen Geräten in WLAN-Netze

Über den Client-Modus können Access Points flexibel für die Einbindung vielfältiger Ethernet-fähiger Geräte in bestehende WLAN-Netzwerke verwendet werden – betriebssystem- und somit herstellerunabhängig. Für passgenaue Sicherheit lässt sich für die zertifikatsbasiert verschlüsselte Kommunikation der Modus IEEE 802.1X oder WPA2/3-PSK wählen.

4.5.2.1 Verbindungen

Konfigurieren Sie unter **Wireless-LAN** > **WDS** > **Verbindungen** alle generellen Einstellungen rund um die WDS-Verbindung. Fügen Sie je WDS-Verbindung eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.



WDS-Verbindungsname

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

SSID-Name

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

Modus

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.

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).

Verschlüsselungsprofil

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

Key (PSK)

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

zusätzliche 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]).

zusätzl. untagged VLAN

Untagged-Pakete sollen übertragen werden.

LCOS-Client-Bridge-Unterstützung

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.

Roamingprofil

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

Konfigurieren Sie optional ein Verschlüsselungsprofil unter *Verschlüsselung* auf Seite 81.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil. Siehe *RADIUS-Client* auf Seite 83.

Erstellen Sie bei Bedarf ein Roamingprofil. Siehe *Roaming* auf Seite 83.

4.5.2.2 Verschlüsselung

Konfigurieren Sie unter **Wireless-LAN** > **WDS** > **Verschlüsselung** 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.

Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-PSK-WPA2

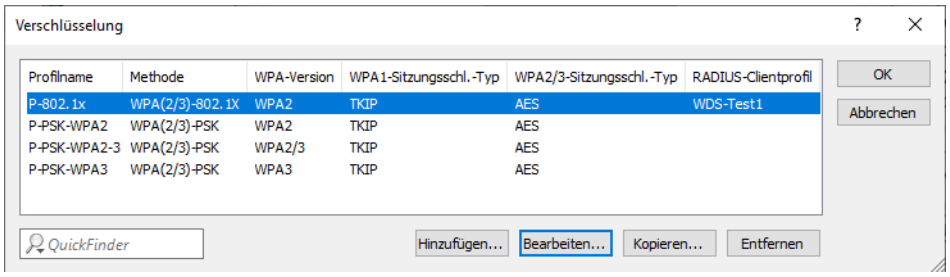
Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.



Profilname

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

Methode

Konfigurieren Sie hier die Verschlüsselungsmethode. Folgende Methoden stehen zur Auswahl:

WPA

WPA(2/3)-PSK: WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal.

RADIUS

WPA(2/3)-802.1X: WPA2 und / oder WPA3 mit RADIUS.

WPA-Version

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode. Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden WPA(2)-PSK und WPA(2)-802.1X verwendet werden. Folgende Versionen stehen zur Auswahl:

- 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.

WPA1-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

WPA2/3-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 und 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

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

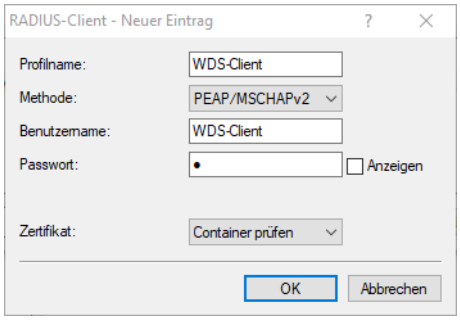
Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

RADIUS-Clientprofil

Geben Sie hier ggf. ein RADIUS-Clientprofil an.

4.5.2.3 RADIUS-Client

Die Einstellungen für ein Einbuchen mittels 802.1X werden unter **Wireless-LAN** > **WDS** > **Client-Einstellungen** > **RADIUS-Client** konfiguriert.



Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

Methode

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von „TLS" ist das Hochladen eines Zertifikates notwendig.

Benutzername

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS" ist hier kein Eintrag notwendig.

Passwort

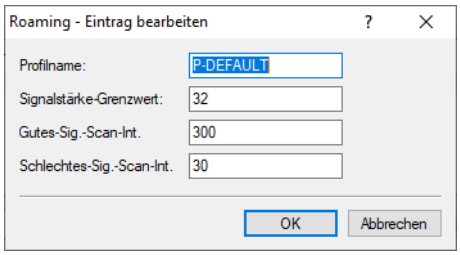
Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS" ist hier kein Eintrag notwendig.

Zertifikat

Sie können das Zertifikat des RADIUS-Servers automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren. Der Zertifikatupload ist nur in der WEBconfig möglich. Siehe *Client-Zertifikat* auf Seite 129.

4.5.2.4 Roaming

Die Einstellungen für das Roaming-Profil werden unter **Wireless-LAN** > **WDS** > **Client-Einstellungen** > **Roaming** konfiguriert.



Profilname

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

Signalstärke-Grenzwert

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.

Gutes-Signal-Scan-Intervall

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.

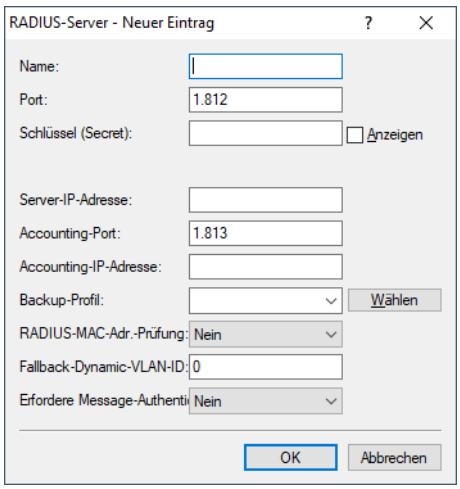
Schlechtes-Signal-Scan-Intervall

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.

4.5.3 RADIUS

Die Einstellungen für RADIUS-Server-Profile zur Verwendung mit WLAN-Netzwerken, die 802.1X als Authentisierungsverfahren verwenden, finden Sie unter **Wireless-LAN** > **RADIUS**.

Konfigurieren Sie die RADIUS-Server-Profile in der Tabelle **RADIUS-Server**.



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.

Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Server zu kontaktieren.

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Schlüssel (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.

Server-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Server erreichbar ist.

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).

Accounting-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Accounting-Server erreichbar ist.

Backup-Profil

Konfigurieren Sie hier ein Backup-Profil, welches verwendet wird, wenn der RADIUS-Server im hier konfigurierten Profil nicht erreichbar ist.

RADIUS-MAC-Adr.-Prüfung

Statt einen Benutzernamen über den RADIUS-Server zu authentifizieren, kann dies auch mit einer MAC-Adresse geschehen.

Erfordere 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.

4.5.3.1 Dynamic VLAN für 802.1X

Mit Dynamic VLAN kann der RADIUS-Server im Rahmen einer 802.1X-Anmeldung die VLAN-ID für den WLAN-Client zuweisen. Clients lassen sich somit dem gewünschten VLAN zuweisen, ohne dafür je VLAN eine separate SSID bereitstellen zu müssen.

Der RADIUS-Server muss dazu folgende Attribute in der Accept-Nachricht mitsenden:

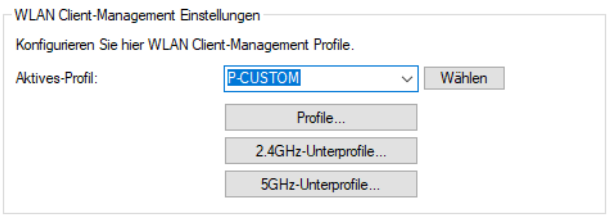
ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS LX
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	13 (VLAN)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	6 (IEEE 802)
81	Tunnel-Private-Group-Id	Definiert die gewünschte VLAN-ID.	1-4096

Besonderheiten bei der Verwendung einer RADIUS-Authentifizierung mit dynamischer VLAN-Zuweisung auf LCOS LX Access Points (802.1X):

Wenn eine RADIUS-Authentifizierung mit dynamischer VLAN-Zuweisung konfiguriert werden soll, gibt es bei LCOS LX-Geräten einige Besonderheiten zu beachten, welche in *diesem Knowledge Base-Artikel zusammengefasst* sind.

4.5.4 Client Management

Die Einstellungen zum Band Steering für WLAN-Netzwerke finden Sie unter **Wireless-LAN** > **Client-Management**.



Aktives Profil

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

P-DEFAULT

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz 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-DISABLED

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

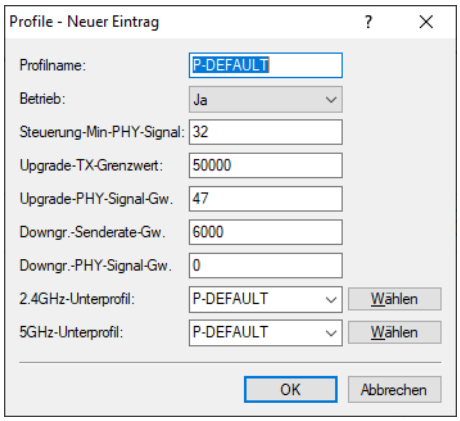
P-LEGACY

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.

4.5.4.1 Profile

Passen Sie unter **Wireless-LAN** > **Client-Management** > **Profile** die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

LANCOM empfiehlt die Verwendung der voreingestellten Profile.



Profilname

Geben Sie diesem Profil einen Namen.

Betrieb

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

Steuerung-Min-PHY-Signal

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

Upgrade-TX-Grenzwert

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

Upgrade-PHY-Signal-Grenzwert

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.

Downgrade-Senderate-Grenzwert

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.

Downgrade-PHY-Signal-Grenzwert

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 **Abwertung-Senderate-Grenzwert** erreicht werden.

2,4-GHz-Unterprofil

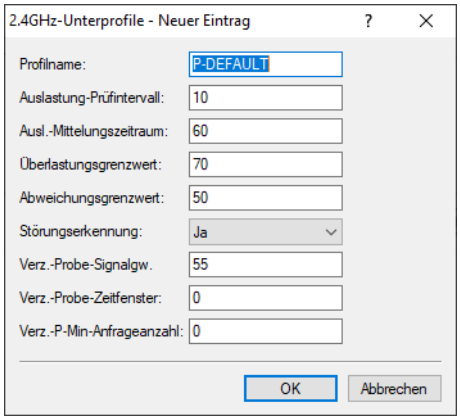
Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

5-GHz-Unterprofil

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

4.5.4.2 2,4-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **2,4 GHz-Unterprofile** die Einstellungen der 2,4-GHz-Unterprofile.



Profilname

Geben Sie diesem 2,4-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

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

Auslastung-Mitteilungszeitraum

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

Überlastungsgrenzwert

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

Abweichungsgrenzwert

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.

Störungserkennung

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

Verzögerung Probe-Signalgrenzwert

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

Verzögerung Probe-Zeitfenster

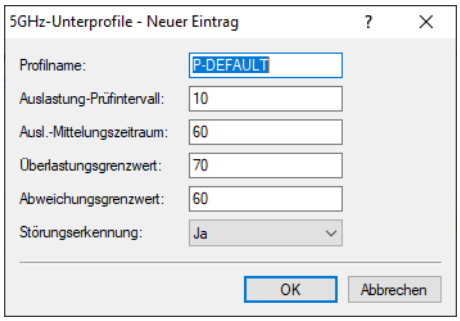
Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Verzögerung Probe-Min.-Anfrageanzahl** konfiguriert wurde, damit diese beantwortet werden.

Verzögerung Probe-Min.-Anfrageanzahl

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Verzögerung Probe Zeitfenster** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

4.5.4.3 5-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **5 GHz-Unterprofile** die Einstellungen der 5-GHz-Unterprofile.



Profilname

Geben Sie diesem 5-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

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

Auslastung-Mitteilungszeitraum

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

Überlastungsgrenzwert

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

Abweichungsgrenzwert

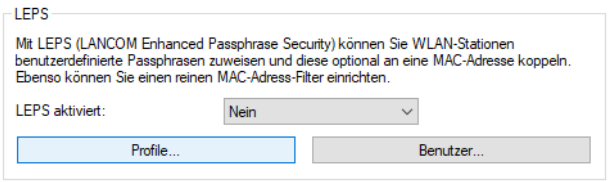
Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Störungserkennung

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

4.5.5 Stationen / LEPS

Die Konfiguration der **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS) finden Sie in LANconfig unter **Wireless-LAN** > **Stationen / LEPS** > **LEPS**. Über den Schalter **LEPS aktiviert** wird LEPS eingeschaltet.



Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profile.

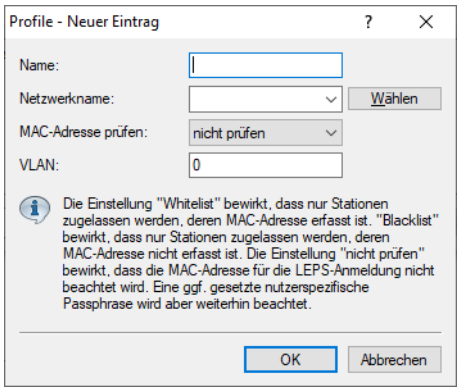
Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

Beachten Sie, dass bei dem Verschlüsselungsmodus WPA2/3 der Client beide WPA-Versionen verwenden kann, was in Verbindung mit LEPS zu unvorhergesehenem Verhalten führen kann.

4.5.5.1 Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.



Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Netzwerkname

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.

MAC-Adresse prüfen

Mögliche Werte:

Nicht prüfen

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

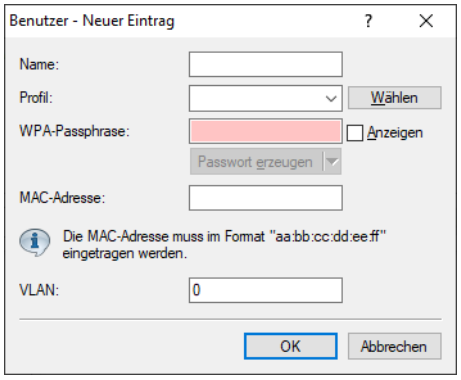
Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer bzw. -Client, der mit diesem Profil verbunden ist, zugewiesen wird.

4.5.5.2 Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.



Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Profil

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.

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der sich der LEPS-Benutzer am WLAN anmelden soll.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

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.

Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

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 beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

4.5.6 WLC

LCOS LX-basierte Access Points können von einem LANCOM WLAN-Controller (WLC) verwaltet werden. Wie bei LCOS-basierten Access Points kommt hierzu das Protokoll CAPWAP zum Einsatz.

Voraussetzung ist ein LANCOM WLAN-Controller mit LCOS-Version 10.40 oder höher.

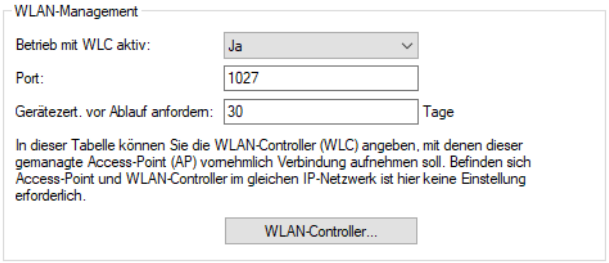
Für Hintergrundinformationen zum WLAN-Management mit LANCOM WLAN-Controllern, konsultieren Sie den Abschnitt „WLAN-Management" im LCOS-Referenzhandbuch.

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 LANCOM Management Cloud zu kontaktieren.

Wird der Access Point von der LANCOM Management Cloud verwaltet und in diesem Zusammenhang durch die LMC eine WLAN-Konfiguration auf den Access Point ausgerollt, wird dieser nicht weiter versuchen, einen WLC 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 mit LANconfig unter **Wireless-LAN** > **WLC** möglich.



Betrieb mit WLC aktiv

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.

Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen. Der Standardwert von 1027 ist der Standardport des CAPWAP-Protokolls. LANCOM WLCs verwenden standardmäßig ebenfalls diesen Port.

Gerätezertifikat vor Ablauf anfordern

Konfiguriert, wie viele Tage vor dem Ablaufdatum das Gerätezertifikat erneuert wird, mit dem sich der Access Point am WLC authentifiziert.

WLAN-Controller

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.

4.5.6.1 Unterstützte Features

In LCOS LX werden folgende Features im Rahmen des WLC-Betriebs unterstützt (aus Sicht des WLAN-Controllers):

Bereich	Feature	Unterstützt?	Anmerkungen
WLAN-Controller > **Allgemein**	Passwortsynchronisation	Ja	
	WLAN-Zeitsteuerung	Ja	
	Angabe alternativer WLAN-Controller	Nein	
WLAN-Controller > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**	LAN am AP mit VLAN-Tagging	Ja	
	WLC-Tunnel	Ja	Ab LCOS LX 5.32 Rel in Verbindung mit LCOS ab 10.42 RU3 auf dem WLAN-Controller
	Verschlüsselung - WPA2	Ja	
	Verschlüsselung - WPA3	Ja	
	Verschlüsselung - Enhanced Open	Ja	
	Verschlüsselung - Enhanced Open Transitional	Nein	
	802.1X	Ja	
	RADIUS-Profile	Ja	
	2,4 / 5 GHz Modus	Ja	
	Autarker Modus	Ja	
	802.11u / Hotspot 2.0	Nein	
	OKC	Ja	
	MAC-Prüfung	Ja	
	RADIUS-Accounting	Ja	
	Inter-Station-Traffic	Ja	
	Fast Roaming	Ja	
	Basisrate einstellbar	Nein	
	Client-Bridge-Unterstützung	Nein	
	Bandbreitenbegrenzung per SSID	Ja	
	Bandbreitenbegrenzung per Client	Ja	Die **Client TX Bandbr.-Begrenzung** funktioniert nicht bei Verwendung eines WLC-Tunnels.
	Maximalzahl der Clients	Ja	

Bereich	Feature	Unterstützt?	Anmerkungen
	Min. Client-Signalstärke	Ja	
	Client-Trennen-Signalstärke	Nein	
	Location Based Services (LBS)	Nein	
	In Unicast konvertieren	Ja	DHCP kann von LCOS LX nicht konvertiert werden. Daher bleibt bei der Einstellung **DHCP** die Unicast-Konvertierung in LCOS LX deaktiviert und bei **DHCP und Multicast** werden nur Multicast-Pakete in Unicast konvertiert.
	Nur Unicasts übertragen	Nein	Mit LCOS LX können Broadcast-Pakete nicht verworfen werden.
	U-APSD	Dauerhaft eingeschaltet	
	Mgmt-Frames verschlüsseln	Ja	
WLAN-Controller > **Profile** > **Physikalische WLAN-Parameter**	Ländereinstellung	Ja	
	2,4 GHz-Modus konfigurieren	Ja	Wird eine vom Access Point nicht unterstützte Einstellung für das 2,4 GHz Band ausgewählt (z. B. 802.11ax in Verbindung mit einem LW-500), kommt es zu einem Profil-Fehler und das WLAN kann auf dem betroffenen Access Point nicht ausgestrahlt werden.
	5 GHz-Modus konfigurieren	Ja	Wird eine vom Access Point nicht unterstützte Einstellung für das 2,4 GHz Band ausgewählt (z. B. 802.11ax in Verbindung mit einem LW-500), kommt es zu einem Profil-Fehler und das WLAN kann auf dem betroffenen Access Point nicht ausgestrahlt werden.
	5 GHz-Unterbänder konfigurieren	Ja	
	DTIM-Periode einstellen	Nein	Die DTIM-Periode ist in LCOS LX fix auf 1 gesetzt.
	Background-Scan-Intervall einstellen	Nein	
	Antennen-Gewinn einstellen	Ja	
	Sendeleistungs-Reduktion einstellen	Ja	LCOS LX berechnet die Reduktion immer ausgehend von 30 dB Sendeleistung. Dadurch ergeben sich für die verschiedenen Frequenzbänder und die Unterbänder im 5 GHz Band folgende Konstellationen: › **2,4 GHz mit 20 dB erlaubter Sendeleistung:** Bei einer Sendeleistungsreduktion von 10 dB muss ein Wert von 20 dB eingetragen werden. › **5 GHz Unterband 1 mit 23 dB erlaubter Sendeleistung:** Bei einer Sendeleistungsreduktion von 3 dB muss ein Wert von 10 dB eingetragen werden.

Bereich	Feature	Unterstützt?	Anmerkungen
			› **5 GHz Unterband 2 mit 30 dB erlaubter Sendeleistung:** Hier ist keine Umrechnung erforderlich. Ein eingetragener Wert von 5 dB ergibt auch 5 dB Sendeleistungsreduktion.
	VLAN-Modul aktivieren	–	Die Aktivierung des VLAN-Moduls ist bei LCOS LX nicht erforderlich und hat keine Auswirkungen.
	ARC: Client Steering	Ja	LCOS LX unterstützt nur **AP-basiertes Band-Steering**. Bei Verwendung der Optionen **Ein** und **Client-Management** wird in LCOS LX das **AP-basierte Band-Steering** aktiviert.
	ARC: Adaptive RF Optimization	Nein	
	QoS nach 802.11e einschalten	Dauerhaft eingeschaltet	
	Indoor-Only-Modus aktivieren	Ja	
	Unbekannte gesehene Clients melden	Nein	
WLAN-Controller > **Profile** > **Erweiterte Profile**	Geräte-LED-Profile	Ja	
	AutoWDS	Nein	
	LBS-Server	Nein	
	Wireless ePaper	Nein	
	Wireless IDS	Nein	
WLAN-Controller > **AP-Update**	Firmware-Management	Ja	
	Skript-Management	Nein	
WLAN-Controller > **Stationen/LEPS**	LEPS-U	Ja	
	LEPS-MAC	Ja	
Sonstiges	ARC: Funkfeldoptimierung	Nein	
	Konfigurations-Verzögerung (WLAN-Profile)	Nein	
	Absende-Adresse (RADIUS-Profile)	Nein	
	IP-Parameter-Profil (AP-Konfiguration)	Ja	
	Antennengruppierung (AP-Konfiguration)	Nein	

4.5.7 Allgemein

LANCOM-UUID verwenden

Alle aktuellen LANCOM Access Points sind Multi-SSID-fähig. D. h., sie können mehreren WLAN-Clients gleichzeitig unterschiedliche „virtuelle" Access Points anbieten.

Bei Geräten mit zwei oder mehr Funkmodulen (Dual Radio) beziehen sich darüber hinaus die BSSIDs der logischen Netzwerke zwar auf das entsprechende Funkmodul, die MAC-Adressen der beiden Funkmodule sind jedoch völlig unabhängig voneinander. Somit lassen sich logische Netzwerke mit unterschiedlicher BSSID nicht eindeutig einem Gerät zuordnen.

Zur Netzwerk-Überwachung und -Planung ist es jedoch sinnvoll, die logischen Netzwerke den entsprechenden Geräten (bzw. Funkmodulen) mittels Tools wie z.B. Ekahau Site Survey zuordnen zu können.

LANCOM Access Points besitzen eine UUID (Universally Unique Identifier), die aus Geräte-Typ und Seriennummer errechnet wird und das Gerät eindeutig im Netzwerk identifizieren kann. Durch eine Verschlüsselung bei der UUID-Erzeugung ist jedoch kein Rückschluss auf Gerät oder Seriennummer möglich.

Sie können die Übertragung der UUID ein- oder ausschalten. Dies ist in der Gerätekonfiguration mit LANconfig unter **Wireless-LAN** > **Allgemein** möglich.

LANCOM-UUID verwenden

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.

4.6 IoT – Das Internet der Dinge (Internet of Things – IoT)

Hier finden Sie die Einstellungen für vom LCOS LX unterstützte IoT-Technologien wie z. B. Wireless ePaper und Bluetooth Low Energy.

Beim IoT werden physische und virtuelle Gegenstände miteinander vernetzt und entstehende Daten und Informationen ausgetauscht. Sensoren, smarte Hausgeräte, digitale Raumbeschilderung oder auch elektronische Preisschilder im Einzelhandel sind typische Beispiele. Die Vernetzung von IoT-Geräten geschieht meist über Funk, zum Einsatz kommen die unterschiedlichsten Funktechnologien wie modifizierte ZigBee-Varianten (Retail IoT), Bluetooth Low Energy (BLE) oder diverse Mobilfunk-Ableger. Einen einheitlichen „IoT-Funkstandard" gibt es nicht, zudem tauchen in kurzen Zyklen neue IoT-Funktechnologien auf.

Die speziellen Einstellungen für IoT erfolgen in LANconfig unter **IoT**.

4.6.1 Wireless ePaper

LANCOM Wireless ePaper Displays bieten Ihnen vielfältige Möglichkeiten zur Anzeige von Informationen – aktualisieren Sie den Belegungsplan Ihres Konferenzraums automatisch und aus der Ferne, erstellen Sie dynamische Wegweiser und Hinweisschilder oder regulieren Sie die Preise Ihrer Waren zentral und in Echtzeit. Die umfangreichen Einstellungsmöglichkeiten erlauben eine individuelle Anpassung an Ihren persönlichen Anwendungsfall.

Die speziellen Einstellungen für den Betrieb der Wireless ePaper Displays erfolgen in LANconfig unter **Extras** > **Optionen** > **Wireless ePaper**. Unter IP / Hostname tragen Sie die IP des Wireless ePaper Servers sowie den zugehörigen Port ein. Der einzustellende Port ist die 8001.

Die Wireless ePaper-Verwaltung starten Sie aus LANconfig über **Extras** > **Wireless ePaper-Verwaltung starten**.

4.6.1.1 Einstellungen für Wireless ePaper

Wireless ePaper Displays von LANCOM bieten eine moderne, digitale Beschilderung für eine Vielzahl an Anwendungen. Die Ansteuerung der Displays basiert auf einer innovativen Funktechnologie mit extrem geringer Leistungsaufnahme.

Für den ePaper-Betrieb ist jeweils ein per USB verbundendes LANCOM Wireless ePaper USB-Erweiterungsmodul erforderlich.

Aktivieren Sie das Wireless ePaper-Funkmodul in LANconfig unter **IoT** > **Wireless ePaper** > **Wireless ePaper**.

Betrieb

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 *LANCOM Support Knowledge Base*. Setzen Sie auf dem gleichen Wege zusätzlich die folgenden beiden Konfigurationsoptionen, um die Kommunikation des Servers mit LCOS LX Access Points zu ermöglichen:

```
accessPointUseThinMode?value=true
accessPointThinUseOutboundMode?value=true
```

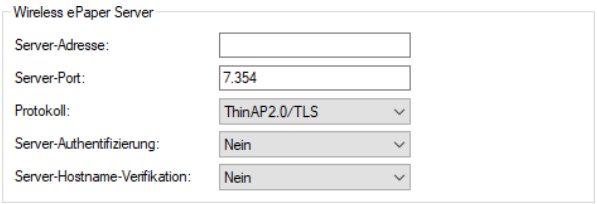
Dies kann z. B. mittels „curl" wie folgt erfolgen:

```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true
curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

Der Legacy-Verbindungsmodus via UDP wird von LCOS LX nicht unterstützt.

Wireless ePaper Server

Konfigurieren Sie den Wireless ePaper Server in LANconfig unter **IoT** > **Wireless ePaper** > **Wireless ePaper Server**.



Server-Adresse

Konfigurieren Sie hier die IP-Adresse des Wireless ePaper Servers, zu dem der Access Point Kontakt aufnehmen soll.

Server-Port

Der TCP-Zielport, welcher für die Kommunikation zum Server verwendet werden soll.

Protokoll

Das für die Kommunikation zum Server verwendete Protokoll.

Server-Authentifizierung

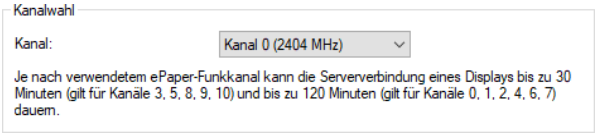
Optional kann der Access Point bei der Verbindungsaufnahme mit dem Wireless ePaper Server dessen Server-Zertifikat überprüfen. Wird diese Option aktiviert, ist zusätzlich ein entsprechendes CA-Zertifikat (bzw. Zertifikatskette) im PEM-Format über die WEBconfig auf den Access Point zu laden.

Server-Hostname-Verifikation

In Zusammenhang mit der Option **Server-Authentifizierung** steuert diese Einstellung, ob überprüft wird, dass der im Zertifikat angegebene „Common Name" mit dem Hostnamen des angesprochenen Wireless ePaper Servers übereinstimmt.

Kanalwahl

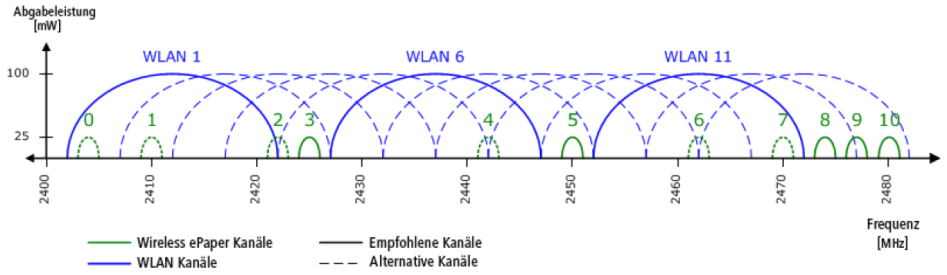
Konfigurieren Sie den Kanal des Wireless ePaper Servers in LANconfig unter **IoT** > **Wireless ePaper** > **Wireless ePaper Server**.



Kanal

Konfigurieren Sie den Funkkanal, der für die Ansteuerung der Wireless ePaper Displays verwendet werden soll.

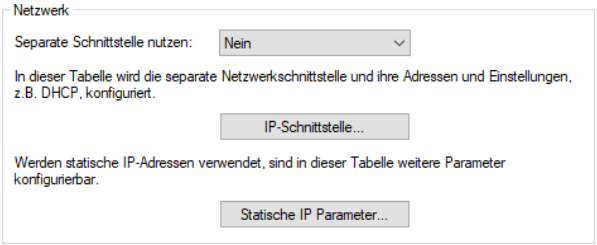
Je nach verwendetem Funkkanal kann die Serververbindung eines Displays bis zu 30 Minuten (Kanäle 3, 5, 8, 9, 10) oder bis zu 120 Minuten (Kanäle 0, 1, 2, 4, 6, 7) dauern. Wählen Sie daher bevorzugt aus Kanäle 3, 5, 8, 9, 10, da diese häufiger von den Wireless ePaper Displays gescannt werden und es keine 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.

Netzwerk

Konfigurieren Sie eine optionale separate Netzwerkschnittstelle des Wireless ePaper Servers in LANconfig unter **IoT** > **Wireless ePaper** > **Netzwerk**. 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.

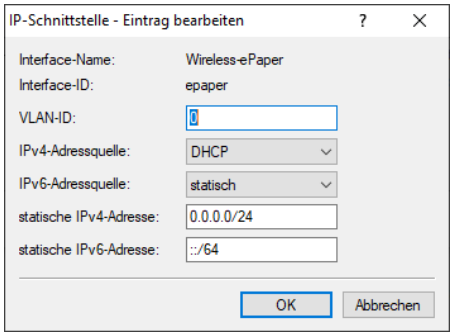


Separate Schnittstelle nutzen

Aktivieren Sie hier ein separates Interface für die Verbindung zum ePaper-Server oder der Vusion Cloud.

IP-Schnittstelle

Konfigurieren Sie hier das separate IP-Interface für die Verbindung zum ePaper-Server oder der Vusion Cloud.



Interface-Name

Das Interface ist hier immer „Wireless-ePaper". Auf dieses beziehen sich die weiteren hier vorgenommenen Einstellungen.

Interface-ID

Der interne Bezeichner für das Interface.

VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll. Der Standardwert „0" bedeutet, dass kein VLAN verwendet wird.

IPv4-Adressquelle

Wählen Sie hier, woher die IPv4-Adresse des Interface bezogen werden soll:

DHCP

Die IP-Adresse wird via DHCP bezogen.

Statisch

Es wird die statisch konfigurierte IP-Adresse für das Interface verwendet.

IPv6-Adressquelle

Wählen Sie hier, woher die IPv6-Adresse des Interface bezogen werden soll:

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.

Statisch

Es wird die statisch konfigurierte IPv6-Adresse für das Interface verwendet.

Statische IPv4-Adresse

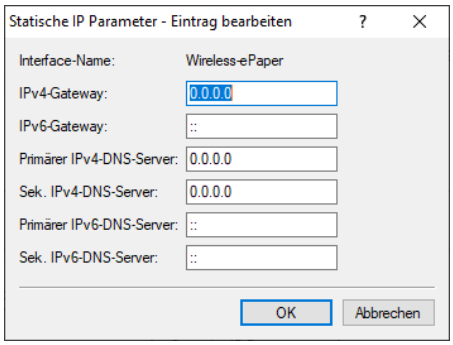
Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv4-Adressquelle **Statisch** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).

Statische IPv6-Adresse

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv6-Adressquelle **Statisch** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Statische IP Parameter

Konfigurieren Sie hier weitere 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 bei der IP-Schnittstelle des Wireless ePaper die IPv4- oder IPv6-Adressquelle **Statisch** gewählt haben. Ansonsten werden alle notwendigen Informationen z. B. via DHCP bezogen, sodass in dieser Tabelle keinerlei Konfiguration notwendig ist.

Interface-Name

Das Interface ist hier immer „Wireless-ePaper“. Auf dieses beziehen sich die weiteren hier vorgenommenen Einstellungen.

IPv4-Gateway

Konfigurieren Sie hier das IPv4-Gateway für das referenzierte Interface.

IPv6-Gateway

Konfigurieren Sie hier das IPv6-Gateway für das referenzierte Interface.

Primärer IPv4-DNS-Server

Konfigurieren Sie hier den primären IPv4-DNS-Server für das referenzierte Interface.

Sekundärer IPv4-DNS-Server

Konfigurieren Sie hier den sekundären IPv4-DNS-Server für das referenzierte Interface.

Primärer IPv6-DNS-Server

Konfigurieren Sie hier den primären IPv6-DNS-Server für das referenzierte Interface.

Sekundärer IPv6-DNS-Server

Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

4.6.2 Bluetooth Low Energy (BLE)

Hier finden Sie die Einstellungen für Bluetooth Low Energy.

Die speziellen Einstellungen für BLE erfolgen in LANconfig unter **IoT** > **Bluetooth LE**.

Betrieb

Schalten Sie das BLE-Radio hier ein, damit fortlaufend Daten über die BLE-Umgebung erhoben werden.

BLE-Scan-Typ

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.

4.6.3 USB

Hier finden Sie die Einstellungen für den USB-Ethernet-Support. Ausgewählte USB-Ethernet-Geräte werden an Access Points mit USB-Port unterstützt. Hierbei kommt das Protokoll CDC-EEM zum Einsatz. Dazu wird das USB-Ethernet-Gerät mit dem LAN des Access Point gebridget. Die Angabe einer VLAN-ID zur Netzsegmentierung ist möglich. Stellen Sie daher sicher, dass das USB-Ethernet-Gerät in Ihrem Netzwerk und ggf. VLAN entsprechend der Herstellerangaben kommunizieren kann. Folgende USB-Ethernet-Geräte sind für den Betrieb mit LCOS LX-basierten Access Points qualifiziert:

- Hanshow HS_C09978 ESL Controller
- SoluM EGU200NA0X ESL GEN2 USB Gateway

Die speziellen Einstellungen für den USB-Ethernet-Support erfolgen in LANconfig unter **IoT** > **USB**.

Betrieb

Schalten Sie den USB-Ethernet-Support hier ein.

VLAN-ID

Optionale Angabe einer VLAN-ID.

4.7 Sonstige Dienste

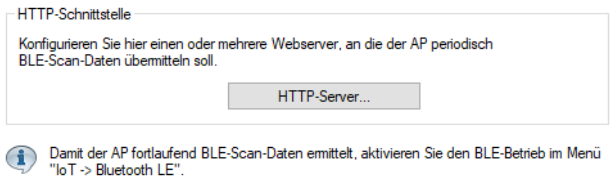
Hier finden Sie die Einstellungen für vom LCOS LX unterstützte Dienste wie z. B. Location Based Services.

4.7.1 Location Based Services (LBS)

Die LANCOM Access Points können als LBS-Client mit einem LBS-Server zusammen arbeiten. Dann melden Sie an den LBS-Server alle in Reichweite befindlichen BLE-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.

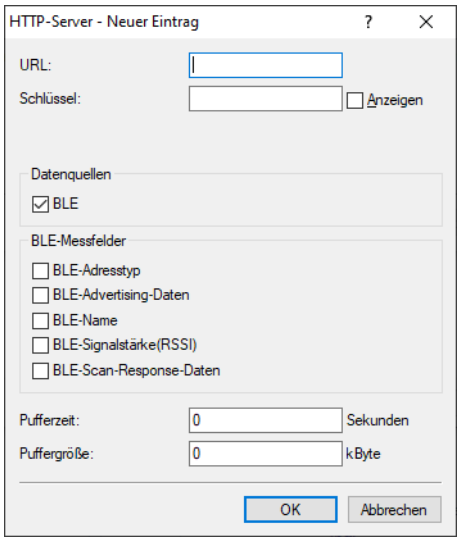
LANconfig: **Sonstige Dienste** > **Location Based Services**



Damit vom Access Point BLE-Daten erhoben werden, muss die BLE-Funktionalität separat eingeschaltet werden. Siehe *Bluetooth Low Energy (BLE)* auf Seite 100 oder *Location Based Services* auf Seite 139.

4.7.1.1 HTTP-Server

Über **HTTP-Server** konfigurieren Sie die HTTP-Endpunkte für die LBS-Daten.



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. Siehe *Location Based Services* auf Seite 139.

Schlüssel

Das Secret (Schlüssel) wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

Datenquellen

Konfigurieren Sie hier, welche Arten von LBS-Daten gesendet werden sollen. Aktuell ist nur BLE verfügbar.

BLE-Messfelder

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.

Pufferzeit

Nachdem die konfigurierte Zeit (in Sekunden) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

Puffergröße

Nachdem die konfigurierte Datenmenge (in Bytes) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

Werden sowohl die **Pufferzeit** als auch die **Puffergröße** auf 0 gesetzt, werden die Nachrichten so rasch wie möglich an den Server gesendet.

Datenformat der an den Endpunkt gesendeten Nachrichten

› Für **BLE**:

```
{
    "deviceMac": "00A0574C49EB",
    "measurements": [
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076493
        },
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076494
            "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
            "scanResponseData": "050974657374"
        }
    ],
    "secret": "",
    "type": "BLE",
    "version": "1.0"
}
```

version

Die Version der verwendeten API. Aktuell ist dies immer 1.0.

secret

Das in der Konfiguration des Access Points festgelegte HTTP-Server-Secret.

type

Der Typ der gesendeten Daten. Kann entweder WLAN oder BLE sein.

deviceMac

Die LAN-MAC-Adresse des Access Point.

measurements

Hierin ist mindestens ein Messwert enthalten. Es können aber auch mehrere enthalten sein.

deviceAddress

Die Adresse des BLE-Gerätes bzw. -Clients.

seenTime

Der Zeitstempel (in Unix-Zeit), zu dem der BLE-Frame vom Client am Access Point empfangen wurde.

addressType

Der BLE-Adresstyp. Folgende Adresstypen sind möglich: `Public` oder `Random`.

rssi

Die Signalstärke in dBm des empfangenen BLE-Frames.

name

Der vom BLE-Gerät übermittelte Name. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

advertisingData

Das komplette vom BLE-Gerät übermittelte Advertisement.

scanResponseData

Die komplette vom BLE-Gerät übermittelte Scan-Response. Kann nur übermittelt werden, wenn der aktive BLE-Scan in den BLE-Betriebseinstellungen aktiviert ist.

5 Features über WEBconfig konfigurieren

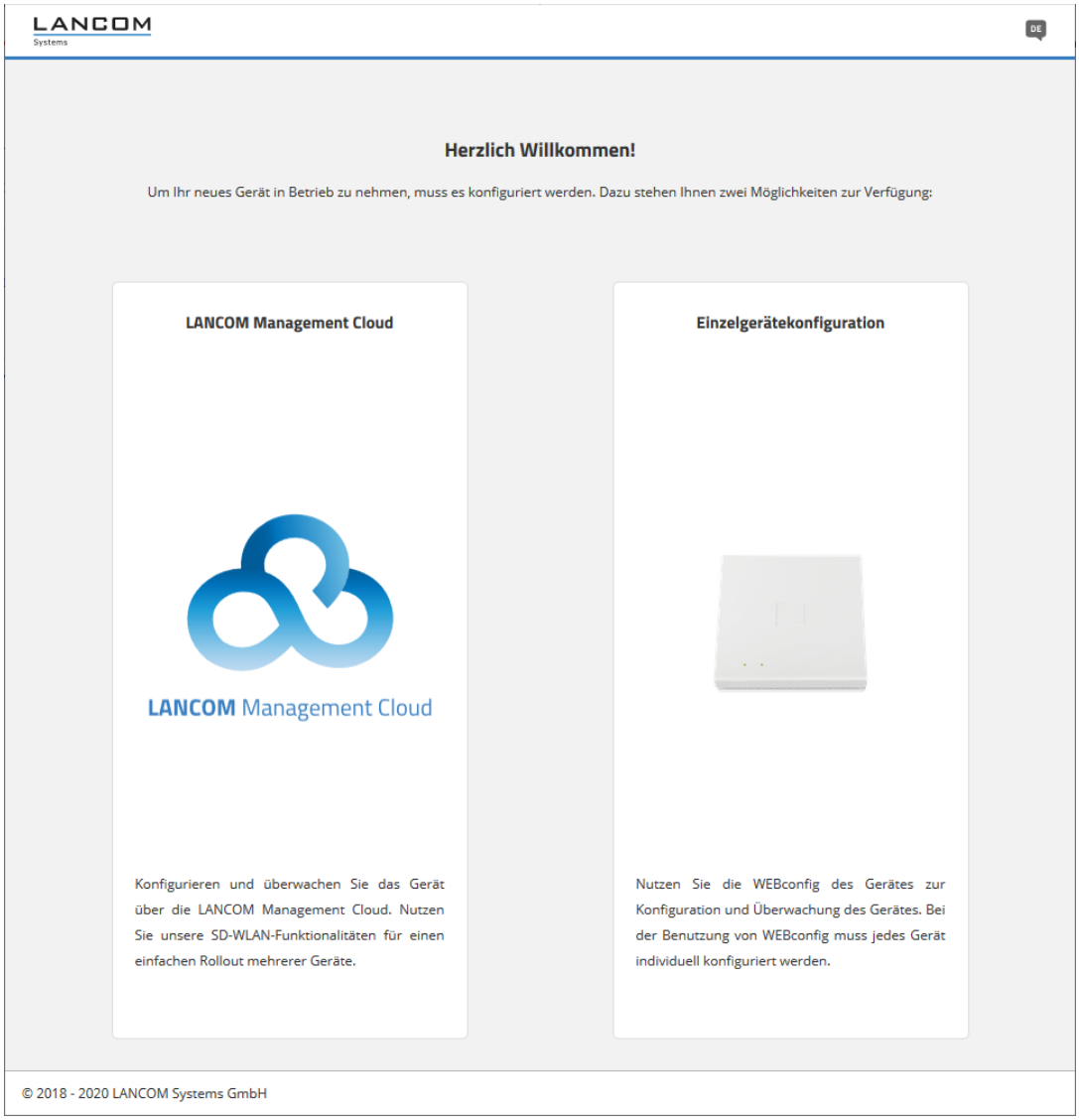
Im Folgenden wird die Inbetriebnahme über WEBconfig sowie alle Einstellungsmöglichkeiten in WEBconfig erläutert. Diese sind abhängig vom Gerät, sodass nicht immer alle aufgeführten Optionen zur Verfügung stehen.

5.1 Inbetriebnahme eines Gerätes über WEBconfig

Sie erreichen die WEBconfig über HTTP und HTTPS. Im Falle von HTTP erfolgt automatisch eine Umleitung auf eine verschlüsselte HTTPS-Verbindung.

Da die WEBconfig mit einem selbst-signierten SSL-Zertifikat arbeitet, muss dieses einmalig (pro Gerät) im Browser als Ausnahme hinzugefügt werden.

Nach Aufruf der WEBconfig-Oberfläche eines unkonfigurierten Gerätes kann ausgewählt werden, ob das Gerät zukünftig mit der LANCOM Management Cloud verwaltet werden soll oder als Stand-alone-Gerät verwaltet werden soll.



Wählen Sie hier durch einen Klick auf die entsprechende Schaltfläche aus, ob das Gerät zukünftig mit der LANCOM Management Cloud verwaltet werden soll, oder als Stand-alone-Gerät verwaltet werden soll.

5.1.1 Verwaltung über LANCOM Management Cloud

Verbinden Sie das Gerät entweder mittels Seriennummer und PIN mit der LANCOM Management Cloud (Zero-Touch) oder geben Sie in das entsprechende Eingabefeld einen Aktivierungscode ein, den Sie vorab in Ihrem LANCOM Management Cloud-Projekt generiert haben:

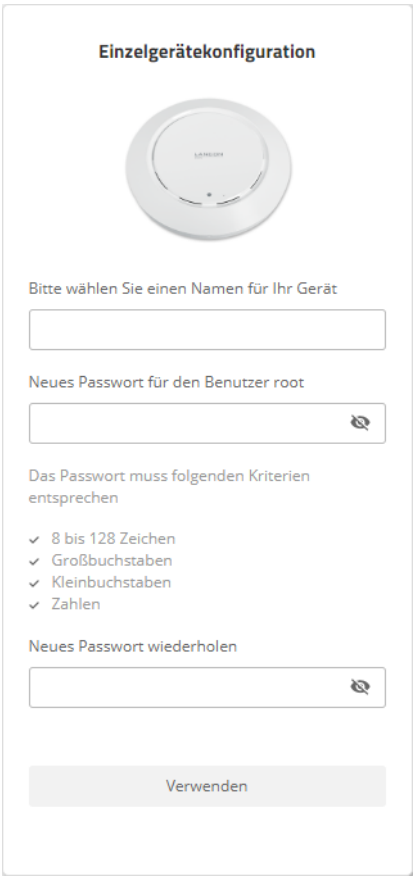
Nach Bestätigung des Aktivierungscodes und Abschluss des Verbindungsvorgangs erhalten Sie eine Erfolgsmeldung und werden auf die Anmeldeseite der WEBconfig weitergeleitet. Das Gerät kann nun über die LMC verwaltet werden.

5.1.2 Verwaltung über Einzelgerätekonfiguration

Legen Sie in den entsprechenden Eingabefeldern einen sprechenden Namen für Ihr Gerät fest und wählen Sie ein Passwort, welches für den Benutzer „root“ verwendet werden soll. Klicken Sie ggfs. auf das durchgestrichene Auge, um sich das von Ihnen eingegebene Passwort anzeigen zu lassen. Dieses Passwort muss die folgenden Kriterien erfüllen:

- mindestens 8 Zeichen
- mindestens ein Buchstabe
- mindestens eine Ziffer
- mindestens ein Sonderzeichen

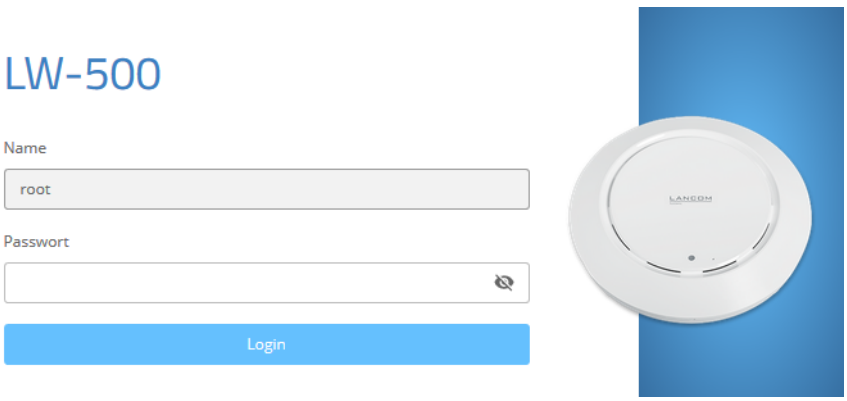
Das hier festgelegte Passwort ist immer für den Benutzer „root“ gültig. Dieser Benutzer wird auch für die spätere Anmeldung an der WEBconfig verwendet.



Nach Klick auf **Verwenden** werden Sie auf die Anmeldeseite geleitet und können sich mit dem Benutzernamen „root“ und dem zuvor festgelegten Passwort an der WEBconfig anmelden.

5.2 Login

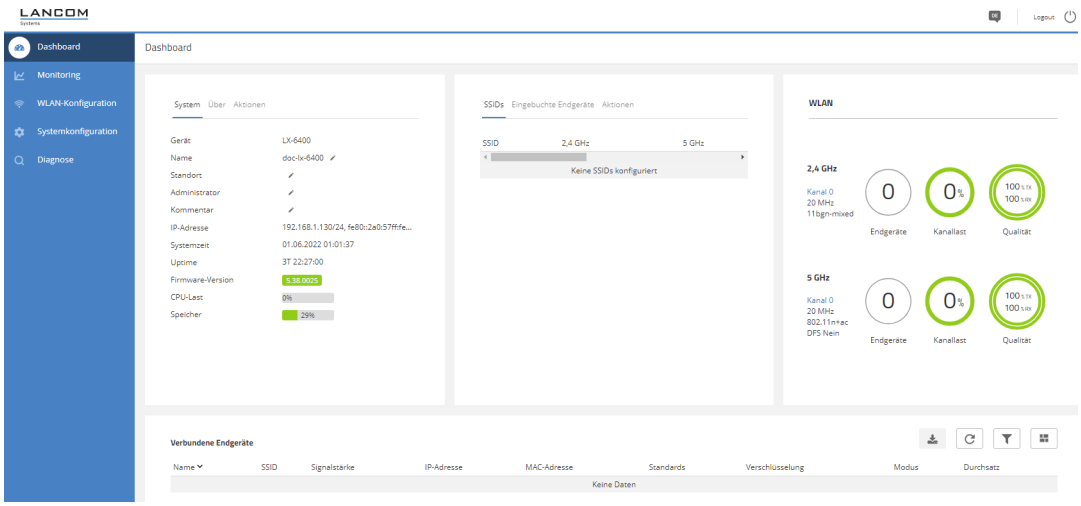
Geben Sie für die Anmeldung den Benutzernamen „root“ und das von Ihnen vergebene Passwort an:



Nach der Anmeldung an der WEBconfig gelangen Sie auf das Dashboard. Informationen zum Dashboard finden Sie im Abschnitt *WEBconfig – Dashboard* auf Seite 108.

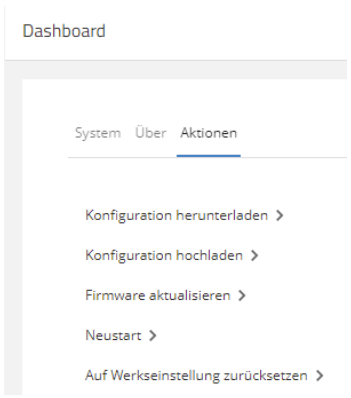
5.3 WEBconfig – Dashboard

Das Dashboard bietet eine Übersicht über die wichtigsten Betriebsdaten Ihres Gerätes.



5.3.1 Aktionen

Innerhalb des Dashboards können Sie in der Systemübersicht mittels des Punkts **Aktionen** die im folgenden beschriebenen Funktionen ausführen.

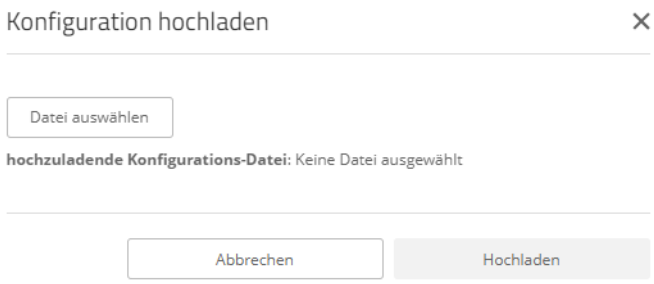


5.3.1.1 Konfiguration herunterladen

Über die Aktion **Konfiguration herunterladen** können Sie eine Gerätekonfiguration im *.lcf-Format Gerät herunterladen. Nach einem Klick auf die Aktion wird die Konfiguration sofort heruntergeladen.

5.3.1.2 Konfiguration hochladen

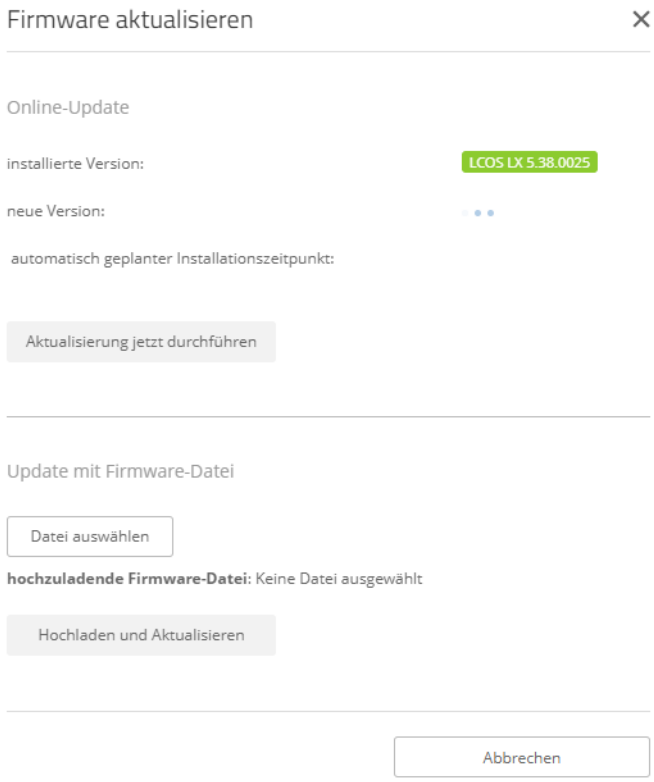
Über die Aktion **Konfiguration hochladen** können Sie eine neue Gerätekonfiguration im *.lcf-Format auf das Gerät hochladen.



Klicken Sie auf **Datei auswählen**, um eine Konfigurationsdatei auszuwählen. Über die Schaltfläche **Hochladen** laden Sie diese Datei anschließend auf das Gerät hoch.

5.3.1.3 Firmware aktualisieren

Über die Aktion **Firmware aktualisieren** können Sie eine neue Firmware auf das Gerät hochladen.



Dazu stehen Ihnen das **Online-Update** und das **Update mit Firmware-Datei** zur Verfügung.

Online-Update

Es wird automatisch nach einer Online zur Verfügung gestellten Firmware gesucht, die neuer als die installierte Version ist. Ggf. wird der automatisch geplante Installationszeitpunkt für diese Version angezeigt, falls der Auto-Updater aktiv

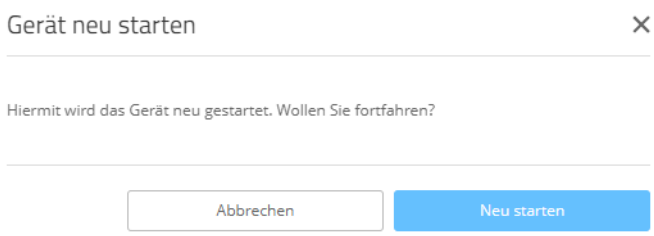
ist. Siehe auch *Software-Update* auf Seite 39 und *Automatisches Firmware Update* auf Seite 132. Über die Schaltfläche **Aktualisierung jetzt durchführen** können Sie die Aktualisierung der Firmware auch sofort durchführen.

Update mit Firmware-Datei

Wählen Sie über **Datei auswählen** eine Firmware-Datei aus, die Sie auf das Gerät hochladen wollen. Dies kann ggf. auch eine vorherige Version sein, auf die Sie zurückgehen wollen. Über die Schaltfläche **Hochladen und Aktualisieren** laden Sie die ausgewählte Firmware-Datei auf das Gerät hoch und aktualisieren somit auf diese Firmware.

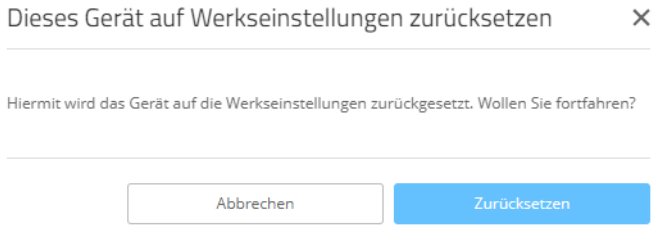
5.3.1.4 Neustart

Über die Aktion **Neustart** wird das Gerät nach einer Sicherheitsabfrage neu gestartet.



5.3.1.5 Auf Werkseinstellung zurücksetzen

Über die Aktion **Auf Werkseinstellung zurücksetzen** wird das Gerät nach einer Sicherheitsabfrage komplett auf die Werkseinstellungen zurückgesetzt.



5.4 Monitoring

Sie erreichen den Bereich Monitoring über den Punkt **Monitoring** in der Sidebar.

Die Monitoring-Ansicht bietet Graphen zur zeitlichen Visualisierung des WLAN-Durchsatzes, des LAN-Durchsatzes, der Anzahl der WLAN-Stationen sowie der Kanalauslastung.

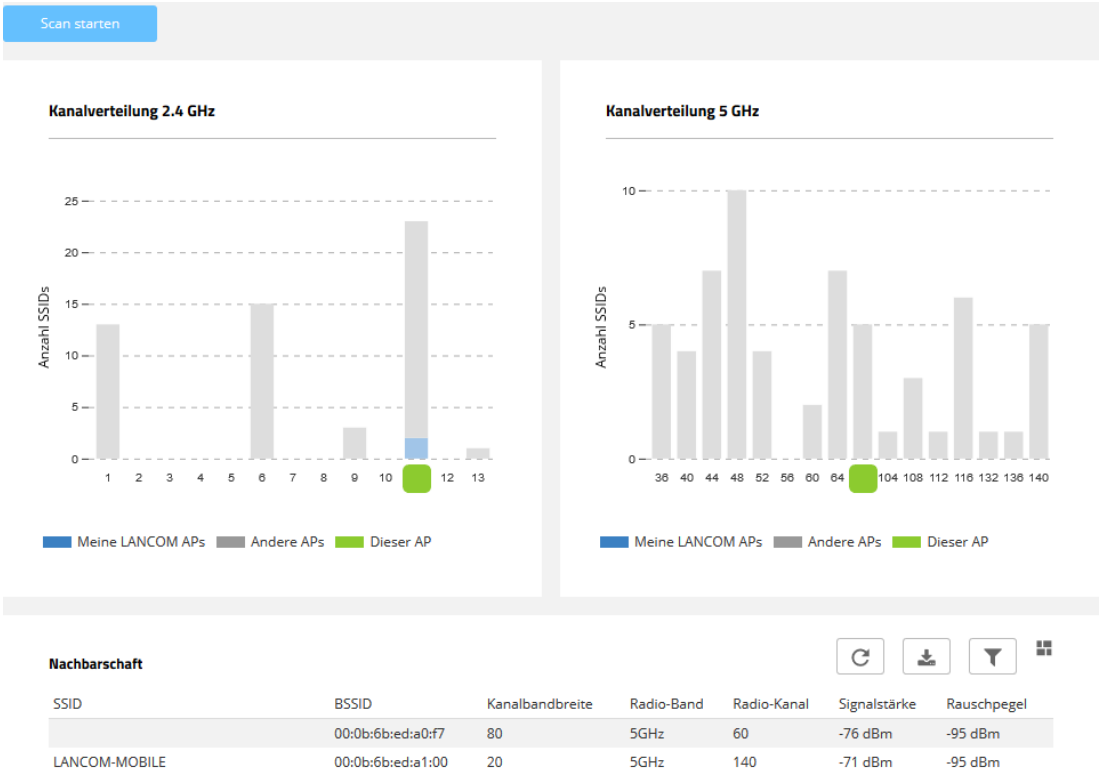
Historische Daten werden maximal für die Laufzeit der aktuellen WEBconfig-Sitzung angezeigt.

5.4.1 Nachbarschaft

Sie erreichen die Nachbarschaftsübersicht über den Punkt **Nachbarschaft** in der Sidebar.

Die Nachbarschaftsübersicht kann dabei helfen, einen Überblick über die WLAN-Umgebung, insbesondere die in der Umgebung aktiven WLAN Access Points und WLAN-Router zu erhalten.

Klicken Sie den Button **Scan starten**, um die WLAN-Umgebung erfassen zu lassen. Nach Abschluss des Scans (Dauer: ca. 10 Sekunden) werden die verschiedenen Diagramme und Tabellen mit den Ergebnissen befüllt:



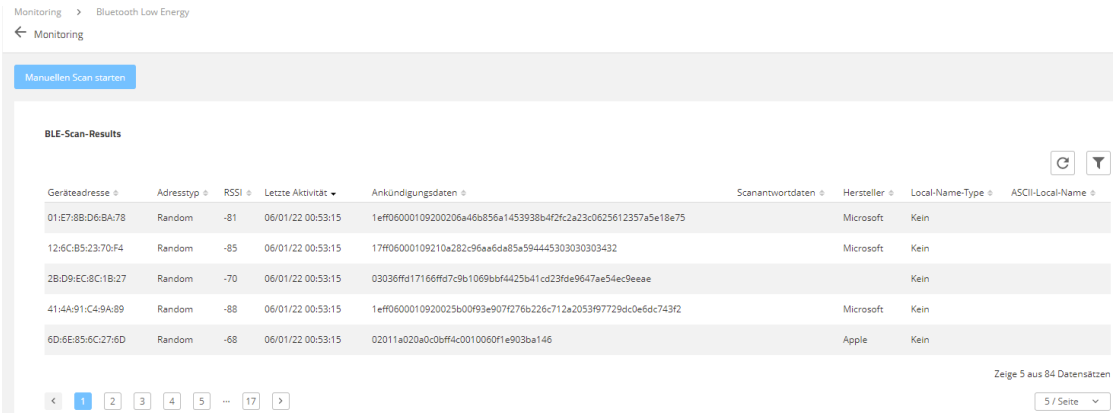
Die oberen beiden Balkendiagramme visualisieren, wie viele SSIDs vom Gerät auf den verschiedenen 2,4-GHz- und 5-GHz-Kanälen erkannt wurden und potentiell eine Belastung des Mediums auf diesem Kanal darstellen. LANCOM Access Points, die vom Scan erkannt wurden und gleicheitig im gleichen LAN-Netzwerk erreichbar sind, wie das aktuelle Gerät, werden in den Diagrammen als „Meine LANCOM APs“ besonders hervorgehoben. Zusätzlich wird visualisiert, auf welchem WLAN-Kanal das aktuelle Gerät selber arbeitet. Die Tabelle **Nachbarschaft** liefert zusätzlich detaillierte Ausgaben zu den vom Scan erkannten SSIDs, z. B. den Namen, die BSSID (MAC-Adresse) und die Signalstärke.

5.4.2 Bluetooth Low Energy

Sie erreichen diese Übersicht über den Punkt **Bluetooth Low Energy** in der Sidebar.

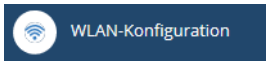
Die **BLE-Scan-Results** geben einen Überblick über die Bluetooth-Umgebung.

Klicken Sie den Button **Manuellen Scan starten**, um die BLE-Umgebung erfassen zu lassen. Nach Abschluss des Scans werden die Ergebnisse angezeigt:



5.5 WLAN-Konfiguration

Sie erreichen diesen Bereich über den Punkt **WLAN-Konfiguration** in der Sidebar.

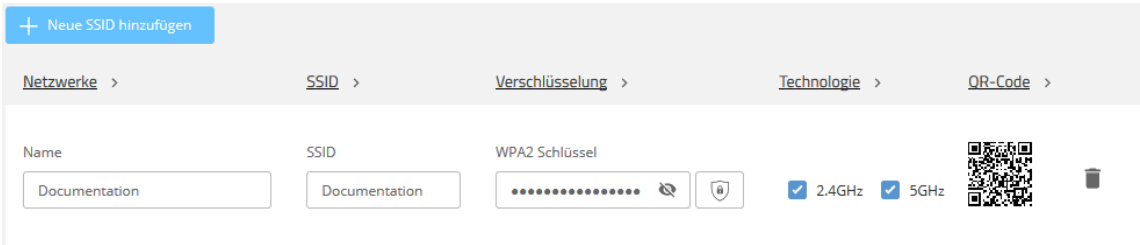


5.5.1 Konzept

Die WLAN-Konfiguration wurde mit dem Ziel entworfen, den Nutzer bei den am häufigsten verwendeten Konfigurationsarbeiten zu unterstützen und die mühevolle Konfiguration kleiner Details unnötig zu machen. Gleichzeitig ist aber weiterhin die Konfiguration davon abweichender Szenarien möglich.

5.5.2 Bedienung

Die angelegten SSIDs werden tabellarisch dargestellt. Klicken Sie auf **Neue SSID hinzufügen**, um eine neue SSID zu konfigurieren. Danach wird eine neue Zeile hinzugefügt. Zur Konfiguration einer SSID mit WPA2-PSK ist nun nur noch das Ausfüllen der Felder **Name**, **SSID** und **WPA2-Schlüssel** erforderlich.



Je nach Bedarf ist es hier auch möglich, einen sicheren WPA2-Schlüssel automatisch generieren zu lassen ( ) sowie die verwendeten Frequenzbänder einzuschränken. Standardmäßig wird die SSID auf 2,4 GHz und 5 GHz ausgestrahlt.

Bei Verwendung der Verschlüsselungsmethode WEP müssen die folgenden Einschränkungen bei Eingabe des WEP-Keys im Feld "WPA2-Schlüssel" 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

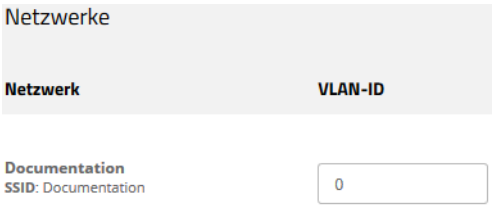
Klicken sie anschließend auf **Speichern**, um die SSID zu übernehmen. Diese wird dann ab sofort vom Gerät ausgestrahlt.

Auf dem 5-GHz-Band kann es bis zu einer Minute nach der erstmaligen Konfiguration dauern, bis die SSID ausgestrahlt wird, da es regulatorisch vorgeschrieben ist, das Band für eine Minute auf Primärnutzer zu überwachen („Radarerkennung", DFS).

Eine weitergehende individuelle Konfiguration ist durch einen Klick auf die jeweilige Überschrift möglich.

5.5.2.1 Netzwerke

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



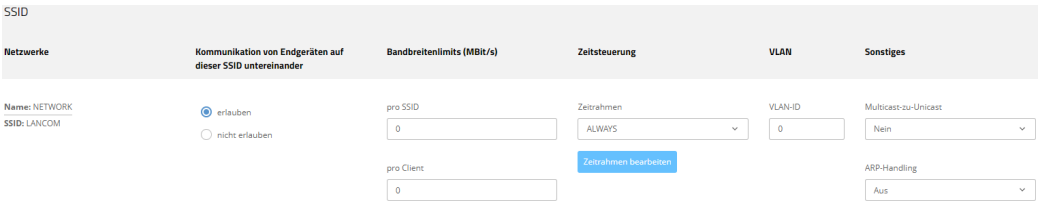
VLAN-ID

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.

5.5.2.2 SSID

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



Kommunikation von Endgeräten auf dieser SSID untereinander

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

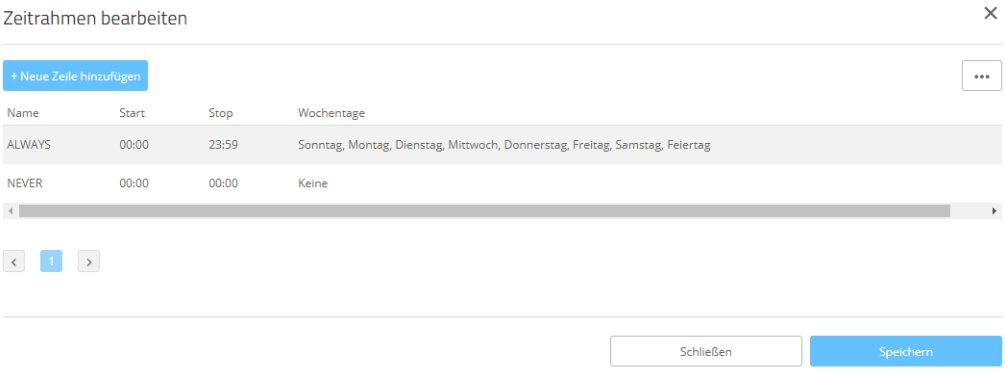
Bandbreitenlimits (MBit/s)

Hier können Sie eine WLAN-Bandbreiten-Begrenzung einstellen, die für das gesamte WLAN-Netzwerk dient (SSID) oder die Bandbreite einschränken, die den Clients jeweils zur Verfügung steht. Alle darin angemeldeten Clients können Daten insgesamt nur mit der hier konfigurierten Übertragungsrate empfangen und senden. Der Wert „0“ bedeutet, dass keine Begrenzung aktiv ist.

Zeitsteuerung

Die Zeitsteuerung über Zeitrahmen wird 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 hier hinzu, damit er für diese SSID beachtet wird.

Zeitrahmen bearbeiten



Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil. Voreingestellt sind die Zeitrahmen ALWAYS und NEVER.

Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stopp

Hier kann die Stoppzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein 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.

Wochentage

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

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

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.

Sonstiges

Multicast-zu-Unicast

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

Nein

Keine Konvertierung durchführen.

Konvertiere zu Unicast

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.

Kapsele in Unicast-Aggregat

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.

Damit das Feature funktioniert, ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren. Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

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.

Aus

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

An

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.

Strikt

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.

5.5.2.3 Verschlüsselung

Für jede eingerichtete SSID können Sie hier ein Verschlüsselungsprofil einstellen. Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-NONE

Keine Verschlüsselung, die SSID ist offen.

P-PSK-WPA2

Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

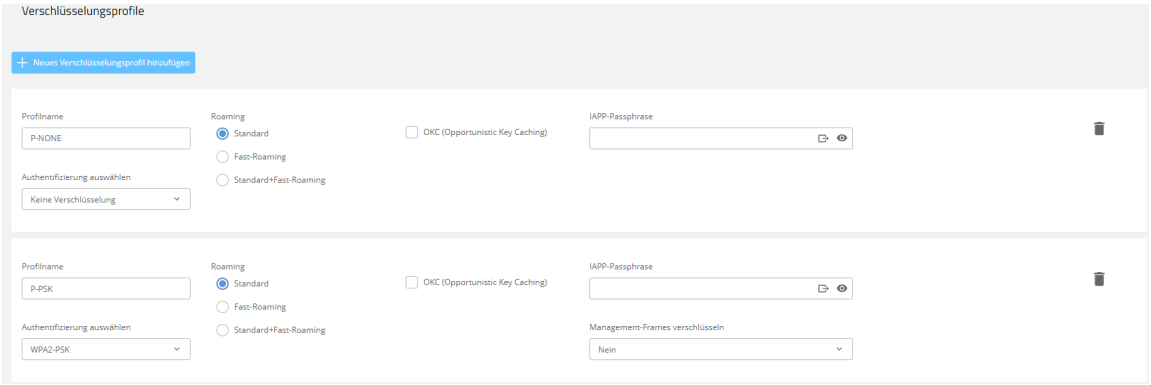
Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WiFi7

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.



Profilname

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

Authentifizierung auswählen

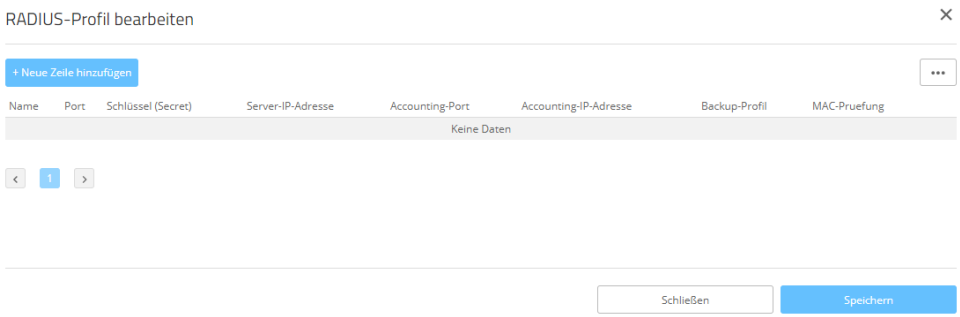
Ändern Sie hier die Verschlüsselungs- und Authentifizierungsmethode. Standardmäßig ist WPA2-PSK (WPA2 mit Pre-shared Key bzw. WPA2-Personal) voreingestellt. Wählen Sie optional **Keine Verschlüsselung** oder aus den folgenden Möglichkeiten:

- WPA3-PSK – WPA3 mit Pre-shared Key bzw. WPA3-Personal

- WPA(2+3)-PSK – WPA2 und / oder WPA3 mit Pre-Shared-Key
- WPA2-801.1X– WPA2 mit 802.1X bzw. WPA2-Enterprise
- WPA3-801.1X– WPA3 mit 802.1X bzw. WPA3-Enterprise
- WPA(2+3)-801.1X– WPA2 und / oder WPA3 mit 802.1X

Im Falle von Verfahren mit Pre-shared Key (PSK) müssen Sie einen **WPA-Schlüssel** eingeben. Schalten Sie die Anzeige über das durchgestrichene Auge um, damit Sie den Schlüssel lesen können. Je nach Bedarf ist es hier auch möglich, einen sicheren WPA-Schlüssel automatisch generieren zu lassen ( )

Im Falle von 802.1X müssen Sie ein RADIUS-Profil anlegen. Klicken Sie dazu auf **RADIUS-Profil bearbeiten** und fügen dort eine neue Zeile hinzu.



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.

Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Server zu kontaktieren.

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Schlüssel (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.

Server-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Server erreichbar ist.

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).

Accounting-IP-Adresse

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Accounting-Server erreichbar ist.

Backup-Profil

Konfigurieren Sie hier ein Backup-Profil, welches verwendet wird, wenn der RADIUS-Server im hier konfigurierten Profil nicht erreichbar ist.

MAC-Prüfung

Statt einen Benutzernamen über den RADIUS-Server zu authentifizieren, kann dies auch mit einer MAC-Adresse geschehen.

Beachten Sie, dass normalerweise dem RADIUS-Server das hier als RADIUS-Client agierende Gerät ebenfalls in seiner Konfiguration bekannt gemacht werden muss.

Sichern Sie die Änderungen durch Klick auf **Speichern**

Roaming

Einstellungen zum Wechsel eines Clients von einem Access Point zu einem anderen Access Point, der die gleiche SSID ausstrahlt.

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 Prä-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r. Siehe auch *Fast Roaming* auf Seite 16.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Standard+Fast-Roaming

Eine Kombination aus dem Standardverhalten 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.

OKC (Opportunistic Key Caching)

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

Authentifizierung von WLAN-Clients über EAP und 802.1X ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation Anwendung. Der Nachteil der Authentifizierung über 802.1X ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und Access Point sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der Access Point Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen Access Points im WLAN-Netzwerk verarbeiten muss.

Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLAN-Controller (WLC) oder zentralen Switch, der alle Access Points im Netzwerk verwaltet. Meldet sich ein Client bei einem Access Point an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem Access Point den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen Access Points eine PMKID und sendet die an den neuen Access

Point in der Erwartung, dass dieser OKC aktiviert hat (deshalb „opportunistisch"). Kann der Access Point mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1X-Authentifizierung aus.

Ein LANCOM Access Point kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle Access Points im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

In von der LANCOM Management Cloud (LMC) verwalteten Netzen oder Netzen aus Standalone-Access-Points werden die PMKs über das IAPP-Protokoll übertragen. In LMC-verwalteten Netzen wird das IAPP automatisch konfiguriert. Sorgen Sie in Netzen aus Standalone-Access-Points dafür, dass das PMK-IAPP-Secret auf allen Access Points des Netzwerks konfiguriert und identisch ist.

IAPP-Passphrase

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.

Management-Frames verschlüsseln

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.

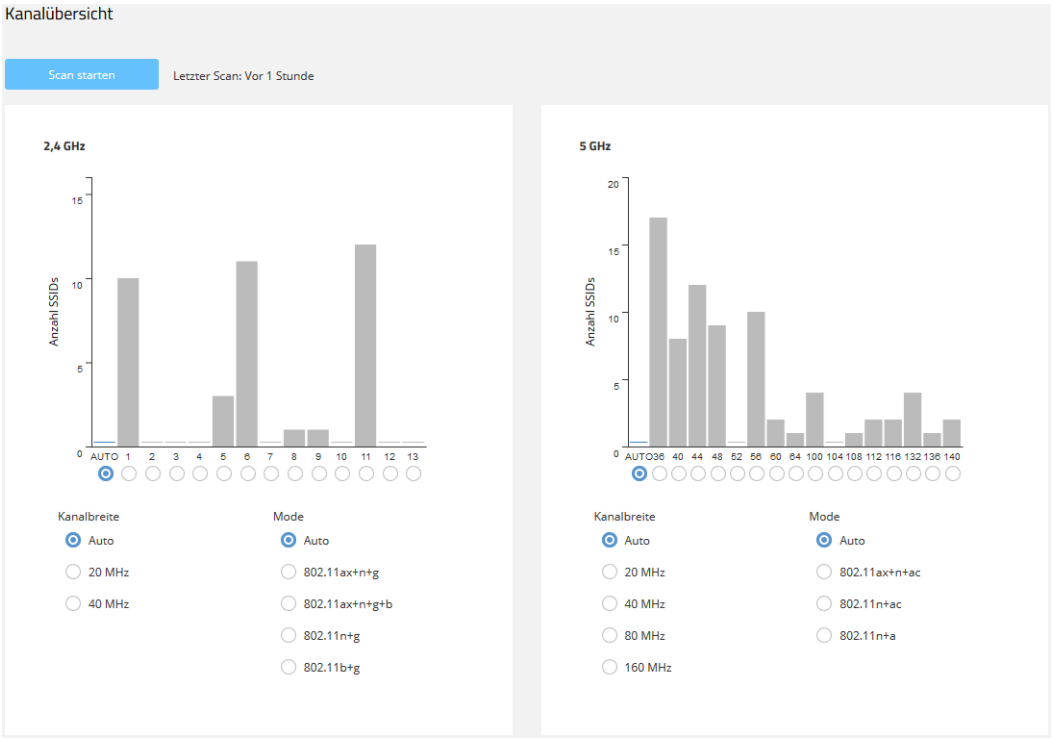
Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf **Notwendig** gesetzt angenommen. Bei WPA2 ist diese Option optional.

5.5.2.4 Technologie

Die Seite **Technologie** bietet die Möglichkeit, feste Kanäle für das 2,4- und 5-GHz-Band festzulegen, sowohl die verwendete Kanalbreite und den verwendeten Radio-Modus zu bestimmen. Voreingestellt ist für alle Möglichkeiten die automatische Auswahl. Weiter unten auf der Seite finden Sie die Einstellungen zum Client-Management.

Die hier konfigurierbaren physikalischen Einstellungen gelten für das gesamte jeweilige Frequenzband und sind nicht SSID-spezifisch.

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

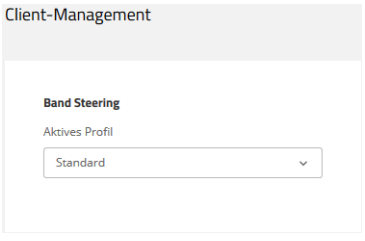


Die beiden Balkendiagramme visualisieren, wie viele SSIDs vom Gerät auf den verschiedenen 2,4- und 5-GHz-Kanälen erkannt wurden und potentiell eine Belastung des Mediums auf diesem Kanal darstellen.

Die Balkendiagramme werden nur mit Informationen befüllt, wenn zuvor entweder hier oder im Bereich **Nachbarschaft** ein Nachbarschaftsscan durchgeführt wurde.

Client Management

Die Einstellungen zum Band Steering für WLAN-Netzwerke finden Sie hier. Mittels Band Steering können Clients vom überlaufenen 2,4-GHz-Frequenzband auf das 5-GHz-Frequenzband gelenkt werden, so dass 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. Siehe auch *Band Steering* auf Seite 15.



Aktives Profil

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

Standard

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz 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.

Ausgeschaltet

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

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.

5.5.2.5 QR-Code

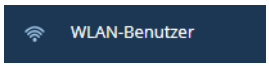
Diese Seite ermöglicht den Zugriff auf einen QR-Code für jede offene oder mit WPA2-PSK gesicherte SSID. Der QR-Code kann von aktuellen Smartphones (ggf. ist eine zusätzliche App erforderlich) gescannt werden und richtet das jeweilige WLAN automatisch auf dem Smartphone ein. So muss keine aufwändige Eingabe eines WLAN-Schlüssels erfolgen.

Zusätzlich besteht die Möglichkeit, einzelne QR-Codes separat auszudrucken.

Es können keine QR-Codes für mit 802.1X gesicherte Netze generiert werden, da diese keinen statischen WLAN-Schlüssel (PSK) verwenden.

5.5.3 WLAN-Benutzer

Sie erreichen diesen Bereich in der WEBconfig über den Punkt **WLAN-Benutzer** in der Sidebar.

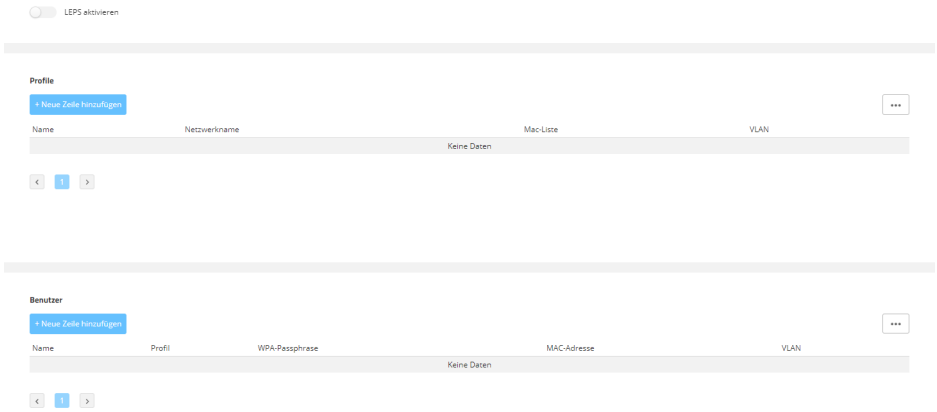


5.5.3.1 LEPS

Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profile.

Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

Hier konfigurieren Sie die **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS). Über den Schalter **LEPS aktivieren** wird LEPS eingeschaltet.



5.5.3.1.1 Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Netzwerkname

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.

MAC-Liste

Mögliche Werte:

Nicht prüfen

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.

VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer bzw. -Client, der mit diesem Profil verbunden ist, zugewiesen wird.

5.5.3.1.2 Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Profil

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.

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der sich der LEPS-Benutzer am WLAN anmelden soll.

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

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.

Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

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 beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

5.5.4 WDS (Wireless Distribution System) / Punkt-zu-Punkt-Verbindungen

Sie erreichen diesen Bereich in der WEBconfig über den Punkt **WDS** in der Sidebar.

Mittels des 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).

Mit LCOS LX 6.10 ist der WDS-Betrieb über eine Strecke von maximal 300 Metern validiert.

5.5.4.1 Verbindungen

Konfigurieren Sie hier alle generellen Einstellungen rund um die WDS-Verbindung. Fügen Sie je WDS-Verbindung eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

WDS-Verbindungsname

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

SSID-Name

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

Modus

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.

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).

Verschlüsselungsprofil

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

Key (PSK)

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

zusätzliche 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]).

zusätzl. untagged VLAN

Untagged-Pakete sollen übertragen werden.

LCOS-Client-Bridge-Unterstützung

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.

Roamingprofil

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

Konfigurieren Sie optional ein Verschlüsselungsprofil unter *Verschlüsselung* auf Seite 126.

Möchten Sie eine Client-Verbindung mittels 802.1X aufbauen, konfigurieren Sie bitte zunächst ein RADIUS-Clientprofil unter *RADIUS-Clientprofile* auf Seite 128.

Erstellen Sie bei Bedarf ein Roamingprofil unter *Roamingprofile* auf Seite 128.

5.5.4.2 Verschlüsselung

Konfigurieren Sie hier 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.

Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-PSK-WPA2

Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

Profilname

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

Methode

Konfigurieren Sie hier die Verschlüsselungsmethode. Folgende Methoden stehen zur Auswahl:

WPA

WPA(2/3)-PSK: WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal.

RADIUS

WPA(2/3)-802.1X: WPA2 und / oder WPA3 mit RADIUS.

WPA-Version

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode. Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden WPA(2)-PSK und WPA(2)-802.1X verwendet werden. Folgende Versionen stehen zur Auswahl:

- 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.

WPA1-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

WPA2/3-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 und 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

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

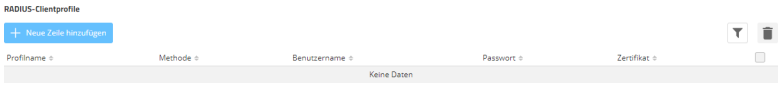
Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

RADIUS-Clientprofil

Geben Sie hier ggf. ein RADIUS-Clientprofil an.

5.5.4.3 RADIUS-Clientprofile

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



Profilname

Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.

Methode

Wählen Sie eine für Ihre Anforderung passende Methode aus. Bei der Verwendung von „TLS“ ist das Hochladen eines Zertifikates notwendig.

Benutzername

Tragen Sie hier den RADIUS-Benutzernamen ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Passwort

Tragen Sie hier das RADIUS-Passwort ein. Bei der Nutzung der Methode „TLS“ ist hier kein Eintrag notwendig.

Zertifikat

Sie können das Zertifikat des RADIUS-Servers automatisch annehmen oder das hochgeladene Zertifikat prüfen lassen. Wir empfehlen immer, ein Zertifikat hochzuladen, um die Integrität des RADIUS-Servers zu verifizieren. Siehe *Client-Zertifikat* auf Seite 129 für den Zertifikatupload.

5.5.4.4 Roamingprofile

Erstellen Sie bei Bedarf hier ein Roamingprofil.

Profilname

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

Signalstärke-Grenzwert

Tragen Sie hier den Schwellenwert ein, ab welchem sich das Scan-Intervall des Access Points verändern soll.

Gutes-Signal-Scan-Intervall

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.

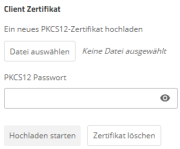
Schlechtes-Signal-Scan-Intervall

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.

5.5.4.5 Client-Zertifikat

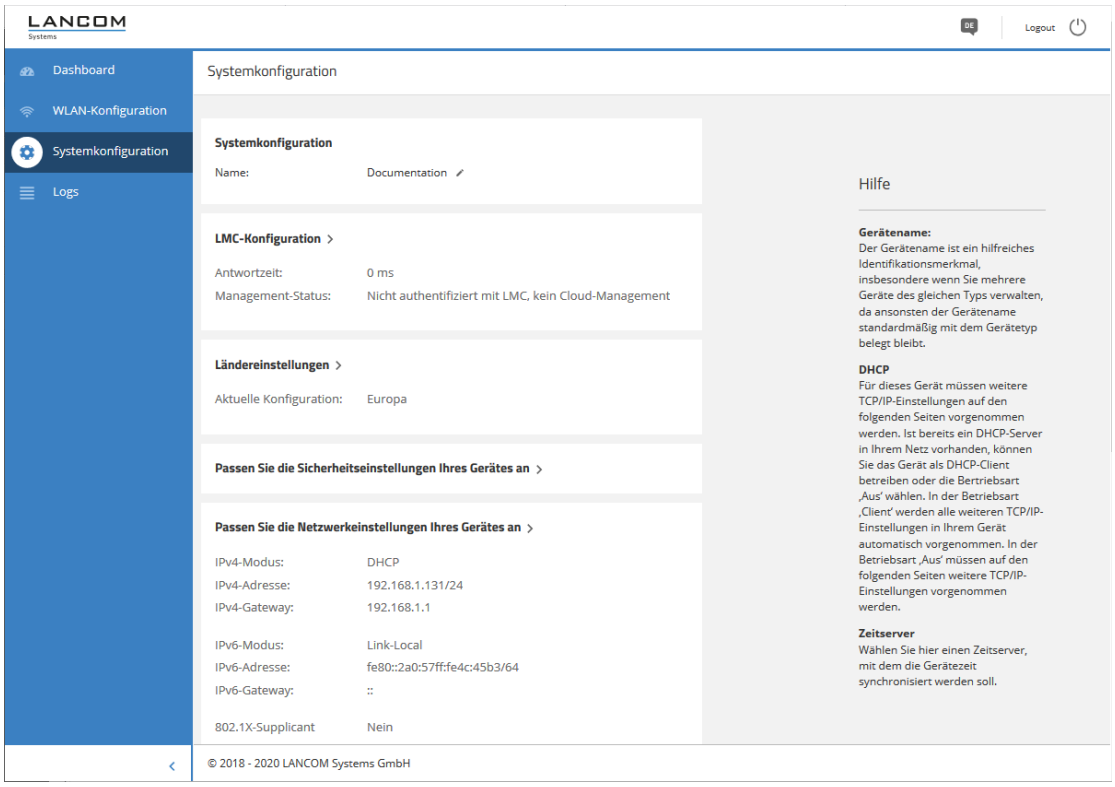
Verwalten Sie hier die Client-Zertifikate für die WDS-Verbindungen.



Wählen Sie einen PKCS12-Container aus und geben das zugehörige Passwort an. Mittels **Hochladen starten** landen Sie das Zertifikat auf das Gerät. Über **Zertifikat löschen** können Sie ggf. vorhandene Zertifikate löschen.

5.6 Systemkonfiguration

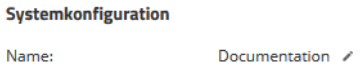
Die Systemkonfiguration bietet die Möglichkeit zur Konfiguration grundsätzlicher Parameter Ihres Gerätes, z. B. den Gerätenamen, die IP-Einstellungen zum Management des Gerätes oder die Aktivierung von SNMP.



Einzelne Felder wie den Systemnamen können Sie nach einem Klick auf den Haken neben diesem direkt bearbeiten. Für Bereiche öffnet sich eine Bearbeitungsmaske nach einem Klick auf die Überschrift.

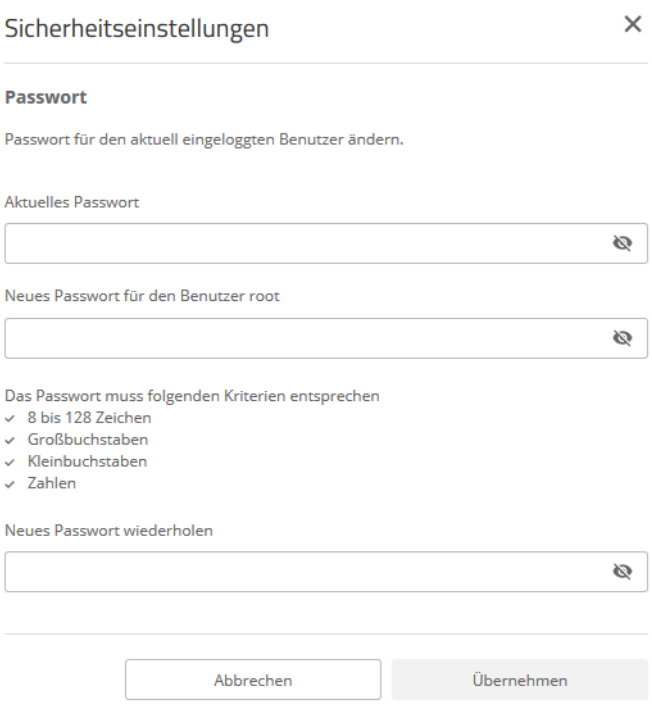
5.6.1 Name

Konfigurieren Sie hier den Gerätenamen.



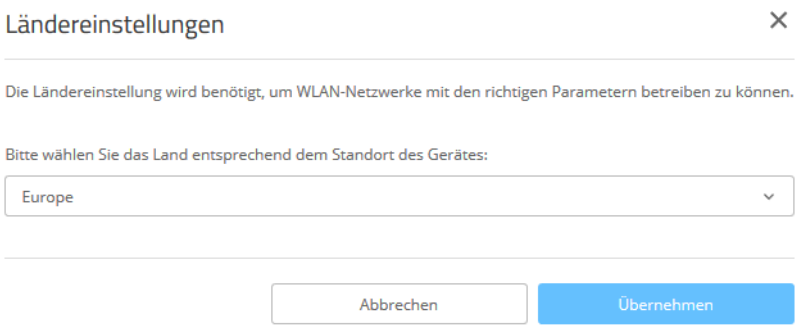
5.6.2 Sicherheitseinstellungen

Ändern Sie hier das Passwort für den aktuellen Benutzer (i. d. R. „root“).

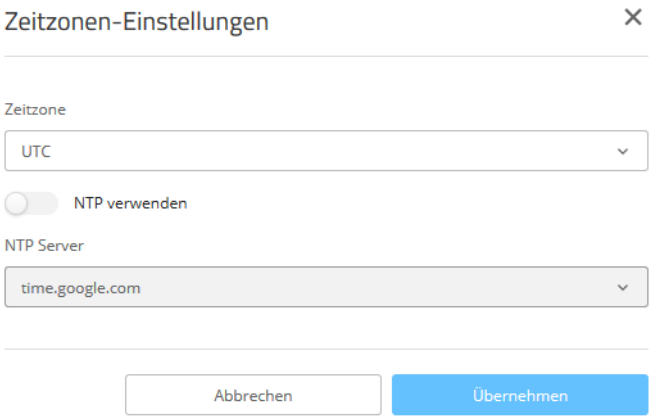


5.6.3 Ländereinstellungen

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



5.6.4 Zeitzonen-Einstellungen



Zeitzone

Wählen Sie eine Zeitzone. Der Standardwert ist „UTC".

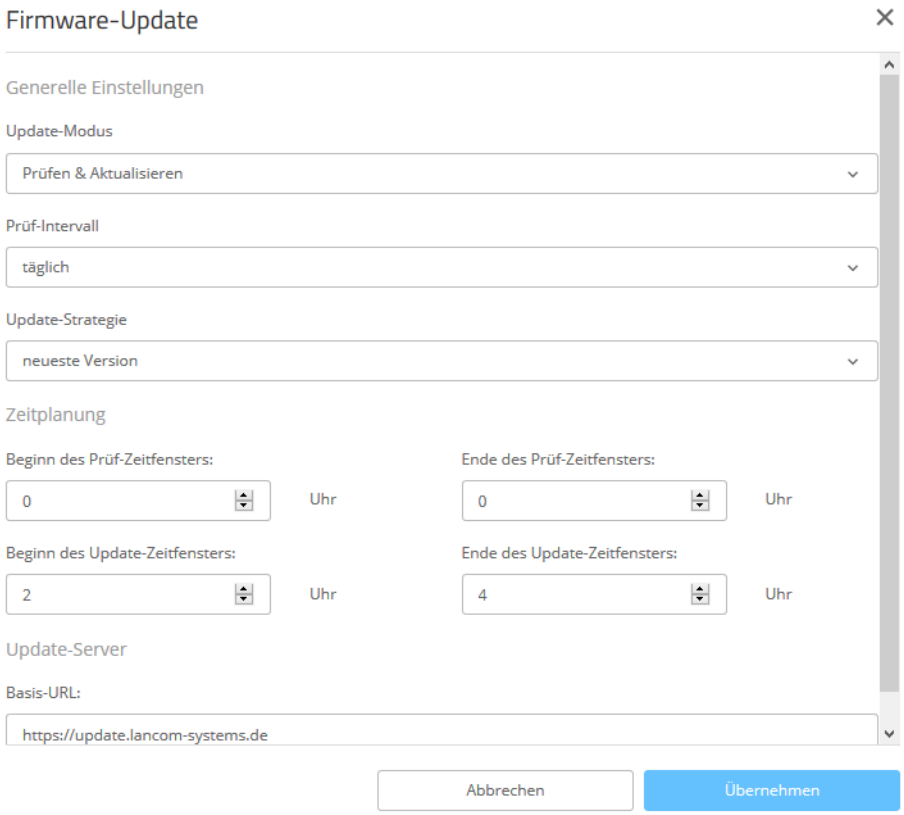
NTP verwenden

Wählen Sie hier, ob die Zeit via Network Time Protocol (NTP) von einem Zeitserver bezogen werden soll.

NTP-Server

Wählen Sie hier einen Zeitserver aus der angebotenen Liste aus, von dem die Zeit via NTP bezogen werden soll.

5.6.5 Automatisches Firmware Update



Update-Modus

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** 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. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. 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.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

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

Manuell

- 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

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

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

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.

aktuelle Version

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.

nur Sicherheitsupdates

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.

neueste Version ohne 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.

Prüf-Zeitfenster

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 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.

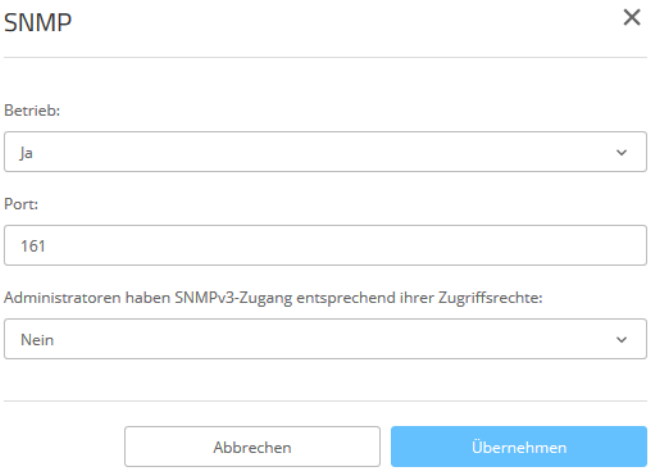
Update-Zeitfenster

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

5.6.6 SNMP



Betrieb

Aktivieren Sie SNMP.

Port

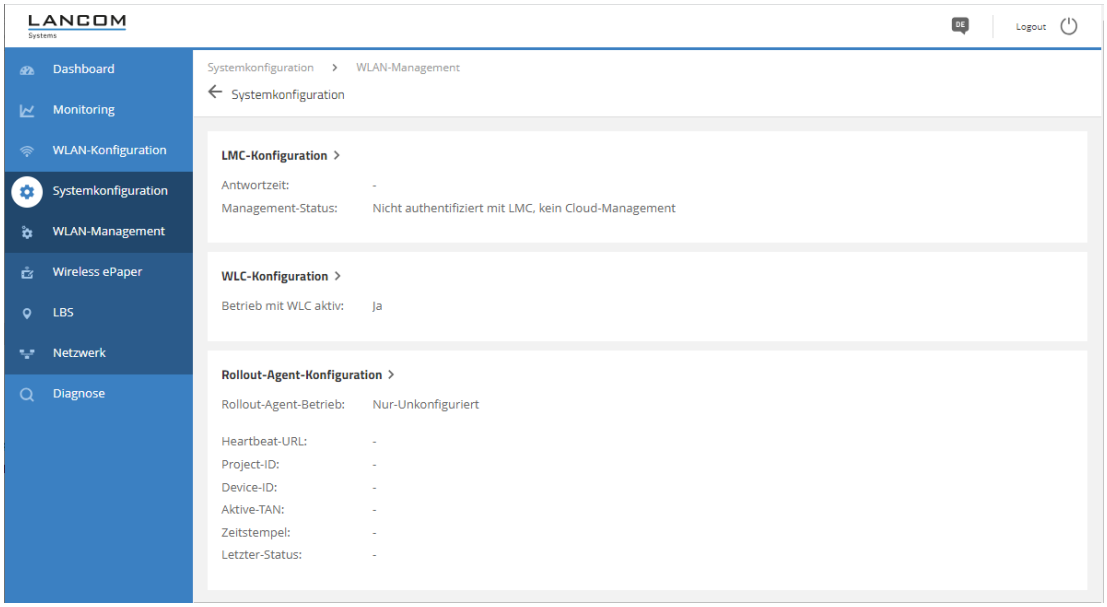
Passen Sie ggfs. den Port für SNMP an. Default: 161

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

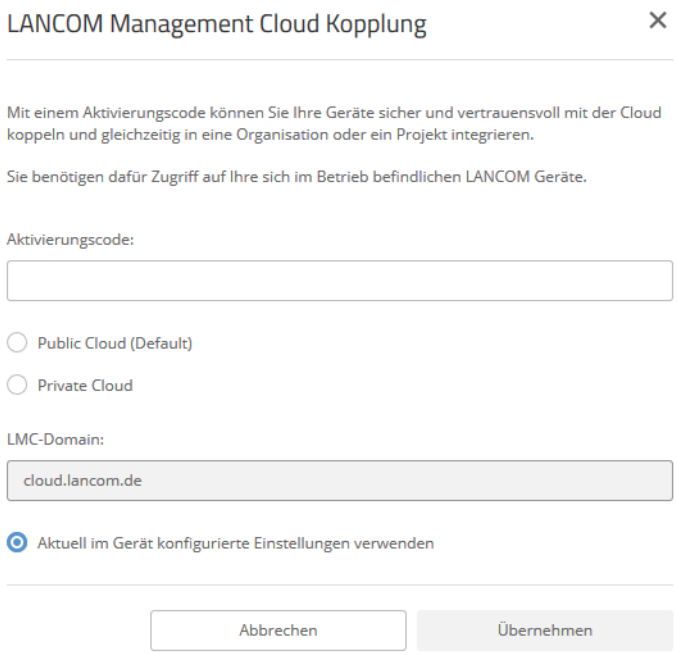
5.6.7 WLAN-Management

In diesem Bereich finden sie Einstellungen zum Management des Access Points über die LANCOM Management Cloud oder einen WLAN-Controller (WLC).



5.6.7.1 LMC-Konfiguration

Koppeln Sie hier ihr Gerät nachträglich mit der LANCOM Management Cloud.



Aktivierungscode

Geben Sie den Aktivierungscode ein, den Sie vorab in Ihrem LANCOM Management Cloud-Projekt generiert haben.

Public Cloud

Diese Option gibt die LMC-Domäne der Public Cloud von LANCOM an.

Private Cloud

Bei dieser Option können Sie die LMC-Domäne ihrer privaten Instanz der LANCOM Management Cloud angeben.

LMC-Domain

Zeigt entweder die LMC-Domäne der Public Cloud an oder Sie geben hier die LMC-Domäne ihrer privaten Instanz der LANCOM Management Cloud an.

Aktuell im Gerät konfigurierte Einstellungen verwenden

Übernimmt die im Gerät bereits konfigurierten Einstellungen.

5.6.7.2 WLC-Konfiguration

Geben Sie hier an, ob ihr Gerät über einen WLAN-Controller gesteuert wird.

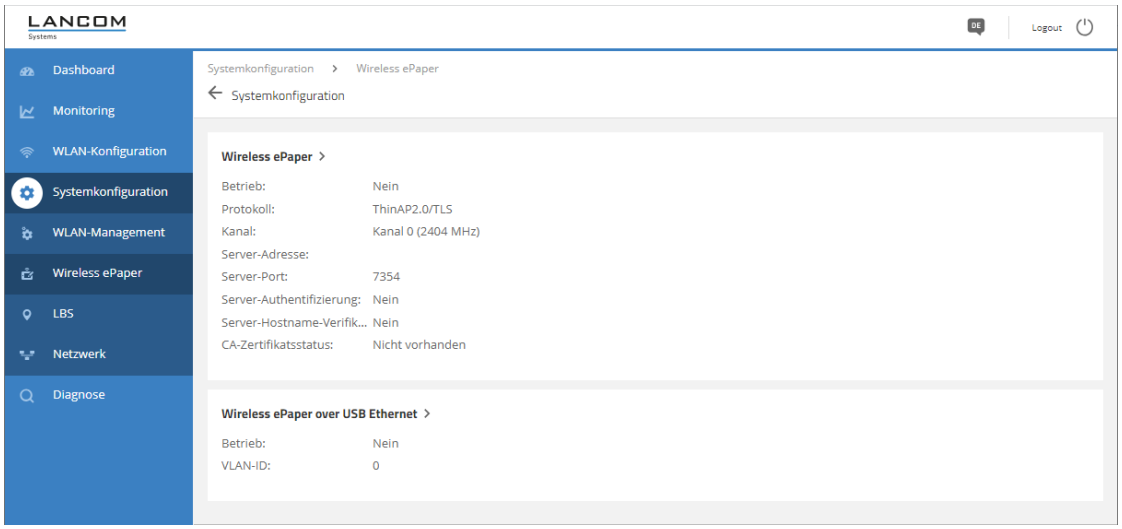
Betrieb

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.

5.6.8 Wireless ePaper

In diesem Bereich finden sie Einstellungen zu Wireless ePaper.

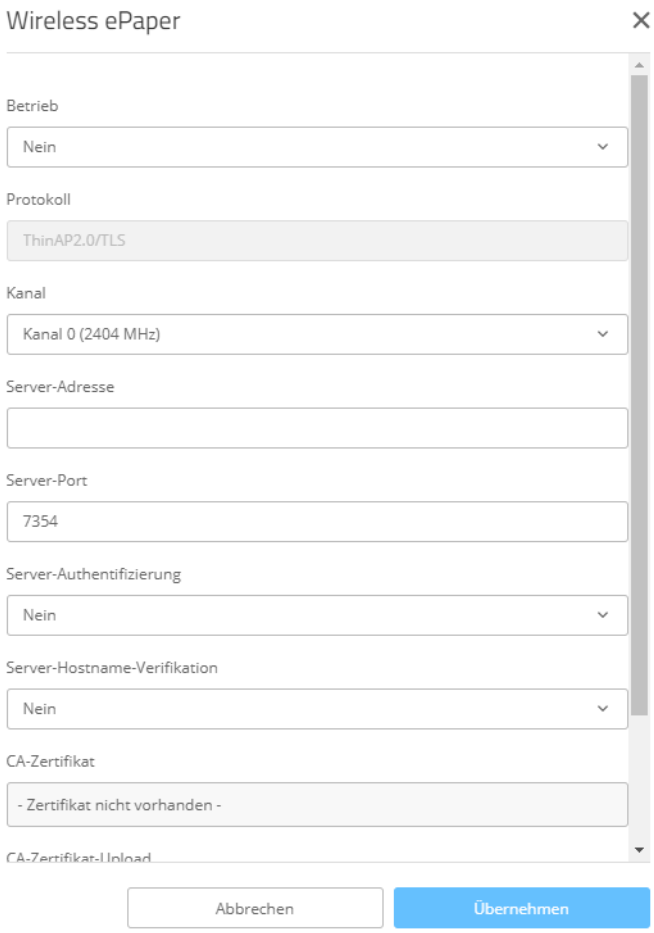


5.6.8.1 Wireless ePaper

LANCOM Wireless ePaper Displays bieten Ihnen vielfältige Möglichkeiten zur Anzeige von Informationen – aktualisieren Sie den Belegungsplan Ihres Konferenzraums automatisch und aus der Ferne, erstellen Sie dynamische Wegweiser und Hinweisschilder oder regulieren Sie die Preise Ihrer Waren zentral und in Echtzeit. Die umfangreichen Einstellungsmöglichkeiten erlauben eine individuelle Anpassung an Ihren persönlichen Anwendungsfall.

Die speziellen Einstellungen für den Betrieb der Wireless ePaper Displays erfolgen in LANconfig unter **Extras** > **Optionen** > **Wireless ePaper**. Unter IP / Hostname tragen Sie die IP des Wireless ePaper Servers sowie den zugehörigen Port ein. Der einzustellende Port ist die 8001.

Die Wireless ePaper-Verwaltung starten Sie aus LANconfig über **Extras** > **Wireless ePaper-Verwaltung starten**.



Betrieb

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 *LANCOM Support Knowledge Base*. Setzen Sie auf dem gleichen Wege zusätzlich die folgenden beiden Konfigurationsoptionen, um die Kommunikation des Servers mit LCOS LX Access Points zu ermöglichen:

```
accessPointUseThinMode?value=true
accessPointThinUseOutboundMode?value=true
```

Dies kann z. B. mittels „curl“ wie folgt erfolgen:

```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true
curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

Der Legacy-Verbindungsmodus via UDP wird von LCOS LX nicht unterstützt.

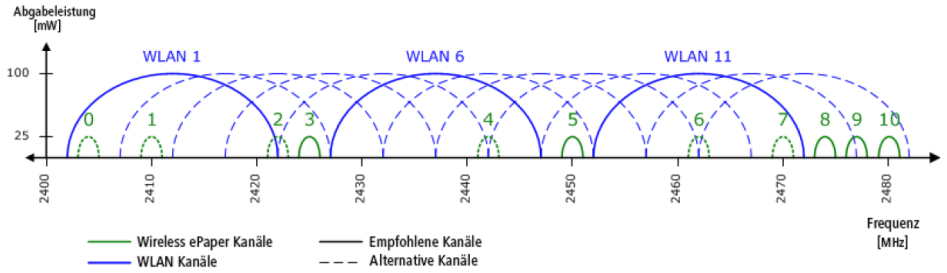
Protokoll

Das für die Kommunikation zum Server verwendete Protokoll.

Kanal

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.

Server-Adresse

Konfigurieren Sie hier die IP-Adresse des Wireless ePaper Servers, zu dem der Access Point Kontakt aufnehmen soll.

Server-Port

Der TCP-Zielport, welcher für die Kommunikation zum Server verwendet werden soll.

Server-Authentifizierung

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.

Server-Hostname-Verifikation

In Zusammenhang mit der Option **Server-Authentifizierung** steuert diese Einstellung, ob überprüft wird, dass der im Zertifikat angegebene „Common Name" mit dem Hostnamen des angesprochenen Wireless ePaper Servers übereinstimmt.

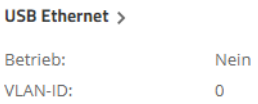
CA-Zertifikat

Falls Sie für die Server-Authentifizierung ein Zertifikat auf das Gerät hochgeladen haben, dann wird dieses hier angezeigt.

CA-Zertifikat-Upload

Bei der Verwendung der Server-Authentifizierung muss zusätzlich ein CA-Zertifikat zur Überprüfung des Servers auf das Gerät hochgeladen werden. Dieses können Sie hier erledigen, indem Sie die Zertifikatsdatei auswählen und anschließend hochladen.

5.6.8.2 Wireless ePaper over USB Ethernet



Hier finden Sie die Einstellungen für den USB-Ethernet-Support. Ausgewählte USB-Ethernet-Geräte werden an Access Points mit USB-Port unterstützt. Hierbei kommt das Protokoll CDC-EEM zum Einsatz. Dazu wird das USB-Ethernet-Gerät mit dem LAN des Access Point gebridget. Die Angabe einer VLAN-ID zur Netzsegmentierung ist möglich. Stellen Sie daher sicher, dass das USB-Ethernet-Gerät in Ihrem Netzwerk und ggf. VLAN entsprechend der Herstellerangaben kommunizieren kann. Folgende USB-Ethernet-Geräte sind für den Betrieb mit LCOS LX-basierten Access Points qualifiziert:

- Hanshow HS_C09978 ESL Controller
- SoluM EGU200NA0X ESL GEN2 USB Gateway

Betrieb

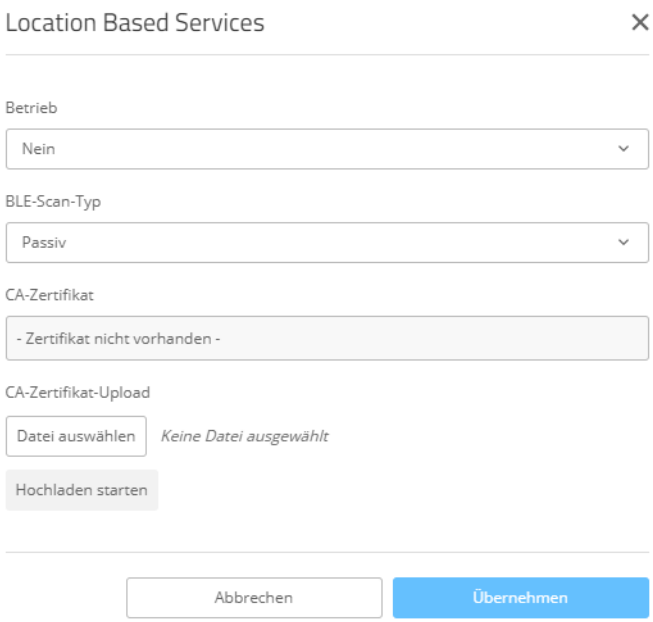
Schalten Sie den USB-Ethernet-Support hier ein.

VLAN-ID

Optionale Angabe einer VLAN-ID.

5.6.9 Location Based Services

Die LANCOM 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. Diese muss über LANconfig konfiguriert werden, siehe *Location Based Services (LBS)* auf Seite 100.



Betrieb

Schalten Sie das BLE-Radio hier ein, damit fortlaufend Daten über die BLE-Umgebung erhoben werden.

BLE-Scan-Typ

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.

CA-Zertifikat

Falls Sie für das HTTPS-Protokoll ein Zertifikat auf das Gerät hochgeladen haben, dann wird dieses hier angezeigt.

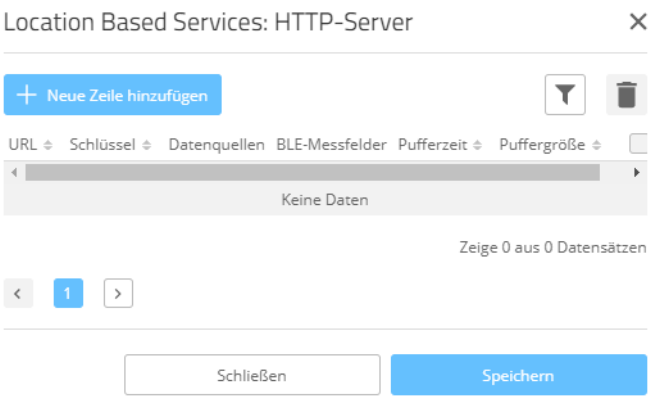
CA-Zertifikat-Upload

Bei der Verwendung von HTTPS muss zusätzlich ein CA-Zertifikat zur Überprüfung des Servers auf das Gerät hochgeladen werden. Dieses können Sie hier erledigen, indem Sie die Zertifikatsdatei auswählen und anschließend hochladen.

Das CA-Zertifikat muss im PEM-Format hochgeladen werden.

5.6.9.1 HTTP-Server

Über **HTTP-Server** konfigurieren Sie die HTTP-Endpunkte für die LBS-Daten.



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. Siehe *Location Based Services* auf Seite 139.

Schlüssel

Das Secret (Schlüssel) wird in den JSON-Nachrichten des Access Points zum Endpunkt übertragen und kann dazu dienen, die Nachrichten zusätzlich zu authentifizieren.

Datenquellen

Konfigurieren Sie hier, welche Arten von LBS-Daten gesendet werden sollen. Aktuell ist nur BLE verfügbar.

BLE-Messfelder

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.

Pufferzeit

Nachdem die konfigurierte Zeit (in Sekunden) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

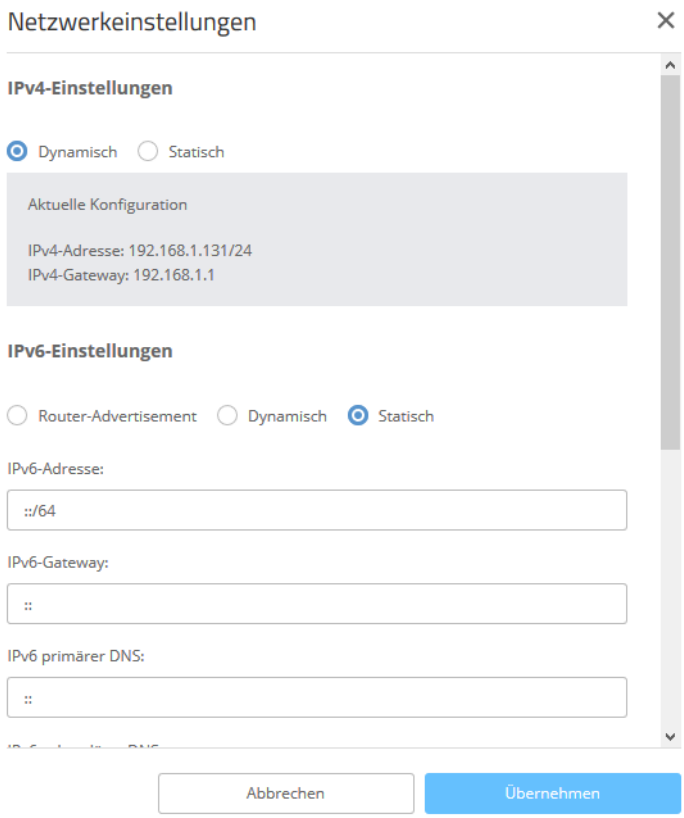
Puffergröße

Nachdem die konfigurierte Datenmenge (in Bytes) erreicht ist, werden alle bis dahin gepufferten BLE-Nachrichten an den Server gesendet.

Werden sowohl die **Pufferzeit** als auch die **Puffergröße** auf 0 gesetzt, werden die Nachrichten so rasch wie möglich an den Server gesendet.

5.6.10 Netzwerkeinstellungen

Hier haben Sie die Möglichkeit, die Netzwerkeinstellungen, wie z. B. die IP-Adresse, Ihres Gerätes anzupasssen.



IPv4-Einstellungen

Dynamisch

Verwendet DHCPv4 zur Konfiguration der IPv4-Parameter. Dies ist der Standardwert.

Statisch

Verwendet die IP-Parameter, die Sie in den folgenden Feldern **IPv4-Adresse**, **IPv4-Gateway**, **IPv4 primärer DNS** und **IPv4 sekundärer DNS** konfigurieren können.

Beachten Sie, dass die IPv4-Adresse in CIDR-Notation angegeben werden muss (z. B. 192.168.1.1/24).

IPv6-Einstellungen

Router-Advertisement

Verwendet Router Advertisements / SLAAC zur Konfiguration der IPv6-Parameter. Ist im empfangenen Router Advertisement das M (managed)-Flag gesetzt, werden weitere Parameter ggf. via DHCPv6 bezogen.

Dynamisch

Verwendet DHCPv6 zur Konfiguration der IPv6-Parameter.

Statisch

Verwendet die IP-Parameter, die Sie in den folgenden Feldern **IPv6-Adresse**, **IPv6-Gateway**, **IPv6 primärer DNS** und **IPv6 sekundärer DNS** konfigurieren können. Dies ist der Standardwert.

802.1X-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.

Benutzername

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

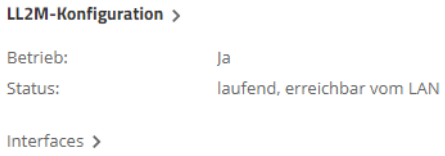
Passwort

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Methode

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

5.6.10.1 LL2M-Konfiguration



Betrieb

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 der Zugriff über die serielle Konfigurationsschnittstelle, die allerdings nicht bei allen Geräten verfügbar ist oder ein Reset des Gerätes auf den Auslieferungszustand. Beide Möglichkeiten setzen 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 **LANCOM 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 *Konsole – Befehlsübersicht* auf Seite 9

Aktivieren Sie hier LL2M.

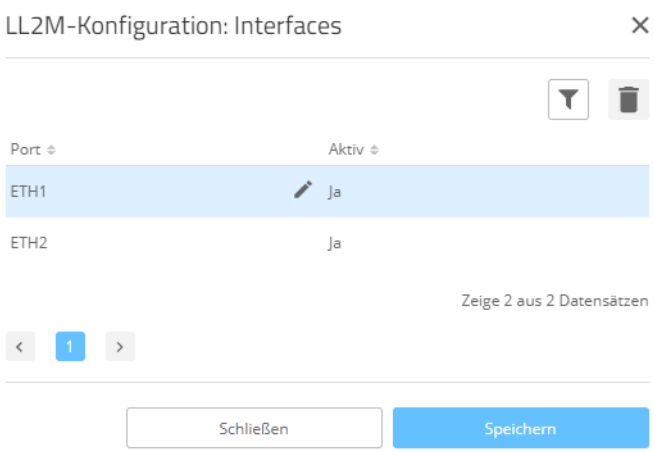
Access Points vom Typ LANCOM LW-500 sind nur über LL2M auffind- und konfigurierbar, wenn LL2M-Pakete den Access Point mit einem VLAN-Tag erreichen, welches in der Konfiguration des Access Points enthalten ist (WLAN-SSID-Konfiguration oder Management-VLAN-Konfiguration).

Status

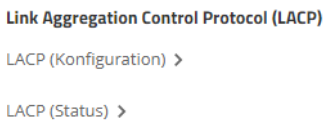
Zeigt den Status der aktuellen LL2M-Konfiguration an.

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.



5.6.10.2 Link Aggregation Control Protocol (LACP)



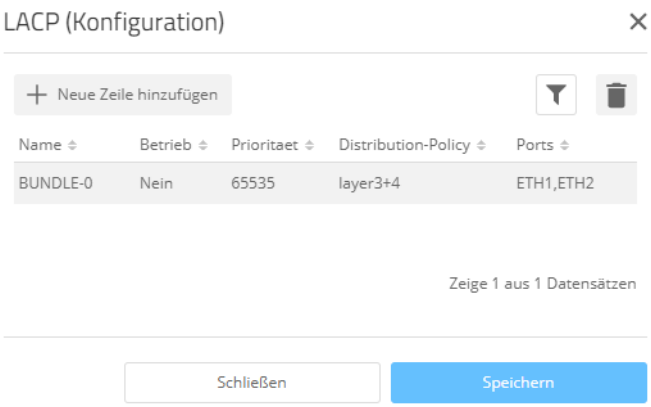
Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von LAN-Ports zu einem virtuellen Link. Physikalische Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, 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.

LANconfig: **Schnittstellen** > **Port-Einstellungen** > **LACP**

5.6.10.2.1 LACP (Konfiguration)

Über **LACP** konfigurieren Sie das Link Aggregation Control Protocol.



Name

Die logische Bündel-Schnittstelle, unter der Sie die gewählten physikalischen Geräte-Schnittstellen bündeln.

Betrieb

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.

Priorität

Tragen Sie hier die LACP-System-Priorität ein. Der Standardwert ist 65.535.

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

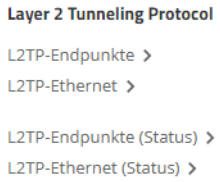
Ports

Über diesen Parameter wählen Sie die physikalischen Schnittstellen als kommaseparierte Liste aus, die das Gerät per LACP bündelt. Default: ETH1,ETH2

5.6.10.2.2 LACP (Status)

Unter **LACP (Status)** werden Ihnen Statusinformationen zu den LACP-Verbindungen angezeigt.

5.6.10.3 Layer-3-Ethernet-Tunnel mit L2TPv3



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.

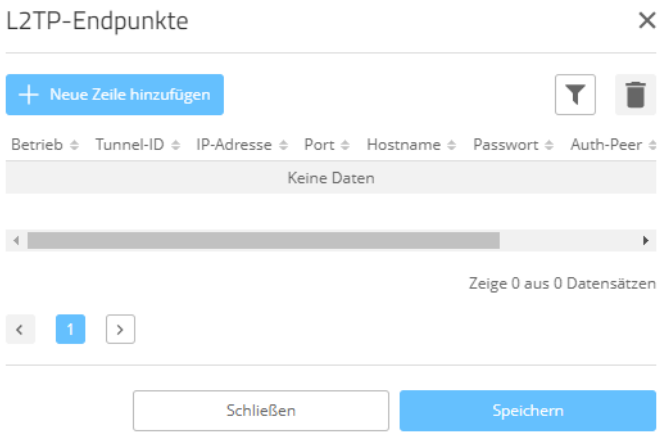
Nutzdaten

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.

5.6.10.3.1 L2TP-Endpunkte

Über **L2TP-Endpunkte** konfigurieren Sie die L2TP-Endpunkte für die L2TPv3-Tunnel. Damit nehmen Sie die Tunnel-Konfiguration für die Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt vor.



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.

Betrieb

Dieser L2TP-Endpunkt ist aktiv oder inaktiv.

IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts.

Port

Der zu nutzende UDP-Port. Default: 1701

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.

Passwort

Das Passwort für die Authentifizierung. Dieses wird auch zur Verschleierung bei der Tunnelaushandlung genutzt, sofern die Funktion aktiviert ist.

Auth-Peer

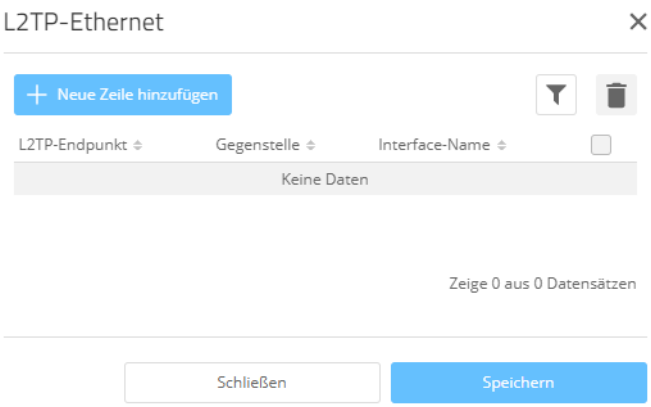
Angabe, ob die Gegenstelle authentifiziert werden soll.

Verstecken

Angabe, ob die Tunnelaushandlung mit Hilfe des angegebenen Passworts verschleiert werden soll.

5.6.10.3.2 L2TP-Ethernet

Über **L2TP-Ethernet** konfigurieren Sie den L2TPv3-Tunnel zwischen einem WLAN-Netzwerk und einem L2TP-Endpunkt.



L2TP-Endpunkt

Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts. Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut.

Gegenstelle

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.

Interface-Name

Die für die L2TPv3-Session zu verwendende virtuelle L2TP-Ethernet-Schnittstelle.

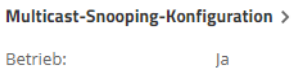
MTU

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. Mögliche Werte: 68-1500

5.6.10.3.3 L2TP-Status

Unter **L2TP-Endpunkte (Status)** und **L2TP-Ethernet (Status)** werden Ihnen Statusinformationen zu den L2TP-Tunneln angezeigt.

5.6.10.4 Multicast-Snooping-Konfiguration



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.

Betrieb

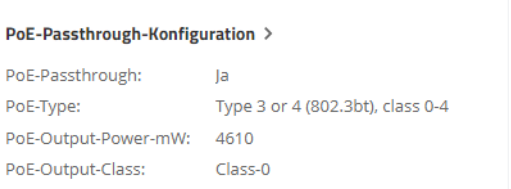
Schalten Sie Multicast-Snooping ein oder aus.

Zusätzlich ist optional eine Konvertierung von Multicast-Datenströmen in Unicast möglich. Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert. Die Pakete werden zwar je Client dupliziert, können aber, da es sich nun um Unicasts handeln, mit der für diesen Client höchstmöglichen Datenrate übertragen werden. Auch wenn die Pakete nun dupliziert werden, wird durch die viel schnellere Übertragung in den meisten Szenarien insgesamt deutlich weniger Airtime verbraucht, die dann für andere Übertragungen zur Verfügung steht. Siehe *Multicast-zu-Unicast* auf Seite 61.

5.6.10.5 PoE-Passthrough-Konfiguration

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. Im Auslieferungszustand ist sie deaktiviert. Zusätzlich werden weitere Statusinformationen hier oder über den LANmonitor angezeigt.



PoE-Passthrough

Schalten Sie die PoE-Passthrough-Funktion hier ein oder aus.

PoE-Type

Statusinformation zum PoE-Type.

PoE-output-Power-mW

Statusinformation zur Energieabgabe in Milliwatt.

PoE-Output-Class

Statusinformation zur PoE-Output-Class.

6 Diagnose

6.1 Trace-Ausgaben

Zur Kontrolle der internen Abläufe im Gerät während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Ein besonderer Vorteil dabei: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Geräte als auch bei der Gegenseite zu finden sein.

Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

6.1.1 Trace – Ein Überblick

Trace-Ausgaben starten Sie in einer Konsolen-Sitzung. Stellen Sie zunächst eine Konsolen-Verbindung zu Ihrem Gerät her. Der Trace-Aufruf erfolgt dann mit dieser Syntax:

```
> trace [--log] [+|-|#|?] <Parameter>
```

Der Befehl trace, der Schlüssel und die Parameter werden jeweils durch Leerzeichen voneinander getrennt. Über die Schlüssel steuern Sie den Trace, während der Parameter die eigentliche Ausgabe bestimmt.

Tabelle 2: Übersicht der Schlüssel

Schlüssel	Bedeutung
`--log`	Ausgabe „historischer" Informationen aus dem Log
`?`	zeigt einen Hilfetext an
`+`	schaltet eine Trace-Ausgabe ein
–	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen den verschiedenen Trace-Ausgaben um („Toggle")
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

Tabelle 3: Übersicht der Parameter

Parameter	Bedeutung	`--log`
WLAN	WLAN-bezogene Ausgaben, z. B. An- und Abmelden von Clients, Schlüsselverhandlungen, …	Ja
	Wenn der Trace nicht aktiv ist, dann werden nur wenige Informationen in das Log eingetragen, sodass die „historischen" Informationen nicht besonders aussagekräftig sind.	
IAPP	Ausgaben zum IAPP (Inter Access Point Protocol).	Ja
Kernel	Ausgaben zum Basissystem und Kernel.	Ja

Parameter	Bedeutung	`--log`
SSH	Ausgaben zum SSH-Dienst.	Ja
*	Joker-Zeichen, welches für alle Dienste steht.	Dienstabhängig

6.1.2 Trace – Bedienung

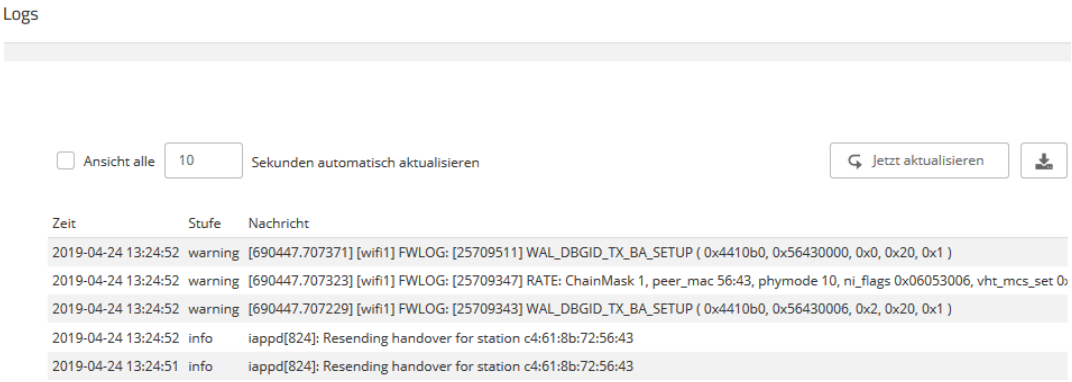
Die folgenden Beispiele dienen zur Veranschaulichung der Trace-Funktionalität:

- Starten eines oder mehrerer Traces:
```
trace + ssh kernel
```
- Stoppen von Traces:
```
trace - ssh kernel
```
- Stoppen aller Traces:
```
trace - *
```
- Umschalten zwischen ein- und ausschalten der Traces („Toggle“):
```
trace # ssh kernel
```
- Ausgeben „historischer“ Informationen, sofern unterstützt und im Log vorhanden:
```
trace --log + kernel
```

6.2 Logs in WEBconfig

Sie erreichen den Bereich „Logs“ über den Punkt **Diagnose** > **Logs** in der Sidebar.

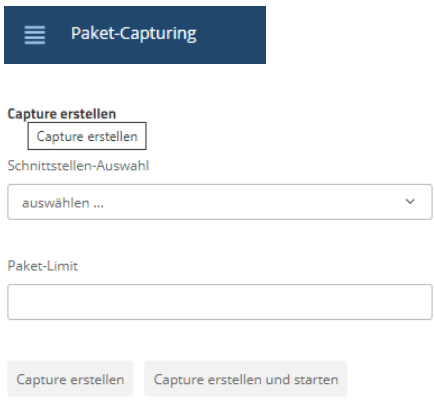
In diesem Bereich wird das Syslog des Gerätes ausgegeben.



6.3 Paket-Capturing in WEBconfig

Hier haben Sie die Möglichkeit zur Aufzeichnung von Wireshark-kompatiblen Paket-Captures.

Sie erreichen diesen Bereich über den Punkt **Diagnose** > **Paket-Capturing** in der Sidebar.

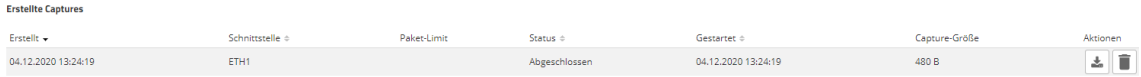


Im Bereich „Capture erstellen" können Sie festlegen, für welche Schnittstelle ein Capture erstellt wird und ob die Capture-Größe über die Anzahl der aufgezeichneten Pakete limitiert werden soll.

Als Schnittstellen stehen sowohl alle Ethernet-Schnittstellen als auch aktive WLAN-SSIDs (getrennt nach Frequenzbändern) zur Auswahl.

Mit Klick auf **Capture erstellen** wird ein Capture-Auftrag mit den gewählten Einstellungen angelegt, aber noch nicht gestartet. Der Capture kann anschließend zu einem beliebigen Zeitpunkt über die Liste „erstellte Captures" gestartet werden. Mit Klick auf **Capture erstellen und starten** wird ein Capture-Auftrag mit den gewählten Einstellungen angelegt und direkt gestartet.

In der Liste „erstellte Captures" können Sie angelegte Captures starten, stoppen und als pcap-Datei herunterladen.



Capture-Daten werden direkt vom Access Point bzw. der WEBconfig in den Cache des Browsers gestreamt. Achten Sie daher darauf, dass beim Schließen der WEBconfig ein einmal gestarteter Capture-Auftrag abgebrochen wird.

Verschiedene Capture-Aufträge können parallel gestartet werden.

6.4 Monitoring der Access Point-Lage und des Montagewinkels

Dieses Feature dient zur Überwachung des Montagewinkels eines Access Points mit entsprechendem Sensor. Modelle wie der LANCOM LX-7500 und der LANCOM LX-7300 sind primär für die Deckenmontage optimiert, wobei auch eine Wandmontage möglich ist. Mittels dieses Sensors lässt sich die Einhaltung einer korrekten Montage auch ohne Vor-Ort-Begehung überprüfen.

Der Access Point meldet die generelle Montageausrichtung Decke / Wand / Boden. „Boden" bezeichnet hierbei eine Montage mit nach oben zeigenden Antennen / Oberseite. Darüber hinaus wird der Winkel bzw. die Neigung des Access Points gemeldet.

Die gemeldetem Werte lassen sich über die CLI unter **Status** > **Hardware-Info** > **Mounting-Type** (1.47.11) bzw. **Status** > **Hardware-Info** > **Mounting-Angle** (1.47.12) auslesen. **Mounting-Type** kann die Werte Unknown (Unbekannt), Ceiling (Decke), Wall (Wand) und Floor (Boden) zurückmelden. **Mounting-Angle** enthält eine Gradzahl.

Die Statusinformationen werden im LANmonitor bei den Systeminformationen des Access Points angezeigt.

6.5 PoE-Statusinformationen

Access Points mit einem entsprechendem Modul ermöglichen eine detaillierte Überwachung der PoE-Stromversorgung.

Dazu meldet der Access Point über die CLI unter **Status** > **Hardware-Info** > **Power** mittels einiger Werte den jeweiligen Status. Diese können auch über den LANmonitor bei den Systeminformationen und den Schnittstellen des Access Points angezeigt werden.

PoE-Type (1.47.42.1)

Zeigt die angeschlossene PoE-Stromquelle als Einzeiler an, anstatt pro Port wie in der Tabelle „Ports". Falls zwei PoE-Stromquellen angeschlossen sind, wird ein String wie „802.3bt-Type-3 + 802.3bt-Type-3" angezeigt.

Ports (1.47.42.6)

Für jeden Port des Access Points werden die folgenden Informationen angezeigt:

PoE-in-Type

Zeigt den Typ der Stromversorgung an: 802.3af-Type-1-or-802.3at-Type-2, 802.3bt-Type-3, 802.3af-Type-1, 802.3at-Type-2 oder no-PoE.

Die Typen IEEE 802.3af Type 1 und IEEE 802.3at Type 2 lassen sich nicht eindeutig erkennen und werden daher als ein Wert angezeigt.

PoE-in-Class

Die Klasse legt genau fest, wie viel Leistung (in Watt) dem Gerät zur Verfügung steht. Folgende Klassen sind möglich: Class-0, Class-1, Class-2, Class-3, Class-4, Class-5, Class-6, Class-7 und Class-8. Die Klasse „None" wird angezeigt, wenn kein PoE-Signal vorhanden ist.

LLDP-Power-Negotiation

Neben der klassenbasierten Aushandlung steht auch die LLDP-Aushandlung zur Verfügung, die auf einer höheren Ebene stattfindet. Dies ermöglicht es dem PD (dem Access Point) und dem PSE (Power Source Equipment, dem Switch), eine Leistung in Watt granular auszuhandeln. Dies ist optional und wird nicht bei allen Switches durchgeführt. Wenn dies verwendet wird, ist das erwartete Verhalten, dass der Switch nur PoE nach IEEE 802.3af Class-0 oder ähnlich, also sehr niedrige Leistung, aktiviert und höhere Leistung nur bei der LLDP-Aushandlung mit dem Access Point aktiviert. In diesem Fall werden Typ und Klasse immer auf einem niedrigen Niveau bleiben, aber Sie können die tatsächlich ausgehandelte Leistung in „PoE-Power-Allocated-W" sehen.

Bitte beachten Sie, dass „PoE-Power-Allocated-W" immer das Maximum der klassenbasierten Verhandlung und der LLDP-basierten Verhandlung anzeigt. Falls es also kein LLDP gibt, aber Class-6 ausgehandelt wurde, wird hier 51W angezeigt.

Device-Functions (1.47.42.7)

WLAN-Streams-2.4GHz

Zeigt die möglichen WLAN-Streams im 2,4 GHz-Band an: Off, One, Two, Three oder Four.

WLAN-Streams-5GHz

Zeigt die möglichen WLAN-Streams im 5 GHz-Band an: Off, One, Two, Three oder Four.

WLAN-Streams-6GHz

Zeigt die möglichen WLAN-Streams im 6 GHz-Band an: Off, One, Two, Three oder Four.

WLAN-Scan-Radio

Zeigt an, ob das Scan-Radio aktiv ist.

USB-Port

Zeigt an, ob der USB-Port aktiv ist.

Failover-Status (1.47.42.10)

Folgende Status sind möglich:

Ready

Wenn beide PoE-Quellen nach IEEE 802.3bt aktiv sind, dann wird auf das Eintreten einer Failover-Bedingung wie z. B. Stromausfall auf einem der beiden Kabel gewartet.

Engaged

Eine Failover-Bedingung wurde erfüllt und der Access Point befindet sich nun im Failover-Status.

Deaktiviert

Failover-Funktion wurde in den Einstellungen deaktiviert, da „Load-Sharing" statt „Failover" eingestellt ist.

Power-Status (1.47.42.11)

Zeigt an, ob der Access Point genug Strom hat, um alle Funktionen zu aktivieren, wie alle WiFi-Radios, USB, etc. („Fully operational") Falls nicht genügend Strom vorhanden ist, wird hier der Wert „Reduced function set" angezeigt. In der Tabelle „Device-Functions" können Sie überprüfen, welche Funktionen genau deaktiviert wurden.

Dual-PoE-Mode (1.47.42.12)

Der konfigurierte Modus.

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 LANCOM 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 LANCOM LX-7500 mit 2x IEEE 802.3at (Klasse 4 / 25,5W).

7 Im Auslieferungszustand aktive Dienste nach EN 18031 GEC-4

In LCOS LX sind folgende Netzwerkdienste im Auslieferungszustand aktiv:

Dienst	Funktion	Port
SSH	Geräte-Management	TCP 22
HTTPS	Geräte-Management	TCP 443
LL2M	Geräte-Management	Layer 2
WTP	WLAN-Controller-Verbindung	UDP 1027
LMC	Verbindung zur LANCOM Management Cloud	TCP 443
TFTP	Geräte-Suche mit LANconfig	UDP 69