connecting your business

Addendum

LCOS 9.00 RC1

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 9.00....6
2 LCMS....7
2.1 Ergänzungen in LANconfig....7
2.1.1 Automatische Authentisierung für den Lesezugriff in LANmonitor....7
2.1.2 Anzeige des Administrator-Benutzernamens....7
2.2 Ergänzungen im LANmonitor....8
2.2.1 Interne IPv6-Unterstützung....8
2.2.2 Anzeige von statischen WAN-IPs im Statusbaum....8
3 Konfiguration....14
3.1 Festlegen eines individuellen SNMP-Ports....14
3.1.1 Ergänzungen im Setup-Menü....14
3.2 Passwortfeld-Schutz für WLAN-Schlüssel....15
3.3 Sortierte Anzeige eines Menüs an der Konsole....15
3.3.1 Management-Ports für den Gerätezugriff anpassen....15
3.3.2 Ergänzungen im Setup-Menü....16
3.4 Kommentarfeld für Zugriffs-Stationen....16
3.4.1 Ergänzungen im Setup-Menü....16
3.5 Elliptic Curve Cryptography (ECC)....17
3.5.1 Ergänzungen im Setup-Menü....18
3.6 Ändern der SIM-Karten PIN....31
3.6.1 Ergänzungen im Status-Menü....31
3.6.2 Ergänzungen im Setup-Menü....32
3.7 Kombinierter UMTS-GPRS-Betrieb für LTE-Geräte....32
3.7.1 Ergänzungen im Setup-Menü....32
4 IPv6....34
4.1 Dual-Stack Lite (DS-Lite)....34
4.1.1 Ergänzungen im Status-Menü....35
4.1.2 Ergänzungen im Setup-Menü....39
4.2 IPv6-Unterstützung für RAS-Dienste....40
4.2.1 RAS-Schnittstellen....41
4.2.2 Präfix-Pools....42
4.2.3 Ergänzungen im Setup-Menü....42
4.3 Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste....49
4.4 Loopback-Adressen für IPv6....50
4.4.1 Loopback-Adressen....50
4.4.2 Ergänzungen im Setup-Menü....51
4.5 Lightweight-DHCPv6-Relay-Agent (LDRA)....52
4.5.1 Ergänzungen im Setup-Menü....54
4.6 Router-Advertisement-Snooping....58
4.6.1 Ergänzungen im Setup-Menü....59

5 RADIUS.....61

5.1 Getrennte RADIUS-Accounting-Server pro SSID 61

5.1.1 Ergänzungen im Setup-Menü.....61

5.2 Zugang zum RADIUS-Server über IPv6.....65

5.2.1 Ergänzungen im Setup-Menü.....66

5.3 Zusätzliches Shell-Privilege-Level-Attribut im RADIUS-Server.....67

5.3.1 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen.....67

5.3.2 Ergänzungen im Setup-Menü.....70

5.4 RADIUS-Client: Alternative Angabe von Hostnamen statt IP-Adressen.....71

5.4.1 Ergänzungen im Setup-Menü.....72

5.5 EAP-SIM-Modul im RADIUS-Server.....75

5.5.1 Ergänzungen im Setup-Menü.....75

6 Public Spot.....82

6.1 Rufnummernformat bei Smart Ticket.....82

6.2 Public Spot-Clients anzeigen.....82

6.3 Public Spot-Benutzern Werbung einblenden.....82

6.3.1 Ergänzungen im Setup-Menü.....83

6.3.2 Ergänzungen zu den RADIUS-Attributen.....87

6.4 Zusätzliche Attribute für die XML-Schnittstelle.....88

6.5 Dynamische Änderung einer Benutzersitzung über die XML-Schnittstelle.....88

7 WLAN.....90

7.1 Client-Bridge-Modus und Bandbreitenlimit pro SSID festlegen.....90

7.1.1 Ergänzungen im Setup-Menü.....91

7.2 Trennung von P2P- und WLAN/SSID-Konfiguration.....94

7.2.1 Konfiguration von P2P-Verbindungen.....94

7.2.2 Ergänzungen im Setup-Menü.....96

7.3 Flexibles WLAN Capture-Format.....112

7.3.1 Ergänzungen im Setup-Menü.....112

7.4 Band Steering mit verzögertem Scan auf 2,4GHz.....113

7.4.1 Ergänzungen im Setup-Menü.....114

7.5 Erweiterte WLAN-Traces.....114

7.5.1 Ergänzungen im Setup-Menü.....115

7.6 Fast Roaming gemäß IEEE 802.11r.....116

7.6.1 Fast Roaming.....116

7.6.2 Konfiguration.....118

7.6.3 Ergänzungen im Status-Menü.....118

7.6.4 Ergänzungen im Setup-Menü.....119

7.7 WPA2 mit AES als Werkseinstellung.....121

7.8 WLAN Protected Management Frames (PMF).....121

7.8.1 Ergänzungen im Status-Menü.....124

7.8.2 Ergänzungen im Setup-Menü.....129

7.9 Redundante Verbindungen mittels PRP.....131

7.9.1 Grundlegende Funktion.....131

7.9.2 Vorteile von WLAN-PRP.....132

7.9.3 PRP-Implementation in den Access Points....132
7.9.4 Dual Roaming....132
7.9.5 Unterstützung von Diagnosemöglichkeiten....133
7.9.6 Tutorial: Einrichtung einer PRP-Verbindung über ein Point-to-Point-Netz (P2P)....134
7.9.7 Tutorial: Roaming mit einem Dual-Radio-Client und PRP....136
7.9.8 Ergänzungen im Setup-Menü....139
8 WLAN-Management....148
8.1 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen....148
8.1.1 Funktionsweise....150
8.1.2 Einrichtung mittels Express-Integration....156
8.1.3 Einrichtung mittels vorkonfigurierter Integration....157
8.1.4 Netz-Rollout: Vorkonfigurierte Integration durch Pairing beschleunigen....159
8.1.5 Netz-Rollout: Umschalten von Express- zu vorkonfigurierter Integration....160
8.1.6 Manuelles Topologie-Mangement....160
8.1.7 Redundante Strecken mittels RSTP....163
8.1.8 Ergänzungen im Status-Menü....164
8.1.9 Ergänzungen im Setup-Menü....193
8.2 IP-abhängige Autokonfiguration und Tagging von APs....211
8.2.1 Einrichten von Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration....211
8.2.2 Einrichten von Tag-Gruppen für die selektive Auswahl von APs....212
8.2.3 Ergänzungen im Status-Menü....213
8.2.4 Ergänzungen im Setup-Menü....219
8.2.5 Ergänzungen der Kommandozeilenbefehle....224
8.3 Automatische Wahl des 2,4/5-GHz-Modus....226
8.3.1 Ergänzungen im Status-Menü....227
8.3.2 Ergänzungen im Setup-Menü....228
8.4 WLC-Cluster....230
8.4.1 CAPWAP im WLC gezielt (de)aktivieren....230
8.4.2 WLC-Tunnel für die interne Kommunikation....231
8.4.3 Ermittlung des idealen WLC....236
8.4.4 Ermittlung der idealen AP-Verteilung....237
8.4.5 Ideale AP-Verteilung manuell initiieren....237
8.4.6 Einrichten einer CA-Hierarchie....237
8.5 One Click Backup der SCEP-CA....243
8.6 Automatischer Neustart verwalteter APs nach Firmware-Update....244
8.6.1 Firmware in verwalteten AP laden....244
8.7 Automatische Suche nach alternativen WLCs....244
8.8 U-APSD per WLC konfigurierbar....244
8.8.1 Ergänzungen im Status-Menü....244
8.8.2 Ergänzungen im Setup-Menü....245
8.9 Gruppenbezogene Funkfeldoptimierung....246
8.10 Neue APs über den WEBconfig Setup-Wizard hinzufügen....247
8.10.1 Ergänzungen im Status-Menü....247
8.11 Maximale Kanalbandbreite je WLAN-Modul einstellbar....249

8.11.1 Ergänzungen im Status-Menü....250
8.11.2 Ergänzungen im Setup-Menü....252
8.12 Client-Steering über den WLC....254
8.12.1 Konfiguration....255
8.12.2 Ergänzungen im Status-Menü....257
8.12.3 Ergänzungen im Setup-Menü....259
8.13 Automatische Wahl des Frequenzbands....265
8.13.1 Ergänzungen im Setup-Menü....266
9 VPN....268
9.1 VPN-Einwahl-Wizard in WEBconfig....268
9.2 L2TPv2 (Layer 2 Tunneling Protocol Version 2)....268
9.2.1 Konfiguration der L2TP-Tunnel....268
9.2.2 Authentifizierung über RADIUS....271
9.2.3 Betrieb als L2TP Access Concentrator (LAC)....272
9.2.4 Betrieb als L2TP Network Server (LNS) für RAS-Clients....274
9.2.5 Betrieb als L2TP Network Server (LNS) mit Authentifizierung über RADIUS....275
9.2.6 Ergänzungen im Status-Menü....277
9.2.7 Ergänzungen im Setup-Menü....285
9.3 Unterstützung der DH-Gruppen 15 und 16....312
9.3.1 Ergänzungen im Setup-Menü....312
10 Routing und WAN-Verbindungen....317
10.1 Überarbeitete Flusssteuerung....317
10.1.1 Ergänzungen im Status-Menü....317
10.1.2 Ergänzungen im Setup-Menü....318
10.2 AC-Name für PPPoE-Server konfigurierbar....319
10.2.1 Ergänzungen im Setup-Menü....319
11 Weitere Dienste....321
11.1 Geräte-LEDs bootpersistent ausschalten....321
11.1.1 Ergänzungen im Setup-Menü....322
11.2 Kommentarfeld für CRON-Jobs....323
11.2.1 Konfiguration der Zeitautomatik....323
11.2.2 Ergänzungen im Setup-Menü....324
11.3 LANCAPI standardmäßig deaktiviert....325
11.3.1 Ergänzungen im Setup-Menü....325
11.4 DHCP-Snooping und DHCP-Option 82....325
11.4.1 Ergänzungen im Setup-Menü....327
11.5 LLDP über LANconfig aktivieren....330
11.6 Wildcard-Zertifikate im LANCOM Content Filter....331
11.6.1 Ergänzungen im Setup-Menü....331

1 Addendum zur LCOS-Version 9.00

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 9.00 gegenüber der vorherigen Version.

2 LCMS

2.1 Ergänzungen in LANconfig

2.1.1 Automatische Authentisierung für den Lesezugriff in LANmonitor

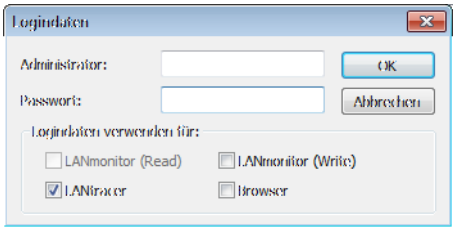
Ab Version 9.00 bietet Ihnen LANconfig ein zusätzliches Komfortverhalten, bei dem sich LANmonitor nach dem Öffnen einer Gerätekonfiguration in LANconfig ohne die Eingabe weiterer Zugangsdaten aufrufen lässt.

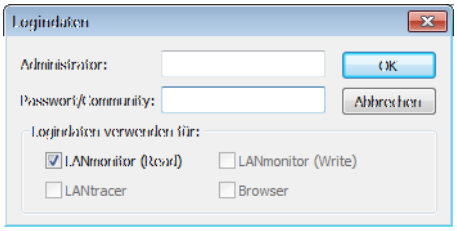
Logindaten

Hinterlegen Sie in diesem Bereich die Zugangsdaten für die externen Programme. Klicken Sie **Neu**, um ein oder mehrere Programm(e) auszuwählen und die dafür geltenden Zugangsdaten einzugeben. Je nach Auswahl fragt das Dialogfenster unterschiedliche Zugangsdaten ab. In jedem Fall haben Sie die Möglichkeit, sich mit dem Benutzernamen und Passwort Ihres Administrator-Zugangs zu authentisieren, wenn Sie das betreffende Programm aus LANconfig heraus aufrufen.

Im Falle von LANmonitor besteht für den Lesezugriff alternativ die Möglichkeit, eine individuelle SNMP-Community anzugeben. Standardmäßig prüft LANconfig beim Öffnen einer Gerätekonfiguration, ob und in welchem Umfang Sie Zugangsdaten für externe Programme hinterlegt haben. Haben Sie keine Zugangsdaten oder ausschließlich eine SNMP-Community für den Lesezugriff konfiguriert, übernimmt LANconfig beim Programmaufruf von LANmonitor die SNMP-Community ersatzweise aus der Gerätekonfiguration. Durch dieses Komfortverhalten wird der Authentisierungsumfang für LANmonitor bereits reduziert.

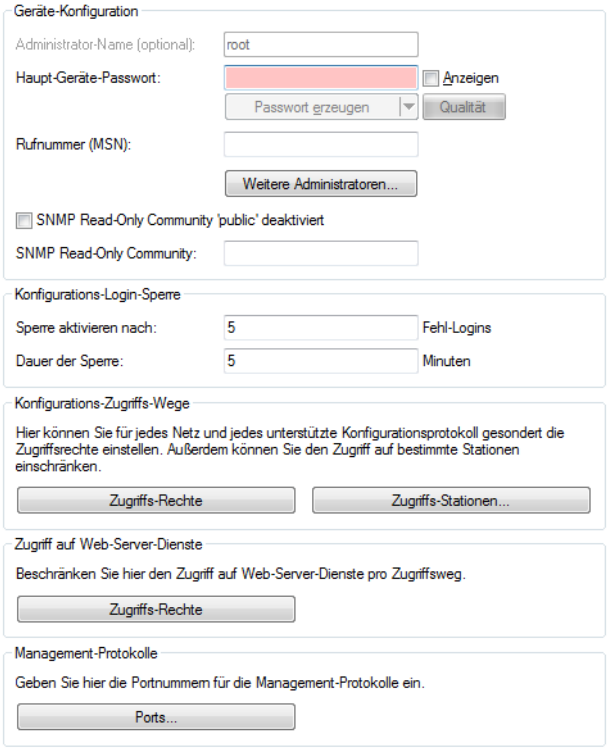
Weitere Informationen zum SNMP-Zugriff über einzelne oder mehrere SNMP-Communities finden Sie im Referenzhandbuch.





2.1.2 Anzeige des Administrator-Benutzernamens

Um zu verdeutlichen, an welchen Benutzernamen das Hauptgerätepasswort gekoppelt ist, zeigt LANconfig ab Version 9.00 sowohl in der Geräte-Konfiguration als auch in relevanten Assistenten **root** als Administrator-Benutzernamen an.



2.2 Ergänzungen im LANmonitor

2.2.1 Interne IPv6-Unterstützung

Ab Version 9.00 ermöglicht LANmonitor den internen Umgang mit IPv6-Adressen und damit die Kommunikation mit Geräten per IPv6.

2.2.2 Anzeige von statischen WAN-IPs im Statusbaum

Sie haben ab Version 9.00 im LANmonitor die Möglichkeit, sich eine statische WAN-IP im Statusbaum anzeigen zu lassen.

Ergänzungen im Status-Menü

IPv4

Diese Tabelle enthält die Liste der statischen IPv4-Gegenstellen im WAN.

SNMP-ID:

1.4.13.1

Pfad Telnet:

Status > **WAN** > **Adressen**

Gegenstelle

Name der Gegenstelle.

SNMP-ID:

1.4.13.1.1

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

Typ

Art der zugewiesenen IPv4-Adresse

SNMP-ID:

1.4.13.1.2

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

Mögliche Werte:

statisch
DHCP
PPP
autoconfig

IP-Adresse

Zugewiesene IPv4-Adresse.

SNMP-ID:

1.4.13.1.3

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

IP-Netzmaske

Zugewiesene IPv4-Netzmaske.

SNMP-ID:

1.4.13.1.4

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

Gateway

Zugewiesenes Gateway.

SNMP-ID:

1.4.13.1.5

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

DNS-Default

Primärer zugewiesener DNS-Server.

SNMP-ID:

1.4.13.1.6

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

DNS-Backup

Alternativer zugewiesener DNS-Server.

SNMP-ID:

1.4.13.1.7

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

NBNS-Default

Primärer zugewiesener NBNS-Server.

SNMP-ID:

1.4.13.1.8

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

NBNS-Backup

Alternativer zugewiesener NBNS-Server.

SNMP-ID:

1.4.13.1.9

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

Domain

Zugewiesene eigene Domain.

SNMP-ID:

1.4.13.1.10

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv4**

IPv6

Diese Tabelle enthält die Liste der statischen IPv6-Gegenstellen im WAN.

SNMP-ID:

1.4.13.2

Pfad Telnet:

Status > **WAN** > **Adressen**

Gegenstelle

Name der Gegenstelle.

SNMP-ID:

1.4.13.2.1

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

Typ

Art der zugewiesenen IPv6-Adresse

SNMP-ID:

1.4.13.2.2

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

Mögliche Werte:

unbekannt
statisch
DHCP
autoconfig
tunnel

IP-Adresse

Zugewiesene IPv6-Adresse.

SNMP-ID:

1.4.13.2.3

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

Praefix-Laenge

Zugewiesene Präfix-Länge.

SNMP-ID:

1.4.13.2.4

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

Gateway

Zugewiesenes Gateway.

SNMP-ID:

1.4.13.2.5

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

DNS-Default

Primärer zugewiesener DNS-Server.

SNMP-ID:

1.4.13.2.6

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

DNS-Backup

Alternativer zugewiesener DNS-Server.

SNMP-ID:

1.4.13.2.7

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

Domain

Zugewiesene eigene Domain.

SNMP-ID:

1.4.13.2.10

Pfad Telnet:

Status > **WAN** > **Adressen** > **IPv6**

3 Konfiguration

3.1 Festlegen eines individuellen SNMP-Ports

Ab LCOS 9.00 haben Sie die Möglichkeit, den für den SNMP-Dienst standardmäßig verwendeten Port 161 zu verändern.

In LANmonitor geben Sie den betreffenden Port z. B. beim Hinzufügen eines Gerätes an. Sie haben alternativ aber auch die Möglichkeit, neue Geräte unter Angabe von IP-Adresse und SNMP-Port direkt beim Programmaufruf zu konfigurieren. Starten Sie LANmonitor dazu über die Syntax `lanmon /add:[<IPv6-Address>]:<Port>`, also z. B. `lanmon /add:[fe80::2a0:57ff:fe1b:3302]:161`.

3.1.1 Ergänzungen im Setup-Menü

Port

Geben Sie hier den Port des Computers ein, auf dem ein SNMP-Manager installiert ist.

SNMP-ID:

2.9.2.5

Pfad Telnet:

Setup > **SNMP** > **IP-Traps**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

0 … 65535

Default-Wert:

leer

Port

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

SNMP-ID:

2.9.21

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

0 … 65535

Default-Wert:

161

3.2 Passwortfeld-Schutz für WLAN-Schlüssel

Ab LCOS 9.00 stellt das System WPA- sowie WEP-Gruppen-Schlüssel an der Konsole nicht mehr im Klartext, sondern als Passworteingabe dar (********). In Folge dessen ist es nicht mehr möglich, diese Schlüssel z. B. per SNMP auszulesen.

3.3 Sortierte Anzeige eines Menüs an der Konsole

Ab LCOS 9.00 haben Sie an der Konsole die Möglichkeit, Menüpunkte über den Optionsschalter `-s` sortiert auszugeben.

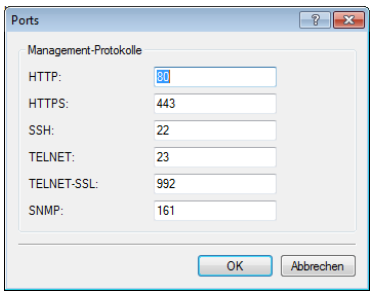
Befehl	Beschreibung
dir|list|ls|llong [-a] [-r] [-s] [<Path>] [<Filter>]	Zeigt den Inhalt des aktuellen Verzeichnisses an. Mögliche Optionsschalter sind: ■ `-a`: Gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte. ■ `-r`: Listet auch alle Unterverzeichnisse sowie die darin befindlichen Tabellen auf. ■ `-s`: Sortiert den angezeigten Menüpunkt aufsteigend in alphabetischer Reihenfolge.

Alternativ haben Sie über den dazugehörigen Setup-Parameter **Setup** > **Config** > **Menue-sortieren** die Möglichkeit, die sortierte Anzeige standardmäßig zu setzen.

3.3.1 Management-Ports für den Gerätezugriff anpassen

Sie haben im LANconfig die Möglichkeit, die Portnummern für die Management-Protokolle zu ändern.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Management** > **Admin** und klicken Sie dort auf **Ports**.
3. Geben Sie die Portnummern für die gewünschten Management-Protokolle ein.



4. Schließen Sie alle geöffneten Dialoge durch einen Klick auf **OK**.

LANconfig schreibt die eingegebene Konfiguration zurück auf das Gerät.

3.3.2 Ergänzungen im Setup-Menü

Menue-sortieren

Über diesen Parameter legen Sie fest, ob das Gerät Menüpunkte an der Konsole standardmäßig in alphabetisch-aufsteigend sortierter Reihenfolge ausgibt. Die Einstellung entspricht dem Optionsschalter `-s` beim Auflisten von Menü- oder Tabelleninhalten.

SNMP-ID:

2.11.73

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

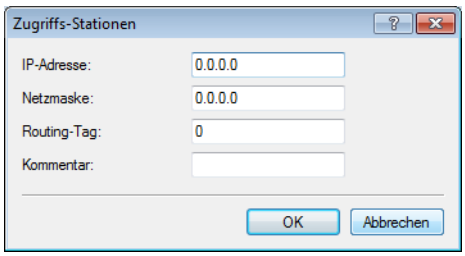
nein
ja

Default-Wert:

nein

3.4 Kommentarfeld für Zugriffs-Stationen

Ab LCOS 9.00 haben Sie die Möglichkeit, Filter-Einträge in der Tabelle der Zugriffs-Stationen mit Kommentaren zu versehen.



3.4.1 Ergänzungen im Setup-Menü

Kommentar

Über diesen Parameter hinterlegen Sie zu dem Eintrag einen Kommentar.

SNMP-ID:

2.7.6.4

Pfad Telnet:

Setup > **TCP-IP** > **Zugangs-Liste**

Mögliche Werte:

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

Default-Wert:

leer

3.5 Elliptic Curve Cryptography (ECC)

Ab LCOS 9.00 haben Sie die Möglichkeit, auf einem Gerät neben den bekannten RSA- und DSA-Schlüsseln auch ECDSA-Schlüssel zu generieren.

SSH-Schlüsselerzeugung unter LCOS

Die Erzeugung eines Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – starten Sie an der Konsole des Gerätes mit folgendem Befehl:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-?, -h

Zeigt eine kurze Hilfe der möglichen Parameter.

-t (dsa|rsa|ecdsa)

Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln:

- RSA-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis zu 16384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 1024 bis 2048 Bit.
- DSA-Schlüssel folgen dem Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST) und werden z. B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. DSA- bzw. DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.
- ECDSA-Schlüssel sind eine Variante von DSA-Schlüsseln, bei der das Gerät für die Schlüsselerzeugung elliptische Kurven verwendet (Elliptic Curve Cryptography, ECC). Die ECC ist eine Alternative zu den klassischen Signatur- und Schlüsselaustauschverfahren wie RSA und Diffie-Hellman. Der Hauptvorteil von elliptischen Kurven liegt darin, dass Sie durch deren mathematische Eigenschaften die gleiche Schlüsselstärke wie bei RSA oder Diffie-Hellman mit einer deutlich kürzeren Schlüssellänge erreichen. Dies erlaubt eine bessere Leistung bei äquivalenter Hardware. ECC und deren Integration in SSL und TLS sind in den RFCs 5656 und 4492 beschrieben.

Wenn Sie keinen Typ angegeben, erzeugt das Kommando immer einen RSA-Schlüssel.

-b <Bits>

Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit.

-f <OutputFile>

Über diesen Parametern geben Sie den Mountingpoint der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Mountingpoints hängt davon ab, was für einen Schlüssel sie von welchem Typ Sie erzeugen. Zur Auswahl stehen Ihnen in diesem Fall:

- **ssh_rsakey** für RSA-Schlüssel
- **ssh_dsakey** für DSA-Schlüssel
- **ssh_ecdsakey** für ECDSA-Schlüssel

-q

Dieser Parameter aktiviert den 'Quiet'-Modus für die Schlüsselerzeugung. Wenn Sie diesen Parameter setzen, überschreibt LCOS bereits existierende RSA- bzw. DSA-Schlüssel ungefragt; Ausgaben über den Fortschritt der Operation entfallen. Nutzen Sie diesen Parameter z. B. in einem Skript, um die Bestätigung von Sicherheitsabfragen durch den Benutzer zu unterdrücken.

3.5.1 Ergänzungen im Setup-Menü

SSL

Hier werden die Parameter für HTTPS-Verbindungen festgelegt.

SNMP-ID:

2.21.40

Pfad Telnet:

Setup > **HTTP**

Port

Port für die HTTPS-Server-Verbindung.

SNMP-ID:

2.21.40.10

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

0 … 65535

Default-Wert:

443

Verwende-benutzer-geliefertes-Zertifikat

Wählen Sie hier, ob Sie ein benutzerkonfiguriertes Zertifikat nutzen möchten.

SNMP-ID:

2.21.40.11

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.21.40.3

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

Schluesselaustausch-Algorithmen

Diese Bitmaske legt fest, welche Verfahren zum Schlüsselaustausch zur Verfügung stehen.

SNMP-ID:

2.21.40.4

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypto-Algorithmen

Diese Bitmaske legt fest, welche Krypto-Algorithmen erlaubt sind.

SNMP-ID:

2.21.40.5

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash-Algorithmen

Diese Bitmaske legt fest, welche Hash-Algorithmen erlaubt sind und impliziert welche HMAC-Algorithmen zum Schutz der Nachrichten-Integrität genutzt werden.

SNMP-ID:

2.21.40.6

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

Schluesselaustausch-Algorithmen

Die MAC-Schluesselaustausch-Algorithmen dienen der Aushandlung des Schlüssel-Algorithmus. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

SNMP-ID:

2.11.28.3

Pfad Telnet:

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

Mögliche Werte:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256

Default-Wert:

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

Hostkey-Algorithmen

Die Hostkey-Algorithmen dienen der Authentifizierung von Hosts. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

SNMP-ID:

2.11.28.4

Pfad Telnet:

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

Mögliche Werte:

ssh-rsa
ssh-dss
ecdsa-sha2
ssh-ed25519

Default-Wert:

ssh-rsa

ssh-dss

Elliptic-Curves

Wählen Sie hier die (NIST-)Kurven aus, die das Gerät für die Elliptic Curve Cryptography (ECC) einsetzt.

Für das ECDH-Key-Agreement sind alle angegebenen NIST-Kurven anwendbar, Host-Keys beruhen auf den Kurven `nistp256` und `nistp384`.

SNMP-ID:

2.11.28.9

Pfad Telnet:

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

Mögliche Werte:

nistp256
nistp384
nistp521

Default-Wert:

nistp256

nistp384

nistp521

Telnet-SSL

Hier werden die Parameter für Telnet-SSL-Verbindungen festgelegt.

SNMP-ID:

2.11.29

Pfad Telnet:

Setup > **Config**

PORT

Dieser Port wird für verschlüsselte Konfigurationsverbindungen über Telnet verwendet.

SNMP-ID:

2.11.29.10

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

0 … 65535

Default-Wert:

992

Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.11.29.2

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

Schluesselaustausch-Algorithmen

Diese Bitmaske legt fest, welche Verfahren zum Schlüsselaustausch zur Verfügung stehen.

SNMP-ID:

2.11.29.3

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypto-Algorithmen

Diese Bitmaske legt fest, welche Krypto-Algorithmen erlaubt sind.

SNMP-ID:

2.11.29.4

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash-Algorithmen

Diese Bitmaske legt fest, welche Hash-Algorithmen erlaubt sind und impliziert welche HMAC-Algorithmen zum Schutz der Nachrichten-Integrität genutzt werden.

SNMP-ID:

2.11.29.5

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

EAP-TLS

Hier werden die Parameter für EAP-TLS-Verbindungen festgelegt.

SNMP-ID:

2.25.10.10.19

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP**

Pruefe-Benutzernamen

Bei TLS authentifiziert sich der Client alleine über sein Zertifikat. Ist diese Option aktiviert, so prüft der RADIUS Server zusätzlich, ob der im Zertifikat hinterlegte Benutzername in der RADIUS-Benutzertabelle enthalten ist.

SNMP-ID:

2.25.10.10.19.10

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Mögliche Werte:

ja
nein

Default-Wert:

nein

Schluesselaustausch-Algorithmen

Diese Bitmaske legt fest, welche Verfahren zum Schlüsselaustausch zur Verfügung stehen.

SNMP-ID:

2.25.10.10.19.3

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypto-Algorithmen

Diese Bitmaske legt fest, welche Krypto-Algorithmen erlaubt sind.

SNMP-ID:

2.25.10.10.19.4

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash-Algorithmen

Diese Bitmaske legt fest, welche Hash-Algorithmen erlaubt sind und impliziert welche HMAC-Algorithmen zum Schutz der Nachrichten-Integrität genutzt werden.

SNMP-ID:

2.25.10.10.19.5

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

RADSEC

Hier werden die Parameter für RADSEC-Verbindungen festgelegt.

SNMP-ID:

2.25.20

Pfad Telnet:

Setup > **RADIUS**

Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

SNMP-ID:

2.25.20.1

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

Schluesselaustausch-Algorithmen

Diese Bitmaske legt fest, welche Verfahren zum Schlüsselaustausch zur Verfügung stehen.

SNMP-ID:

2.25.20.2

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypto-Algorithmen

Diese Bitmaske legt fest, welche Krypto-Algorithmen erlaubt sind.

SNMP-ID:

2.25.20.3

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash-Algorithmen

Diese Bitmaske legt fest, welche Hash-Algorithmen erlaubt sind und impliziert welche HMAC-Algorithmen zum Schutz der Nachrichten-Integrität genutzt werden.

SNMP-ID:

2.25.20.4

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

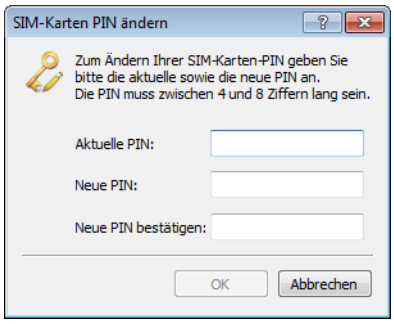
SHA2-384

3.6 Ändern der SIM-Karten PIN

Bei Geräten mit Mobilfunkmodem haben Sie über LANconfig die Möglichkeit, die PIN der SIM-Karte zu ändern. Die Änderung kann einfach vollzogen werden, indem Sie sowohl die alte PIN als auch die neue PIN eingeben. Zur Sicherheit verlangt LANconfig zusätzlich eine Bestätigung der neuen PIN. Alternativ haben Sie auch die Möglichkeit, die Änderung auf der Kommandozeile über die Aktion **PIN-Aendern** durchzuführen.

Die nachfolgenden Schritte beschreiben den Änderungsweg in LANconfig.

1. Wählen Sie in der Geräteübersicht von LANconfig das Gerät aus, dessen PIN Sie ändern wollen.
2. Wählen Sie über die Menüleiste **Gerät** > **SIM-Karten PIN ändern**. Ein neuer Dialog öffnet sich.



3. Geben Sie die bisher aktuelle PIN und die neue PIN ein. Bestätigen Sie die neue PIN durch wiederholte Eingabe.
4. Klicken Sie **OK**, um die Änderung zu übernehmen.

3.6.1 Ergänzungen im Status-Menü

PIN-Aendern

Mit dieser Aktion ändern Sie die PIN der SIM-Karte. Die Syntax für die eingegebenen Argumente lautet:

```
<oldPIN> <newPIN> <newPIN>
```

Die Aktion kann nur durchgeführt werden, nachdem das Modem erfolgreich initialisiert wurde. Dies ist insbesondere zu beachten, wenn Skripte eingesetzt werden, um eine entsprechende Konfiguration vorzunehmen.

SNMP-ID:

1.49.42

Pfad Telnet:

Status > **Modem-Mobilfunk**

Mögliche Argumente:

<oldPIN>

Alter PIN

<newPIN>

Neuer PIN

<newPIN>

Bestätigung des neuen PIN

3.6.2 Ergänzungen im Setup-Menü

PIN-Aendern

Über diese Aktion ändern Sie die PIN der SIM-Karte Ihres Gerätes. Syntax:

```
do pin-aendern <alter_PIN> <neuer_PIN> <neuer_PIN>
```

SNMP-ID:

2.23.41.12

Pfad Telnet:

Setup > **Schnittstellen** > **Mobilfunk**

Mögliche Werte:

4 Zeichen aus `[0-9]`

3.7 Kombinierter UMTS-GPRS-Betrieb für LTE-Geräte

LCOS 9.00 bietet Ihnen die Möglichkeit, LTE-Geräte beim Verzicht auf den LTE-Betrieb in einem kombinierten Modus sowohl über UMTS als auch über GPRS zu erreichen. Eine Entscheidung zwischen UMTS und GPRS ist in diesem Fall also nicht mehr zwingend notwendig.

3.7.1 Ergänzungen im Setup-Menü

Modus

Wählen Sie hier die Mobilfunk-Übertragungs-Betriebsart.

SNMP-ID:

2.23.41.1.6

Pfad Telnet:

Setup > **Schnittstellen** > **Mobilfunk** > **Profile**

Mögliche Werte:

Auto.
Automatische Wahl der Übertragungs-Betriebsart

UMTS
Ausschließlicher UMTS-Betrieb

GPRS
Ausschließlicher GPRS-Betrieb

UMTS-GPRS
Kombinierter UMTS-GPRS-Betrieb

LTE
Ausschließlicher LTE-Betrieb

Default-Wert:

Auto.

4 IPv6

4.1 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, kurz DS-Lite, dient dazu, dass Internet-Provider ihren Kunden über eine IPv6-Verbindung Zugang zu IPv4-Servern verschaffen können. Das ist z. B. dann erforderlich, wenn der Kunde weiterhin IPv4-Geräte verwendet, der Internet-Provider allerdings aufgrund knapper IPv4-Adressen dem Kunden nur eine IPv6-Adresse vergeben kann. Im Gegensatz zu den anderen drei IPv6-Tunnelverfahren "6in4", "6rd" und "6to4" dient DS-Lite also dazu, IPv4-Pakete über eine IPv6-Verbindung zu übertragen (IPv4-über-IPv6-Tunnel).

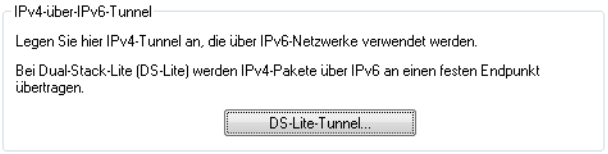
Der Router verpackt dazu die IPv4-Pakete in einen IPv4-in-IPv6-Tunnel und übermittelt sie unmaskiert an den Provider. Der führt anschließend eine NAT mit einer seiner eigenen verbliebenen IPv4-Adressen durch.

Zur Definition eines DS-Lite-Tunnels benötigt der Router nur die IPv6-Adresse des Tunnel-Endpunkts sowie das Routing-Tag, über das er diese Adresse erreichen kann.

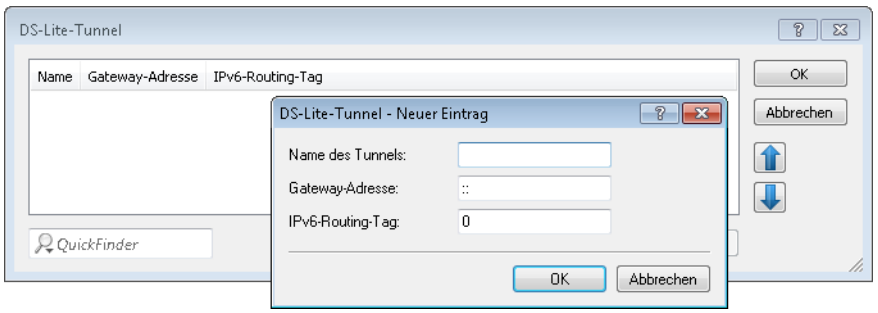
Standardmäßig verwendet der Router die IPv4-Adresse des entsprechenden internen Netzes, z. B. vom "INTRANET". Möchte man stattdessen eine andere IP-Adresse (z. B. 192.0.0.2) vorgeben, muss diese zusammen mit dem Gegenstellennamen des DS-Lite-Tunnels in der IP-Parameter-Liste angelegt sein.

Die Angabe eines IPv4-DNS-Servers ist für einen DS-Lite-Tunnel nicht ratsam, da dessen Einträge die NAT-Tabelle des Internet-Providers unnötig füllen würden.

Einen DS-Lite-Tunnel richten Sie in LANconfig ein über **IPv4** > **Tunnel** mit einem Klick auf **DS-Lite-Tunnel**.



Klicken Sie anschließend auf **Hinzufügen** und geben Sie die Bezeichnung des Tunnels, die IPv6-Adresse des Gateways und das Routing-Tag ein.



Name des Tunnels

Dieser Eintrag bestimmt den Namen des IPv4-über-IPv6-Tunnels.

Gateway-Adresse

Dieser Eintrag definiert die Adresse des DS-Lite-Gateways, den sogenannten Address Family Transition Router (AFTR).

Die folgenden Werte sind möglich:

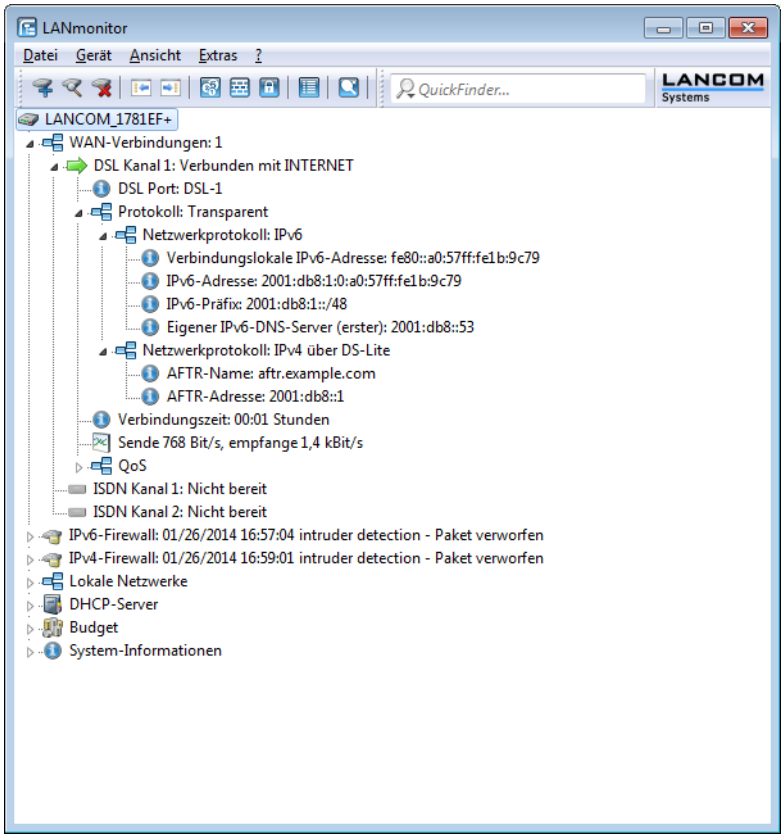
- Eine IPv6-Adresse, z. B. 2001:db8::1
- Ein per DNS auflösbarer FQDN (Fully Qualified Domain Name), z. B. aftr.example.com
- Die IPv6 Unspecified Address "::" bestimmt, dass das Gerät die Adresse des AFTRs per DHCPv6 beziehen soll (Werkseinstellung).
- Ein leeres Feld verhält sich wie bei der Eingabe von "::".

IPv6-Routing-Tag

Das Routing-Tag spezifiziert eindeutig die Route zum DS-Lite-Gateway.

Da bei DS-Lite das NAT durch den Provider erfolgt, ist die Funktion vieler Anwendungen von den Einstellungen des Provider-NATs abhängig (z. B. SIP, H.323, IRC oder IPSec). PPTP funktioniert über DS-Lite gar nicht. Wenn der Provider kein Portforwarding eingerichtet hat, funktionieren auch IPv4-Serverdienste nicht mehr.

Über den LANmonitor lassen sich die Status-Tabelle und die Anzahl der aktuellen DS-Lite-Verbindungen darstellen:



4.1.1 Ergänzungen im Status-Menü

DS-Lite

In diesem Verzeichnis finden Sie Statistiken der DS-Lite-Tunnel.

SNMP-ID:

1.81

Pfad Telnet:

Status

Rx-Pakete

Dieser Eintrag zeigt die Anzahl der auf allen DS-Lite-Schnittstellen empfangenen Datenpakete an.

SNMP-ID:

1.81.1

Pfad Telnet:

Status > **DS-Lite**

Tx-Pakete

Dieser Eintrag zeigt die Anzahl der auf allen DS-Lite-Schnittstellen gesendeten Datenpakete an.

SNMP-ID:

1.81.2

Pfad Telnet:

Status > **DS-Lite**

Queue-Fehler

Dieser Eintrag zeigt die Anzahl der auf allen DS-Lite-Schnittstellen beim Empfang verloren gegangenen Datenpakete an.

SNMP-ID:

1.81.3

Pfad Telnet:

Status > **DS-Lite**

Verbindungen

Diese Tabelle zeigt eine Übersicht der aktiven DS-Lite-Verbindungen.

Wenn das Gerät eine DS-Lite-Verbindung hergestellt hat, taucht sie in dieser Tabelle auf. Nach einem fehlerfreien Verbindungsende erlischt der Tabelleneintrag automatisch. Bei einem Fehler bleibt der Eintrag so lange erhalten, bis die Verbindung erneut zustande kommt oder Sie ihn manuell löschen.

Jede Zustandsänderung einer DS-Lite-Verbindung sendet einen SNMP-Trap (ID 83) mit dem Inhalt der entsprechenden Status-Tabellen-Zeile.

SNMP-ID:

1.81.4

Pfad Telnet:

Status > **DS-Lite**

Gegenstelle

Dieser Eintrag zeigt den Namen des DS-Lite-Tunnels.

SNMP-ID:

1.81.4.1

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

Status

Dieser Eintrag zeigt den Status des DS-Lite-Tunnels.

SNMP-ID:

1.81.4.2

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

Letzter-Fehler

Dieser Eintrag zeigt den letzten Fehler der Verbindung.

SNMP-ID:

1.81.4.3

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

IPv4-Adresse

Dieser Eintrag zeigt die IPv4-Adresse des Gerätes an, wenn es Datenpakete sendet.

SNMP-ID:

1.81.4.4

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

phys.-Verb.

Dieser Eintrag zeigt den Namen der IPv6-Schnittstelle an, über die die DS-Lite-Verbindung läuft.

SNMP-ID:

1.81.4.5

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

AFTR-Name

Dieser Eintrag zeigt den DNS-Namen des Tunnel-Endpunktes an (Address Family Transition Router, AFTR).

SNMP-ID:

1.81.4.6

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

AFTR-IPv6-Adresse

Dieser Eintrag zeigt die IPv6-Adresse des DS-Lite-Tunnel-Endpunktes an.

SNMP-ID:

1.81.4.7

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

Verb.-Zeit

Dieser Eintrag zeigt die Dauer an, für die die Verbindung bereits besteht. Die Abfrage über SNMP ergibt die Verbindungsdauer in Sekunden; TELNET nennt die Systemzeit des Verbindungsaufbaus.

SNMP-ID:

1.81.4.8

Pfad Telnet:

Status > **DS-Lite** > **Verbindungen**

Tunnel

Dieser Eintrag zeigt die Anzahl der aktiven DS-Lite-Verbindungen an.

SNMP-ID:

1.81.5

Pfad Telnet:

Status > **DS-Lite**

Tunnel

Diese Aktion löscht alle Werte der DS-Lite-Statistik fehlerfrei abgebauter Verbindungen.

SNMP-ID:

1.81.6

Pfad Telnet:

Status > **DS-Lite**

4.1.2 Ergänzungen im Setup-Menü

DS-Lite-Tunnel

Dual-Stack Lite, kurz DS-Lite, dient dazu, dass Internet-Provider ihren Kunden über eine IPv6-Verbindung Zugang zu IPv4-Servern verschaffen können. Das ist z. B. dann erforderlich, wenn der Kunde weiterhin IPv4-Geräte verwendet, der Internet-Provider allerdings aufgrund knapper IPv4-Adressen dem Kunden nur eine IPv6-Adresse vergeben kann. Im Gegensatz zu den anderen drei IPv6-Tunnelverfahren "6in4", "6rd" und "6to4" dient DS-Lite also dazu, IPv4-Pakete über eine IPv6-Verbindung zu übertragen (IPv4-über-IPv6-Tunnel).

Der Router verpackt dazu die IPv4-Pakete in einen IPv4-in-IPv6-Tunnel und übermittelt sie unmaskiert an den Provider. Der führt anschließend eine NAT mit einer seiner eigenen verbliebenen IPv4-Adressen durch.

Zur Definition eines DS-Lite-Tunnels benötigt der Router nur die IPv6-Adresse des Tunnel-Endpunkts sowie das Routing-Tag, über das er diese Adresse erreichen kann.

SNMP-ID:

2.2.40

Pfad Telnet:

Setup > **WAN**

Name

Geben Sie hier eine Bezeichnung für den Tunnel ein.

SNMP-ID:

2.2.40.1

Pfad Telnet:

Setup > **WAN** > **DS-Lite-Tunnel**

Mögliche Werte:

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

Default-Wert:

leer

Gateway-Adresse

Dieser Eintrag definiert die Adresse des DS-Lite-Gateways, den sogenannten Address Family Transition Router (AFTR). Geben Sie einen gültigen Wert aus folgender Auswahl ein:

- Eine IPv6-Adresse, z. B. 2001:db8::1
- Ein per DNS auflösbarer FQDN (Fully Qualified Domain Name), z. B. aftr.example.com
- Die IPv6 Unspecified Address "::" bestimmt, dass das Gerät die Adresse des AFTRs per DHCPv6 beziehen soll (Werkseinstellung).
- Ein leeres Feld verhält sich wie bei der Eingabe von "::".

SNMP-ID:

2.2.40.2

Pfad Telnet:

Setup > **WAN** > **DS-Lite-Tunnel**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Rtg-Tag

Geben Sie hier das Routing-Tag ein, unter dem der Router das Gateway erreicht.

SNMP-ID:

2.2.40.3

Pfad Telnet:

Setup > **WAN** > **DS-Lite-Tunnel**

Mögliche Werte:

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

Default-Wert:

leer

4.2 IPv6-Unterstützung für RAS-Dienste

Ab LCOS 9.00 sind RAS-Gegenstellen dazu in der Lage, sich auch über IPv6 anzumelden. Die Konfiguration erfolgt im LANconfig unter **IPv6** > **Allgemein**, die Einrichtung von Präfix-Pools unter **IPv6** > **Router-Advertisement**.

4.2.1 RAS-Schnittstellen

Grundsätzlich existieren zwei Wege, um die Konfiguration von RAS-Gegenstellen zu verwalten:

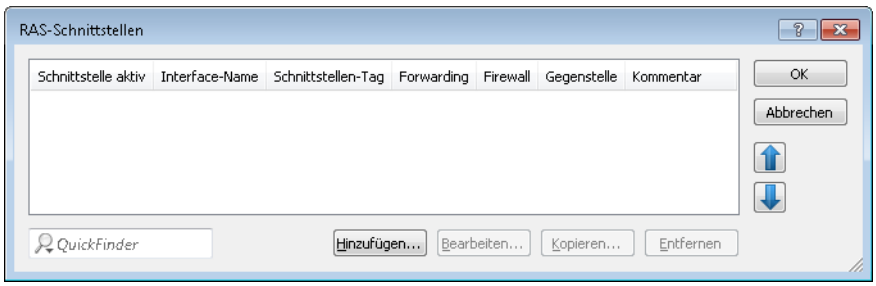
Die Benutzerdaten bzw. die Konfigurationen sind lokal im Gerät gespeichert.

Der Vorteil dieser Variante ist, dass man auf einen RADIUS-Server verzichtet und damit Verwaltung und Kosten der Netzinfrastruktur gering hält.

Die Benutzerdaten bzw. die Konfigurationen sind auf einen externen RADIUS-Server ausgelagert.

Der Vorteil dieser Variante liegt in der zentralen Benutzerverwaltung bei umfangreichen verteilten Netzwerk-Szenarien.

Für RAS-Zugänge über IPv6 müssen Sie zusätzlich unter **RAS-Schnittstellen** die entsprechende RAS-Schnittstelle einrichten.



Die Einträge in der Tabelle **RAS-Schnittstellen** haben folgende Bedeutung:

- **Schnittstelle aktiv**: Aktivieren oder deaktivieren Sie hier diese Schnittstelle.
- **Interface-Name**: Definieren Sie hier den Namen der RAS-Schnittstelle, über die die IPv6-Gegenstellen zugreifen.
- **Schnittstellen-Tag**: Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.
- **Forwarding**: Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.
- **Firewall**: Hier haben Sie die Möglichkeit, die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, markieren Sie unter **Firewall/QoS** > **Allgemein** die Option **IPv6-Firewall/QoS aktiviert**.

  Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.
- **Gegenstelle**: Bestimmen Sie hier eine Gegenstelle oder eine Liste von Gegenstellen für RAS-Einwahl-Benutzer.

  Die folgenden Werte sind möglich:

  - Eine einzelne Gegenstelle aus den Tabellen unter **Setup** > **WAN** > **PPTP-Gegenstellen**, **Setup** > **WAN** > **L2TP-Gegenstellen** oder **Setup** > **PPPoE-Server** > **Namenliste**.
  - Dem Platzhalter "*", der bewirkt, dass diese Schnittstelle für alle PPTP-, PPPoE- und L2TP-Gegenstellen gilt.
  - Dem Platzhalter "*" als Suffix oder Präfix von Gegenstellen, z. B. "FIRMA*" oder "*TUNNEL".

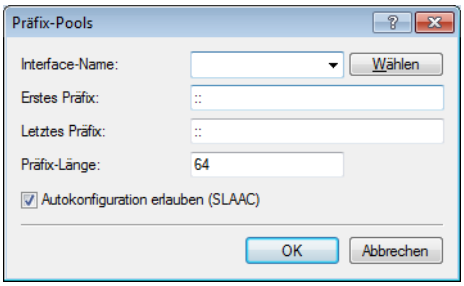
  Durch den Platzhalter-Mechanismus bilden Sie bei IPv6-RAS-Diensten mehrere Gegenstellen auf sogenannte Template-Schnittstellen ab. Diese Template-Schnittstellen sind als normale Schnittstellen bei IPv6-Diensten wie DHCPv6-Server oder Router Advertisements einsetzbar. Darüber lässt sich z. B. eine Gruppe von RAS-Schnittstellen aus einem IPv6-Präfix-Pool bedienen.
- **Kommentar**: Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Informationen zu den RADIUS-Attributen für IPv6-RAS-Dienste finden Sie unter *Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste* auf Seite 49.

Wenn RAS-Clients einen IPv6-DNS-Server zugewiesen oder per Präfix-Delegation Präfixe delegiert bekommen sollen, so müssen Sie unter **IPv6** > **DHCPv6** einen entsprechenden Eintrag in der Tabelle **DHCPv6-Netzwerke** anlegen.

Wollen Sie einen Benutzer anhand der PPP-Liste authentifizieren, so müssen Sie unter **Kommunikation** > **Protokolle** > **PPP-Liste** bei diesem Benutzer die Option **IPv6-Routing** aktivieren.

4.2.2 Präfix-Pools



Diese Tabelle enthält Präfix-Pools, aus denen RAS-Benutzer einen Präfix bei der Einwahl über IPv6 erhalten. Möglich sind folgende Einstellungen:

Interface-Name

Bestimmt den Namen der RAS-Schnittstelle, für die dieser Präfix-Pool gelten soll.

Erster Präfix

Definiert das erste Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db8::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Letzter Präfix

Definiert das letzte Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db9:FFFF::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Präfix-Länge

Definiert die Länge des Präfixes, das der Einwahl-Benutzer per Router-Advertisement zugewiesen bekommt. Die Größe des Einwahl-Pools richtet sich nur nach dem ersten und letzen Präfix. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool zugewiesen.

Damit ein Client aus dem Präfix per Autokonfiguration eine IPv6-Adresse bilden kann, muss die Präfix-Länge immer 64 Bit betragen.

SLAAC

Gibt an, ob der Client das Präfix für eine Stateless Address Autoconfiguration (SLAAC) verwenden kann.

4.2.3 Ergänzungen im Setup-Menü

RAS-Interface

In diesem Verzeichnis legen Sie die Einstellungen für die RAS-Zugänge über IPv6 fest.

SNMP-ID:

2.70.14

Pfad Telnet:

Setup > **IPv6**

Interface-Name

Definieren Sie hier den Namen der RAS-Schnittstelle, über die die IPv6-Gegenstellen zugreifen.

SNMP-ID:

2.70.14.1

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

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

Default-Wert:

leer

Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netz eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netz empfängt, erhalten intern diesen Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netz gültigen Routen auch ohne explizite Firewall-Regel.

SNMP-ID:

2.70.14.2

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

0

Interface-Status

Aktivieren oder deaktivieren Sie hier diese Schnittstelle.

SNMP-ID:

2.70.14.3

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

Aktiv
Inaktiv

Default-Wert:

Aktiv

Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.

SNMP-ID:

2.70.14.4

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Firewall

Hier haben Sie die Möglichkeit, die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, schalten Sie unter **IPv6** > **Firewall** > **Aktiv** auf **ja**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

SNMP-ID:

2.70.14.5

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

ja
nein

Default-Wert:

ja

DaD-Versuche

Bevor das Gerät eine IPv6-Adresse auf einem Interface verwendet, prüft es per 'Duplicate Address Detection (DAD)', ob diese IPv6-Adresse bereits im lokalen Netz vorhanden ist. Auf diese Art vermeidet das Gerät Adresskonflikte im Netz.

Diese Option gibt die Anzahl der Versuche an, mit denen das Gerät doppelte IPv6-Adressen im Netz sucht.

SNMP-ID:

2.70.14.6

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

1 Zeichen aus `0123456789`

Default-Wert:

0

Gegenstelle

Bestimmen Sie hier eine Gegenstelle oder eine Liste von Gegenstellen für RAS-Einwahl-Benutzer.

Die folgenden Werte sind möglich:

- Eine einzelne Gegenstelle aus den Tabellen unter **Setup** > **WAN** > **PPTP-Gegenstellen** oder **Setup** > **PPPoE-Server** > **Namenliste**.
- Dem Platzhalter "*", der bewirkt, dass diese Schnittstelle für alle PPTP- und PPPoE-Gegenstellen gilt.
- Dem Platzhalter "*" als Suffix oder Präfix von Gegenstellen, z. B. "FIRMA*" oder "*TUNNEL".

Durch den Platzhalter-Mechanismus können Sie sogenannte Template-Schnittstellen realisieren, die für entsprechend angepasste Gegenstellen gültig sind. Der Name der IPv6-RAS-Schnittstelle ist somit an vielen Stellen in der IPv6-Konfiguration verwendbar.

SNMP-ID:

2.70.14.7

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

SNMP-ID:

2.70.14.8

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

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

Default-Wert:

leer

Praefix-Pools

In diesem Verzeichnis können Sie Präfix-Pools für Einwahl-Benutzer bzw. die zugehörigen RAS-Schnittstellen (PPTP, PPPoE) definieren. Die Präfixe für Ethernet-Interfaces definieren Sie in WEBconfig unter **Setup** > **IPv6** > **Router** > **Router-Advertisements** > **Praefix-Optionen** bzw. im LANconfig unter **IPv6** > **Router-Advertisement** > **Präfix-Liste**.

SNMP-ID:

2.70.2.6

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements**

Interface-Name

Bestimmen Sie hier den Namen der RAS-Schnittstelle, für die dieser Präfix-Pool gelten soll.

SNMP-ID:

2.70.2.6.1

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

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

Default-Wert:

leer

Start-Praefix-Pool

Definieren Sie hier das erste Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db8::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

SNMP-ID:

2.70.2.6.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

Default-Wert:

leer

Ende-Praefix-Pool

Definieren Sie hier das letzte Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db9:FFFF::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

SNMP-ID:

2.70.2.6.3

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

Default-Wert:

::

Praefix-Laenge

Definieren Sie hier die Länge des Präfixes, das der Einwahl-Benutzer per Router-Advertisement zugewiesen bekommt. Die Größe des Einwahl-Pools richtet sich nur nach dem ersten und letzten Präfix. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool zugewiesen.

Damit ein Client aus dem Präfix per Autokonfiguration eine IPv6-Adresse bilden kann, muss die Präfix-Länge immer 64 Bit betragen.

SNMP-ID:

2.70.2.6.4

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

Default-Wert:

64

Adv.-OnLink

Gibt an, ob das Präfix "On Link" ist.

SNMP-ID:

2.70.2.6.5

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Adv.-Autonomous

Gibt an, ob ein Client das Präfix für eine "Stateless Address Autoconfiguration (SLAAC)" verwenden kann.

SNMP-ID:

2.70.2.6.6

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Adv.-Pref.-Lifetime

Legt die Dauer in Millisekunden fest, für die eine IPv6-Adresse als "Preferred" gilt. Diese Lifetime verwendet der Client auch für seine generierte IPv6-Adresse. Wenn die Lifetime des Präfix abgelaufen ist, nutzt der Client auch nicht mehr die entsprechende IPv6-Adresse. Ist diese "Preferred Lifetime" einer Adresse abgelaufen, so wird sie als "deprecated" markiert. Nur noch bereits aktive Verbindungen verwenden diese Adresse bis zum Verbindungsende. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

SNMP-ID:

2.70.2.6.7

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

604800

Adv.-Valid-Lifetime

Definiert die Dauer in Sekunden, nach der die Gültigkeit einer IPv6-Adresse abläuft. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

SNMP-ID:

2.70.2.6.8

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

2592000

4.3 Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste

Der RADIUS-Client kann RADIUS-Attribute wie „Framed-IP-Address“ etc. von einem externen RADIUS-Server anfragen und diese dann z. B. dem PPPoE-Server zur Verfügung stellen, um diese am PPPoE-, PPTP- oder L2TP-Server zu authentifizieren. Die folgenden Attribute werden vom LANCOM in Access-Accept-Nachrichten akzeptiert:

96

Framed-Interface-ID

Das Attribut definiert den IPv6-Interface-Identifier, der für den Benutzer im IPv6CP festgelegt werden soll.

97

Framed-IPv6-Prefix

Präfix, welches dem Benutzer über Router Advertisements übermittelt wird.

99

Framed-IPv6-Route

Dieses Attribut definiert die Route, die für diesen Benutzer festgelegt werden soll. Das Gerät legt in der IPv6-Routing-Tabelle diese Route mit Next-Hop zu diesem Benutzer an.

100

Framed-IPv6-Pool

Angabe des IPv6-Pools, aus dem ein Präfix für den Benutzer bereitgestellt werden soll. Der IPv6-Pool wird per Name referenziert und muss unter **IPv6** > **Router Advertisement** > **Präfix-Pool** vorhanden sein.

123

Delegated-IPv6-Prefix

Präfix, welches dem Benutzer über DHCPv6 Präfix Delegierung übermittelt wird.

Die neu verfügbaren RADIUS-Attribute sind nach den RFCs 3162 und 4818 implementiert. Ein Beispiel für einen PPP-Benutzer `test` mit IPv6 im FreeRADIUS lautet wie folgt:

```
test Cleartext-Password := "1234"
 Service-Type = Framed-User,
 Framed-Protocol = PPP,
 Framed-IPv6-Prefix = "fec0:1:2400:1::/64",
 Delegated-IPv6-Prefix = "fec0:1:2400:1100::/56",
 Framed-IP-Address = 172.16.3.33,
```

Der Benutzer "test" erhält in einer Dual Stack PPP-Session die IPv4-Adresse 172.16.3.33, per Router Advertisement das Präfix fec0:1:2400:1::/64 sowie per DHCPv6-Präfix Delegation das Präfix fec0:1:2400:1100::/56.

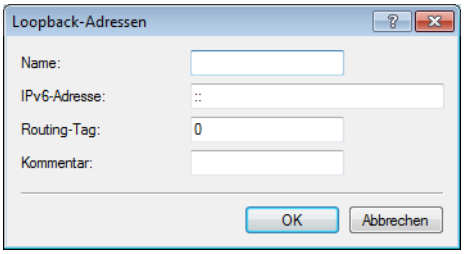
4.4 Loopback-Adressen für IPv6

Ab LCOS 9.00 lassen sich IPv6-Loopback-Adressen als Absenderadresse für den Ping-Befehl über die Kommandozeile verwenden.

Parameter	Bedeutung
-6 <Loopback-Interface>	Setzt ein IPv6-Loopback-Interface als Absenderadresse.

4.4.1 Loopback-Adressen

In der Tabelle **Loopback-Adressen** lassen sich IPv6-Loopback-Adressen festlegen. Das Gerät sieht jede dieser Adressen als eigene Adresse an, die auch dann verfügbar ist, wenn z. B. eine physikalische Schnittstelle deaktiviert ist.



Die Einträge in der Tabelle **Loopback-Adressen** haben folgende Bedeutung:

- **Name**: Vergeben Sie hier einen eindeutigen Namen für diese Loopback-Adresse.
- **IPv6-Adresse**: Geben Sie hier eine gültige IPv6-Adresse ein.
- **Routing-Tag**: Geben Sie hier das Routing-Tag des Netzes an, zu dem die Loopback-Adresse gehört. Nur die Pakete mit dem entsprechenden Routing-Tag erreichen diese Adresse.
- **Kommentar**: Tragen Sie hier einen optionalen Kommentar ein.

4.4.2 Ergänzungen im Setup-Menü

Loopback

Hier können Sie IPv6-Loopback-Adressen festlegen. Das Gerät sieht jede dieser Adressen als eigene Adresse an, die auch dann verfügbar ist, wenn z. B. eine physikalische Schnittstelle deaktiviert ist.

SNMP-ID:

2.70.4.3

Pfad Telnet:

Setup > **IPv6** > **Netz**

Name

Vergeben Sie hier einen eindeutigen Namen für diese Loopback-Adresse.

SNMP-ID:

2.70.4.3.1

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

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

Default-Wert:

leer

IPv6-Loopback-Addr.

Geben Sie hier eine gültige IPv6-Adresse ein.

SNMP-ID:

2.70.4.3.2

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 39 Zeichen aus `0123456789ABCDEFabcdef:./`

Default-Wert:

leer

Rtg-Tag

Geben Sie hier das Routing-Tag des Netzes an, zu dem die Loopback-Adresse gehört. Nur die Pakete mit dem entsprechenden Routing-Tag erreichen diese Adresse.

SNMP-ID:

2.70.4.3.3

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

0

Kommentar

Tragen Sie hier einen optionalen Kommentar ein.

SNMP-ID:

2.70.4.3.4

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

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

Default-Wert:

leer

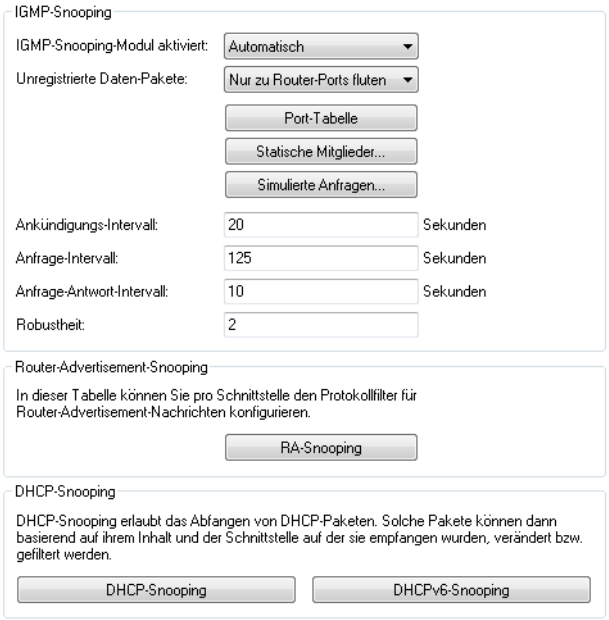
4.5 Lightweight-DHCPv6-Relay-Agent (LDRA)

Im Gegensatz zu einem DHCPv6-Relay-Agent, der über alle IPv6-Funktionen (wie z. B. ICMPv6) verfügt und Datenpakete im Netz routen kann (Layer-3), ermöglicht ein Lightweight-DHCPv6-Relay-Agent nach RFC 6221 nur die Erzeugung und Weitergabe von Relay-Agent-Informationen zwischen DHCPv6-Clients und DHCPv6-Servern (Layer-2).

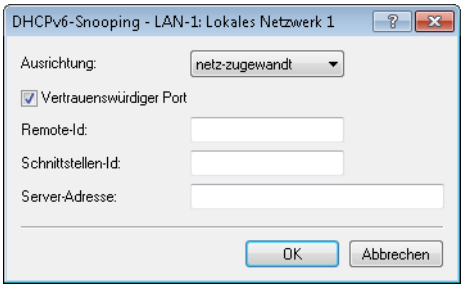
Anders als beim DHCPv4-Snooping fügt der LDRA den DHCPv6-Paketen nicht einfach Informationen zum Relay-Agent an, sondern er verpackt die Nachricht des Clients in eine eigene Option, stellt seinen Relay-Agent-Header voran und schickt erst anschließend dieses DCHPv6-Paket mit zusätzlichen Informationen an den DHCPv6-Server weiter (Relay Forward Message).

Der DHCPv6-Server wertet dieses Datenpaket aus und schickt eine gleichermaßen verpackte Antwort an den Relay-Agent. Der extrahiert die Nachricht und sendet sie an den anfragenden Client (Relay Reply Message).

Im LANconfig können Sie das DHCPv6-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCPv6-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Ausrichtung

Hier aktivieren bzw. deaktivieren Sie das DHCPv6-Snooping. Die folgende Auswahl ist möglich:

- **netz-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit einem DHCPv6-Server.
- **client-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit den ans Netz angeschlossenen DHCPv6-Clients.

In der Werkseinstellung **netz-zugewandt** ist der LDRA deaktiviert.

Vertrauenswürdiger Port

Der LDRA leitet sowohl DHCP-Anfragen von Clients als auch DHCP-Antworten von DHCP-Servern weiter, wenn diese Option aktiviert ist. Ist diese Schnittstelle als nicht vertrauenswürdig eingestuft, verwirft der LDRA DHCPv6-Anfragen an dieser Schnittstelle. DHCPv6-Antworten, die nicht die korrekte Interface-ID enthalten, leitet der LDRA ebenfalls nicht an den Client weiter.

Remote-Id

Die Remote-ID nach RFC 4649 kennzeichnet eindeutig den Client, der eine DHCPv6-Anfrage stellt.

Schnittstellen-Id

Die Interface-ID kennzeichnet eindeutig die Schnittstelle, über die ein Client eine DHCPv6-Anfrage stellt.

Server-Adresse

Hier können Sie die IPv6-Adresse eines DHCPv6-Servers festlegen.

Lassen Sie dieses Feld leer, wenn Sie Antworten von allen DHCPv6-Servern im Netz erhalten wollen. Ansonsten reagiert der LDRA nur auf DHCPv6-Antworten des Servers, dessen Adresse Sie angegeben haben. Antworten von anderen DHCPv6-Servern verwirft der LDRA in diesem Fall.

Sie können für **Remote-Id** und **Schnittstellen-Id** die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

4.5.1 Ergänzungen im Setup-Menü

DHCPv6-Snooping

Hier können Sie den Lightweight-DHCPv6-Relay-Agent konfigurieren.

SNMP-ID:

2.20.41

Pfad Telnet:

Setup > **LAN-Bridge**

Port

Zeigt das physikalische oder logische Interface an, für das die DHCPv6-Snooping-Konfiguration gültig ist.

SNMP-ID:

2.20.41.1

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen
WLAN-x
Alle physikalischen WLAN-Schnittstellen
WLAN-x-x
Alle logischen WLAN-Schnittstellen
P2P-x-x
Alle logischen P2P-Schnittstellen
WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

Orientierung

Aktivieren bzw. deaktivieren Sie hier das DHCPv6-Snooping.

SNMP-ID:

2.20.41.2

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

Netz-seitig
Deaktiviert das DHCPv6-Snooping für dieses Interface. Der LDRA leitet keine DHCPv6-Anfragen an einen DHCPv6-Server weiter.
Client-seitig
Aktiviert das DHCPv6-Snooping für dieses Interface.

Default-Wert:

Netz-seitig

Typ

Bestimmen Sie hier, wie der DHCP-Relay-Agent mit der "Relay Agent Info" in ankommenden DHCP-Datenpaketen umgehen soll.

SNMP-ID:

2.20.41.3

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

vertrauenswuerdig

Der LDRA leitet sowohl DHCP-Anfragen von Clients als auch DHCP-Antworten von DHCP-Servern weiter.

nicht-vertrauenswuerdig

Ist diese Schnittstelle als nicht vertrauenswürdig eingestuft, verwirft der LDRA DHCPv6-Server-Anfragen an dieser Schnittstelle. Das verhindert, dass unbefugte Clients als "Rogue DHCPv6-Server" agieren können. DHCPv6-Antworten, die nicht die korrekte Interface-ID enthalten, leitet der LDRA ebenfalls nicht an den Client weiter.

Schnittstellen, die Clients zugewandt sind, sollten grundsätzlich als nicht vertrauenswürdig festgelegt sein.

Default-Wert:

vertrauenswuerdig

Remote-Id

Die Remote-ID nach RFC 4649 kennzeichnet eindeutig den Client, der eine DHCPv6-Anfrage stellt.

Diese Option ist analog zur DHCP-Option "Remote-ID" des Relay-Agenten bei IPv4.

Sie können die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.41.4

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

max. 30 Zeichen `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Interface-Id

Die Interface-ID kennzeichnet eindeutig die Schnittstelle, über die ein Client eine DHCPv6-Anfrage stellt.

Sie können die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.41.5

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

max. 30 Zeichen `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Server-Adresse

Hier können Sie die IPv6-Adresse eines DHCPv6-Servers festlegen.

Lassen Sie dieses Feld leer, wenn Sie Antworten von allen DHCPv6-Servern im Netz erhalten wollen. Ansonsten reagiert der LDRA nur auf DHCPv6-Antworten des Servers, dessen Adresse Sie angegeben haben. Antworten von anderen DHCPv6-Servern verwirft der LDRA in diesem Fall.

SNMP-ID:

2.20.41.6

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCPv6-Snooping**

Mögliche Werte:

max. 39 Zeichen `0123456789ABCDEFabcdef:.`

Default-Wert:

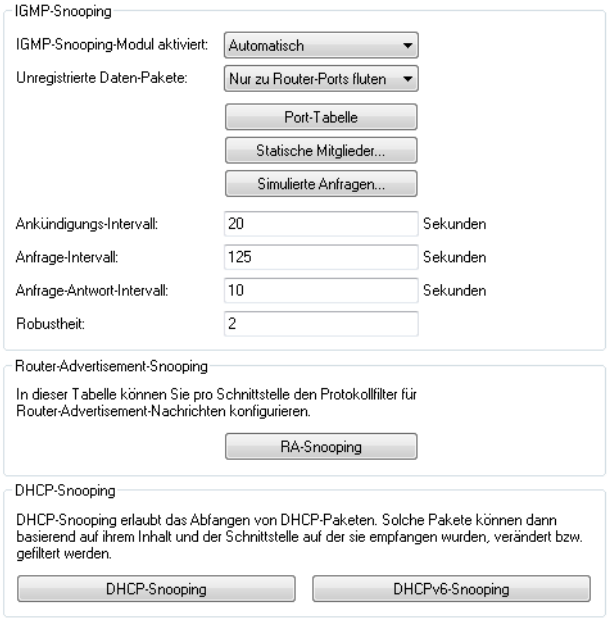
leer

4.6 Router-Advertisement-Snooping

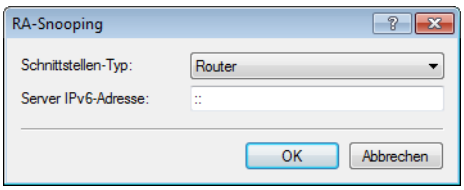
In einem IPv6-Netz senden Router periodisch oder auf Anfrage Router-Advertisments, um sich angeschlossenen Clients als Gateway zu präsentieren. Diesen Mechanismus können Angreifer wie beim DHCPv4 nutzen, um anfragenden Clients eine fehlerhafte oder schadhafte Netzkonfiguration zu übermitteln.

Beim RA-Snooping vermittelt das Gerät nur Router-Advertisements von Routern, nicht aber von Clients. Über die Angabe einer Router-Adresse lassen sich die Router-Advertisments auf einen bestimmten Router als Sender einschränken.

Im LANconfig können Sie das RA-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **RA-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Schnittstellen-Typ

Bestimmen Sie hier den bevorzugten Schnittstellen-Typ. Die folgende Auswahl ist möglich:

- **Router**: Das Gerät vermittelt alle RAs, die an dieser Schnittstelle ankommen (Default).
- **Client**: Das Gerät verwirft alle RAs, die an dieser Schnittstelle ankommen.

Router-Adresse

Sofern Sie den Schnittstellen-Typ **Router** gewählt haben, geben Sie hier eine optionale Router-Adresse an. Bei Angabe einer Router-Adresse vermittelt das Gerät nur RAs des entsprechenden Routers.

Unter dem Schnittstellen-Typ **Client** ignoriert das Gerät dieses Eingabefeld.

4.6.1 Ergänzungen im Setup-Menü

RA-Snooping

Hier können Sie den das RA-Snooping konfigurieren.

SNMP-ID:

2.20.42

Pfad Telnet:

Setup > **LAN-Bridge**

Port

Zeigt das physikalische oder logische Interface an, für das die RA-Snooping-Konfiguration gültig ist.

SNMP-ID:

2.20.42.1

Pfad Telnet:

Setup > **LAN-Bridge** > **RA-Snooping**

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen
WLAN-x
Alle physikalischen WLAN-Schnittstellen
WLAN-x-x
Alle logischen WLAN-Schnittstellen
P2P-x-x
Alle logischen P2P-Schnittstellen
WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

Orientierung

Bestimmen Sie hier den bevorzugten Schnittstellen-Typ.

SNMP-ID:

2.20.42.3

Pfad Telnet:

Setup > **LAN-Bridge** > **RA-Snooping**

Mögliche Werte:

Router

Das Gerät vermittelt alle RAs, die an dieser Schnittstelle ankommen.

Client

Das Gerät verwirft alle RAs, die an dieser Schnittstelle ankommen.

Default-Wert:

Router

Router-Adresse

Sofern Sie den Schnittstellen-Typ **Router** gewählt haben, geben Sie hier eine optionale Router-Adresse an. Bei Angabe einer Router-Adresse vermittelt das Gerät nur RAs des entsprechenden Routers. Unter dem Schnittstellen-Typ **Client** ignoriert das Gerät dieses Eingabefeld.

SNMP-ID:

2.20.42.4

Pfad Telnet:

Setup > **LAN-Bridge** > **RA-Snooping**

Mögliche Werte:

max. 39 Zeichen `0123456789ABCDEFabcdef:.`

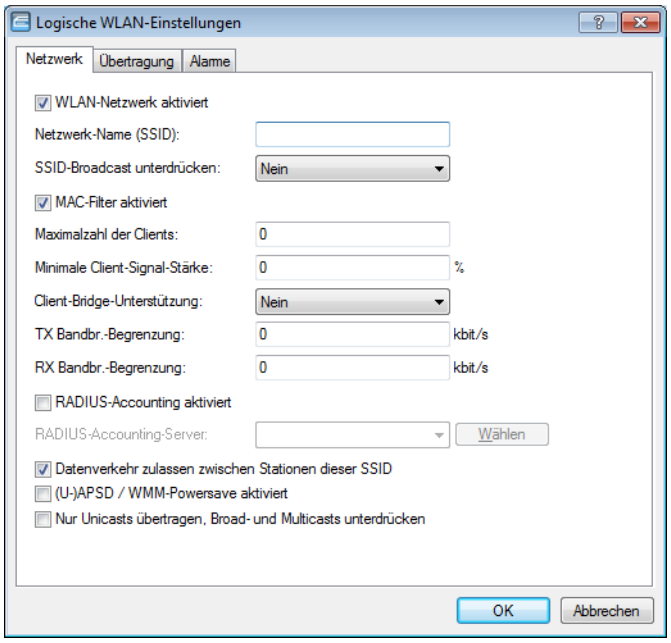
Default-Wert:

leer

5 RADIUS

5.1 Getrennte RADIUS-Accounting-Server pro SSID

Ab LCOS 9.00 haben Sie die Möglichkeit, einzelnen logischen WLAN-Interfaces separate RADIUS-Accounting-Server zuzuweisen.



Die nachfolgenden Einstellungen nehmen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** vor.

- **RADIUS-Accounting aktiviert**

  Aktivieren Sie die Option, um RADIUS-Accounting für diese SSID einzuschalten.

- **RADIUS-Accounting-Server**

  Geben Sie einen RADIUS-Accounting-Server für die betreffende SSID an. Die hier auswählbaren Server definieren Sie in der Tabelle **Wireless-LAN** > **Stationen** > **RADIUS-Accounting-Server**.

5.1.1 Ergänzungen im Setup-Menü

Server

In dieser Tabelle legen Sie optional alternative RADIUS-Accounting-Server für logische WLAN-Interfaces fest. Dadurch erhalten Sie die Möglichkeit, für ausgewählte WLAN-Interfaces spezielle Accounting-Server an Stelle des global festgelegten einzusetzen.

SNMP-ID:

2.12.45.17

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting**

Name

Name des RADIUS-Servers, welcher das Accounting von WLAN-Clients durchführt. Sie verwenden den hier eingetragenen Namen, um aus anderen Tabellen auf den betreffenden Server zu referenzieren.

SNMP-ID:

2.12.45.17.1

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting.

SNMP-ID:

2.12.45.17.3

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Schluessel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend festgelegt ist.

SNMP-ID:

2.12.45.17.4

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, an die der RADIUS Accounting-Server seine Antwort-Nachrichten schickt. Wählen Sie dazu aus:

- Name des IP-Netzs (ARF-Netz), dessen Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets
- `DMZ` für die Adresse der ersten DMZ

Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!

- `LB0...LBF` für eine der 16 Loopback-Adressen oder deren Name
- Beliebige IPv4-Adresse

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet!

Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

SNMP-ID:

2.12.45.17.5

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der Accounting-Server verwendet.

SNMP-ID:

2.12.45.17.6

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Backup

Name des RADIUS-Backup-Servers, welcher das Accounting von WLAN-Clients durchführt, falls der eigentliche Accounting-Server nicht verfügbar ist. Auf diese Weise lassen sich auch Backup-Server miteinander verketten, um mehrere Ausfall-Server festzulegen ("Backup-Chaining").

SNMP-ID:

2.12.45.17.7

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Server**

Mögliche Werte:

Name aus **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**

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

Default-Wert:

leer

Host-Name

Geben Sie hier die IPv4- oder IPv6-Adresse oder den Host-Namen des RADIUS-Servers an, mit dem der RADIUS-Client das Accounting von WLAN-Clients durchführt.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

Die allgemeinen Werte für Wiederholung und Timeout müssen Sie im RADIUS-Bereich ebenfalls festlegen.

SNMP-ID:

2.12.45.17.8

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Accounting** > **Servers**

Mögliche Werte:

IPv4-/IPv6-Adresse oder Hostname, max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Accounting-Server

Über diesen Parameter definieren Sie einen RADIUS-Accounting-Server für die ausgewählte logische WLAN-Schnittstelle.

SNMP-ID:

2.23.20.1.22

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Name aus **Setup** > **WLAN** > **RADIUS-Accounting** > **Server**

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

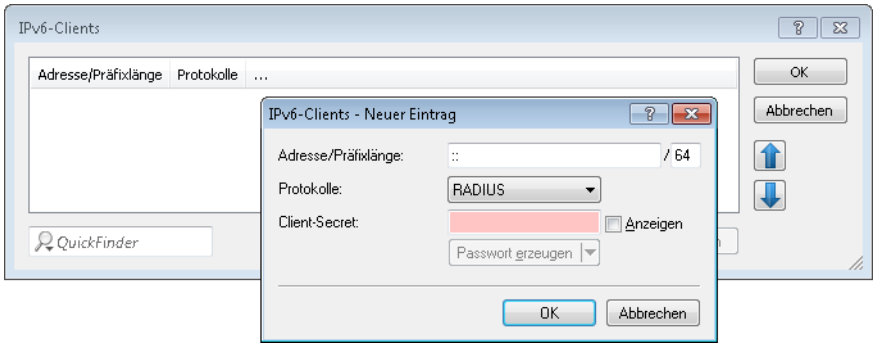
Default-Wert:

leer

5.2 Zugang zum RADIUS-Server über IPv6

Ab LCOS 9.00 ist der RADIUS-Server auch für IPv6-Clients erreichbar. In LANconfig können Sie diese Clients unter **RADIUS-Server** > **Allgemein** mit Klick auf die Schaltfläche **IPv6-Clients** konfigurieren.

IPv6-Clients



Folgende Werte sind je Client einzutragen:

Adresse/Präfixlänge

IP-Adresse (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Kennwort gilt.

Für die Verwendung einer Adresse muss die Präfix-Länge 128 Bit betragen. Der Eintrag "fd00::/64" z. B. erlaubt das gesamte Netzwerk, der Eintrag "fd00::1/128" erlaubt hingegen nur genau einen Client.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Kennwort, das die Clients für den Zugang zum internen Server benötigen.

Damit der RADIUS-Server für IPv6-Clients erreichbar ist, muss ggf. in der IPv6-Firewall eine entsprechende Inbound-Regel eingetragen sein.

5.2.1 Ergänzungen im Setup-Menü

IPv6-Clients

Hier bestimmen Sie die RADIUS-Zugangsdaten von IPv6-Clients.

SNMP-ID:

2.25.10.16

Pfad Telnet:

Setup > **RADIUS** > **Server**

Adress-Praefix-Laenge

Dieser Wert legt das IPv6-Netz und die Präfix-Länge fest, z. B. "fd00::/64". Der Eintrag "fd00::/64" z. B. erlaubt das gesamte Netz, der Eintrag "fd00::1/128" erlaubt hingegen nur genau einen Client.

SNMP-ID:

2.25.10.16.1

Pfad Telnet:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

Default-Wert:

leer

Adress-Praefix-Laenge

Dieser Wert legt das Kennwort fest, das die Clients für den Zugang zum internen Server benötigen.

SNMP-ID:

2.25.10.16.2

Pfad Telnet:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Mögliche Werte:

max. 43 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Protocols

Diese Auswahl legt das Protokoll fest für die Kommunikation zwischen dem internen Server und den Clients.

SNMP-ID:

2.25.10.16.4

Pfad Telnet:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Mögliche Werte:

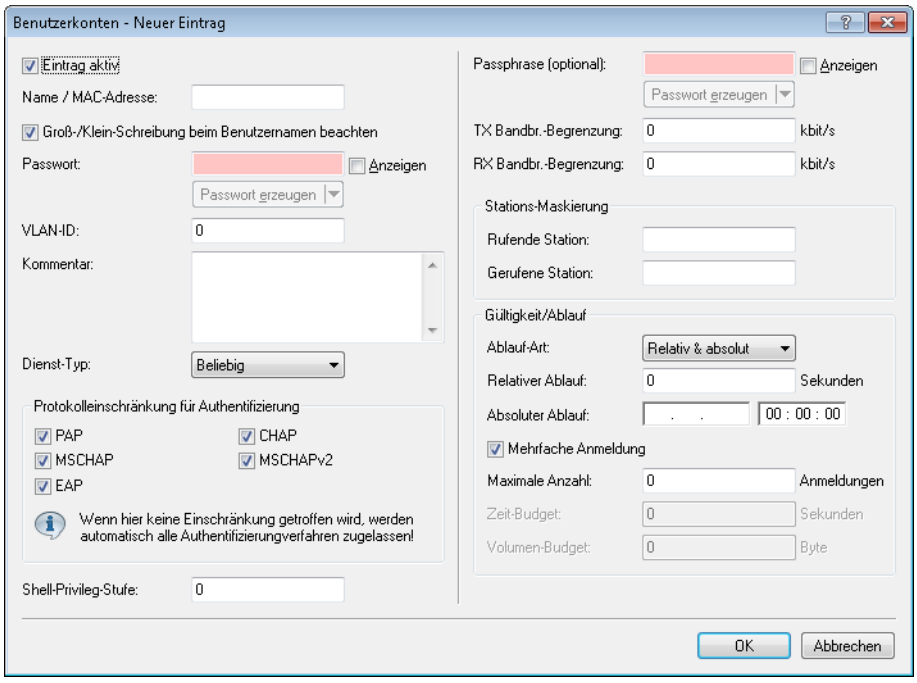
RADIUS
RADSEC
Alle

Default-Wert:

RADIUS

5.3 Zusätzliches Shell-Privilege-Level-Attribut im RADIUS-Server

Ab LCOS 9.00 unterstützt der Radius-Server ein Vendor spezifisches RADIUS-Attribut, um in einem RADIUS-Accept die Privilegstufe des Nutzers zu kommunizieren. Dieses Attribut lässt sich im LANconfig unter **RADIUS-Server** > **Allgemein** > **Benutzerkonten** festlegen.



5.3.1 Über RADIUS in die LCOS-Verwaltungsoberfläche einloggen

Aktuell können sich Benutzer über RADIUS, TACACS+ oder die interne Benutzerverwaltung des Gerätes in die Verwaltungsoberfläche eines Gerätes einloggen. Mit RADIUS ist das für folgende Protokolle möglich:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

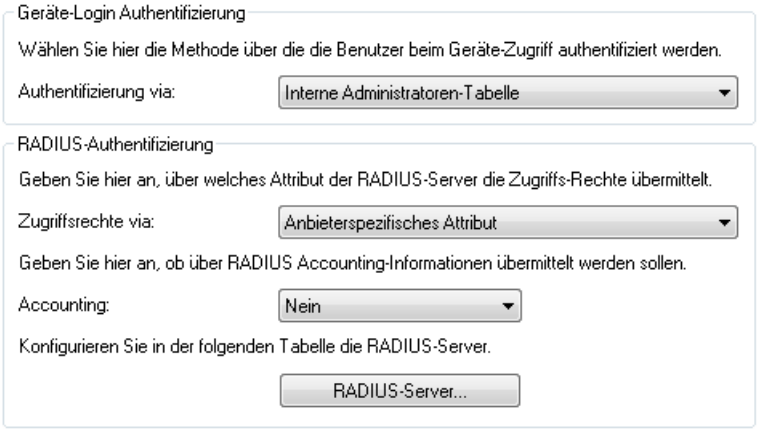
Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im Gerät gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Autorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netz-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

1. Bei der Anmeldung sendet das Gerät die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im Gerät gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem Gerät eine entsprechende Nachricht, und das Gerät bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem Gerät mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das Gerät die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und – wenn vorhanden – den genutzten Port.

Im LANconfig können Sie die Authentifizierungsmethode unter **Management** > **Authentifizierung** festlegen.



Geräte-Login Authentifizierung

Im Abschnitt **Geräte-Login Authentifizierung** wählen Sie die Methode aus, über die sich Benutzer beim Zugriff auf die Verwaltungsoberfläche des Gerätes authentifizieren sollen:

- **Interne Administratoren-Tabelle**: Das Gerät übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.
- **RADIUS**: Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netz.
- **TACACS+**: Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netz.

RADIUS-Authentifizierung

Im Abschnitt **RADIUS-Authentifizierung** geben Sie die notwendigen RADIUS-Server-Daten sowie zusätzliche Verwaltungsdaten an.

Zugriffssrechte via

Im RADIUS-Server ist die Autorisierung der Anwender gespeichert. Bei einer Anfrage sendet der RADIUS-Server die Zugriffs- und Funktionsrechte zusammen mit den Login-Daten an das Gerät, das daraufhin den Anwender mit entsprechenden Rechten einloggt.

Normalerweise sind Zugriffsrechte im RADIUS Management-Privilege-Level (Attribut 136) festgelegt, sodass das Gerät den übertragenen Wert nur auf die internen Zugriffsrechte zu mappen braucht. Es kann jedoch auch sein, dass der RADIUS-Server zusätzlich Funktionsrechte übertragen soll oder das Attribut 136 bereits anderweitig bzw. andere, hersteller-spezifische Attribute für die Autorisierung verwendet. In diesem Fall kann das Gerät auch eine herstellerabhängige Autorisierung auswerten.

- **Anbieterspezifisches Attribut**: Das Gerät wertet das anbieterspezifische Attribut aus.
- **Management-Privilege-Level-Attribut**: Das Gerät wertet das Management-Privilege-Level-Attribut des RADIUS-Servers aus.
- **Shell-Privilege Attribut**: Das Gerät wertet das Shell-Privilege Attribut des RADIUS-Servers aus.

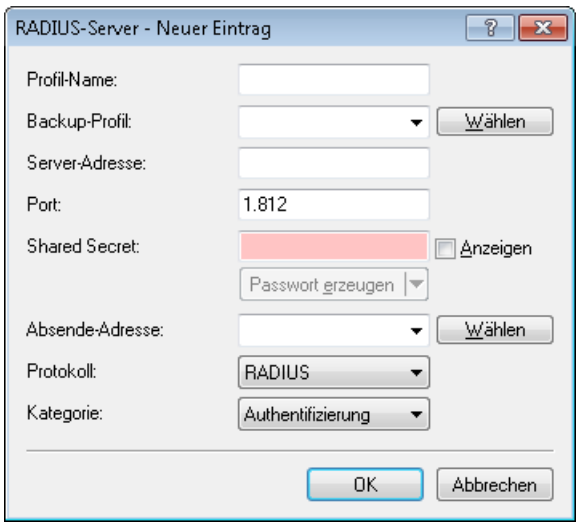
Accounting

Hier bestimmen Sie, ob das Gerät die Sitzung des Anwenders aufzeichnet.

- **Nein**: Das Gerät zeichnet die Sitzung nicht auf.
- **Ja**: Das Gerät zeichnet die Sitzung auf (Start, Ende, Benutzername, Authentifizierungsmodus, Port).

RADIUS-Server

In dieser Tabelle können Sie die Einstellungen für den RADIUS-Server vornehmen



- **Profil-Name**: Vergeben Sie hier einen Namen für den RADIUS-Server.
- **Backup-Profil**: Geben Sie den Namen des alternativen RADIUS-Servers an, an den das Gerät Anfragen weiterleitet, wenn der erste RADIUS-Server nicht erreichbar ist.

  Für den Backup-Server müssen Sie einen weiteren Eintrag in der Server-Tabelle vornehmen.

- **Server-Adresse**: Vergeben Sie hier die IPv4-Adresse des RADIUS-Servers.
- **Port**: Geben Sie hier den Port an, über den der RADIUS-Server mit dem Gerät kommuniziert.
- **Shared Secret**: Geben Sie hier das Kennwort für den Zugang zum RADIUS-Server an und wiederholen Sie es im zweiten Eingabefeld.

- **Absende-Adresse**: Hier können Sie optional eine Absende-Adresse festlegen, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.
- **Protokoll**: Geben Sie hier das Protokoll an, mit dem der RADIUS-Server mit dem Gerät kommuniziert.
- **Kategorie**: Bestimmen Sie, für welche Kategorie der RADIUS-Server gelten soll.

5.3.2 Ergänzungen im Setup-Menü

Zugriffsrechte-Uebertragung

Im RADIUS-Server ist die Autorisierung der Anwender gespeichert. Bei einer Anfrage sendet der RADIUS-Server die Zugriffs- und Funktionsrechte zusammen mit den Login-Daten an Ihr Gerät, welches daraufhin den Anwender mit entsprechenden Rechten einloggt.

Normalerweise sind Zugriffsrechte im RADIUS Management-Privilege-Level (Attribut 136) festgelegt, sodass das Gerät den übertragenen Wert nur auf die internen Zugriffsrechte zu mappen braucht (Option **mapped**). Das Attribut kann die folgenden Werte annehmen, die das Gerät anschließend mappt:

Attribut	Zugriffsrechte
1	User, nur lesen
3	User, nur schreiben
5	Admin, nur lesen, keine Trace-Rechte
7	Admin, schreiben und lesen, keine Trace-Rechte
9	Admin, nur lesen
11	Admin, schreiben und lesen
15	Supervisor

Alle anderen Werte mappt das Gerät auf 'Kein Zugriff'.

Es kann jedoch auch sein, dass der RADIUS-Server zusätzlich Funktionsrechte übertragen soll oder das Attribut 136 bereits anderweitig bzw. andere, hersteller-spezifische Attribute für die Autorisierung verwendet. In diesem Fall müssen Sie herstellerabhängige Attribute auswählen. Diese Attribute sind wie folgt festgelegt, basierend auf der Herstellerkennung '2356':

- Zugriffsrechte-ID: 11
- Funktionsrechte-ID: 12

Die übertragenen Werte für die Zugriffsrechte sind identisch zu den oben genannten. Soll der RADIUS-Server auch Funktionsrechte mit übertragen, dann erreichen Sie das wie folgt:

1. Öffnen Sie die Konsole des Gerätes.
2. Wechseln Sie in das Verzeichnis **Setup** > **Config** > **Admins**.
3. Der Befehl `set ?` zeigt Ihnen das aktuelle Mapping von Funktionsrechten zum entsprechenden Hexadezimalcode (z. B. `Device-Search (0x80)`).
4. Um Funktionsrechte zu kombinieren, addieren Sie deren Hex-Werte.
5. Wandeln Sie den hexadezimalen Wert in eine Dezimalzahl um.
6. Diesen Dezimalwert können Sie in der Funktionsrechte-ID verwenden, um die entsprechenden Funktionsrechte zu übertragen.

SNMP-ID:

2.11.81.2

Pfad Telnet:

Setup > **Config** > **Radius**

Mögliche Werte:

Herstellerabhaengig
Mapped
Shell-Privileg

Default-Wert:

Herstellerabhaengig

Shell-Priv.-Level

Dieses Feld enthält ein Vendor spezifisches RADIUS-Attribut, um in einem RADIUS-Accept die Privilegstufe des Nutzers zu kommunizieren.

SNMP-ID:

2.25.10.7.21

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Benutzer**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

5.4 RADIUS-Client: Alternative Angabe von Hostnamen statt IP-Adressen

Ab LCOS 9.00 ist die Angabe einer RADIUS-Serveradresse als IPv4- oder IPv6-Adresse sowie alternativ als DNS-Name möglich.

Mit dieser Erweiterung ändern sich die folgenden Pfade im Setup-Teil des LCOS-Menübaums.

- **2.2.22.11: Server-Hostname** ersetzt **2.2.22.2: Server-Adresse**
- **2.12.29.16: Server-Hostname** ersetzt **2.12.29.1: Server-Adresse**
- **2.12.29.17: Backup-Server-Hostname** ersetzt **2.12.29.4: Backup-Server-IP-Adresse**
- **2.12.45.17.8: Host-Name** ersetzt **2.12.45.17.2: Server-Adresse**
- **2.24.3.13: Auth.-Server-Host-Name** ersetzt **2.24.3.2: Auth.-Server-Adresse**
- **2.24.3.14: Acc.-Server-Host-Name** ersetzt **2.24.3.5: Acc.-Server-Adresse**
- **2.25.10.3.13: Host-Name** ersetzt **2.25.10.3.2: IP-Adresse**
- **2.25.10.3.14: Host-Name** ersetzt **2.25.10.3.8: Accnt.-IP-Adresse**
- **2.30.3.8: Host-Name** ersetzt **2.30.3.2: IP-Adresse**

5.4.1 Ergänzungen im Setup-Menü

Server-Hostname

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie die Benutzer zentral verwalten möchten.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.2.22.11

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Server-Hostname

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem der RADIUS-Client die Berechtigungen von WLAN-Clients über die MAC-Adresse prüft (Authentifizierung).

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

Zur Nutzung der RADIUS-Funktion für WLAN-Clients müssen Sie im LANconfig unter **Wireless-LAN** > **Stationen** für den Parameter **Stationen filtern** die Option "Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern" auswählen. Die allgemeinen Werte für Wiederholung und Timeout müssen Sie im RADIUS-Bereich ebenfalls festlegen.

Im RADIUS-Server müssen Sie die WLAN-Clients folgendermaßen eintragen:

- Der Benutzername ist die MAC-Adresse im Format AABBCC-DDEEFF
- Das Passwort ist für alle Benutzer identisch mit dem Schlüssel (Shared-Secret) für den RADIUS-Server.

SNMP-ID:

2.12.29.16

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Zugriffspruefung**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Backup-Server-Hostname

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des Backup-RADIUS-Servers an, mit dem der RADIUS-Client die Berechtigungen von WLAN-Clients über die MAC-Adresse prüft (Authentifizierung).

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.12.29.17

Pfad Telnet:

Setup > **WLAN** > **RADIUS-Zugriffspruefung**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Auth.-Server-Host-Name

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, den der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter kontaktiert.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.24.3.13

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Anbieter-Tabelle**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Acc.-Server-Host-Name

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, den der Public-Spot für das Accounting der Zugänge bei diesem Anbieter kontaktiert.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.24.3.14

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Anbieter-Tabelle**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Host-Name

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, an den der RADIUS-Client die Anfrage von WLAN-Clients weiterleiten soll.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.25.10.3.13

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Weiterleit-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Host-Name

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, an den der RADIUS-Client die Accounting-Datenpakete weiterleitet.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.25.10.3.14

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Weiterleit-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Host-Name

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an.

Der RADIUS-Client erkennt automatisch, um welchen Adresstyp es sich handelt.

SNMP-ID:

2.30.3.8

Pfad Telnet:

Setup > **IEEE802.1x** > **RADIUS-Server**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Besondere Werte:

DEFAULT

Der Name "DEFAULT" ist reserviert für alle WLAN-Netze, die eine Authentifizierung über IEEE 802.1x nutzen und die keinen RADIUS-Server definiert haben. Jedes WLAN, das eine Authentifizierung über IEEE 802.1x verwendet, kann den eigenen RADIUS-Server durch die Angabe des entsprechenden Wertes in "Schlüssel1/Passphrase" nutzen.

5.5 EAP-SIM-Modul im RADIUS-Server

Ab LCOS 9.00 enthält der RADIUS-Server ein EAP-SIM-Modul, welches das Gerät um die Fähigkeit erweitert, das Home Location Register (HLR) eines Mobilfunkproviders zu simulieren. Ein HLR generiert in der Regel die nötigen Keys für die registrierten SIM-Karten, damit ein RADIUS-Server einen Client per EAP-SIM authentifizieren kann.

Die notwendigen Keys lassen sich im RADIUS-Server manuell festlegen und hinterlegen, sodass ein HLR nicht notwendig ist. EAP-SIM wird z. B. im Zusammenhang mit Hotspot 2.0 verwendet.

5.5.1 Ergänzungen im Setup-Menü

EAP-SIM

802.11u-Netze ermöglichen den WLAN-Clients im Empfangsbereich, sich automatisch per Zugangsdaten der SIM-Karte des entsprechenden Providers an dessen Hot-Spot anzumelden.

In diesem Verzeichnis legen Sie die SIM-Zugangsdaten für die automatische Authentifizierung fest.

SNMP-ID:

2.25.10.10.18

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP**

Card-Keys

In dieser Tabelle konfigurieren Sie die jeweilige SIM-Karten für die automatische Authentifizierung mit EAP-SIM.

SNMP-ID:

2.25.10.10.18.1

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM**

Benutzername

Tragen Sie hier den Benutzernamen für die EAP-SIM-Authentifizierung ein. Der Benutzername setzt sich bei EAP-SIM aus

- einer führenden `1`,
- dem Mobile Country Code (MCC),
- dem Mobile Network Code (MNC),
- der International Mobile Subscriber Identity (IMSI) sowie
- dem @Realm

zusammen. Dadurch ergibt sich die folgende Syntax:

```
Syntax:   1<MCC><MNC><IMSI>@<Realm>
Example:  1262011234567890@wlan.mnc001.mcc262.3gppnetwork.org
```

SNMP-ID:

2.25.10.10.18.1.1

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 48 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.# `

Default-Wert:

leer

Rufende-Station-Id-Maske

Mit dieser Maske schränken Sie die Gültigkeit des Eintrags auf bestimmte IDs ein. Die betreffende ID wird von der rufenden Station (WLAN-Client) übermittelt. Bei der Authentifizierung über 802.1x wird die MAC-Adresse der rufenden Station im ASCII-Format übertragen (nur Großbuchstaben). Die einzelnen Zeichenpaare werden dabei durch einen Bindestrich getrennt (z. B. `00-10-A4-23-19-C0`).

SNMP-ID:

2.25.10.10.18.1.5

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

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

Besondere Werte:

*****

Mit dem * als Platzhalter lassen sich ganze Gruppen von IDs erfassen und als Maske definieren.

Default-Wert:

leer

Gerufene-Station-Id-Maske

Mit dieser Maske schränken Sie die Gültigkeit des Eintrags auf bestimmte IDs ein. Die betreffende ID wird von der gerufenen Station (BSSID und SSID eines AP) übermittelt. Bei der Authentifizierung über 802.1x wird die MAC-Adresse (BSSID) der gerufenen Station im ASCII-Format übertragen (nur Großbuchstaben). Die einzelnen Zeichenpaare werden dabei durch einen Bindestrich getrennt; die SSID wird nach einem Doppelpunkt als Trennzeichen angehängt (z. B. `00-10-A4-23-19-C0:AP1`).

SNMP-ID:

2.25.10.10.18.1.6

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

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

Besondere Werte:

*****

Mit dem * als Platzhalter lassen sich ganze Gruppen von IDs erfassen und als Maske definieren.

Mit der Maske `*:AP1` definieren Sie beispielsweise einen Eintrag, der für einen Client in der Funkzelle mit dem Namen `AP1` gilt – egal über welchen AP sich der Client eingebucht hat. Auf diese Weise kann der Client von einem AP zum nächsten wechseln (Roaming) und jeweils mit den gleichen Authentifizierungsdaten arbeiten.

Default-Wert:

leer

Rand1

Die Authentifizierung über GSM basiert auf einem Challenge-Response-Mechanismus mit Zufallszahlen und Authentifizierungsschlüsseln. In diesem Feld bestimmen Sie die eine 128 Bit lange Zufallszahl, die der Client zur Erstellung zweier Schlüssel (Authentifizierung, Verschlüsselung der Nutzdaten) zugeschickt bekommt.

SNMP-ID:

2.25.10.10.18.1.7

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

SRES1

Dieses Feld enthält den Schlüssel SRES (Signed RESponse), den der Client aus der 128 Bit langen Zufallszahl zur korrekten Authentifizierung generieren muss.

SNMP-ID:

2.25.10.10.18.1.8

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

Kc1

Dieses Feld enthält den Schlüssel Kc (Ciphering Key), den der Client aus der 128 Bit langen Zufallszahl zur Verschlüsselung der Nutzdaten erzeugen muss.

SNMP-ID:

2.25.10.10.18.1.9

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

Rand2

Die Authentifizierung über GSM basiert auf einem Challenge-Response-Mechanismus mit Zufallszahlen und Authentifizierungsschlüsseln. In diesem Feld bestimmen Sie die eine 128 Bit lange Zufallszahl, die der Client zur Erstellung zweier Schlüssel (Authentifizierung, Verschlüsselung der Nutzdaten) zugeschickt bekommt.

SNMP-ID:

2.25.10.10.18.1.10

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

SRES2

Dieses Feld enthält den Schlüssel SRES (Signed RESponse), den der Client aus der 128 Bit langen Zufallszahl zur korrekten Authentifizierung generieren muss.

SNMP-ID:

2.25.10.10.18.1.11

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

Kc2

Dieses Feld enthält den Schlüssel Kc (Ciphering Key), den der Client aus der 128 Bit langen Zufallszahl zur Verschlüsselung der Nutzdaten erzeugen muss.

SNMP-ID:

2.25.10.10.18.1.12

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

Rand3

Die Authentifizierung über GSM basiert auf einem Challenge-Response-Mechanismus mit Zufallszahlen und Authentifizierungsschlüsseln. In diesem Feld bestimmen Sie die eine 128 Bit lange Zufallszahl, die der Client zur Erstellung zweier Schlüssel (Authentifizierung, Verschlüsselung der Nutzdaten) zugeschickt bekommt.

SNMP-ID:

2.25.10.10.18.1.13

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

SRES3

Dieses Feld enthält den Schlüssel SRES (Signed RESponse), den der Client aus der 128 Bit langen Zufallszahl zur korrekten Authentifizierung generieren muss.

SNMP-ID:

2.25.10.10.18.1.11

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

Kc3

Dieses Feld enthält den Schlüssel Kc (Ciphering Key), den der Client aus der 128 Bit langen Zufallszahl zur Verschlüsselung der Nutzdaten erzeugen muss.

SNMP-ID:

2.25.10.10.18.1.15

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-SIM** > **Card-Keys**

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

6 Public Spot

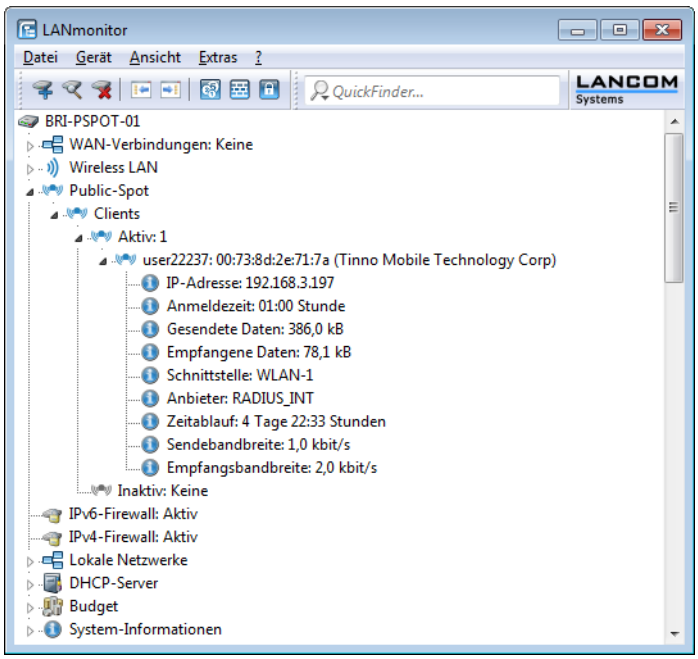
6.1 Rufnummernformat bei Smart Ticket

Ab Version 9.00 überprüft LCOS die eingegebene Rufnummer auf ungültige Zeichen. Erlaubt sind ausschließlich Zahlen zwischen 0 und 9. Der Nutzer muss 5 bis 15 Zahlen (exklusive Landesvorwahl) eingeben.

6.2 Public Spot-Clients anzeigen

Sie haben die Möglichkeit, sich im LANmonitor detaillierte Informationen zu Public Spot-Clients anzeigen zu lassen.

1. Öffnen Sie den Menüzweig **Public-Spot** > **Clients**.
2. Doppelklicken Sie auf **Aktiv**, um aktive Clients anzuzeigen, oder auf **Inaktiv**, um inaktive Clients anzuzeigen.
3. Doppelklicken Sie auf einen Client, um detaillierte Informationen zu diesem abzurufen.



6.3 Public Spot-Benutzern Werbung einblenden

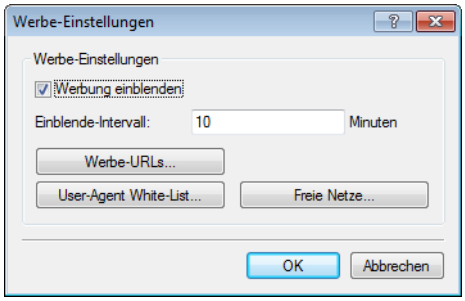
Sie haben die Möglichkeit, Public Spot-Benutzern in konfigurierbaren Zeitabständen Werbung einzublenden. Der Public Spot zeigt die Werbung im normalen Browser-Fenster des Benutzers an und nicht über Pop-ups, da alle modernen Browser Pop-ups in der Regel blocken. In der Public Spot-Stationstabelle gibt es somit drei Zustände für einen Client:

- Authentifiziert: Der Client ist angemeldet und darf surfen.
- Unauthentifiziert: Der Client ist nicht angemeldet und darf nicht surfen.

- Werbung: Der Client wird beim nächsten Aufruf einer URL auf eine Werbeseite umgeleitet.

Dabei haben Sie die Möglichkeit, über eine Whitelist bestimmte Netze und User-Agents von den Werbe-Einblendungen auszunehmen.

1. Wählen Sie in der Geräte-Konfiguration den Menüzweig **Public-Spot** > **Server** aus und klicken Sie dort auf **Werbe-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Werbung einblenden**.



Sie haben jetzt die Möglichkeit, den Einblende-Intervall zu verändern und weitere Einstellungen vorzunehmen.

3. Geben Sie unter **Einblende-Intervall** ein Intervall in Minuten, nach dem der Public Spot einen Benutzer auf eine Werbe-URL umleitet. Bei einem Intervall von `0` erfolgt die Umleitung direkt nach der Anmeldung.
4. Klicken Sie auf **Werbe-URLs**, um eine Werbe-URL hinzuzufügen. Wenn Sie mehrere Werbe-URLs hinzufügen, blendet der Public Spot diese im festgelegten Intervall nacheinander ein.
5. Optional: Klicken Sie auf **User-Agent White-List**, um User-Agents hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt.
6. Optional: Klicken Sie auf **Freie Netze**, um Netze hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt. Hier besteht beispielsweise die Möglichkeit, die automatischen Such-URLs der Browser eingeben, z. B. `*.google.com`. Normalerweise sendet ein Browser jede Tastatureingabe in der Adressleiste an eine Suchmaschine; durch das Setzen der Ausnahme reagiert die Werbeseite aber nicht auf diesen Zugriff.

   Anmeldungsfreie Netze sind generell werbefrei. Eine explizite Aufnahme derartiger Netze in die Whitelist ist somit nicht erforderlich.
7. Schließen Sie alle Dialoge durch einen Klick auf **OK**.

Public Spot-Benutzer werden nach Ablauf des Einblende-Intervalls auf eine Werbe-URL umgeleitet, sofern ihr User-Agent nicht auf der White-List steht oder sie sich innerhalb eines Freien Netzes bewegen.

Der Zeitpunkt der Werbe-Einblendungen bezieht sich auf die Session-Zeit eines aktiven Public Spot-Clients. Sendet ein Client eine bestimmte Zeit keine Daten, so verschiebt sich auch der Zeitpunkt, zu dem der Public Spot das nächste Mal Werbung einblendet.

6.3.1 Ergänzungen im Setup-Menü

Werbung

An dieser Stelle haben Sie die Möglichkeit, Werbe-Einblendungen ein- oder auszuschalten und zu bearbeiten.

SNMP-ID:

2.24.43

Pfad Telnet:

Setup > **Public-Spot-Modul**

Aktiv

An dieser Stellen schalten Sie die Werbe-Einblendungen ein oder aus.

SNMP-ID:

2.24.43.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Intervall

An dieser Stelle geben Sie ein Intervall ein, nach dem der Public Spot einen Benutzer auf eine Werbe-URL umleitet.

SNMP-ID:

2.24.43.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Mögliche Werte:

0 … 65535 Minuten

Default-Wert:

10

Besondere Werte:

0

Die Umleitung erfolgt direkt nach der Anmeldung.

URL

An dieser Stelle fügen Sie Werbe-URLs hinzu. Wenn Sie mehrere URLs eingeben, blendet der Public Spot diese im festgelegten Intervall nacheinander ein.

SNMP-ID:

2.24.43.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Mögliche Werte:

max. 150 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

Inhalt

SNMP-ID:

2.24.43.3.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung** > **URL**

Mögliche Werte:

max. 150 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

User-Agent-White-List

An dieser Stelle fügen Sie User-Agents hinzu, die der Public Spot von Werbe-Einblendungen ausnimmt.

SNMP-ID:

2.24.43.4

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Mögliche Werte:

max. 150 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

User-Agent

SNMP-ID:

2.24.43.4.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung** > **User-Agent-White-List**

Mögliche Werte:

max. 150 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

WISPr-Redirect-URL-Verarbeiten

Enthält die Access-Accept-Nachricht des RADIUS-Servers das Attribut 'WISPr-Redirection-URL', so wird der Public-Spot-Client nach erfolgreicher Authentifizierung auf diese URL umgeleitet. Dabei verhält das Szenario genauso, als ob 'LCS-Advertisement-URL=beliebig' und 'LCS-Advertisement-Interval=0' vom RADIUS-Server zurückgegeben werden. Der Schalter **aktiv** braucht nicht gesetzt zu werden. Es reicht das Attribut 'WISPr-Redirection-URL'. Diese Konfiguration kann immer dann eingesetzt werden, wenn ein Client einmalig nach der Authentifizierung (z. B. MAC-Authentifizierung) auf eine Seite umgeleitet werden soll.

SNMP-ID:

2.24.43.5

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Freie-Netze

An dieser Stelle fügen Sie Netze hinzu, die der Public Spot von Werbe-Einblendungen ausnimmt.

SNMP-ID:

2.24.43.6

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung**

Host-Name

Tragen Sie die IP-Adresse des zusätzlichen Netzwerks oder Servers ein, auf den die Public Spot-Benutzer werbefreien Zugriff erhalten.

Alternativ haben Sie auch die Möglichkeit, Domain-Namen (mit oder ohne Wildcard "*") einzutragen. Durch Wildcards können Sie z. B. auch den werbefreien Zugriff auf alle Subdomains einer Domäne erlauben. Der Eintrag `*.google.com` gibt somit auch die Adressen `mail.google.com`, `maps.google.com` etc. frei.

SNMP-ID:

2.24.43.6.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung** > **Freie-Netze**

Mögliche Werte:

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

Default-Wert:

leer

Maske

Tragen Sie die Netzmaske des zusätzlichen Netzwerks oder Servers ein, auf den die Public Spot-Benutzer werbefreien Zugriff erhalten.

Wenn Sie nur eine einzelne Station mit der zuvor benannten Adresse oder eine Domain freischalten wollen, geben Sie als Netzmaske `255.255.255.255` ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie dafür die zugehörige Netzmaske an. Sofern Sie keine Netzmaske setzen (Wert `0.0.0.0`), ignoriert das Gerät den betreffenden Tabelleneintrag.

SNMP-ID:

2.24.43.6.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Werbung** > **Freie-Netze**

Mögliche Werte:

max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

6.3.2 Ergänzungen zu den RADIUS-Attributen

Folgende herstellerspezifischen RADIUS-Attribute wertet der Public Spot im Access Accept des RADIUS-Authentifizierungs-Servers zusätzlich aus.

Der Schalter **Werbung aktiv** braucht nicht gesetzt zu werden. Es reicht alleine das Vorhandensein der Attribute in der RADIUS-Nachricht.

26

Vendor 2356(LCS) Id 13

LCS-Advertisement-URL

Definiert eine kommaseparierte Liste von Werbe-URLs.

26

Vendor 2356(LCS) Id 14

LCS-Advertisement-Interval

Definiert das Intervall in Minuten, nach dem der Public Spot einen Benutzer an eine Werbe-URL umleitet. Bei einem Intervall von `0` erfolgt die Umleitung direkt nach der Anmeldung.

6.4 Zusätzliche Attribute für die XML-Schnittstelle

Mit LCOS 9.00 erweitert sich die Umfang der Attribute, die Ihnen für das Anlegen eines neuen Benutzers über die XML-Schnittstelle zu Verfügung stehen. Die untenstehenden Attribute entsprechen weitgehend den Parametern, die auch über die RADIUS-Benutzertabelle konfigurierbar sind.

Folgende XML-Elemente kann das XML-Interface künftig ebenfalls im **Login-Request** verarbeiten:

`VLAN_ID` (optional)

Individuelle VLAN-ID, die das Gerät dem Public Spot-Benutzer beim Login zuweist. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das XML-Interface erhalten würde.

Der Wert `0` deaktiviert die Verwendung eines VLANs.

`PROVIDER` (teilweise erforderlich)

Name des RADIUS-Servers, den der Public Spot für den Benutzer verwendet (Authentifizierung und Accounting). Wenn Sie keinen RADIUS-Server angeben, verwendet der Public Spot den für das Modul global konfigurierten Server.

Dieses XML-Element ist zwingend erforderlich, wenn Sie

- für das Public Spot-Modul mehrere RADIUS-Server konfiguriert haben.
- die XML-Schnittstelle ohne RADIUS-Authentifizierung, aber mit RADIUS-Accounting verwenden wollen.

In den übrigen Fällen ist die Angabe dieses XML-Elements optional.

Der referenzierte RADIUS-Server muss in der Konfiguration vorhanden sein.

`TXRATELIMIT` (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Uplink zur Verfügung steht.

`RXRATELIMIT` (optional)

Maximale Bandbreite (in KBit/s), die dem Public Spot-Benutzer im Downlink zur Verfügung steht.

`SECONDSEXPIRE` (optional)

Nutzungsdauer (die maximale Online-Zeit) für einen Benutzer-Account in Sekunden. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Der Wert `0` schaltet die Überwachung der Nutzungsdauer aus.

`TRAFFICEXPIRE` (optional)

Maximales Datenvolumen für einen Benutzer-Account in Bytes. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Der Wert `0` schaltet die Überwachung des Datenvolumens aus.

6.5 Dynamische Änderung einer Benutzersitzung über die XML-Schnittstelle

Für die Anmeldung eines Public Spot-Benutzers ohne Änderungen während des Anmeldezeitraums genügt der Parameter `RADIUS_LOGIN`. Mittels `RADIUS_CoA` hingegen haben Sie die Möglichkeit, die für einen Public Spot-Benutzer geltenden Rahmenbedingungen auch während einer laufenden Sitzung zu verändern. Dazu sendet Ihr externes

Hotspot-Gateway einen `RADIUS-CoA-Request` an den Public Spot, welcher die darin enthaltenen Änderungen direkt auf die **Stations-Tabelle** unter **Status** > **Public-Spot** überträgt.

Ein möglicher Anwendungsfall für CoA-Nachrichten ist z. B. die automatische Drosselung der Bandbreite: Hat ein Public Spot-Benutzer sein Volumenbudget verbraucht, kann ein externe Hotspot-Gateway diesen Benutzer drosseln, indem das Hotspot-Gateway nach Auswerten der Accounting-Daten eine entsprechende CoA-Nachricht an den Public Spot schickt

Die XML-Nachrichten für die Verhandlung zwischen Hotspot-Gateway und Public Spot sehen wie folgt aus:

RADIUS-CoA-Request

Das externe Gateway sendet die Daten für die Änderung einer Sitzung an den Public Spot. Der Public Spot ändert daraufhin die Sitzungsdaten des angemeldeten Benutzers 'user2350' in der Stations-Tabelle:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Im obigen Beispiel werden dem Benutzer eine Sitzungsdauer von 3.600 Sekunden sowie ein übertragbares Datenvolumen von 10.000.000 Byte bei einer Sende- und Empfangsbandbreite von 100 kBit/s zugewiesen.

RADIUS-CoA-Response:

Das XML-Interface sendet eine Bestätigung über die Änderung der Sitzungsdaten an das externe Hotspot-Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

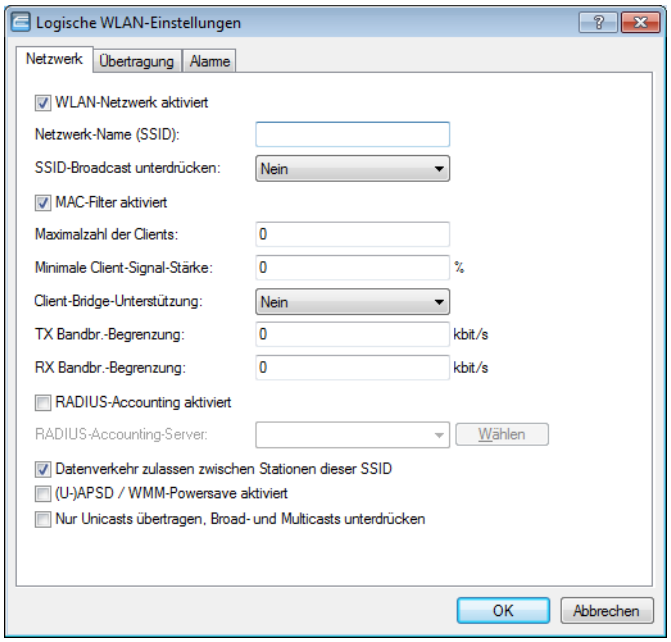
Im Falle des Drosselungsbeispiels betrifft die Änderung der Benutzersitzung immer das Kontingent, das dem Benutzer ab Änderungszeitpunkt noch zusteht. War der Benutzer z. B. bereits eine Stunde angemeldet, stehen ihm nach der Änderung des Zeitkontingents auf sechs Stunden anschließend noch fünf Stunden zur Verfügung. Fällt das zugewiesene Zeitkontingent dagegen geringer aus als der Benutzer bereits angemeldet ist, loggt der Public Spot den betreffenden Nutzer aus und sendet eine Logout-Nachricht an das Hotspot-Gateway.

7 WLAN

7.1 Client-Bridge-Modus und Bandbreitenlimit pro SSID festlegen

Ab LCOS 9.00 haben Sie die Möglichkeit, Client-Bridge-Modus und Bandbreitenlimits für einzelne SSIDs festzulegen.

Änderungen auf Standalone-APs



Die nachfolgenden Einstellungen nehmen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** vor.

- **Client-Bridge-Unterstützung**

  Aktivieren Sie diese Option für einen Access Point, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

  Sie können den Client-Bridge-Modus ausschließlich zwischen zwei LANCOM-Geräten verwenden.

- **TX Bandbr.-Begrenzung**

  Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

- **RX Bandbr.-Begrenzung**

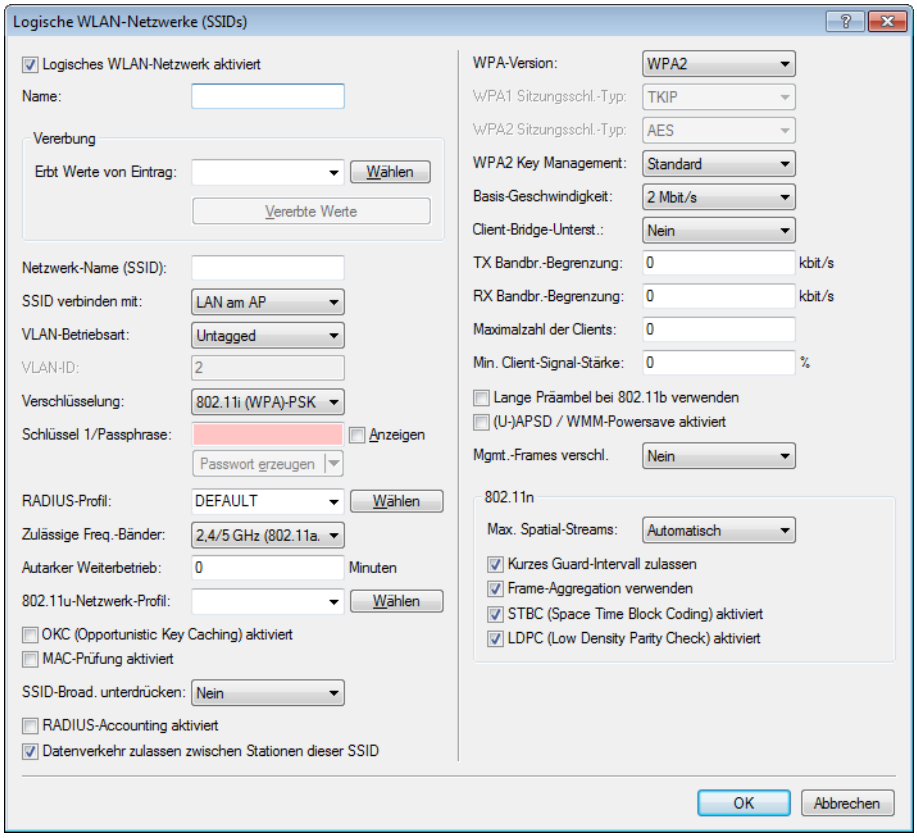
  Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

In Folge dessen entfallen die gleichnamigen Einstellungen im LANconfig unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** > **Client-Modus** sowie im WEBconfig die folgenden Menüpunkte:

- **Setup** > **Schnittstellen** > **WLAN** > **Client-Einstellungen** > **Cl.-Brg.-Support**

- **Setup** > **Schnittstellen** > **WLAN** > **Client-Einstellungen** > **Tx-Limit**
- **Setup** > **Schnittstellen** > **WLAN** > **Client-Einstellungen** > **Rx-Limit**

Änderungen auf WLCs



Die für einen Standalone-AP hinzugefügten Erläuterungen zu den Änderungen in LANconfig gelten für einen WLC unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** analog.

7.1.1 Ergänzungen im Setup-Menü

Cl.-Brg.-Support

Während mit der Adress-Anpassung nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.

Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestoßen werden.

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

SNMP-ID:

2.23.20.1.11

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netz**

Mögliche Werte:

Ja

Aktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.

Nein

Deaktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.

Exklusiv

Akzeptiert nur Clients, die ebenfalls den Client-Bridge-Modus unterstützen.

Default-Wert:

Nein

Tx-Limit

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID.

SNMP-ID:

2.23.20.1.20

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

Rx-Limit

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID.

SNMP-ID:

2.23.20.1.21

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

Tx-Limit

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID.

SNMP-ID:

2.37.1.1.44

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

Rx-Limit

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID.

SNMP-ID:

2.37.1.1.45

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

7.2 Trennung von P2P- und WLAN/SSID-Konfiguration

Ab LCOS 9.00 sind die Übertragungs- und Verschlüsselungseinstellungen für P2P-Verbindungen getrennt von den Einstellungen des 1. logischen WLAN-Netzes im verwendeten physikalischen WLAN-Interface konfigurierbar. Als Verwaltungsnetz für den Verbindungaufbau und die Erreichbarkeitsprüfung ('Alive') eines Punkt-zu-Punkt-Partner verwenden die betreffenden Geräte künftig nicht mehr die dazugehörige SSID, sondern die fixe SSID ***** P2P INFO *****.

Dieses Feature bildet u. a. die Grundlage für den Aufbau von *AutoWDS-Netzen*.

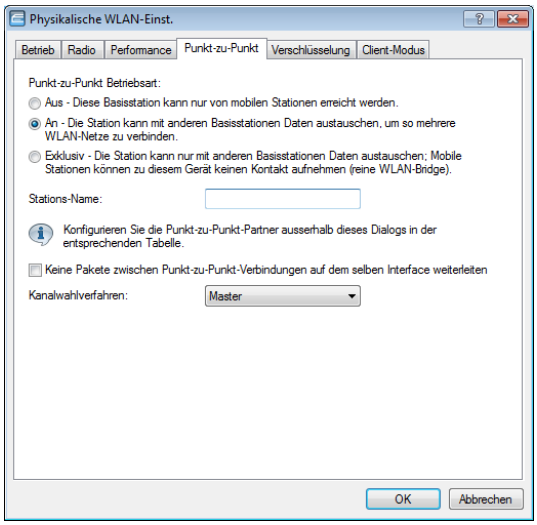
7.2.1 Konfiguration von P2P-Verbindungen

Bei der Konfiguration von Punkt-zu-Punkt-Verbindungen (P2P-Verbindungen) geben Sie neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren wahlweise die MAC-Adressen oder die Stationsnamen der Gegenstellen an. Die Konfiguration kann in LANconfig entweder über den Setup-Assistenten **WLAN konfigurieren** oder manuell über den Konfigurationsdialog erfolgen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie manuell eine verschlüsselte oder unverschlüsselte P2P-Basis-Konfiguration erstellen.

Parallel zu einer P2P-Verbindung spannen die betreffenden APs automatisch je eine fixe SSID ***** P2P INFO ***** auf. Diese SSID dient als reines Verwaltungsnetz für den Verbindungaufbau und die Erreichbarkeitsprüfung ('Alive') eines Punkt-zu-Punkt-Partners. Den WLAN-Clients ist es nicht möglich, sich mit solch einem Netz zu verbinden.

1. Öffnen Sie den Konfigurationsdialog für das Gerät, das als P2P-Master bzw. P2P-Slave agieren soll, und wechseln Sie auf die Seite **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.**.
2. Wählen Sie das WLAN-Interface aus, welches Sie ausschließlich für die P2P-Verbindung benutzen wollen, und wechseln Sie auf die Registerkarte **Punkt-zu-Punkt**.



3. Aktivieren Sie die gewünschte **Punkt-zu-Punkt Betriebsart**, z. B. **An**.
4. Setzen Sie das **Kanalwahlverfahren** auf **Master** bzw. **Slave**.
5. Optional: Sofern die Gegenstelle die physikalische Schnittstelle nicht über die MAC-Adresse, sondern einen Alias-Namen identifizieren soll, geben Sie im Eingabefeld **Stations-Name** eine entsprechende Bezeichnung ein, z. B. P2P_MASTER bzw. P2P_SLAVE.

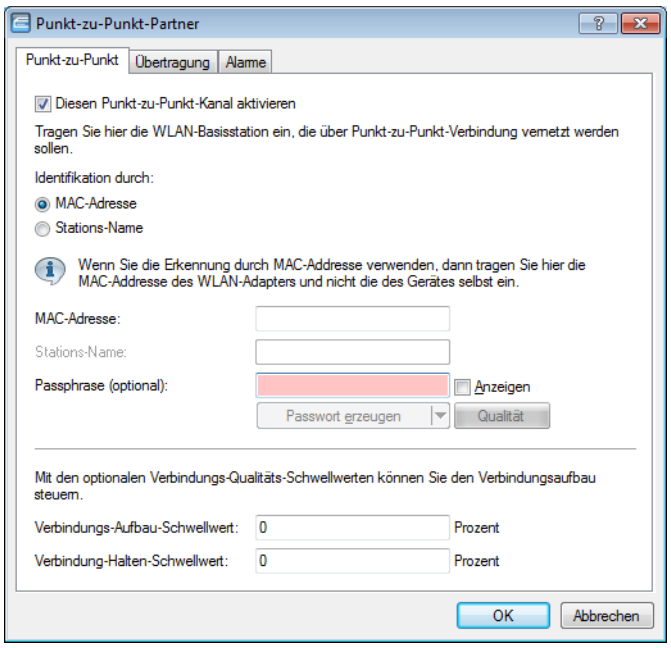
6. Optional: Passen Sie auf der Registerkarte **Verschlüsselung** bei Bedarf die Einstellungen für die IEEE 802.11i-Verschlüsselung der P2P-Verbindung an.

   Mit IEEE 802.11i lässt sich die Sicherheit von Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessern. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security (LEPS).

   Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der physikalischen WLAN-Interfaces. Standardmäßig ist die P2P-Verschlüsselung aktiviert und mit sinnvollen Werten vorbelegt.

   In LCOS-Versionen vor 9.00 sind die Einstellungen zur Verschlüsselung an die Einstellungen für das erste logische WLAN-Netz im verwendeten physikalischen WLAN-Interface gekoppelt (also WLAN-1, wenn Sie das erste WLAN-Modul für die P2P-Verbindung nutzen; WLAN-2, wenn Sie das zweite WLAN-Modul bei einem Access Point mit zwei WLAN-Modulen nutzen). In diesem Fall finden Sie die Einstellungen unter **Wireless-LAN** > **802.11i/WEP** > **WPA- / Einzel-WEP-Einstellungen**.

7. Schließen Sie den Dialog mit **OK** und wählen Sie im Konfigurationdialog auf der gleichen Seite unter **Punkt-zu-Punkt-Partner** eine logische P2P-Verbindung aus, z. B. **P2P-1-1**.



8. Aktivieren Sie auf der Registerkarte **Punkt-zu-Punkt** den gewählten P2P-Kanal und geben Sie an, ob Ihr Gerät die Gegenstelle über eine **MAC-Adresse** oder einen **Stations-Name**n identifiziert. Je nach Auswahl tragen Sie anschließend im gleichnamigen Eingabefeld entweder die MAC-Adresse des physikalischen WLAN-Interfaces, das die Gegenstelle für die P2P-Verbindung benutzt, oder deren Stations-Namen ein.
   Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweiligen Antennenanschlusses am Gehäuse des Gerätes angebracht ist. Verwenden Sie nur die als "WLAN-MAC" oder "MAC-ID" gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!

   Alternativ finden Sie die MAC-Adresse auch im Status-Menü unter **WLAN** > **Interfaces** > **MAC-Adresse**.

9. Geben Sie unter **Passphrase** ein gemeinsames Kennwort aus mindestens 8 Zeichen an (empfohlen: 32 Zeichen), mit dem Sie die P2P-Verbindung zusätzlich verschlüsseln. Die P2P-Verschlüsselung muss dafür aktiviert sein (siehe oben). In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der Access Point diese Informationen an die Gegenseite, um sich dort anzumelden.

10. Optional: Wechsel Sie auf die Registerkarte **Übertragung**, um die Grenzwerte und Einstellung für die Paketübertragung vorzunehmen.

Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der logischen WLAN-Netze. Standardmäßig sind sämtliche Parameter auf Optimierung und Automatik ausgerichtet.

11. Schließen Sie den Dialog mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

12. Nehmen Sie die äquivalenten Konfigurationsschritte für die Gegenstelle (Slave bzw. Master) vor.

7.2.2 Ergänzungen im Setup-Menü

Interpoint-Uebertragung

Diese Tabelle enthält die Übertragungseinstellungen für die einzelnen P2P-Strecken.

SNMP-ID:

2.23.20.19

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Ifc

Name des logischen P2P-Interfaces, welches Sie ausgewählt haben.

SNMP-ID:

2.23.20.19.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auswahl aus den verfügbaren P2P-Strecken.

Paketgroesse

Wählen Sie die maximale Größe von Datenpaketen auf einer P2P-Strecke.

Bei kleinen Datenpaketen ist die Gefahr für Übertragungsfehler geringer als bei großen Paketen, allerdings steigt auch der Anteil der Header-Informationen am Datenverkehr, die effektive Nutzlast sinkt also. Erhöhen Sie den voreingestellten Wert nur, wenn das FunkNetz überwiegend frei von Störungen ist und nur wenig Übertragungsfehler auftreten. Reduzieren Sie den Wert entsprechend, um die Übertragungsfehler zu vermeiden.

SNMP-ID:

2.23.20.19.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

600 … 2347

Default-Wert:

1600

Min-Tx-Rate

Legen Sie die minimale Übertragungsgeschwindigkeit in MBit/s in Senderichtung fest.

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus (Auto). Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Sie haben aber auch die Möglichkeit, durch Angabe einer festen Übertragungsgeschwindigkeit die dynamische Geschwindigkeitsanpassung zu unterbinden.

SNMP-ID:

2.23.20.19.3

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
1M
2M
5,5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default-Wert:

Auto

Max-Tx-Rate

Legen Sie die maximale Übertragungsgeschwindigkeit in MBit/s in Senderichtung fest.

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus (Auto). Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Sie haben aber auch die Möglichkeit, durch Angabe einer festen Übertragungsgeschwindigkeit die dynamische Geschwindigkeitsanpassung zu unterbinden.

SNMP-ID:

2.23.20.19.9

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
1M
2M
5,5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default-Wert:

Auto

EAPOL-Rate

Legen Sie die Datenrate in MBit/s für die Übertragung der EAPOL-Pakete fest.

WLAN-Clients verwenden EAP over LAN (EAPOL) zur Anmeldung über WPA und/oder 802.1x am Access-Point. Dabei kapseln sie die EAP-Pakete zum Austausch der Authentisierungs-Informationen in Ethernet-Frames, um die EAP-Kommunikation über eine Layer-2 Verbindung zu ermöglichen.

In manchen Fällen ist es sinnvoll, die Datenrate für die Übertragung der EAPOL-Pakete niedriger zu wählen als die Datenrate für die Nutzdaten. Bei bewegten WLAN-Clients z. B. kann eine zu hohe Datenrate der EAPOL-Pakete zu Paketverlusten führen und so den Anmeldevorgang deutlich verzögern. Durch die gezielte Auswahl der EAPOL-Datenrate lässt sich dieser Vorgang stabilisieren.

SNMP-ID:

2.23.20.19.19

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

wie-Daten
In dieser Einstellung überträgt das Gerät die EAPOL-Daten mit der gleichen Datenrate wie die Nutzdaten.

1M
2M
5,5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
HT-1-6.5M
HT-1-13M
HT-1-19.5M
HT-1-26M
HT-1-39M
HT-1-52M
HT-1-58.5M
HT-1-65M
HT-2-13M
HT-2-26M
HT-2-39M
HT-2-52M
HT-2-78M
HT-2-104M
HT-2-117M
HT-2-130M

Default-Wert:

wie-Daten

Soft-Retries

Geben Sie die Anzahl der gesamten Sendeversuche an, die das Gerät unternimmt, wenn die Hardware ein Datenpaket nicht senden kann. Die Gesamtzahl der Sendeversuche ergibt sich somit aus der Rechnung `(Soft-Retries + 1) * Hard-Retries`.

Der Vorteil von Soft-Retries auf Kosten von Hard-Retries ist, dass aufgrund des Raten-Adaptionalgorithmus die nächste Serie von Hard-Retries direkt mit einer niedrigeren Rate beginnt.

SNMP-ID:

2.23.20.19.11

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

0 … 255

Default-Wert:

10

Hard-Retries

Geben Sie die Anzahl der Sendeversuche an, die das Gerät unternimmt, bevor die Hardware einen Tx-Fehler meldet. Je kleiner Sie den Wert wählen, desto kürzer blockiert ein nicht zu sendendes Paket den Sender. Sofern die Hardware ein Datenpaket nicht senden kann, haben Sie die Möglichkeit, die Sendeversuche softwareseitig fortzusetzen. Weitere Informationen dazu erhalten Sie unter dem Parameter **Soft-Retries**.

SNMP-ID:

2.23.20.19.12

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

0 … 255

Default-Wert:

10

11b-Praeambel

Legen Sie fest, ob Ihr Gerät im 802.11b-Modus eine lange Präambel verwendet.

Normalerweise handelt jeder WLAN-Client (hier: der P2P-Slave) selbstständig die notwendige Länge der Präambel zur Kommunikation mit der Basisstation (hier: dem P2P-Master) aus. In einigen seltenen Fällen ist es jedoch erforderlich, diese Aushandlung zu ignorieren und die lange WLAN-Präambel zu benutzen, obwohl dies wenig vorteilhaft ist.

Schalten Sie die lange WLAN-Präambel nur dann ein, wenn genau dies Ihre Wireless-Probleme löst.

SNMP-ID:

2.23.20.19.7

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto

Der P2P-Slave handelt die notwendige Länge der Präambel (kurz/lang) zur Kommunikation mit dem P2P-Master automatisch aus.

Lang

Der P2P-Slave nimmt keine Aushandlung vor und benutzt immer eine lange Präambel.

Default-Wert:

Auto

Min.-HT-MCS

MCS (Modulation Coding Scheme) dient der automatischen Geschwindigkeitsanpassung und definiert im 802.11n-Standard eine Reihe von Variablen, die beispielsweise die Anzahl der Spatial-Streams, Modulation und die Datenrate eines jeden Datenstroms festlegen.

In der Werkseinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich während des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

Weiterhin haben Sie die Möglichkeit, die MCS bewusst auf einen konstanten Wert einzustellen. Das kann für den Testbetrieb hilfreich sein oder bei wechselnden Umgebungsbedingungen ein unnötiges Parametrieren vermeiden, wenn kein optimaler Betriebspunkt zu erwarten ist.

SNMP-ID:

2.23.20.19.16

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default-Wert:

Auto

Max.-HT-MCS

MCS (Modulation Coding Scheme) dient der automatischen Geschwindigkeitsanpassung und definiert im 802.11n-Standard eine Reihe von Variablen, die beispielsweise die Anzahl der Spatial-Streams, Modulation und die Datenrate eines jeden Datenstroms festlegen.

In der Werkseinstellung wählt die Station automatisch die für den jeweiligen Stream optimalen MCS entsprechend den derzeitigen Kanalbedingungen aus. Wenn sich während des Betriebs beispielsweise Interferenzen durch Bewegung des Senders oder Abschwächung des Signals ergeben und sich dadurch die jeweiligen Kanalbedingungen ändern, wird das MCS dynamisch an die neuen Bedingungen angepasst.

Weiterhin haben Sie die Möglichkeit, die MCS bewusst auf einen konstanten Wert einzustellen. Das kann für den Testbetrieb hilfreich sein oder bei Chaotischen Umgebungsbedingungen ein unnötiges Parametrieren vermeiden, wenn sowieso kein optimaler Betriebspunkt zu erwarten ist.

SNMP-ID:

2.23.20.19.17

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default-Wert:

Auto

Nutze-STBC

Aktivieren Sie hier das Space Time Block Coding (STBC).

STBC ist eine Methode zur Verbesserung der Empfangsbedingungen. Die Funktion variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen.

Wenn der WLAN-Chipsatz STBC nicht unterstützt, lässt sich dieser Parameter nicht auf **Ja** ändern.

SNMP-ID:

2.23.20.19.23

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Nutze-LDPC

Aktivieren Sie hier den Low Density Parity Check (LDPC).

LDPC ist eine Methode zur Fehlerkorrektur. Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von

Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenrate.

Wenn der WLAN-Chipsatz STBC nicht unterstützt, können Sie diesen Wert nicht auf **Ja** ändern.

SNMP-ID:

2.23.20.19.24

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Kurzes-Guard-Intervall

Aktivieren oder deaktivieren Sie das kurze Guard-Intervall.

Das Guard-Intervall dient – grob gesagt – dazu die Störanfälligkeit bei Mehrträgerverfahren (OFDM) durch Intersymbolinterferenz (ISI) zu minimieren. Die Option reduziert die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval). Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite ist das WLAN-System damit anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

SNMP-ID:

2.23.20.19.13

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
Im Automatik-Modus aktiviert das Gerät das kurze Guard-Intervall, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt.

Nein
Deaktiviert das kurze Guard-Intervall.

Default-Wert:

Auto

Min.-Spatiale-Stroeme

Geben Sie die Mindestanzahl der erlaubten Spatial-Streams an.

Die Spatial-Streams fügen der bisherigen Frequenz-Zeit-Matrix vom Prinzip her eine 3. Dimension – den Raum – hinzu. Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was das Gerät zur Steigerung der Übertragungsrate (Spatial-Multiplexing) nutzen kann: Hierbei lassen sich mehrere Datenströme parallel in einem Funkkanal übertragen. Gleichzeitig sind auch mehrere Sende- und Empfangsantennen parallel einsetzbar. Dadurch verbessert sich die Leistung des ganzen Funksystems erheblich.

In der Werkseinstellung stellt das Gerät die Spatial-Streams automatisch ein, um das Funksystem optimal zu nutzen. Alternativ haben Sie die Möglichkeit, die Spatial-Streams auf einen oder zwei einzustellen, um das Funksystem beispielsweise bewusst geringer zu belasten.

SNMP-ID:

2.23.20.19.18

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
Einer
Zwei
Drei

Default-Wert:

Auto

Max.-Spatiale-Stroeme

Geben Sie die Maximalanzahl der erlaubten Spatial-Streams an.

Die Spatial-Streams fügen der bisherigen Frequenz-Zeit-Matrix vom Prinzip her eine 3. Dimension – den Raum – hinzu. Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was das Gerät zur Steigerung der Übertragungsrate (Spatial-Multiplexing) nutzen kann: Hierbei lassen sich mehrere Datenströme parallel in einem Funkkanal übertragen. Gleichzeitig sind auch mehrere Sende- und Empfangsantennen parallel einsetzbar. Dadurch verbessert sich die Leistung des ganzen Funksystems erheblich.

In der Werkseinstellung stellt das Gerät die Spatial-Streams automatisch ein, um das Funksystem optimal zu nutzen. Alternativ haben Sie die Möglichkeit, die Spatial-Streams auf einen oder zwei einzustellen, um das Funksystem beispielsweise bewusst geringer zu belasten.

SNMP-ID:

2.23.20.19.14

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

Auto
Einer
Zwei
Drei

Default-Wert:

Auto

Sende-Aggregate

Über dieser Einstellung konfigurieren Sie den Versand aggregierter Datenpakete. Frame-Aggregation ist als offizieller Standard und herstellerunabhängig im 802.11n Standard vorgesehen. Er gleicht dem seit längerem bekannten Burst-Modus.

Bei der Frame-Aggregation fasst das Gerät – durch Verlängerung des WLAN-Frames – mehrere Datenpakete (Frames) zu einem größeren Paket zusammen und sendet diese gemeinsam. Das Verfahren verkürzt die Wartezeit zwischen den Datenpaketen und reduziert gleichzeitig deren Overhead, wodurch der Datendurchsatz steigt.

Mit zunehmender Länge der Frames steigt allerdings auch die Wahrscheinlichkeit, dass das Gerät durch z. B. Funkstörungen die Pakete erneut senden muss. Außerdem müssen andere Stationen länger auf einen freien Kanal warten und ihre Datenpakete sammeln, bis sie ihrerseits mehrere Pakete auf einmal senden können.

In der Werkseinstellung ist die Frame-Aggregation eingeschaltet. Wenn Sie den Datendurchsatz Ihre Gerätes erhöhen möchten und andere auf diesem Medium nicht von Bedeutung sind, ist dies sinnvoll. Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für Datenübertragungen in Echtzeit wie Voice over IP.

SNMP-ID:

2.23.20.19.15

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Empfange-Aggregate

Über dieser Einstellung konfigurieren Sie den Empfang aggregierter Datenpakete. Frame-Aggregation ist als offizieller Standard und herstellerunabhängig im 802.11n Standard vorgesehen. Er gleicht dem seit längerem bekannten Burst-Modus.

Bei der Frame-Aggregation fasst das Gerät – durch Verlängerung des WLAN-Frames – mehrere Datenpakete (Frames) zu einem größeren Paket zusammen und sendet diese gemeinsam. Das Verfahren verkürzt die Wartezeit zwischen den Datenpaketen und reduziert gleichzeitig deren Overhead, wodurch der Datendurchsatz steigt.

Mit zunehmender Länge der Frames steigt allerdings auch die Wahrscheinlichkeit, dass das Gerät durch z. B. Funkstörungen die Pakete erneut senden muss. Außerdem müssen andere Stationen länger auf einen freien Kanal warten und ihre Datenpakete sammeln, bis sie ihrerseits mehrere Pakete auf einmal senden können.

In der Werkseinstellung ist die Frame-Aggregation eingeschaltet. Wenn Sie den Datendurchsatz Ihre Gerätes erhöhen möchten und andere auf diesem Medium nicht von Bedeutung sind, ist dies sinnvoll. Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für Datenübertragungen in Echtzeit wie Voice over IP.

SNMP-ID:

2.23.20.19.22

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Max.-Aggr.-Paket-Anzahl

Über diesen Parameter definieren Sie, wie viele Pakete das Gerät maximal zu einem Aggregat zusammenfassen darf. Die Aggregierung bei WLAN-Übertragungen nach IEEE 802.11n fasst mehrere Datenpakete zu einem großen Paket zusammen, reduziert so den Overhead und beschleunigt die Übertragung.

SNMP-ID:

2.23.20.19.20

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

0 … 11/16/24 (geräteabhängig)

Besondere Werte:

0

Das Gerät verwendet automatisch den höchsten Wert, der hardwareseitig zulässig ist.

Default-Wert:

0

RTS-Schwelle

Über dieses Eingabefeld legen Sie den RTS-Schwellwert fest. Wenn die Größe der zu sendenden RTS-Pakete diesen Wert überschreitet, verwendet das Gerät das RTS/CTS-Protokoll, um die erhöhte Wahrscheinlichkeit von Kollisionen und damit das 'Hidden-Station'-Phänomen zu vermeiden.

Da RTS-Pakete allgemein recht kurz sind und die Verwendung von RTS/CTS den Overhead erhöht, lohnt sich der Einsatz dieses Verfahrens ausschließlich für längere Datenpakete, bei denen Kollisionen wahrscheinlich sind. Der passende Wert ist in der jeweiligen Umgebung im Versuch zu ermitteln.

Der RTS/CTS-Schwellwert muss auch in den WLAN-Clients entsprechend den Möglichkeiten des Treibers bzw. des Betriebssystems eingestellt werden.

SNMP-ID:

2.23.20.19.6

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

60 … 2347

Default-Wert:

2347

Min.-Frag.-Laenge

Über dieses Eingabefeld definieren Sie die minimale Paket-Fragmentlänge, unterhalb der das Gerät Fragmente von Datenpaketen verwirft.

SNMP-ID:

2.23.20.19.10

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Uebertragung**

Mögliche Werte:

0 … 65535

Besondere Werte:

0, 1

Das Gerät lässt Paket-Fragmente mit beliebiger Länge zu.

Default-Wert:

16

Interpoint-Verschluesselung

Diese Tabelle enthält die Verschlüsselungseinstellungen der physikalischen WLAN-Schnittstelle für P2P-Strecken.

SNMP-ID:

2.23.20.20

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Ifc

Name des physikalischen WLAN-Interfaces

SNMP-ID:

2.23.20.20.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Verschluesselung

Aktiviert oder deaktiviert die WPA-/WEP-Verschlüsselung für P2P-Verbindungen über das betreffende Interface.

SNMP-ID:

2.23.20.20.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Vorgabeschluessel

WEP-Schlüssel, mit welchem das Gerät die über dieses Interface gesendeten Pakete verschlüsselt.

SNMP-ID:

2.23.20.20.3

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

0 … 9

Default-Wert:

1

Methode

Wählt das Verschlüsselungsverfahren bzw. bei WEP die Schlüssellange aus, welche das Gerät für die Verschlüsselung von P2P-Datenpaketen verwendet.

Beachten Sie, dass nicht jeder Client (bzw. dessen WLAN-Hardware) jedes Verschlüsselungsverfahren unterstützt.

SNMP-ID:

2.23.20.20.4

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

802.11i-WPA-PSK
WEP-128-Bit
WEP-104-Bit
WEP-40-Bit

Default-Wert:

802.11i-WPA-PSK

WPA-Version

WPA-Version, die das Gerät einem Client für die WPA-Verschlüsselung anbietet.

SNMP-ID:

2.23.20.20.9

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

WPA1
WPA2
WPA1/2

Default-Wert:

WPA1/2

WPA1-Sitzungsschluessel

Wählen Sie das bzw. die Verfahren aus, die das Gerät der Gegenstelle zur Generierung der WPA-Sitzungs- bzw. -Gruppen-Schlüssel bei WPA1 anbietet. Das Gerät kann das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide anbieten.

SNMP-ID:

2.23.20.20.12

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

TKIP
AES
TKIP/AES

Default-Wert:

TKIP

WPA2-Sitzungsschluessel

Wählen Sie das bzw. die Verfahren aus, die das Gerät der Gegenstelle zur Generierung der WPA-Sitzungs- bzw. -Gruppen-Schlüssel bei WPA2 anbietet. Das Gerät kann das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide anbieten.

SNMP-ID:

2.23.20.20.13

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

TKIP
AES
TKIP/AES

Default-Wert:

AES

WPA-Rekeying-Zyklus

Geben Sie an, in welchen Abständen das Gerät den WPA-Key-Handshake wiederholt.

Bei WPA1/2 erfolgt die Authentifizierung an einem Netz mit einem Pre-Shared-Key (PSK), welcher Teil eines 128 Bit langen individuellen Schlüssels ist. Das Gerät (als Authenticator) generiert diesen Schlüssel mit einem 48 Bit langen Initialization Vector (IV), welcher die Berechnung des WPA-Schlüssels für Angreifer erschwert. Die Wiederholung des aus

IV und WPA-Schlüssel bestehenden echten Schlüssels erfolgt so erst nach 2^{48} Datenpaketen, die in absehbarer Zeit kein WLAN erreicht.

Um die (theoretische) Wiederholung des echten Schlüssels zu verhindern, sieht der WPA-Standard eine automatische Neuaushandlung des Schlüssels mit dem WLAN-Client (als Supplicant) in regelmäßigen Abständen vor (Rekeying). Damit wird der Wiederholung des echten Schlüssels vorweggegriffen. Durch Einstellen eines individuellen Zyklusses haben Sie die Möglichkeit, die Rekeying-Abstände zu verkürzen.

SNMP-ID:

2.23.20.20.11

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert geräteseitig die vorzeitige Aushandlung eines neuen WPA-Schlüssels. Ein Rekeying kann aber weiterhin vom Supplicant angestoßen werden.

Default-Wert:

0

WPA2-Schluessel-Management

Mit diesen Optionen können Sie die WPA2-Schlüsselverwaltung konfigurieren.

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.

SNMP-ID:

2.23.20.20.19

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

SHA256

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.

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.

Default-Wert:

Standard

7.3 Flexibles WLAN Capture-Format

Ab LCOS 9.00 stehen Ihnen für das Paket-Capturing im WLAN verschiedene Formate zur Auswahl, unter denen das Gerät die aufgezeichneten Paketdaten speichern kann.

7.3.1 Ergänzungen im Setup-Menü

Paket-Capture

In diesem Menü nehmen Sie die Einstellungen für das Paket-Capturing vor.

SNMP-ID:

2.12.86

Pfad Telnet:

Setup > **WLAN**

WLAN-Capture-Format

Über diese Einstellung legen Sie fest, in welchem Format die Paket-Capture-Funktion die WLAN-spezifischen Informationen in der Capture-Datei abspeichert.

Die Wahl eines geeigneten Capture-Formats hängt von den in Ihrem WLAN-Netz verwendeten Übertragungsstandards und dem Umfang der Informationen ab, die Sie erfassen möchten. Die IEEE 802.11 Norm mit ihren zahlreichen Erweiterungen ist über viele Jahre gewachsen. Die parallel dazu entwickelten Capture-Formate sind jedoch nicht flexibel genug, um jede Erweiterung (insbesondere 802.11n) optimal abzudecken. Somit existiert kein universelles Capture-Format, welches sich für sämtliche Standards gleichermaßen gut eignet. Möglich sind jedoch Empfehlungen, die ein breites Spektrum an Standards bei hohem Informationsgehalt abdecken: *Radiotap* und *PPI*.

SNMP-ID:

2.12.86.1

Pfad Telnet:

Setup > **WLAN** > **Paket-Capture**

Mögliche Werte:

Radiotap

Verwendet den Radiotap-Header. Radiotap ist ein unter Linux- und BSD-WLAN-Treibern weit verbreitetes Format, welches mit seiner flexiblen Struktur die Erstellung kompakter Captures erlaubt. Mit Radiotap haben Sie somit die Möglichkeit, zahlreiche WLAN-spezifische Informationen mit hoher Kompression aufzuzeichnen. Dies gilt auch für Datenpakete aus 802.11n-konformen Verbindungen. Einschränkungen ergeben sich hierbei lediglich bei der Aufzeichnung der antennenspezifischen RSSI und Signal-Stärken sowie Aggregierungen (A-MPDU). Sofern Sie hierzu detaillierte WLAN-spezifische Informationen benötigen, wählen Sie stattdessen das PPI-Format.

AVS

Verwendet den AVS-Header. Der AVS-Header stellt eine Weiterentwicklung des PRISM-Headers und wird von LCOS bis Version 8.60 als Standard-Header verwendet. Da AVS jedoch ebenfalls keine Informationen aus 802.11n-konformen Verbindungen verarbeiten kann, sollten Sie nach Möglichkeit das leistungsfähigere Radiotap wählen.

PPI

Verwendet den Wireshark-prioritären PPI-Header. Nutzen Sie diese Einstellung, wenn Sie die Capture-Datei mit Wireshark analysieren wollen. PPI entspricht dem Leistungsumfang von Radiotap und ist darüber hinaus auch dazu in der Lage, dessen Einschränkungen bei der Aufzeichnung von Informationen zu 802.11n-konformen Verbindungen zu umgehen. Nachteilig gegenüber Radiotap sind jedoch die schwächere Kompression und gröbere Header-Struktur.

PRISM

Verwendet den klassischen PRISM-Header. Nutzen Sie diese Einstellung lediglich, wenn Sie die Capture-Datei mit einem Programm analysieren wollen, welches keine anderen Formate unterstützt. PRISM eignet sich nicht, um Informationen aus 802.11n-konformen Verbindungen aufzuzeichnen. Es gilt mittlerweile als veraltet und sollte nicht mehr verwendet werden.

Plain

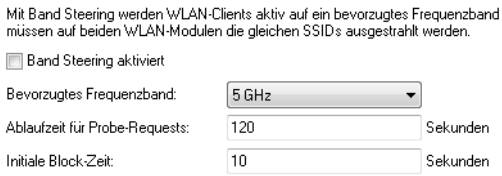
Deaktiviert sämtliche Header. Nutzen Sie diese Einstellung, wenn Sie lediglich an den Packetdaten selbst interessiert sind.

Default-Wert:

Radiotap

7.4 Band Steering mit verzögertem Scan auf 2,4GHz

Unter **Wireless-LAN** > **Band Steering** lässt sich ab LCOS 9.00 das Band Steering auf dem 2,4GHz-Band verzögern.



Initiale Block-Zeit

Geht ein Access Point mit einem 5GHz-DFS-Funkmodul und aktiviertem Band Steering erstmalig oder nach einem Neustart in Betrieb, kann er während des DFS-Scans keine Dual-Band-fähigen WLAN-Clients erkennen. Als Folge kann der Access Point einen vorhandenen WLAN-Client nicht auf ein ggf. bevorzugtes 5GHz-Band leiten. Stattdessen würde das 2,4GHz-Funkmodul die Anfrage des Clients beantworten und ihn auf das 2,4GHz-Band leiten.

Durch die Eingabe einer initialen Block-Zeit beantwortet das auf 2,4GHz konfigurierte Funkmodul des Access Points Anfragen eines WLAN-Clients um die entsprechend angegebene Zeit später. Der Default-Wert ist 10 Sekunden.

Durch die verzögerte Antwort auf 2,4GHz-Probe-Responses veranlasst der Access Point zusätzlich einen WLAN-Client, der ggf. den 5GHz-Scan überspringt, weil er bereits einen Access Point auf 2,4GHz erwartet, erneut auf 5GHz zu scannen.

Das Einbuchen eines reinen 2,4GHz-WLAN-Clients erfolgt ebenfalls erst nach der eingestellten Verzögerungszeit. Wenn keine 5GHz-WLAN-Clients im Netzwerk vorhanden sind, sollte die Verzögerungszeit 0 Sekunden betragen.

7.4.1 Ergänzungen im Setup-Menü

Initiale Block-Zeit

Geht ein Access Point mit einem 5GHz-DFS-Funkmodul und aktiviertem Band Steering erstmalig oder nach einem Neustart in Betrieb, kann er während des DFS-Scans keine Dual-Band-fähigen WLAN-Clients erkennen. Als Folge kann der Access Point einen vorhandenen WLAN-Client nicht auf ein ggf. bevorzugtes 5GHz-Band leiten. Stattdessen würde das 2,4GHz-Funkmodul die Anfrage des Clients beantworten und ihn auf das 2,4GHz-Band leiten.

Durch die Eingabe einer initialen Block-Zeit startet das auf 2,4GHz konfigurierte Funkmodul des Access Points um die entsprechend angegebene Zeit später.

Das Einbuchen eines reinen 2,4GHz-WLAN-Clients erfolgt ebenfalls erst nach der eingestellten Verzögerungszeit. Wenn keine 5GHz-WLAN-Clients im Netz vorhanden sind, sollte die Verzögerungszeit 0 Sekunden betragen.

SNMP-ID:

2.12.87.5

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Besondere Werte:

0

Dieser Wert deaktiviert die Verzögerung.

Default-Wert:

10

7.5 Erweiterte WLAN-Traces

Ab LCOS 9.00 lassen sich für einen WLAN-Daten-Trace auch die jeweiligen Klassen von Management-Frames separat auswählen. Die Einstellung dazu finden Sie im WEBconfig unter **Setup** > **WLAN**. Der Menüpunkt **Setup** > **WLAN** > **Trace-Beacons** entfällt ab LCOS 9.00

Trace-Mgmt-Packete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Management-Frames im WLAN-DATA-Trace auftauchen sollen.

Mögliche Werte:

Assoziierung: (Re)Association Request/Response, Disassociate

Authentisierung: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Andere: alle restlichen Management-Frametypen

Default:

Assoziierung

Authentisierung

Probes

Action

Andere

7.5.1 Ergänzungen im Setup-Menü

Trace-Mgmt-Pakete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Management-Frames im WLAN-DATA-Trace auftauchen sollen.

SNMP-ID:

2.12.124

Pfad Telnet:

Setup > WLAN

Mögliche Werte:

Assoziierung
(Re)Association Request/Response
Disassociate
Authentisierung
Authentication
Deauthentication
Probes
Probe Request
Probe Response
Action
Beacon
Andere
alle restlichen Management-Frametypen

Default-Wert:

Assoziierung

Authentisierung

Probes

Action

Andere

Trace-Daten-Pakete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Daten-Frames im WLAN-DATA-Trace auftauchen sollen.

SNMP-ID:

2.12.125

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

normal
Alle normalen Daten-Pakete

NULL
Alle leeren Daten-Pakete

andere
alle restlichen Daten-Pakete

7.6 Fast Roaming gemäß IEEE 802.11r

Ab LCOS 9.00 unterstützt ein Access Point das Fast Roaming nach dem Standard IEEE 802.11r.

7.6.1 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.

Aktuelle WLAN-Geräte besitzen Hardware-Beschleuniger, mit denen die Ver- und Entschlüsselung der Nutzerdaten während einer Verbindung in Echtzeit ohne spürbare Verzögerung oder auffällige Netzlast erfolgt. Auch die clientseitige Erstellung von Schlüsseln stellt mittlerweile durch die ausreichende Rechenleistung keine bemerkenswerte Beeinträchtigung dar.

Die Verzögerungen bei Verbindungen über EAP/802.1X oder WPA beruhen deshalb hauptsächlich auf der Zeit, die Client und Server zum Aushandeln der Sicherheitsprotokolle bei der Anmeldung benötigen.

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

Diese verlängerte Anmeldezeit des WLAN-Clients am Access Point ist für nicht zeitkritische Anwendung ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem Access Point zum nächsten (wie es z. B. bei Voice-over-IP-Anwendungen oder in industriellen Echtzeit-Umgebungen notwendig ist), ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel.

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

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim Access Point zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim Access Point. Beim Roaming von einem Access Point zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen Access 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 Access 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 WLAN-Controllers, der die angeschlossenen Access Points mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der Access Point 802.11r beherrscht.

Die vom WLAN-Controller verwalteten Access 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 Access 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 Access Point mitgeteilt bekommen.

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

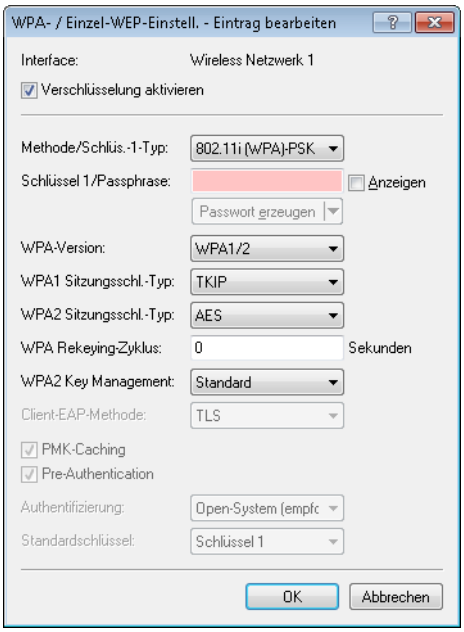
Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen Access Point einen neuen PMK aushandeln. Dieser ist auch auf dem Access 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 Access 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** > **802.11i/WEP** > **WPA-/Einzel-WEP-Einstellungen**.

7.6.2 Konfiguration



WPA2 Key Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll. Mögliche Werte sind:

- 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.
- SHA256: Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.
- Fast Roaming: Aktiviert Fast Roaming über 802.11r
- Kombinationen der drei Einstellungen

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.

7.6.3 Ergänzungen im Status-Menü

Schnelles-Roaming

Zeigt an, ob der WLAN-Client Fast Roaming einsetzt.

SNMP-ID:

1.3.32.63

Pfad Telnet:

Status > **WLAN** > **Stationstabelle**

WPA2-Schluessel-Management

Zeigt an, welches WPA2-Schlüsselmanagement der WLAN-Client einsetzt.

SNMP-ID:

1.3.32.64

Pfad Telnet:

Status > **WLAN** > **Stationstabelle**

WPA2-Schluessel-Management

Zeigt an, welches WPA2-Schlüsselmanagement der P2P-Access Point einsetzt.

SNMP-ID:

1.3.36.1.44

Pfad Telnet:

Status > **WLAN** > **Interpoints** > **Accesspoint-Liste**

WPA2-Schluessel-Management

Zeigt an, welches WPA2-Schlüsselmanagement der Access Point im Client-Betrieb einsetzt.

SNMP-ID:

1.3.43.51.40

Pfad Telnet:

Status > **WLAN** > **Client** > **Interfaces**

7.6.4 Ergänzungen im Setup-Menü

WPA2-Schluessel-Management

Mit diesen Optionen konfigurieren Sie die WPA2-Schlüsselverwaltung.

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.

SNMP-ID:

2.23.20.3.19

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Verschluesselung**

Mögliche Werte:

Schnelles-Roaming
Aktiviert Fast Roaming über 802.11r

SHA256
Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.

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.

Default-Wert:

Standard

WPA2-Schluessel-Management

Mit diesen Optionen können Sie die WPA2-Schlüsselverwaltung konfigurieren.

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.

SNMP-ID:

2.23.20.20.19

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

SHA256
Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.

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.

Default-Wert:

Standard

WPA2-Schluessel-Management

Mit diesen Optionen konfigurieren Sie die WPA2-Schlüsselverwaltung.

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.

SNMP-ID:

2.37.1.1.41

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Schnelles-Roaming

Aktiviert Fast Roaming über 802.11r

SHA256

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.

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.

Default-Wert:

Standard

7.7 WPA2 mit AES als Werkseinstellung

Ab LCOS 9.00 ist in LANconfig und LCOS für die Verschlüsselungsmethode WPA2 der Sitzungsschlüsseltyp AES standardmäßig festgelegt.

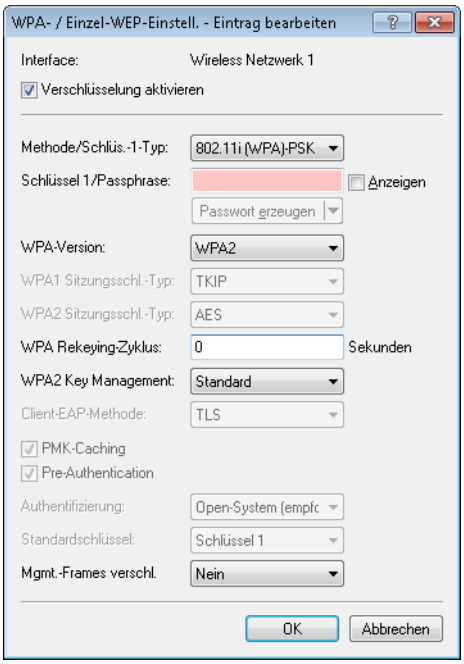
7.8 WLAN Protected Management Frames (PMF)

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.

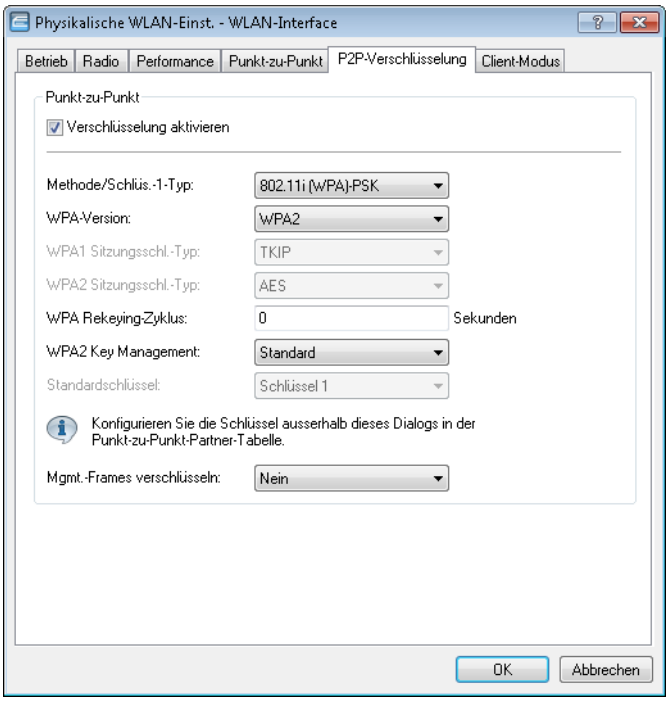
Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen, so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Um Protected Management Frames für ein logisches WLAN-Interface zu aktivieren, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **802.11i/WEP**, klicken auf **WPA- / Einzel-WEP-Einstellungen**, öffnen die Konfiguration der

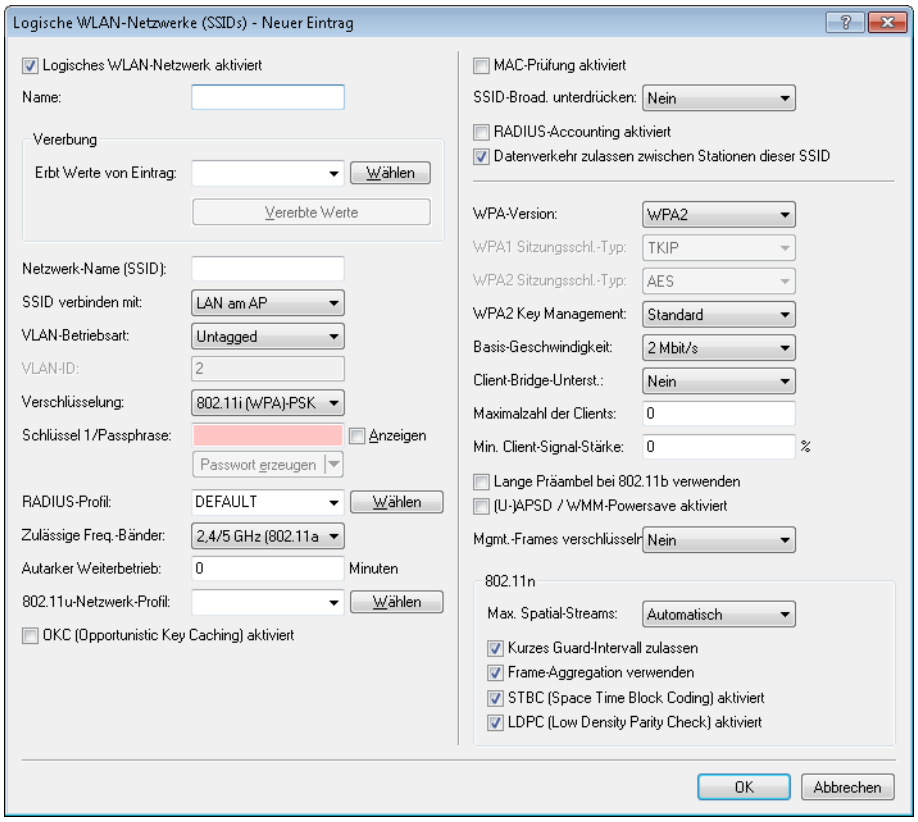
entsprechenden WLAN-Schnittstelle und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Um die Management-Frames bei P2P-Verbindung zwischen den Basisstationen zu verschlüsseln, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **General**, klicken auf **Physikalische WLAN-Einst.** und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Um die Verschlüsselung von Management-Frames über einen WLAN-Controller zu verwalten, wechseln Sie in LANconfig in die Ansicht **WLAN-Controller** > **Profiles**, klicken auf **Logische WLAN-Netze (SSIDs)** und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Folgende Optionen stehen bei allen Konfigurationen zur Auswahl:

Nein

Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

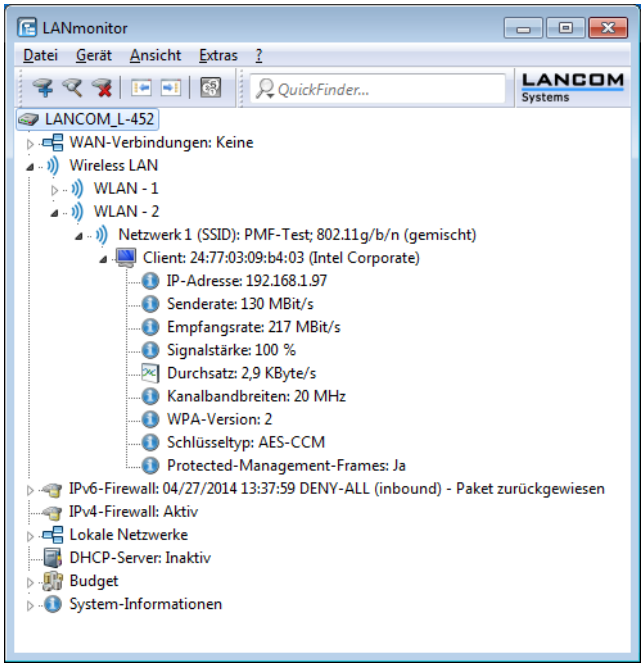
Erzwingen

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Der LANmonitor zeigt unterhalb des entsprechenden Clients an, ob dieser die WLAN-Management-Frames verschlüsselt.



7.8.1 Ergänzungen im Status-Menü

Gesch.-Mgmt-Frames

Zeigt an, ob der WLAN-Client eine PMF-geschützte Verbindung aufgebaut hat.

SNMP-ID:

1.3.32.67

Pfad Telnet:

Status > **WLAN** > **Stationstabelle**

Mögliche Werte:

Nein
Ja

Gesch.-Mgmt-Frames

Zeigt an, ob das jeweilige Netz PMF unterstützt.

SNMP-ID:

1.3.34.47

Pfad Telnet:

Status > **WLAN** > **Scan-Resultate**

Mögliche Werte:

Nein
Ja
Optional

Gesch.-Mgmt-Frames

Zeigt an, ob auf der jeweiligen P2P-Verbindung PMF aktiviert ist.

SNMP-ID:

1.3.36.1.47

Pfad Telnet:

Status > **WLAN** > **Interpoints** > **Accesspoint-Liste**

Mögliche Werte:

Nein
Ja

Schluesseltyp

Zeigt an, von welchem Typ der Sitzungsschlüssel für die P2P-Verbindung ist.

SNMP-ID:

1.3.36.3.3

Pfad Telnet:

Status > **WLAN** > **Interpoints** > **Schluessel-Liste**

Mögliche Werte:

Keiner
Unbekannt
WEP-40-Bit
WEP-104-Bit
WEP-128-Bit
TKIP
AES-OCB
AES-CCM
BIP

Der Typ "Broadcast Integrity Protection" zeigt an, dass der AP Management-Frames sichert, die als Broad- oder Multicast an mehrere Clients gerichtet sind.

RSC-MGMT

Zeigt den Sequenzzähler des letzten empfangenen verschlüsselten Management-Frames. Der Wert dient der Replay-Protection.

SNMP-ID:

1.3.36.3.24

Pfad Telnet:

Status > **WLAN** > **Interpoints** > **Schluessel-Liste**

Schluesseltyp

Zeigt an, von welchem Typ der Sitzungsschlüssel für die P2P-Verbindung ist.

SNMP-ID:

1.3.41.3

Pfad Telnet:

Status > **WLAN** > **Gruppen-Schluessel**

Mögliche Werte:

Keiner
Unbekannt
WEP-40-Bit
WEP-104-Bit
WEP-128-Bit
TKIP
AES-OCB
AES-CCM
BIP

Der Typ "Broadcast Integrity Protection" zeigt an, dass der AP Management-Frames sichert, die als Broad- oder Multicast an mehrere Clients gerichtet sind.

RSC-MGMT

Zeigt den Sequenzzähler des letzten empfangenen verschlüsselten Management-Frames. Der Wert dient der Replay-Protection.

SNMP-ID:

1.3.41.24

Pfad Telnet:

Status > **WLAN** > **Gruppen-Schluessel**

RSC-MGMT

Zeigt den Sequenzzähler des letzten empfangenen verschlüsselten Management-Frames. Der Wert dient der Replay-Protection.

SNMP-ID:

1.3.42.23

Pfad Telnet:

Status > **WLAN** > **Kanal-Scan-Resultate**

Gesch.-Mgmt-Frames

Zeigt an, ob im Client-Modus die jeweilige WLAN-Schnittstelle eine PMF-geschützte Verbindung aufgebaut hat.

SNMP-ID:

1.3.43.51.41

Pfad Telnet:

Status > **WLAN** > **Client** > **Interfaces**

Mögliche Werte:

Nein
Ja

Gesch.-Mgmt-Frames

Zeigt an, ob das jeweilige Netz PMF unterstützt.

SNMP-ID:

1.3.44.47

Pfad Telnet:

Status > **WLAN** > **Andere-Netze**

Mögliche Werte:

Nein
Ja
Optional

Schluesseltyp

Zeigt an, von welchem Typ der Sitzungsschlüssel für die P2P-Verbindung ist.

SNMP-ID:

1.3.47.3

Pfad Telnet:

Status > **WLAN** > **Paarweise-Schluessel**

Mögliche Werte:

Keiner
Unbekannt
WEP-40-Bit
WEP-104-Bit
WEP-128-Bit
TKIP
AES-OCB
AES-CCM
BIP

Der Typ "Broadcast Integrity Protection" zeigt an, dass der AP Management-Frames sichert, die als Broad- oder Multicast an mehrere Clients gerichtet sind.

RSC-MGMT

Zeigt den Sequenzzähler des letzten empfangenen verschlüsselten Management-Frames. Der Wert dient der Replay-Protection.

SNMP-ID:

1.3.47.24

Pfad Telnet:

Status > **WLAN** > **Paarweise-Schluessel**

Gesch.-Mgmt-Frames

Zeigt an, ob das jeweilige WLAN-Interface PMF unterstützt.

SNMP-ID:

1.3.55.41

Pfad Telnet:

Status > **WLAN** > **Andere-Netze**

Mögliche Werte:

Nein
Ja

7.8.2 Ergänzungen im Setup-Menü

Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

SNMP-ID:

2.23.20.3.14

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Verschluesselung**

Mögliche Werte:

Nein
Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

Zwingend
Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional
Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Default-Wert:

Nein

Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

SNMP-ID:

2.23.20.20.14

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Verschluesselung**

Mögliche Werte:

Nein

Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

Zwingend

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Default-Wert:

Nein

Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

SNMP-ID:

2.37.1.1.43

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Nein

Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

Zwingend

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Default-Wert:

Nein

7.9 Redundante Verbindungen mittels PRP

Anwendungen, die empfindlich auf Kommunikationsausfälle reagieren, benötigen eine möglichst unterbrechungsfreie Kommunikation. Zu solchen Anwendungen zählen zum Beispiel die Automation, der Transport und mobile Anwendungen.

Ab LCOS 9.00 haben Sie die Möglichkeit, in Ihrem WLAN redundante Funkstrecken mit dem Parallel Redundancy Protocols (PRP) herzustellen. Diese redundanten Funkstrecken bieten Ihnen eine hohe Ausfallsicherheit.

Die hohe Ausfallsicherheit erreicht PRP, indem PRP ein Zwillingspaket (verdoppeltes Paket) durch 2 unabhängige WLANs sendet. Solange 1 WLAN aktiv ist, transportiert PRP Datenpakete.

7.9.1 Grundlegende Funktion

PRP-Geräte agieren als Sender und Empfänger von PRP-Paketen, wobei PRP-Geräte beide Rollen einnehmen.

Der Sender geht wie folgt vor:

1. Er dupliziert Pakete, Zwillingspakete, und sendet sie durch 2 unabhängige (W)LANs.
2. Er fügt beim Senden jedem Paket einen Redundancy Control Trailer (RCT) an.

Der RCT enthält folgende Informationen für den Empfänger:

- Er identifiziert das Paket als PRP-Paket.
- Er enthält eine Sequence-ID.
- Er weist aus, über welches (W)LAN das Paket kam.
- Er enthält die Paketgröße.

Die Sequence-ID ist eine fortlaufend hochgezählte Nummer. Die Sequence-ID sorgt mit der Quellen-MAC-Adresse dafür, dass das Paket in die Duplicate Detection eingeht. Die Duplicate Detection erkennt Duplikate und verwirft das später eingetroffene Paket.

Der Empfänger geht wie folgt vor:

- Er liest den RCT.
- Er leitet das zuerst emfpangene Zwillingspaket ohne RCT weiter.
- Über die Duplicate Detection erkennt der Empfänger später eingetroffene Zwillingspakete und verwirft diese.

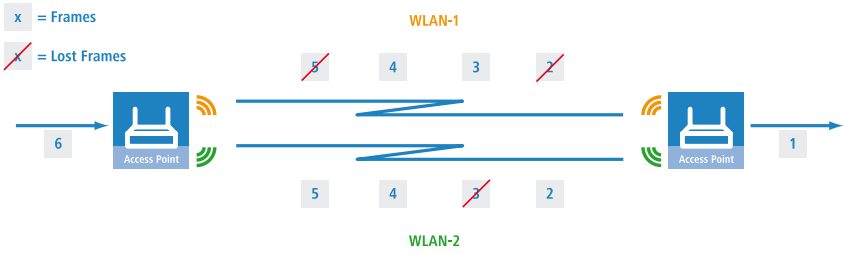
7.9.2 Vorteile von WLAN-PRP

PRP bietet Ihnen aufgrund seiner Funktionsweise bei WLAN deutliche Vorteile. In der Praxis verbesserten sich mit PRP die 3 bedeutendsten Qualitätsindikatoren eines Netzwerkes: Laufzeitschwankungen, Latenz und Paketverluste.

Mit PRP leiten Empfänger stets das zuerst eingetroffene Paket weiter und verwerfen das später eingetroffene. Da die Geräte stets das zuerst eingetroffene Paket weiterleiten, verringert sich die Latenz. In der Praxis waren deutliche Verbesserungen sowohl bei der durchschnittlichen als auch maximalen Laufzeitschwankung zu beobachten.

WLAN ist wie Ethernet als geteiltes Medium ausgelegt. In einer einzelnen WLAN-Verbindung halten die Geräte Pakete zurück, wenn das Medium belegt ist. Da die Geräte mit PRP Daten über 2 unabhängige WLANs transportieren, stehen wegen der Frequenzteilung praktisch 2 Medien zur Verfügung.

Mit PRP senden die Geräte jedes Paket doppelt, deswegen ist PRP teilweise in der Lage unsystematische Paketverluste auszugleichen. Solange der Empfänger eines der Pakete empfängt, ist die Kommunikation erfolgreich. Eine Neuübertragung eines einzelnen, verlorenen Paketes entfällt unter Umständen, was sich ebenfalls positiv auf Laufzeitschwankungen auswirkt.



7.9.3 PRP-Implementation in den Access Points

Jeder Access Point (AP) mit mindestens 3 Schnittstellen bietet Ihnen die Möglichkeit zum Aufbau eines PRP-Netzwerkes. Der AP übernimmt alle Funktionen, die für den Aufbau eines PRP-Netzwerkes notwendig sind.

Die Geräte bieten Ihnen folgende Möglichkeiten:

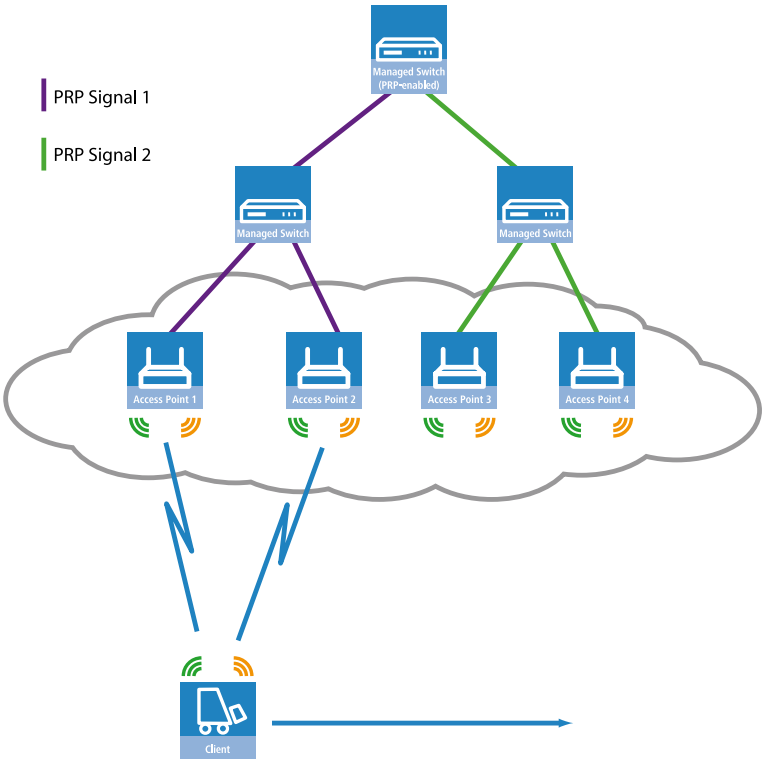
1. PRP-Netzwerke über drahtlose Schnittstellen realisierbar
2. pro Gerät sind bis zu 2 PRP-Netzwerke realisierbar
3. zusätzlich zu einem PRP-Netzwerk an einen AP weitere Clients anschließen
4. Dual Roaming aktivieren, sodass mit PRP die 2 WLAN-Module zeitverzögert roamen
5. umfassende Diagnosemöglichkeiten

7.9.4 Dual Roaming

Verfügt ein Gerät über 1 WLAN-Modul, unterbricht der Datenverkehr in einem Handover-Szenario.

Verfügt ein Gerät über 2 WLAN-Module lassen sich mit PRP Unterbrechungen verringern, wenn der Anwender in LANconfig verbietet, dass beide WLAN-Module gleichzeitig roamen. Dieser Modus heißt Dual Roaming.

Eine praktische Anwendung ist ein Client, der sich an Access Points vorbeibewegt. Durch den spezifischen Aufbau des Netzwerkes ist im Regelfall 1WLAN-Modul verbunden und empfängt PRP-Pakete, während das andere WLAN-Modul sich in den nächsten AP einwählen kann.



Ein konkretes Anwendungsbeispiel ist die Materialwirtschaft, dort insbesondere das Überwachen von Warenbewegungen in Echtzeit.

Ein weiteres Anwendungsbeispiel ist der Bahnverkehr. Ein AP in einem Zug verbindet sich während der Fahrt mit den APs an der Strecke.

Zusätzlich können Sie im LANconfig die Block-Zeit bestimmen. Die Block-Zeit legt die Mindestsperrzeit fest, die zwischen den Roaming-Vorgängen unterschiedlicher WLAN-Module des gleichen Gerätes vergeht.

7.9.5 Unterstützung von Diagnosemöglichkeiten

Empfänger von PRP-Paketen verwerfen im Normalbetrieb Duplikate und entfernen den RCT von Paketen, die sie an ihren gebündelten Ausgangsport weiterleiten.

Um das Netzwerk auf korrekte Funktion zu untersuchen, stellt Ihnen LCOS folgende Optionen zur Verfügung, die Sie bei der Netzwerkdiagnose unterstützen:

1. Weiterleiten von Paket-Duplikaten ohne RCT
2. Weiterleiten von Einzelpaketen mit RCT
3. Weiterleiten von Paket-Duplikaten mit RCT

Zusätzlich verfügt LCOS über folgende Trace-Optionen:

1. trace # PRP-DATA
2. trace # PRP-NODES

PRP-DATA enthält Informationen zu gesendeten und empfangenen Paketen. Enthaltene Informationen: Name der Schnittstellen-Gruppe, die das Paket transportiert; Transportrichtung des Paketes (RX|TX); Trailer-Sequenznummer; MAC-Adresse des Partner-Gerätes; Schnittstelle innerhalb der PRP-Gruppe (A|B), die das Paket transportiert; Behandlung des Paketes (accept|discard)

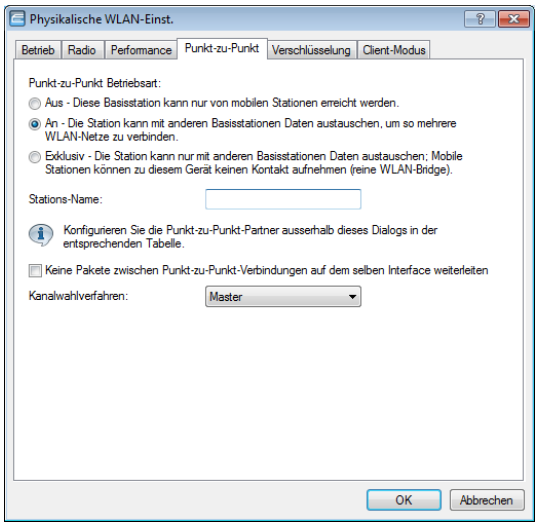
PRP-NODES enthält die folgenden Informationen: Neue Adresse in der (Proxy-)Node-Tabelle, Adresse aus der (Proxy-)Node-Tabelle entfernt, Node-Typ einer Adresse hat sich geändert.

7.9.6 Tutorial: Einrichtung einer PRP-Verbindung über ein Point-to-Point-Netz (P2P)

Die folgenden Schritte sind für beide P2P-Partner konform durchzuführen.

Um eine P2P-Verbindung zwischen zwei PRP-fähigen APs einzurichten, gehen Sie wie folgt vor:

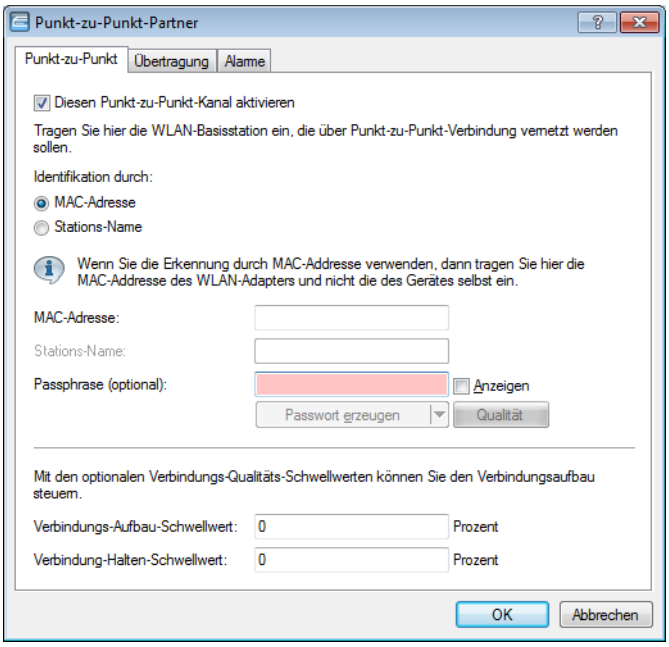
1. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** in der Ansicht **Betrieb** beide physikalischen WLAN-Schnittstellen (WLAN-Interface 1, WLAN-Interface 2) und in der Ansicht **Punkt-zu-Punkt** die **Punkt-zu-Punkt Betriebsart**.



2. Vergeben Sie für die physikalischen WLAN-Schnittstellen jeweils im Feld **Stations-Name** einen im WLAN eindeutigen Namen. Falls der P2P-Partner die betreffende Schnittstelle über die MAC-Adresse identifizieren kann oder soll, lassen Sie dieses Feld leer.

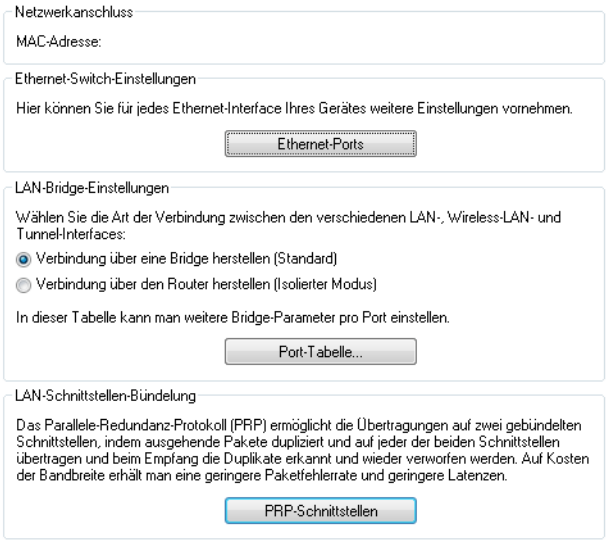
Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

3. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Punkt-zu-Punkt-Partner** die Punkt-zu-Punkt-Kanäle "P2P-1-1" und "P2P-2-1" und bestimmen Sie die Schnittstellen-Kennungen der jeweiligen Punkt-zu-Punkt-Partner (**MAC-Adresse** oder **Stations-Name**).

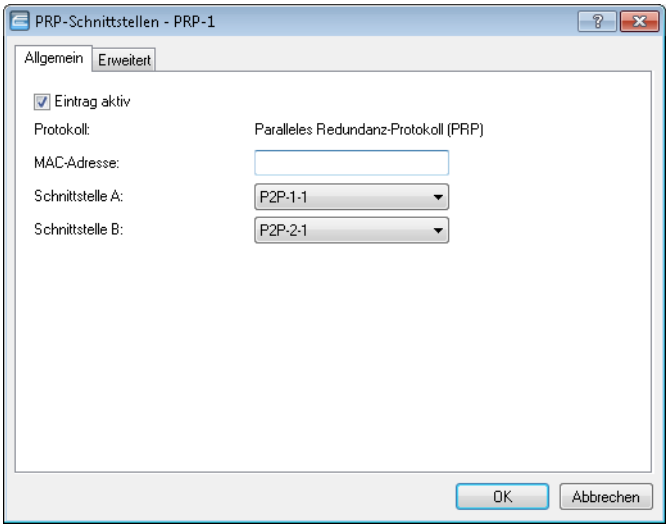


Geben Sie entweder die MAC-Adresse oder den Stations-Namen der entsprechenden WLAN-Schnittstelle des P2P-Partners an. Den Stations-Namen haben Sie im vorherigen Schritt vergeben.

4. Öffnen Sie die PRP-Konfiguration unter **Schnittstellen** > **LAN** mit einem Klick auf **PRP-Schnittstellen**.



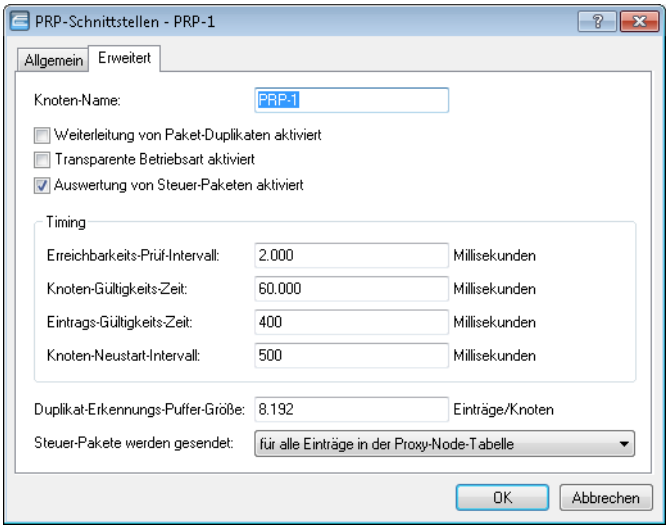
5. Aktivieren Sie die PRP-Schnittstellen und bestimmen Sie, welche Schnittstellen der AP zur Bündelung verwendet.



Wählen Sie hier die zuvor aktivierten Punkt-zu-Punkt-Schnittstellen "P2P-1-1" und "P2P-2-1" aus.

Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

6. Die Standard-Konfiguration der erweiterten Einstellungen übernehmen Sie mit einem Klick auf **OK**.



Die Einrichtung einer PRP-Verbindung über ein Point-to-Point-Netz ist damit abgeschlossen.

7.9.7 Tutorial: Roaming mit einem Dual-Radio-Client und PRP

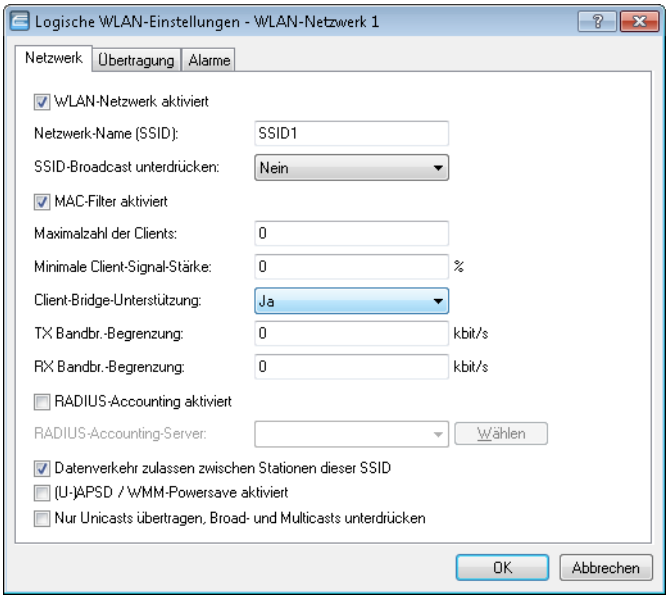
Ein gängiger Weg, die Ausfallsicherheit einer WLAN-Infrastruktur zu erhöhen, ist der Betrieb der dazugehörigen APs in unterschiedlichen Frequenzbänden. Hierzu strahlen die physikalischen WLAN-Schnittstellen der APs z. B. eine SSID-1 im 2,4-Ghz-Band und eine SSID-2 im 5-GHz-Band aus. Wechselt ein PRP-fähiger Dual-Radio-Client von der Funkzelle einer physikalischen WLAN-Schnittstelle in eine benachbarte-Funkzelle der gleichen Infrastruktur, ermöglicht PRP einen verlustfreien Zellenübergang.

Dazu koppelt der Dual-Radio-Client über PRP anfangs z. B. seine physikalische WLAN-Schnittstelle WLAN-1 mit SSID-1 und WLAN-2 mit SSID-2. Verschlechtert sich der Empfang von SSID-1 und ist eine andere Funkzelle mit besserem Empfang in Reichweite, führt der Dual-Radio-Client einen Zellenwechsel durch. Beim Zellenübergang sendet der Dual-Radio-Client über WLAN-2 die Daten noch an SSID-2, während WLAN-1 bereits dieselben Daten an SSID-1 der besseren Funkzelle überträgt. Ein PRP-fähiger Switch filtert die doppelten PRP-Datenpakete heraus, bevor er die Daten ins LAN weiterleitet.

Die APs der WLAN-Infrastruktur müssen in einem solchen Szenario nicht für den PRP-Betrieb konfiguriert sein.

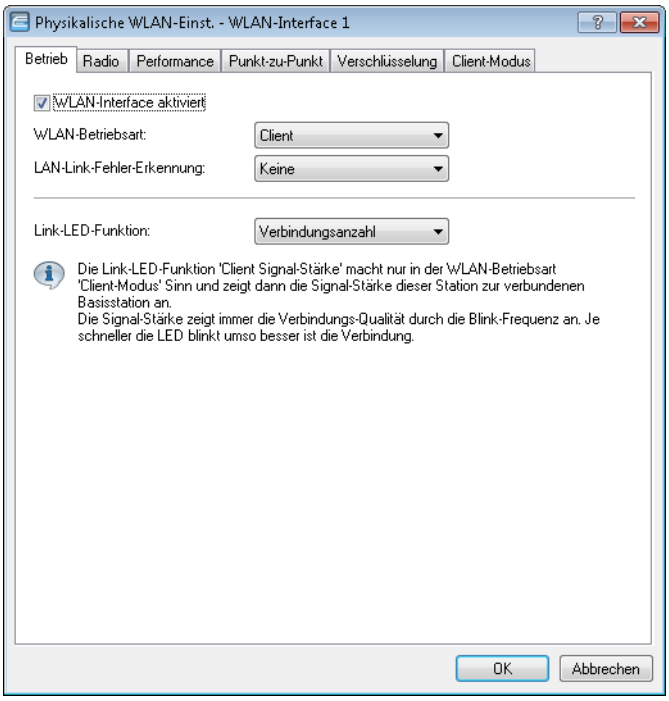
Damit der Empfänger Duplikate der Datenpakete erkennt, müssen die APs der WLAN-Infrastruktur im Client-Bridge-Modus arbeiten. Die MAC-Adresse des Dual-Radio-Clients sorgt zusammen mit dem RCT dafür, dass der Empfänger die doppelten Datenpakete erkennt. Ohne den Client-Bridge-Support würden die APs der WLAN-Infrastruktur die MAC-Adresse des Dual-Radio-Clients durch die eigene MAC-Adresse ersetzen und damit eine Erkennung der Duplikate verhindern.

Die Client-Bridge-Unterstützung lässt sich im LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** in der Ansicht **Netzwerk** aktivieren.



Die PRP-Konfiguration des Dual-Radio-Clients erfolgt in den folgenden Schritten:

1. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** in der Ansicht **Betrieb** beide physikalische WLAN-Schnittstellen (WLAN-Interface 1, WLAN-Interface 2) und wechseln Sie die **WLAN-Betriebsart** jeweils zu **Client**.

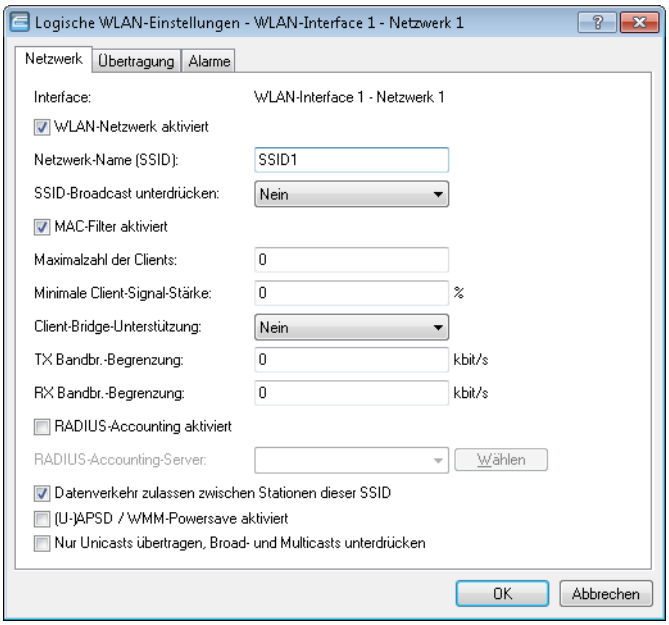


Legen Sie die restlichen WLAN-Parameter unter **Radio**, **Performance**, **Verschlüsselung** und **Client-Modus** entsprechend den Vorgaben der WLAN-Funkzellen fest.

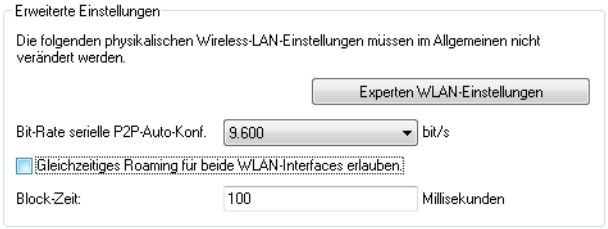
Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

2. Zum Eintragen der SSID wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**, klicken **Logische WLAN-Einstellungen** und wählen jeweils das Netz 1 der entsprechenden WLAN-Schnittstelle aus.

3. Tragen Sie im Feld **Netz-Name (SSID)** die Bezeichnung des WLANs ein, an das Sie die WLAN-Schnittstelle koppeln wollen.



4. Deaktivieren Sie unter **Wireless-LAN** > **Allgemein** im Abschnitt **Erweiterte Einstellungen** die Option **Gleichzeitiges Roaming für beide WLAN-Interfaces erlauben**.



Mit der Deaktivierung des gleichzeitigen Roamings verhindern Sie, dass beide physikalischen WLAN-Schnittstellen gleichzeitig Roaming bzw. Background-Scans durchführen und dadurch ggf. zusammen die Verbindung zu ihren Funkzellen verlieren.

So konfiguriert, kann sich der Dual-Radio-Client z. B. entlang einer Strecke von APs vorbeibewegen und zwischen den einzelnen APs roamen.

7.9.8 Ergänzungen im Setup-Menü

Schnittstellen-Buendelung

In dieser Tabelle nehmen Sie die Einstellungen für die Bündelung von physikalischen und logischen Schnittstellen vor.

Die Schnittstellen-Bündelung ermöglicht Ihnen die Übertragung von Datenpaketen auf zwei miteinander gepaarten Schnittstellen. Hierzu dupliziert das Gerät ausgehende Datenpakete und überträgt sie auf jeder der beiden Schnittstellen parallel. Beim Empfang akzeptiert das Gerät zuerst eingehende Datenpakete; Duplikate hingegen erkennt und verwirft das Gerät.

Durch Einsetzen einer Schnittstellen-Bündelung lassen sich die Paketfehlerrate und die Latenzzeiten bei der Datenübertragung reduzieren, dies geht allerdings zu Lasten der maximalen Bandbreite auf der betreffenden Schnittstelle.

SNMP-ID:

2.4.13.11.1

Pfad Telnet:

Setup > **LAN**

Schnittstellen

In dieser Tabelle nehmen Sie die allgemeinen Einstellungen für die Schnittstellen-Bündelung vor.

SNMP-ID:

2.4.13.1

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung**

Schnittstelle

Dieser Parameter zeigt die logische Bündel-Schnittstelle, unter der Sie die gewählten logischen und physikalischen Geräte-Schnittstellen bündeln.

SNMP-ID:

2.4.13.1.1

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

BUNDLE-1
BUNDLE-2

In-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 A und B als eigenständige Schnittstellen nutzbar.

SNMP-ID:

2.4.13.1.2

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Protokoll

Über diesen Parameter legen Sie das für die Schnittstellen-Bündelung verwendete Protokoll fest.

SNMP-ID:

2.4.13.1.3

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

PRP

Legt das Parallel Redundancy Protocol (PRP) fest.

MAC-Adresse

Über diesen Parameter stellen Sie optional eine alternative MAC-Adresse ein, welche die ausgewählte Bündel-Schnittstelle verwendet.

SNMP-ID:

2.4.13.1.4

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

max. 12 Zeichen aus `[a-f][0-9]`

Besondere Werte:

leer

Wenn Sie dieses Feld leer lassen, verwendet das Gerät die systemweite MAC-Adresse.

Default-Wert:

abhängig von der MAC-Adresse Ihres Gerätes

Schnittstelle-A

Über diesen Parameter wählen Sie die 1. physikalische oder logische Schnittstelle aus, die das Gerät bündelt.

SNMP-ID:

2.4.13.1.5

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Auswahl aus den verfügbaren Schnittstellen

Default-Wert:

WLAN-1

Schnittstelle-B

Über diesen Parameter wählen Sie die 2. physikalische oder logische Schnittstelle aus, die das Gerät bündelt.

SNMP-ID:

2.4.13.1.6

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Auswahl aus den verfügbaren Schnittstellen

Default-Wert:

WLAN-2

Schnittstellen

In diesem Menü nehmen Sie die Einstellungen speziell für PRP als Bündelungsprotokoll vor.

SNMP-ID:

2.4.13.11

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Schnittstellen

Diese Tabelle enthält die Schnittstellen mit allen PRP-relevanten Einstellungen.

SNMP-ID:

2.4.13.11.1

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Schnittstelle

Das Parallele-Redundanz-Protokoll (PRP) ermöglicht redundante Übertragungen auf zwei (gebündelten) Schnittstellen. Dazu wählen Sie zwei Schnittstellen aus, die das Gerät intern zu einer Schnittstelle zusammenfasst. Das Gerät dupliziert ausgehende Pakete, sodass das Gerät alle Pakete auf jeder der beiden Schnittstellen überträgt. Empfangsseitig erkennt das Gerät die Duplikate verwirft sie. Dies führt zu einer geringeren Paketfehlerrate und zu geringeren Latenzen auf der gebündelten Schnittstelle im Vergleich zu einer Übertragung auf einer einzelnen Schnittstelle.

Hier geben Sie den Namen für diese Schnittstellen ein.

SNMP-ID:

2.4.13.11.1.1

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

max. 13 Zeichen aus `[A-Z][a-z][0-9].*()/&%$[]*`

Duplikate-annehmen

Schaltet das Weiterleiten von Paket-Duplikaten ein oder aus.

SNMP-ID:

2.4.13.11.1.2

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

Besondere Werte:

ja
nein

Transparenter-Modus

Schaltet die Transparente Betriebsart ein oder aus. Wenn die Transparente Betriebsart aktiv ist, leitet der Empfänger von PRP-Paketen die Pakete mit Redundancy Control Trailer weiter.

SNMP-ID:

2.4.13.11.1.3

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

ja
nein

Default-Wert:

nein

Lebens-Pruefungs-Intervall

Bestimmt, wie oft das Gerät Steuer-Pakete sendet.

SNMP-ID:

2.4.13.11.1.4

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

100 … 60000 Millisekunden

Default-Wert:

2000

Knoten-Vergessens-Zeit

Gibt die Zeit an, bis das Gerät einen Knoten aus seiner Knoten- oder Proxy-Knoten-Tabelle löscht.

SNMP-ID:

2.4.13.11.1.5

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

1000 … 3600000 Millisekunden

Default-Wert:

60000

Eintrag-Vergessens-Zeit

Legt fest, ab wann das Gerät einen Eintrag aus dem Duplikat-Erkennungs-Puffer löscht.

SNMP-ID:

2.4.13.11.1.6

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

10 … 60000 Millisekunden

Default-Wert:

400

Knoten-Reboot-Intervall

Legt die Zeit fest, die ein PRP-Gerät passiv auf einem Link horcht, bis das Gerät Pakete über den Link sendet.

SNMP-ID:

2.4.13.11.1.7

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

0 … 60000 Millisekunden

Default-Wert:

500

Dup-Eliminations-Puffer-Groesse

Begrenzt die Anzahl der Einträge im Duplicate-Erkennungs-Speicher.

SNMP-ID:

2.4.11.1.8

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

16 … 65536 Einträge/Knoten

Default-Wert:

8192

Sende-Ueberwachungs-Pakete

Legt die Einstellungen zum Versenden von Supervision-Paketen fest.

SNMP-ID:

2.4.13.11.1.9

Pfad Telnet:

LAN > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

0
keine

1
nur-eigene-MAC

2
alle-Knoten

Default-Wert:

2

Knoten-Name

Der Knoten-Name ist die Bezeichnung für den Knoten. Sie haben die Möglichkeit, einen beliebigen Namen festzulegen.

SNMP-ID:

2.4.13.11.1.10

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9].*()/&%$[]`

Werte-Sup.-Frames-aus

Schaltet die Überwachung von Steuer-Paketen ein oder aus.

SNMP-ID:

2.4.13.11.1.11

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

ja
nein

Default-Wert:

ja

8 WLAN-Management

8.1 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen

In einem zentral gemanagten WLAN sind die angeschlossenen Access Points (APs) klassischerweise über das LAN mit dem WLAN-Controller (WLC) verbunden. Diese LAN-Verbindungen geben gleichzeitig die Topologie des verwalteten Netzes vor. Eine Erweiterung des Netzes um zusätzliche APs ist jedoch auf die Reichweite der kabelgebundenen Netzarchitektur beschränkt und erfordert ggf. einen Ausbau der betreffenden Infrastruktur.

Mittels **AutoWDS** haben Sie die Möglichkeit, die Erweiterung eines WLANs auf Basis von Funkstrecken (P2P) vorzunehmen und dadurch kostengünstig und schnell sehr skalierbare Netze zu errichten. "AutoWDS" steht dabei für "Automatic Wireless Distribution System". Die Funktion erlaubt Ihnen, ein FunkNetz aus mehreren APs herzustellen, welche ausschließlich drahtlos untereinander verbunden sind: die logische Verbindung allein genügt. Die möglichen Einsatzgebiete erstrecken sich z. B. auf die flächendeckende Anbindung kleiner Areale oder ganzer Gebiete an das Internet oder ein FirmenNetz, in denen eine Verbindung über LAN nicht sinnvoll oder unpraktikabel ist.

Im einfachsten Fall benötigen Sie lediglich einen WLC, der mit einem AutoWDS-fähigen AP via LAN verbunden ist. Der AP spannt das gemanagte WLAN auf und agiert gleichzeitig als "Zugangs-AP". Über den Zugangs-AP stellen hinzukommende AutoWDS-fähige APs die Verbindung zum WLC her, welcher ihnen mittels CAPWAP eine Konfiguration übermittelt. Nach Erhalt der Konfiguration und Eingliederung in das gemanagte WLAN nutzen die einzelnen APs P2P-Strecken, um Nutzerdaten weiterzuleiten, miteinander zu kommunizieren und die Topologie aufrecht zu erhalten. Weitere hinzukommende APs sind in der Lage, die eingebundenen APs ihrerseits als Zugangs-APs zu nutzen. Auf diese Weise lassen sich mehrere APs miteinander verketten und vermaschte Netze aufbauen, die optional via RSTP redundante

Verbindungen aufweisen. Aus Sicht eines hinzukommenden AP sind eingebundene APs "Master-APs". Aus Sicht des Master-AP sind hinzukommende APs "Slave-APs".

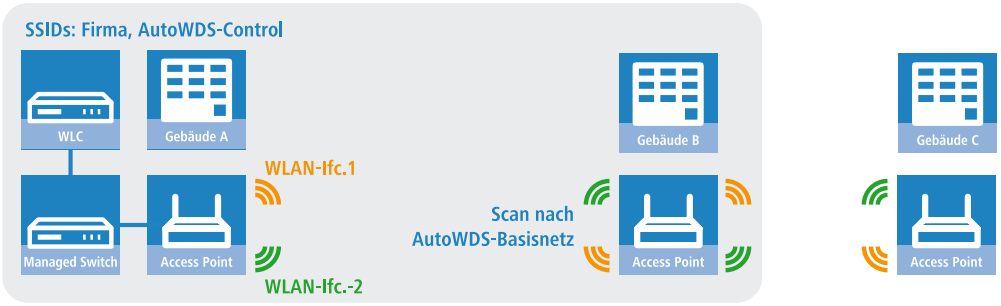


Abbildung 1: Phase 1 – Hinzukommender AP in Gebäude B sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude A

Abbildung 2: Phase 2 – Hinzukommender AP in Gebäude B findet WLC und bezieht AP-Konfiguration über CAPWAP

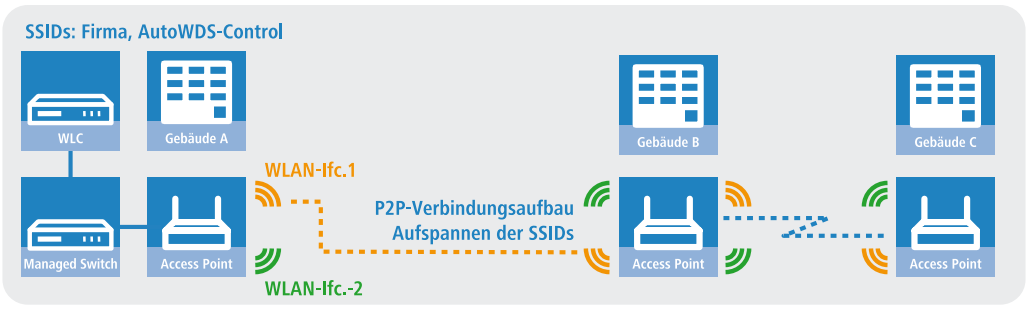


Abbildung 3: Phase 3 – Hinzukommender AP in Gebäude B integriert sich in das gemanagte WLAN. Hinzukommender AP in Gebäude C sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude B.

Genauere Informationen zum Integrationsablauf und zu den Betriebsmodi beim Topologie-Management erhalten Sie in den nachfolgenden Abschnitten zur Funktionsweise von AutoWDS.

AutoWDS eignet sich ausschließlich für statische Infrastrukturen, nicht für sich bewegende APs. Sollte ein AP aus der Reichweite seines P2P-Partners wandern und die Verbindung zum Netz verlieren, erfolgt eine temporäre Downtime mit anschließender *Rekonfiguration*. Das Roaming von WLAN-Clients zwischen einzelnen AutoWDS-APs hingegen unterscheidet sich nicht von dem zwischen normalen APs.

Das DFS-Verhalten eines AP im 5-GHz-Betrieb ist von AutoWDS unberührt und besitzt höhere Priorität. Die DFS-Radarerkennung kann bewirken, dass der AP während des Betriebs einen plötzlichen Kanalwechsel durchführt oder das WLAN bei Ausfall der möglichen Frequenzen – aufgrund mehrerer Radarerkennungen auf verschiedenen Kanälen – für einige Zeit komplett deaktiviert. Der betroffene AP kann somit für Störungen des gesamten AutoWDS-Verbundes verantwortlich sein oder eine Zeit lang gar keine SSIDs aufspannen. Innerhalb von Gebäuden haben Sie die Möglichkeit, evtl. auftretenden Störungen durch Aktivieren des Indoor-Modus entgegenzuwirken.

Wenn Sie AutoWDS auf einem Gerät mit einer einzigen physikalischen WLAN-Schnittstelle einsetzen, drittelt sich im Betrieb deren Datenrate, da das Gerät eingehende/ausgehende Daten mehrfach senden muss: An die WLAN-Clients, an einen Master-AP und ggf. an einen Slave-AP. Um diesen Effekt zu mildern, sollten Sie auf Geräten mit zwei physikalischen WLAN-Schnittstellen eine Trennung des Datenverkehrs vornehmen. Dazu reservieren Sie eine physikalische WLAN-Schnittstelle für die Anbindung der APs und eine physikalische WLAN-Schnittstelle für die Anbindung der Clients.

8.1.1 Funktionsweise

Aufspannen des AutoWDS-Basisnetzes

AutoWDS stellt verschiedene Integrationsmodi bereit, über die das Management von P2P-Strecken zum Errichten vermaschter Netze erfolgen kann. Den Großteil der Konfiguration nehmen Sie auf dem WLC vor, der die einzelnen logischen WLAN-Netze verwaltet. Dazu ergänzen Sie ein eingerichtetes WLAN-Profil Ihres gemanagten WLANs um ein aktives AutoWDS-Profil. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

Das AutoWDS-Basisnetz bzw. die dazugehörige SSID (Vorgabename: **AutoWDS-Control**) ist ein reines Managementnetz: Es dient ausschließlich der Authentifizierung eines AP bei der vorkonfigurierten Integration sowie dem Aufbau des WLC-Tunnels für den Konfigurationsaustausch. Auf diese Weise werden hinzukommende APs bei der Integration in das gemanagte WLAN vom operativen Betrieb isoliert. Sobald eine P2P-Verbindung zu einem Master-AP besteht, gilt ein hinzukommender AP als integriert und wickelt die weitere Kommunikation über die Bridge auf Layer 2 ab. Ähnlich wie bei klassischen P2P-Verbindungen spannen die P2P-Partner dazu eine Management-SSID auf, über die sie den Datenverkehr und den CAPWAP-Tunnel zum WLC abwickeln (siehe *Update der AP-Konfiguration und Aufbau der P2P-Strecke* auf Seite 152).

Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb der WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

Nachdem Sie Ihrem gemanagten WLAN ein aktives AutoWDS-Profil zugewiesen haben, spannen die betreffenden (Zugangs-)APs das AutoWDS-Basisnetz auf und senden in ihren Beacons eine zusätzliche, herstellerspezifische Kennung aus. Diese auch als "AutoWDSInfoFlags" bezeichnete Kennung signalisiert hinzukommenden AutoWDS-fähigen APs die generelle Unterstützung der Funktion und teilt ihnen mit, …

- ob AutoWDS für die erkannte SSID aktiv/inaktiv ist;
- ob der AP der betreffenden SSID eine aktive/inaktive WLC-Verbindung besitzt;
- ob der WLC hinzukommende APs im Express-Modus akzeptiert oder verbietet; und
- ob sich APs für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden müssen (strikte Schnittstellen-Paarung, d. h. mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder gemischte Schnittstellen-Paarungen erlaubt sind.

Zum hinzukommenden AP wird ein AP automatisch, sobald Sie in seiner Konfiguration die AutoWDS-Funktion aktivieren und sich seine physikalische WLAN-Schnittstelle im **Managed**-Modus befindet. Der betreffende AP wechselt die Betriebsart daraufhin temporär in den **Client**-Modus und scannt solange die einzelnen WLANs, bis er einen geeigneten Zugangs-AP erkennt. Der Scan erfolgt sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband.

Sofern Ihr Gerät über zwei physikalische WLAN-Schnittstellen verfügt und beide aktiv sind, scannen beide WLAN-Schnittstellen gleichzeitig nach einem geeigneten AutoWDS-Basisnetz. Erkennt eine physikalische WLAN-Schnittstelle eine geeignete SSID, assoziiert sie sich mit dem Zugangs-AP, sofern es die oben erwähnte Schnittstellen-Paarung erlaubt. Die andere physikalische WLAN-Schnittstelle scannt für den Fall weiter, dass die bereits assoziierte physikalische WLAN-Schnittstelle die Verbindung wieder verliert. Die andere physikalische WLAN-Schnittstelle verbindet sich aber bis dahin mit keinem weiteren AutoWDS-Basisnetz. Sobald Ihr Gerät die WLC-Konfiguration erhalten hat, verhalten sich beide physikalischen WLAN-Schnittstellen wie im Profil festgelegt und spannen die Ihnen zugewiesenen SSIDs und das AutoWDS-Basisnetz auf.

Der Ablauf des Suchvorgangs nach einem AutoWDS-Basisnetz ist identisch mit dem der Rekonfiguration bei Verlust der WLAN-Verbindung (siehe *Verlust der Konnektivität und Rekonfiguration* auf Seite 153).

Unterschiede der Integrationsmodi

Bei der Integration von hinzukommenden APs in Ihr gemanagtes WLAN haben Sie die Wahl zwischen zwei verschiedenen Integrationsmodi. Der Integrationsmodus legt die Bedingungen fest, unter denen Ihr WLC einen hinzukommenden AP akzeptiert:

- Die **vorkonfigurierte Integration** stellt den kontrollierten und bevorzugten Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus gestattet der WLC ausschließlich die Integration von APs, die über eine lokal vorkonfigurierte SSID und gültige WPA2-Passphrase für das AutoWDS-Basisnetz verfügen.

  Der Modus eignet sich für sämtliche Produktivumgebungen und dient dazu, einen vorgegebenen Bezug zwischen einem hinzukommenden AP und einem AutoWDS-Basisnetz herzustellen. Sobald der betreffende AP eine Konfiguration vom WLC erhält, priorisiert der AP diese Konfiguration höher als die lokale AutoWDS-Konfiguration, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

- Die **Express-Integration** stellt den schnellen Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus erlaubt der WLC sowohl die Integration vorkonfigurierter Geräte als auch die Integration vollkommen unkonfigurierter Geräte. Unkonfigurierte APs verfügen weder über eine eingetragene SSID noch über eine individuelle WPA2-Passphrase für ein AutoWDS-Basisnetz. Für die Authentifizierung an einem beliebigen AutoWDS-Basisnetz nutzen die Geräte stattdessen einen fest in die Firmware implementierten Pre-Shared-Key.

  Der Modus eignet sich zur einfachen Integration neuer APs in ein gemanagtes WLAN. Die Wahl eines AutoWDS-Basisnetzes geschieht hierbei automatisch und entzieht sich Ihrer Kontrolle. Sobald die betreffenden APs vom WLC eine Konfiguration erhalten, speichern die Geräte die Einstellungen als voringestellte Werte, bis der WLC via CAPWAP die Konfiguration widerruft, das Gerät nach einem Verbindungsabbruch die Express-*Rekonfiguration* ausführt oder Sie das Gerät resetten.

  Achten Sie bei der Express-Integration darauf, dass sich keine anderen AutoWDS-Basisnetze in Reichweite befinden. Andernfalls ist es möglich, dass ein fremder WLC Ihren AP übernimmt und so Ihrem weiteren Fernzugriff entzieht. Generell sollten Sie den Express-Modus so wenig wie möglich einsetzen, um die Angriffsmöglichkeiten zu reduzieren.

  LANCOM empfiehlt aus o. g. Sicherheitsgründen vornehmlich die vorkonfigurierte Integration. Über das Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Mehr dazu erfahren Sie im Abschnitt *Netz-Rollout: Vorkonfigurierte Integration durch Pairing beschleunigen* auf Seite 159.

Nach erfolgreicher Authentifizierung am AutoWDS-Basisnetz scannen die hinzukommenden APs das Netz nach einem WLC. Sobald sie einen WLC erkannt haben, versuchen sie, sich mit ihm zu verbinden und eine Konfiguration zu beziehen. Im LANmonitor erscheinen diese APs als neue Geräte, deren Aufnahme in das gemanagte WLAN der Administrator noch bestätigen und ihnen noch ein WLAN-Profil zuweisen muss. Die Zuweisung unterscheidet sich dabei nicht von der Aufnahme normaler APs. Alternativ kann die Zuweisung durch den WLC erfolgen, wenn Sie

- ein Default-WLAN-Profil eingerichtet und die automatische Zuweisung dessen aktiviert haben; oder
- den betreffenden AP in die Access-Point-Tabelle eingetragen und mit einem WLAN-Profil verknüpft haben.

Durch gleichzeitiges Setzen der automatischen Annahme hinzukommender APs durch den WLC ("Auto Accept") lässt sich die Integration hinzukommender APs automatisieren. Für die Express-Integration sollten Sie diese Einstellung jedoch unbedingt deaktivieren, um ein Mindestmaß an Sicherheit zu erhalten und Rogue-AP-Intrusion zu erschweren.

Der Ablauf der Zertifikatserstellung und die Zertifikatsprüfung sowie die automatische Annahme oder Verweigerung von Verbindungsanfragen durch den WLC gleichen dem eines WLAN-Szenarios mit kabelgebundenen APs. Weitere Informationen dazu finden Sie im Referenzhandbuch.

Gestaltung der Topologie

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie die Topologie des vermaschten Netzes aufgebaut ist. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Für deren Gestaltung bietet Ihnen der WLC folgende Management-Modi an:

- **Automatisch**: Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.
- **Halb-automatisch**: Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.
- **Manuell**: Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology**. Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest. Mehr dazu finden Sie im Abschnitt *Manuelles Topologie-Mangement* auf Seite 160.

Die automatische Berechnung einer P2P-Konfiguration (z. B. bei Initial- oder Wiederverbindung eines AP) ersetzt einen in der AutoWDS-Auto-Topology-Tabelle ggf. bereits vorhandenen Eintrag.

Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

Update der AP-Konfiguration und Aufbau der P2P-Strecke

Hat ein hinzukommender AP vom WLC via CAPWAP das WLAN-Profil mit sämtlichen darin enthaltenen Einstellungen empfangen, versucht er, als Slave eine P2P-Strecke zu dem ihm zugewiesenen Master-AP aufzubauen. Bei diesem Prozess wechselt der AP gleichzeitig seine WLAN-Betriebsart von **Client** zurück zu **Managed**.

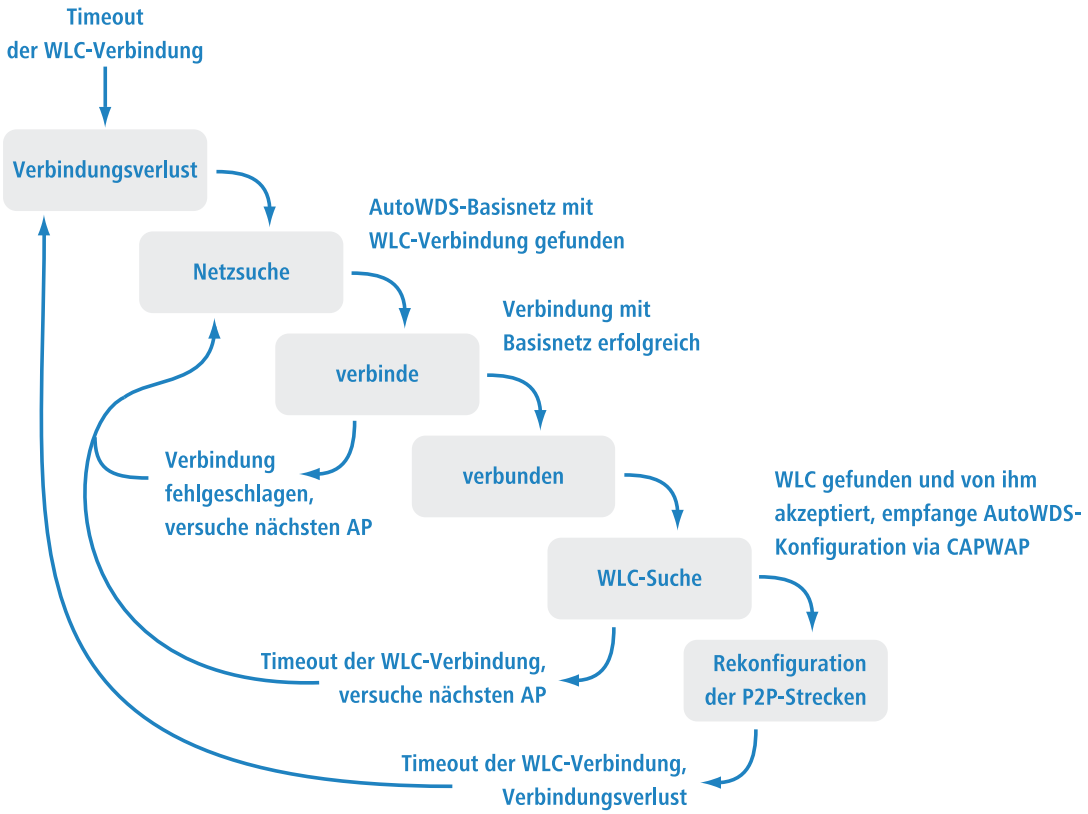
Da der Master-AP bereits im Managed-Modus agiert, erhält er vom WLC via CAPWAP lediglich ein Update seiner P2P-Konfiguration. Diese aktiviert P2P für die physikalische WLAN-Schnittstelle, setzt das Kanalwahlverfahren auf **Master** und teilt dem AP neben der WPA2-Passphrase die Peer-Identifikation des AP mit. Bei einer automatisch generierten P2P-Konfiguration entspricht die Peer-Identifikation der MAC-Adresse; bei einer manuellen P2P-Konfiguration dem Namen des Slave-AP. Der Master-AP kennzeichnet derartige SSIDs mit der Kennung ***** P2P Info *****.

Sobald beide APs eine P2P-Verbindung aufgebaut haben, ist der AutoWDS-Integrationsprozess abgeschlossen. Der hinzukommende AP ist dann für Clients (Smartphones, Laptops, andere APs im Client-Modus auf der Suche nach einem Master, etc.) benutzbar.

Solange sich der hinzukommende AP im Client-Modus befindet, ist das Bridging zwischen einer physikalischen WLAN-Schnittstelle und einer LAN-Schnittstelle oder einer anderen physikalischen Funkschnittstelle während des gesamten Integrationsprozesses deaktiviert. Dazu legt das Gerät die physikalischen WLAN-Schnittstellen automatisch auf verschiedene Bridges. Erst nach dem erfolgreichen Aufbau der P2P-Verbindung schaltet der AP das Bridging wieder in den Ursprungszustand zurück.

Verlust der Konnektivität und Rekonfiguration

Sobald Sie AutoWDS auf einem hinzukommenden AP aktivieren, die Anmeldung an einem Zugangs-AP fehlschlägt oder ein eingebundener AP die Verbindung zum WLC verliert, setzt dies einen automatischen (Re-)Konfigurationsprozess in Gang, der gemäß dem abgebildeten Schema verläuft:



Ein AP durchläuft den (Re-)Konfigurationsprozess nicht, wenn er im Client-Modus zwar eine Verbindung zu einem Zugangs-AP, jedoch nicht zum WLC aufbauen kann. Der AP wartet 5 Minuten ab Verbindung zum AutoWDS-Basisnetz, ob der WLC eine Konfiguration des Gerätes durchführt. Erfolgt in dieser Zeit keine Konfiguration (z. B. weil kein Administrator den AP akzeptiert), trennt sich der AP vom AutoWDS-Basisnetz und scannt nach weiteren passenden SSIDs. Ist nur eine SSID in Reichweite, wählt der AP diese erneut für den Integrationsvorgang.

Sofern Verbindung zu einem LAN besteht, versucht der AP während der kompletten Downtime zusätzlich, per Broadcast den WLC über LAN zu erreichen. Findet der AP den WLC via LAN, erfolgt kein Aufsetzen einer neuen P2P-Strecke und der WLC löscht sämtliche automatisch generierten P2P-Strecken, die den AP als Slave festlegten.

Konfigurations-Timeouts

Sowohl die initiale Konfiguration als auch die Rekonfiguration eines hinzukommenden APs werden durch den Ablauf einzelner Zähler ausgelöst, deren Zusammenspiel das Verhalten des Gerätes steuert. Hierzu gehören, sofern festgelegt:

1. die Zeit für den autarken Weiterbetrieb der P2P-Strecke bei Verlust der CAPWAP-Verbindung (ausschließlich Rekonfiguration);
2. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration; sowie
3. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die

Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit 0 festgelegt ist, verwirft der AP den betreffenden Konfigurationsteil sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und Express-Integration – die eingestellte Zeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen. Nach Ablauf dieser Wartezeit schaltet das Gerät seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus um und scannt die verfügbaren SSIDs nach dem zuletzt erkannten AutoWDS-Basisnetz. Parallel dazu beginnt der Zähler bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration herabzuzählen.

Hat das Gerät bei Ablauf des Express-Zählers das ihm bekannte AutoWDS-Basisnetz nicht gefunden, stellt das Gerät automatisch auf Express-Integration um. Anschließend sucht der AP solange nach einem beliebigen AutoWDS-fähigen Netz, bis schließlich ein geeigneter Zugangs-AP erkannt ist.

Durch intelligentes Zusammenspiel der einzelnen Wartezeiten haben Sie die Möglichkeit, das Gerät auf unvorhergesehene Ereignisse flexibel reagieren zu lassen. So lässt sich z. B. eine Fallback-Lösung für den Fall realisieren, dass Sie den Pre-Shared-Key für das AutoWDS-Basisnetz ändern, die Änderung am hinzukommenden AP jedoch fehlschlägt und sich das Gerät aufgrund einer ungültigen Konfiguration nicht mehr erreichen lässt. Bitte beachten Sie dabei die unter *Unterschiede der Integrationsmodi* auf Seite 151 aufgeführten Hinweise.

Die betreffenden Zähler konfigurieren Sie sowohl auf dem AP (z. B. via LANconfig) als auch auf dem WLC (ausschließlich im Setup-Menü). Auf dem AP werden die Zähler ausschließlich dann beachtet, wenn noch keine WLC-Konfiguration vorliegt (initiale Konfiguration). Sobald eine Konfiguration vorliegt, sind die im AutoWDS-Profil festgelegten Zählerwerte maßgebend (Rekonfiguration). Näheres zur Prioritätensetzung der Konfigurationen finden Sie unter *Unterschiede der Integrationsmodi* auf Seite 151.

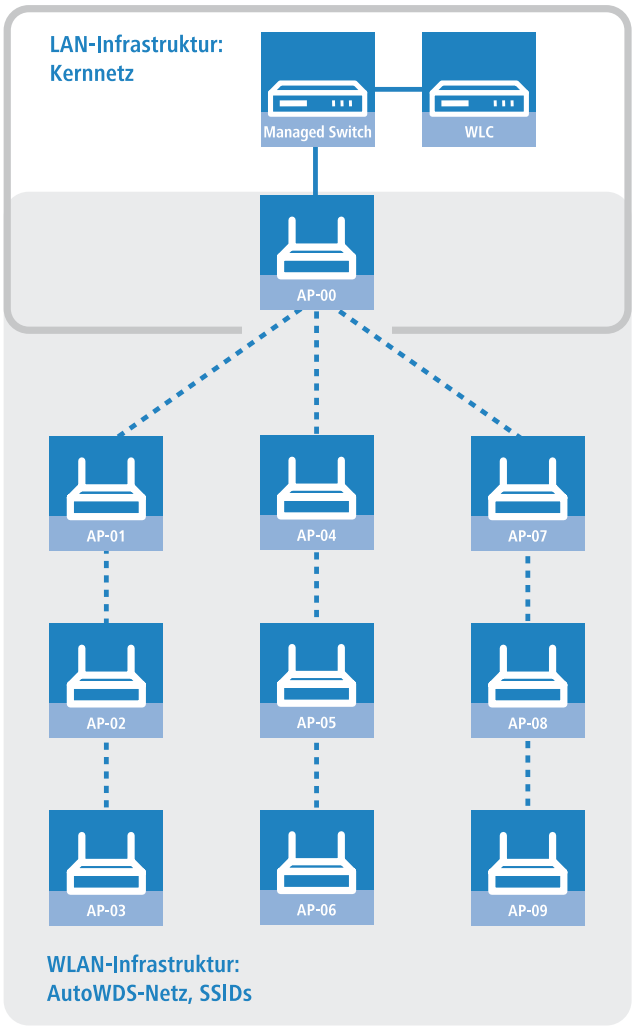
Wenn Sie den Express- oder den Vorkonfigurations-Zähler deaktivieren, überspringt das Gerät den entsprechenden Integrationsschritt. Durch Deaktivieren beider Zähler lässt sich die automatische Rekonfiguration ausschalten. Das Gerät ist dann nach einem entsprechend langen Verbindungsabbruch nicht mehr mittels AutoWDS zu erreichen. Das Gerät bleibt aber über die LAN-Schnittstelle erreichbar und sucht im LAN nach einem WLC, sofern eine entsprechende Verbindung besteht.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei 0 liegt.

Beispiel: Ausfall eines AP

Die CAPWAP-Verbindung eines jeden AP sichert sich in einem festgelegten Intervall durch Echo-Requests zum WLC ab. Fällt ein AP aus oder ist seine Anbindung gestört, läuft ein solcher Request ins Leere. Erhalten die betreffenden APs nach mehrmaliger Wiederholung des Echo-Requests keine Antwort des WLC, gilt die CAPWAP-Verbindung als verloren und

die betreffenden APs beginnen mit dem unter *Verlust der Konnektivität und Rekonfiguration* auf Seite 153 beschriebenen Rekonfigurationsprozess.



Für die oben abgebildete Infrastruktur hätte ein Ausfall von AP-01 die nachfolgenden Auswirkungen, sofern das automatische Topologie-Management aktiviert ist:

1. AP-01 ist defekt.
2. AP-02 und AP-03 wiederholen ihre Echo-Requests; alle Wiederholungen schlagen fehl.
3. AP-02 und AP-03 gehen in den autarken Weiterbetrieb (sofern konfiguriert) und versuchen weiterhin, den WLC zu erreichen (sowohl über WLAN als auch LAN, sofern Konnektivität besteht).
4. AP-02 und AP-03 beenden den autarken Weiterbetrieb für die P2P-Verbindungen.
5. AP-02 und AP-03 zählen die Wartezeit für den Beginn der vorkonfigurierten Integration herunter.
6. AP-02 und AP-03 schalten nach Ablauf der Wartezeit in den Client-Modus und scannen das WLAN nach dem letzten bekannten AutoWDS-Basisnetz.
7. AP-02 und AP-03 finden einen neuen Zugangs-AP (z. B. AP-05 oder AP-06) und buchen sich als Client ein.
8. AP-02 und AP-03 stellen über den **WLC-TUNNEL-AUTOWDS** die CAPWAP-Verbindung wieder her und melden dem WLC den neuen Zugangs-AP sowie die verwendeten physikalischen WLAN-Schnittstellen.
9. Der WLC generiert für die betroffenen physikalischen WLAN-Schnittstellen eine P2P-Strecke und übermittelt den APs die Konfiguration via CAPWAP.
10. Die APs setzen die neue P2P-Strecke zu den Ihnen zugewiesenen Master-APs auf und kommunizieren mit dem WLC nicht mehr über den **WLC-TUNNEL-AUTOWDS**, sondern ins LAN gebridged.

8.1.2 Einrichtung mittels Express-Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die Express-Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

In diesem Szenario erweitert ein Unternehmen seine Geschäftsräume um einen weiteren Gebäudekomplex. Das Unternehmen will die neuen Geschäftsräume in sein bestehendes gemanagtes WLAN integrieren. Dazu sollen die betreffenden APs ausschließlich per Funkstrecke verbunden sein. Zwischen Gebäude A (alt) und Gebäude B (neu) ist keine kabelgebundene Netzverbindung erwünscht.

Um die Konfiguration einfach zu halten, konfiguriert das Unternehmen alle APs mit einem einzelnen WLC. Die genaue Anzahl der APs in Gebäude A und Gebäude B ist nebensächlich. Besonderheiten wie mehrere physikalische WLAN-Schnittstellen berücksichtigt der WLC beim Topologie-Management automatisch.

Die Konfiguration selbst gliedert sich in zwei Teile:

1. Konfiguration des WLC in Gebäude A
2. Konfiguration aller APs in Gebäude B

Das Anwendungsbeispiel setzt eine gültige WLAN-Konfiguration mit gültigen Zertifikaten im WLC voraus. Wie Sie ein gemanagtes WLAN einrichten, entnehmen Sie bitte dem Kapitel zum WLAN-Management.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die Express-Integration.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.

2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Klicken Sie **AutoWDS-Einbindungs-Modus 'Express' erlaubt**, um die Express-Integration von APs über Ihren WLC zu aktivieren.
4. Wählen Sie das **WLAN-Profil** aus, dessen SSIDs Sie mittels AutoWDS erweitern wollen.

   Die APs des betreffenden WLAN-Profils fungieren als Zugangs-APs und spannen das AutoWDS-Basisnetz auf. Gleichzeitig erhalten via AutoWDS eingebundene APs dieses WLAN-Profil als Standardkonfiguration, unter der sie nach erfolgreicher Integration die dazugehörige SSID aussenden.

5. Geben Sie unter **Netz-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein. Standardmäßig verwendet LANconfig die Bezeichnung `AutoWDS-Control`.

   Die hier festgelegte SSID agiert als Managementnetz für sämtliche ein AutoWDS-Netz suchenden APs und ist – bis auf die Passphrase – nicht weiter konfigurierbar. Der WLC verbindet die angegebene SSID intern automatisch mit einem WLC-Tunnel (**WLC-TUNNEL-AUTOWDS**). Normale WLAN-Clients sind nicht in der Lage, dieses Managementnetz zu benutzen.

Die Einrichtung des AutoWDS-Basisnetzes reduziert die Anzahl der SSIDs, die Ihr Gerät über eine physikalische WLAN-Schnittstelle maximal aufspannen kann, um den Wert 1.

6. Geben Sie unter **WPA2-Passphrase** einen Schlüssel ein, mit dem Sie das AutoWDS-Basisnetz absichern.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

7. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

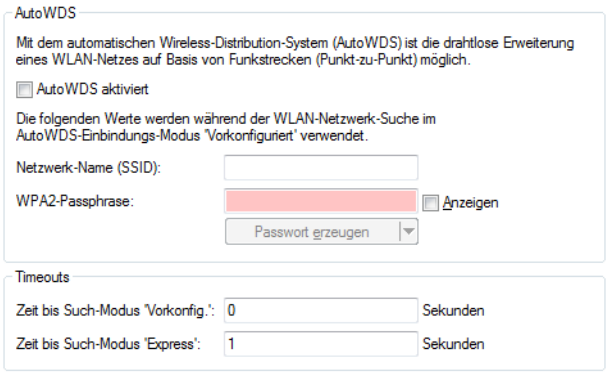
Der WLC weist nun allen gemanagten AutoWDS-fähigen APs in Ihrem WLAN die AutoWDS-Einstellungen zu, woraufhin diese das AutoWDS-Basisnetz aufspannen. Für künftige Rekonfigurationsprozesse verwenden die APs ausschließlich die hier hinterlegte SSID und Passphrase, sofern nicht anders festgelegt (siehe *Unterschiede der Integrationsmodi* auf Seite 151).

Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die Express-Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
4. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach einem beliebigen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie im *Kapitel zur Funktionsweise*.

8.1.3 Einrichtung mittels vorkonfigurierter Integration

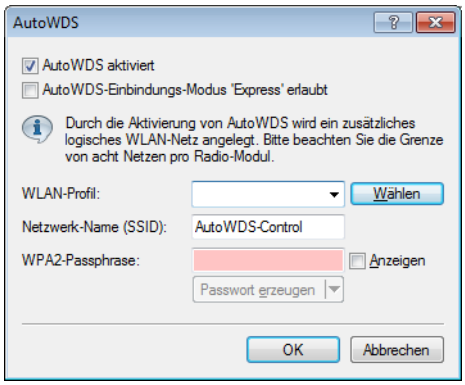
Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die vorkonfigurierte Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

Das Ausgangsszenario gleicht dem der *Express-Integration*. Allerdings verfolgt das Unternehmen in diesem Beispiel die Integration durch ein in den Geräten vorkonfiguriertes AutoWDS-Basisnetz.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die vorkonfigurierte Integration.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Wählen Sie das **WLAN-Profil** aus, dessen SSIDs Sie mittels AutoWDS erweitern wollen.

   Die APs des betreffenden WLAN-Profils fungieren als Zugangs-APs und spannen das AutoWDS-Basisnetz auf. Gleichzeitig erhalten via AutoWDS eingebundene APs dieses WLAN-Profil als Standardkonfiguration, unter der sie nach erfolgreicher Integration die dazugehörige SSID aussenden.

4. Geben Sie unter **Netz-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein. Standardmäßig verwendet LANconfig die Bezeichnung `AutoWDS-Control`.

   Die hier festgelegte SSID agiert als Managementnetz für sämtliche ein AutoWDS-Netz suchenden APs und ist – bis auf die Passphrase – nicht weiter konfigurierbar. Der WLC verbindet die angegebene SSID intern automatisch mit einem WLC-Tunnel (**WLC-TUNNEL-AUTOWDS**). Normale WLAN-Clients sind nicht in der Lage, dieses Managementnetz zu benutzen.

   Die Einrichtung des AutoWDS-Basisnetzes reduziert die Anzahl der SSIDs, die Ihr Gerät über eine physikalische WLAN-Schnittstelle maximal aufspannen kann, um den Wert 1.

5. Geben Sie unter **WPA2-Passphrase** einen Schlüssel ein, mit dem Sie das AutoWDS-Basisnetz absichern.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

6. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

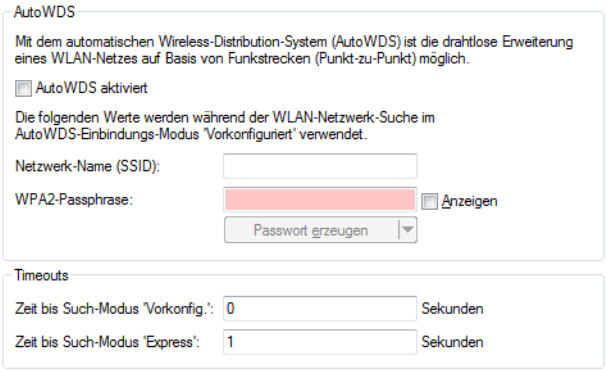
Der WLC weist nun allen gemanagten AutoWDS-fähigen APs in Ihrem WLAN die AutoWDS-Einstellungen zu, woraufhin diese das AutoWDS-Basisnetz aufspannen. Für künftige Rekonfigurationsprozesse verwenden die APs ausschließlich die hier hinterlegte SSID und Passphrase, sofern nicht anders konfiguriert (siehe *Unterschiede der Integrationsmodi* auf Seite 151).

Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die vorkonfigurierte Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **Netz-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein, das Sie auf dem WLC konfiguriert haben (z. B. `AutoWDS-Control`).
4. Geben Sie unter **WPA2-Passphrase** den Schlüssel des AutoWDS-Basisnetzes ein, den Sie auf dem WLC konfiguriert haben.
5. Ändern Sie die Timeout-Werte für die **Zeit bis Such-Modus 'Vorkonfig'** auf `1` und die **Zeit bis Such-Modus 'Express'** auf `0`.
6. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
7. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach dem eingetragenen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie im *Kapitel zur Funktionsweise*.

8.1.4 Netz-Rollout: Vorkonfigurierte Integration durch Pairing beschleunigen

Über das Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Beim Pairing verbinden Sie im Vorfeld einen frisch resetteten AP via LAN mit dem WLC, auf dem Sie Ihr gemanagtes WLAN inklusive AutoWDS eingerichtet haben. Im zurückgesetzten Zustand befindet sich der AP nach dem Einschalten automatisch im Managed-Modus. Findet der AP den WLC und akzeptiert der WLC den AP, erhält der AP automatisch die relevanten Zertifikate und Konfigurationsteile, welche die notwendigen Parameter im Gerät konfigurieren. Das Pairing ist dann abgeschlossen. Am Einsatzort installiert ein Mitarbeiter den AP und schaltet ihn ein. Das Gerät sucht dann automatisch nach dem vorkonfigurierten AutoWDS-Basisnetz.

Die nachfolgenden Schritte fassen die Vorgehensweise beim Pairing zusammen. Zusätzlich beinhalten Sie die Schritte zur automatischen Konfigurationszuweisung, um das Pairing bei einer hohen Anzahl von APs weiter zu vereinfachen.

1. Starten Sie LANconfig und richten Sie auf Ihrem WLC ein gemanagtes WLAN mit einem gültigen WLAN-Profil ein, sofern noch nicht geschehen. In LANconfig konfigurieren Sie ein solches Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile**.
2. Aktivieren Sie für dieses WLAN-Profil die AutoWDS-Funktion, wie im Abschnitt *Konfiguration des WLC* auf Seite 157 beschrieben.
3. Legen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** über die Schaltfläche **Default** ein für sämtliche APs allgemein gültiges Profil an. Weisen Sie diesem Profil dabei das zuvor eingerichtete **WLAN-Profil** zu
4. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Option **APs automatisch eine Default-Konfiguration zuweisen**.

5. **Optional:** Um die Annahme hinzukommender APs in LANmonitor nicht manuell zu bestätigen, sondern dies durch den WLC zu automatisieren, aktivieren Sie in dem Dialog zusätzlich die Option **Automatische Annahme neuer APs aktiviert (Auto-Accept)**.

   Aus Sicherheitsgründen sollten Sie diese Option lediglich dann aktivieren, wenn Sie die hinzukommenden APs über eine LAN-Schnittstelle mit dem WLC verbunden haben. Achten Sie darauf, dass keine weiteren Geräte mit dem WLC verbunden sind, um ein mögliches Rogue-AP-Intrusion auszuschließen.

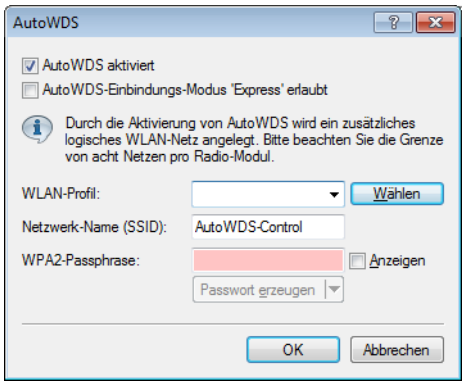
6. Übertragen Sie die Konfiguration zum WLC.
7. Resetten Sie den hinzukommenden AP und schließen Sie das Gerät via LAN an den WLC an.
   Das Gerät beginnt automatisch damit, nach einem WLC zu suchen.
8. Akzeptieren Sie im LANmonitor unter **Wireless LAN** > **Neue APs** den AP, sofern Sie keine automatische Annahme eingerichtet haben.
   Das Gerät erhält daraufhin vom WLC die benötigten Konfigurationsteile für den zukünftigen gemanagten Betrieb. Nach erfolgreicher Konfiguration listet LANmonitor das Gerät im Zweig **Aktive APs**.

Das Pairing ist damit abgeschlossen und der AP für den zukünftigen AutoWDS-Betrieb einsatzbereit.

8.1.5 Netz-Rollout: Umschalten von Express- zu vorkonfigurierter Integration

Sofern die für den Netz-Rollout die Express-Integration gewählt haben, erhalten die betreffenden APs eine WLC- bzw. AutoWDS-Konfiguration, die ein AutoWDS-Netz für spätere Rekonfigurationsprozesse vorkonfiguriert. Ein Umschalten der APs selber entfällt somit. Alles, was Sie tun müssen, ist, die Express-Integration auf dem WLC zu deaktivieren.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Deaktivieren Sie die Einstellung **AutoWDS-Einbindungs-Modus 'Express' erlaubt**, indem Sie das Häkchen entfernen.
3. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Damit haben Sie die Express-Integration für weitere hinzukommende APs deaktiviert.

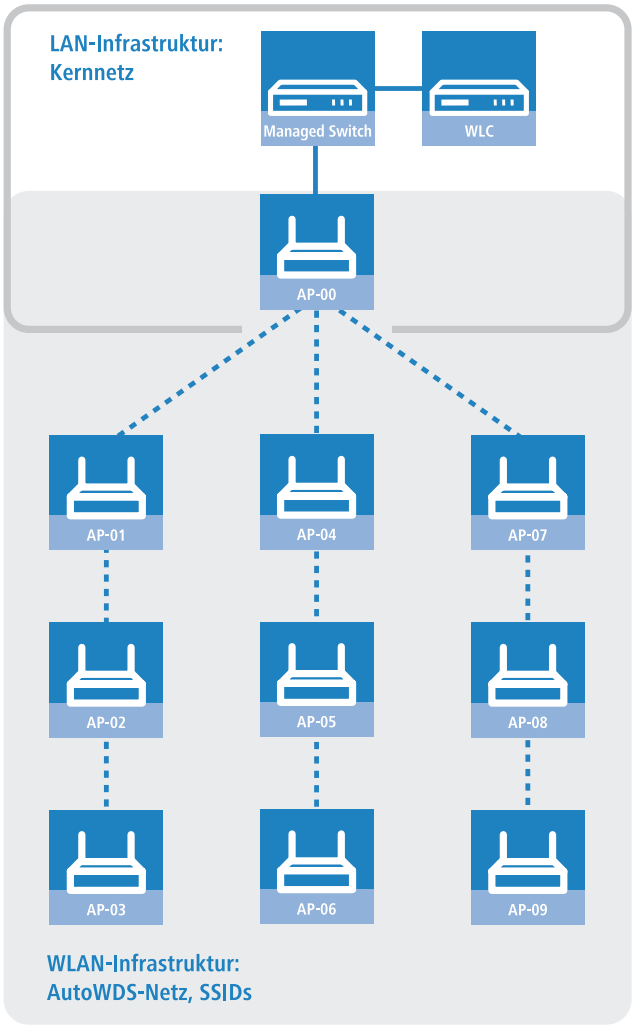
8.1.6 Manuelles Topologie-Mangement

Die Einrichtungsbeispiele für AutoWDS verfolgen das automatische Topologie-Management durch den WLC, um die Konfiguration zu vereinfachen. Je nach Einsatzszenario kann es jedoch erforderlich sein, einzelne oder sämtliche P2P-Strecken manuell zu definieren.

Der nachfolgende Abschnitt zeigt Ihnen, wie Sie das automatische Topologie-Management auf dem WLC deaktivieren und eine manuelle P2P-Konfiguration anlegen. Für die Konfiguration der P2P-Strecken ordnen Sie den APs zunächst eindeutige Namen zu, die Sie anschließend mit der Topologiekonfiguration und den verwendeten physikalischen WLAN-Schnittstellen verknüpfen. Das Kapitel geht davon aus, dass Sie die unter *Einrichtung mittels vorkonfigurierter Integration* auf Seite 157 beschriebenen Schritte für den WLC bereits ausgeführt haben, um die Basis-Konfiguration abzuschließen und AutoWDS auf dem WLC generell zu aktivieren.

Änderungen am Ausgangsszenario

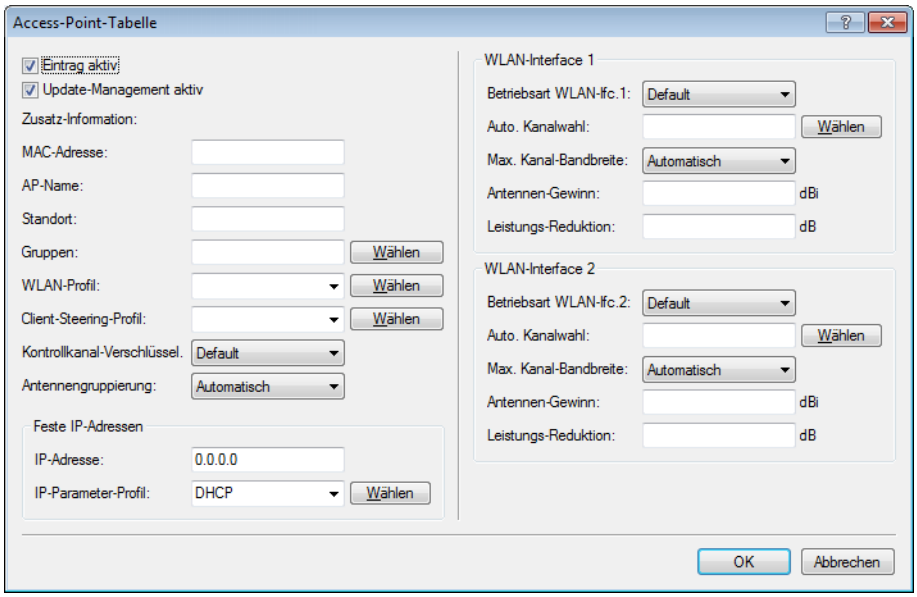
Das Ausgangsszenario gleicht dem der vorkonfigurierten Integration bzw. *Express-Integration*. Für die gesamte WLAN-Infrastruktur kommen ausschließlich Dual-Radio-APs zum Einsatz, die entsprechend der untenstehenden Grafik angeordnet sind. Das gemanagte WLAN besteht zu Beginn aus einem einzigen AP, der den hinzukommenden APs als initialer Zugangs-AP dient.



Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die Deaktivierung des automatischen Topologie-Managements und die Konfiguration manueller P2P-Strecken gemäß des unter *Manuelles Topologie-Mangement* auf Seite 160 beschriebenen Szenarios.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**, um zur Liste der verwalteten APs zu gelangen.



2. Geben Sie für jeden hinzukommenden AP die **MAC-Adresse** und unter **AP-Name** einen eindeutigen Namen an. Auf diesen Namen referenzieren Sie später in der Topologie-Konfiguration.

   Für das Beispielszenario lauten die einzelnen Konfigurationseinträge wie folgt:

Tabelle 1: Konfiguration der hinzukommenden APs in der Access-Point-Tabelle

Eintrag	MAC-Adresse	AP-Name
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

Der Tabelleneintrag AP-00 bezieht sich auf Ihren bereits vorhandenen AP, welchen die hinzukommenden APs als Zugangs-AP nutzen.

3. Wählen Sie das **WLAN-Profil** aus, für das Sie AutoWDS aktiviert haben.
   Über das betreffende WLAN-Profil erhalten die APs automatisch die Einstellungen für AutoWDS und damit auch die P2P-Konfiguration zugewiesen.
4. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
5. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
6. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.

7. Klicken Sie auf den Eintrag **AUTOWDS_PROFILE**, um das AutoWDS-Standardprofil zu bearbeiten.
8. Ändern Sie den Parameter **Topology-Management** auf **Manuell** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.
9. Wechseln Sie in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology** und klicken Sie **Hinzufügen**.
10. Legen Sie für jedes P2P-Paar eine manuelle P2P-Konfiguration an. Die festgelegte P2P-Strecke gilt stets aus Sicht des Slave-AP.
    a) Geben Sie im Feld **AutoWDS-Profil** das AutoWDS-Profil an, für das die manuelle P2P-Konfiguration gilt, z. B. `AUTOWDS_PROFILE`.
    b) Setzen Sie die **Priorität** der P2P-Konfiguration auf `0` (höchste Priorität).
    c) Geben Sie für **Slave-AP-Name** und **Master-AP-Name** den Namen der APs entsprechend der von Ihnen gewählten Hierarchie ein.

       Für das Beispielszenario lauten die einzelnen Konfigurationseinträge bei strikter Schnittstellen-Paarung wie folgt:

       Tabelle 2: Konfiguration der P2P-Paare in der AutoWDS-Topology-Tabelle

Eintrag	Slave-AP-Name	Slave-AP-WLAN-Ifc.	Master-AP-Name	Master-AP-WLAN-Ifc.
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

    d) Geben Sie unter **Schluessel** die WPA2-Passphrase an, mit der die P2P-Partner die P2P-Strecke verschlüsseln.

       Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.
    e) Schalten Sie den Eintrag **Aktiv** auf **Ja**.
    f) Speichern Sie den jeweiligen Eintrag mit einem Klick auf **Setzen**.

Waren bereits APs angeschlossen, übermittelt der WLC die neue Konfiguration an die APs und löst damit einen Rekonfigurationsprozess auf diesen aus. Waren noch keine APs angeschlossen, überträgt der WLC die P2P-Konfiguration beim ersten Verbindungsaufbau der hinzukommenden APs.

8.1.7 Redundante Strecken mittels RSTP

Das manuelle Topologie-Management eröffnet Ihnen in Kombination mit dem Rapid Spanning Tree Protocol (RSTP) die Möglichkeit, redundante P2P-Strecken einzurichten, um die Ausfallsicherheit Ihres gesamten AutoWDS-Basisnetzes zu verbessern. Hierzu müssen Sie RSTP zunächst im Setup-Menü eines jeden APs aktivieren, da sich die Management-Einstellungen des WLC nicht auf diesen Konfigurationsteil erstrecken. Um den Konfigurationsaufwand zu reduzieren, ist der Einsatz eines Skripts empfehlenswert, welches Sie über das Skript-Management des WLC an sämtliche APs übertragen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie dabei vorgehen. Die Schritte implizieren, dass Sie ein AutoWDS-Basisnetz bereits erfolgreich eingerichtet haben. Nach seiner Aktivierung führt RSTP die Pfadsuche vollautomatisch durch.

1. Erstellen Sie eine Textdatei mit dem Namen `WLC_Script_1.lcs`.
2. Kopieren die folgenden Codezeilen in die Textdatei und speichern Sie.

```
# Script (8.890.0000 / 14.02.2013)

lang English
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version        Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation   Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating               yes

flash Yes

# done
exit
```

3. Melden Sie sich an der WEBconfig-Oberfläche Ihres WLCs an und wählen Sie **Dateimanagement** > **Zertifikat oder Datei hochladen**.
4. Wählen Sie in der Auswahlliste **Dateityp** den Eintrag **CAPWAP - WLC_Script_1.lcs** und über die Schaltfläche **Durchsuchen** die zuvor angelegte Skriptdatei aus. Klicken Sie anschließend auf **Upload starten**.
   Den erfolgreichen Upload des Skripts in den WLC prüfen Sie z. B. über das Status-Menü unter **Dateisystem** > **Inhalt**.
5. Wechsel Sie im Setup-Menü zum Menüpunkt **WLAN-Management** > **Zentrales-Firmware-Management** > **Skriptverwaltung** und klicken Sie **Hinzufügen**.
6. Geben Sie als **Profil** `AUTOWDS_PROFILE` und als **Name** `WLC_Script_1.lcs` ein, um das AutoWDS-Profil mit dem Skriptnamen zu verbinden und an die APs auszurollen.
7. Weisen Sie – wie in Kapitel *Konfiguration des WLC* auf Seite 161 beschrieben – den APs im WLC eindeutige Namen zu und richten Sie die manuellen P2P-Strecken ein.

Damit haben Sie die Konfiguration erfolgreich abgeschlossen.

8.1.8 Ergänzungen im Status-Menü

AutoWDS

Zeigt an, ob es sich bei dem verbundenen Client um einen AutoWDS-fähigen AP im Client-Modus handelt und in welchem Modus dieser aktuell mit Ihrem gemanagten WLAN verbunden ist.

SNMP-ID:

1.3.32.62

Pfad Telnet:

Status > **WLAN** > **Stationstabelle**

Mögliche Werte:

nein
AutoWDS nicht aktiviert oder nicht unterstützt.

Preconfigured
AutoWDS ist aktiviert; SSID und WPA2-Passphrase sind vorkonfiguriert.

Express
AutoWDS ist aktiviert; SSID und WPA2-Passphrase sind nicht vorkonfiguriert.

AutoWDS

Zeigt an, ob das erkannte WLAN ein AutoWDS-Basisnetz ist.

SNMP-ID:

1.3.34.42

Pfad Telnet:

Status > **WLAN** > **Scan-Resultate**

Mögliche Werte:

Nein
Ja

AutoWDS

Zeigt an, ob das erkannte WLAN ein AutoWDS-Basisnetz ist.

SNMP-ID:

1.3.44.42

Pfad Telnet:

Status > **WLAN** > **Andere-Netze**

Mögliche Werte:

Nein
Ja

AutoWDS-Profil

Diese Tabelle zeigt die Einstellungen des AutoWDS-Profils, das Ihr Gerät vom WLC erhalten hat.

SNMP-ID:

1.59.106

Pfad Telnet:

Status > **WLAN-Management**

Name

Name des AutoWDS-Profils, das der WLC Ihrem Gerät zugewiesen hat.

SNMP-ID:

1.59.106.1

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

SSID

Name des logischen WLAN-Netzs (SSID), das der AP zum Aufspannen des AutoWDS-Basisnetzes heranzieht. Hinzukommende APs im Client-Modus nutzen die hier angegebene SSID außerdem, um eine Konfiguration vom WLC beziehen.

Die betreffende SSID ist exklusiv für AutoWDS reserviert. Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar.

SNMP-ID:

1.59.106.3

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Key

Zeigt die für das AutoWDS-Basisnetz verwendete WPA2-Passphrase an.

SNMP-ID:

1.59.106.4

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Netz-Nummer

Zeigt die interne Repräsentation des verwendeten Gesamtprofils als Nummer an.

SNMP-ID:

1.59.106.5

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Aktiv

Zeigt an, ob das zugewiesene AutoWDS aktiv oder inaktiv ist.

SNMP-ID:

1.59.106.6

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Mögliche Werte:

Nein
Ja

Erlaube-Express-Integration

Gibt an, ob Ihr Gerät anhand des ihm zugewiesenen AutoWDS-Profils die Express-Integration für hinzukommende APs erlaubt.

SNMP-ID:

1.59.106.7

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Mögliche Werte:

Nein
Ja

Zeit-bis-Preconf-Scan

Zeigt die festgelegte Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der im AutoWDS-Profil hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten abgelaufen sind. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

SNMP-ID:

1.59.106.15

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Zeit-bis-Express-Scan

Zeigt die festgelegte Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten sowie die *Wartezeit für den Beginn der vorkonfigurierten Integration* (sofern gesetzt) abgelaufen sind. Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

SNMP-ID:

1.59.106.16

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Schnittstellen-Paarung

Zeigt an, welche Art der Schnittstellen-Paarung ein Zugangs-AP anhand des ihm zugewiesenen AutoWDS-Profils erlaubt.

Die Schnittstellung-Paarung beeinflusst die Suche eines AP im Client-Modus nach geeigneten Zugangs-APs unter Beachtung der beteiligten WLAN-Schnittstellen. Sie legt fest, ob sich der hinzukommende AP für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden muss (mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder auch Paarungen mit anderen physikalischen WLAN-Schnittstellen eingehen darf. Die Definition der Schnittstellen-Paarung erlaubt, schon im Vorfeld ungültige Paarungen auszuschließen, die sich evtl. ansonsten durch die Zuweisung unterschiedlicher Frequenzbänder im Rahmen der WLC-Konfiguration ergeben würden.

SNMP-ID:

1.59.106.17

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Profil**

Mögliche Werte:

Automatisch

Der WLC prüft, ob eine Problemkonfiguration auftreten kann. Tritt keine Problemkonfiguration auf, akzeptiert er die betreffende Schnittstellen-Paarung über den Zugangs-AP. Andernfalls lehnt der WLC diese ab und der hinzukommende AP muss sich neu verbinden.

Strikt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X ausschließlich mit der äquivalenten WLAN-Schnittstelle eines Zugangs-AP verbinden.

Gemischt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X mit einer beliebigen WLAN-Schnittstelle eines Zugangs-AP verbinden.

AutoWDS-Topology

Diese Tabelle zeigt die Topologie bzw. P2P-Konfiguration des AutoWDS-Netzes, die der WLC Ihrem Gerät übermittelt hat. Anhand der hier hinterlegten Informationen baut Ihr Gerät die P2P-Strecke zu den ihm untergeordneten Slave-APs sowie den ihm übergeordneten Master-APs auf.

SNMP-ID:

1.59.107

Pfad Telnet:

Status > **WLAN-Management**

AutoWDS-Profil

Name des AutoWDS-Profils, vor dem die gewählte P2P-Konfiguration gilt.

SNMP-ID:

1.59.107.1

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Priorität

Zeigt die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

SNMP-ID:

1.59.107.2

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Slave-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Slaves einnimmt.

SNMP-ID:

1.59.107.3

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Slave-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

SNMP-ID:

1.59.107.4

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC-Adresse des Slave-AP.

SNMP-ID:

1.59.107.5

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Master-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Masters einnimmt.

SNMP-ID:

1.59.107.6

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Master-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

SNMP-ID:

1.59.107.7

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Master-AP-WLAN-MAC

MAC-Adresse des Master-AP.

SNMP-ID:

1.59.107.8

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Schluessel

WPA2-Passphrase der P2P-Verbindung.

SNMP-ID:

1.59.107.9

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Aktiv

Zeigt an, ob die betreffende P2P-Konfiguration aktiv oder inaktiv ist.

SNMP-ID:

1.59.107.10

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Mögliche Werte:

Nein
Ja

Slave-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.59.107.12

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Master-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt (in kBit/s). Der Wert 0 bedeutet 'unlimitiert'.

SNMP-ID:

1.59.107.13

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Link-Verlust-Timeout

Zeigt die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

SNMP-ID:

1.59.107.14

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Weiterbetrieb

Zeigt die Weiterbetriebszeit der vom WLC erhaltenen P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit 0 festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

1.59.107.16

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

generiert

Zeigt an, ob die erhaltene P2P-Konfiguration automatisch vom WLC generiert oder vom Netzadmin manuell im WLC determiniert wurde.

SNMP-ID:

1.59.107.17

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Mögliche Werte:

Nein
Ja

P2P-Index

Dieser Status-Wert zeigt auf den statischen P2P-Port, den die APs benutzen (z. B. P2P-1-1).

SNMP-ID:

1.59.107.19

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

P2P-Role

SNMP-ID:

1.59.107.20

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Topology**

Mögliche Werte:

Keine
Slave
Master

AutoWDS-Betrieb

Dieses Menü zeigt die Status-Werte Ihres Gerätes für den AutoWDS-Betrieb.

SNMP-ID:

1.59.109

Pfad Telnet:

Status > **WLAN-Management**

Aktiver-WLAN-Suchmodus

Zeigt an, ob und in welchem AutoWDS-Integrationsmodus Ihr Gerät sich aktuell befindet.

SNMP-ID:

1.59.109.1

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

Mögliche Werte:

Nein

Ihr Gerät sucht momentan kein AutoWDS-Basisnetz.

Preconfigured

Ihr Gerät sucht momentan nach dem vorkonfigurierten AutoWDS-Basisnetz.

Express

Ihr Gerät sucht momentan nach einem beliebigen AutoWDS-Basisnetz.

AutoWDS-Profile

Diese Tabelle zeigt die Einstellungen der AutoWDS-Profile, die der WLC den einzelnen APs zugewiesen hat.

SNMP-ID:

1.73.2.11

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Name

Name des AutoWDS-Profils, das der WLC den APs zugewiesen hat.

SNMP-ID:

1.73.2.11.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Gesamtprofil

Name des WLAN-Profils, dem das AutoWDS-Basisnetz zugewiesen ist. Alle APs, denen Sie das betreffende WLAN-Profil zugewiesen haben, spannen gleichzeitig das dazugehörige AutoWDS-Basisnetz auf.

SNMP-ID:

1.73.2.11.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

SSID

Name des logischen WLAN-Netzs (SSID), das der AP zum Aufspannen des AutoWDS-Basisnetzes heranzieht. Hinzukommende APs im Client-Modus nutzen die hier angegebene SSID außerdem, um eine Konfiguration vom WLC beziehen.

Die betreffende SSID ist exklusiv für AutoWDS reserviert. Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar.

SNMP-ID:

1.73.2.11.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Key

Zeigt die für das AutoWDS-Basisnetz verwendete WPA2-Passphrase an.

SNMP-ID:

1.73.2.11.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Aktiv

Zeigt an, ob das betreffende AutoWDS aktiv oder inaktiv ist.

SNMP-ID:

1.73.2.11.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Nein
Ja

Erlaube-Express-Integration

Gibt an, ob die APs des betreffenden WLAN-Profils über das AutoWDS-Basisnetz die Express-Integration für hinzukommende APs erlauben.

SNMP-ID:

1.73.2.11.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Nein
Ja

Topology-Management

Gibt an, welche Art des Topologie-Managements der WLC für das betreffende AutoWDS-Profil verfolgt.

Weitere Informationen dazu finden Sie unter dem korrespondierenden Setup-Parameter *2.37.1.15.8 Topology-Management* auf Seite 199.

SNMP-ID:

1.73.2.11.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

automatisch
Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.

semi-automatisch
Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.

manuell
Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Slave-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.11.10

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Master-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.11.11

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Link-Verlust-Timeout

Zeigt die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

SNMP-ID:

1.73.2.11.12

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Weiterbetrieb

Zeigt die Weiterbetriebszeit der automatisch generierten P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

1.73.2.11.14

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Zeit-bis-Preconf-Scan

Zeigt die festgelegte Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der im AutoWDS-Profil hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten abgelaufen sind. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

SNMP-ID:

1.73.2.11.15

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Zeit-bis-Express-Scan

Zeigt die festgelegte Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten sowie die *Wartezeit für den Beginn der vorkonfigurierten Integration* (sofern gesetzt) abgelaufen sind. Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

SNMP-ID:

1.73.2.11.16

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Schnittstellen-Paarung

Zeigt an, welche Art der Schnittstellen-Paarung ein Zugangs-AP anhand des ihm zugewiesenen AutoWDS-Profils erlaubt.

Die Schnittstellung-Paarung beeinflusst die Suche eines AP im Client-Modus nach geeigneten Zugangs-APs unter Beachtung der beteiligten WLAN-Schnittstellen. Sie legt fest, ob sich der hinzukommende AP für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden muss (mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder auch Paarungen mit anderen physikalischen WLAN-Schnittstellen eingehen darf. Die Definition der Schnittstellen-Paarung erlaubt, schon im Vorfeld ungültige Paarungen auszuschließen, die sich evtl. ansonsten durch die Zuweisung unterschiedlicher Frequenzbänder im Rahmen der WLC-Konfiguration ergeben würden.

SNMP-ID:

1.73.2.11.17

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Automatisch

Der WLC prüft, ob eine Problemkonfiguration auftreten kann. Tritt keine Problemkonfiguration auf, akzeptiert er die betreffende Schnittstellen-Paarung über den Zugangs-AP. Andernfalls lehnt der WLC diese ab und der hinzukommende AP muss sich neu verbinden.

Strikt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X ausschließlich mit der äquivalenten WLAN-Schnittstelle eines Zugangs-AP verbinden.

Gemischt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X mit einer beliebigen WLAN-Schnittstelle eines Zugangs-AP verbinden.

AutoWDS-Topology

Diese Tabelle zeigt manuellen Bestandteile der AutoWDS-Topologie; genauer gesagt: die manuellen P2P-Strecken zwischen den einzelnen Slave-APs und Master-APs, die der WLC an die einzelnen APs übermittelt hat. Die angelegten P2P-Strecken sind dabei immer aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP zu sehen.

SNMP-ID:

1.73.2.12

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

AutoWDS-Profil

Name des AutoWDS-Profils, vor dem die gewählte P2P-Konfiguration gilt.

SNMP-ID:

1.73.2.12.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Priorität

Zeigt die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

SNMP-ID:

1.73.2.12.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Slave-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Slaves einnimmt.

SNMP-ID:

1.73.2.12.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Slave-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

SNMP-ID:

1.73.2.12.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC-Adresse des Slave-AP.

SNMP-ID:

1.73.2.12.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Master-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Masters einnimmt.

SNMP-ID:

1.73.2.12.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Master-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

SNMP-ID:

1.73.2.12.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Master-AP-WLAN-MAC

MAC-Adresse des Master-AP.

SNMP-ID:

1.73.2.12.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Schluessel

WPA2-Passphrase der P2P-Verbindung.

SNMP-ID:

1.73.2.12.9

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Aktiv

Zeigt an, ob die betreffende P2P-Konfiguration aktiv oder inaktiv ist.

Der WLC überträgt keine inaktiven P2P-Konfigurationen zum AP und ignoriert inaktive Einträge bei der Auswertung der manuellen AutoWDS-Topology-Tabelle im halbautomatischen Modus.

SNMP-ID:

1.73.2.12.10

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Nein
Ja

Slave-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die manuelle P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.12.12

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Master-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die manuelle P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.12.13

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Link-Verlust-Timeout

Zeigt die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

SNMP-ID:

1.73.2.12.14

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Weiterbetrieb

Zeigt die Weiterbetriebszeit der manuellen P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

1.73.2.12.16

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

generiert

Zeigt an, ob die P2P-Konfiguration automatisch vom WLC generiert oder vom Netzadmin manuell im WLC determiniert wurde.

SNMP-ID:

1.73.2.12.17

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Nein
Ja

Status

Zeigt den Status der betreffenden P2P-Strecke an.

SNMP-ID:

1.73.2.12.18

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Keiner

Der Status der betreffenden P2P-Partner konnte nicht erkannt werden ('Unbekannt').

Aktiv

Die betreffenden P2P-Partner sind miteinander verbunden.

Inaktiv

Die betreffenden P2P-Partner sind nicht miteinander verbunden.

AutoWDS-Auto-Topology

Diese Tabelle zeigt automatisch durch den WLC generierten Bestandteile der AutoWDS-Topologie; genauer gesagt: die generierten P2P-Strecken zwischen den einzelnen Slave-APs und Master-APs, die der WLC an die einzelnen APs übermittelt hat. Die generierten P2P-Strecken sind dabei immer aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP zu sehen.

SNMP-ID:

1.73.2.13

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

AutoWDS-Profil

Name des AutoWDS-Profils, vor dem die gewählte P2P-Konfiguration gilt.

SNMP-ID:

1.73.2.13.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Priorität

Zeigt die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

SNMP-ID:

1.73.2.13.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Slave-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Slaves einnimmt.

SNMP-ID:

1.73.2.13.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Slave-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

SNMP-ID:

1.73.2.13.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC-Adresse des Slave-AP.

SNMP-ID:

1.73.2.13.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Master-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Masters einnimmt.

SNMP-ID:

1.73.2.13.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Master-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

SNMP-ID:

1.73.2.13.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Mögliche Werte:

Automatisch
WLAN-1
WLAN-2

Master-AP-WLAN-MAC

MAC-Adresse des Master-AP.

SNMP-ID:

1.73.2.13.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Schluessel

WPA2-Passphrase der P2P-Verbindung.

SNMP-ID:

1.73.2.13.9

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Aktiv

Zeigt an, ob die betreffende P2P-Konfiguration aktiv oder inaktiv ist.

Der WLC überträgt keine inaktiven P2P-Konfigurationen zum AP und ignoriert inaktive Einträge bei der Auswertung der manuellen AutoWDS-Topology-Tabelle im halbautomatischen Modus.

SNMP-ID:

1.73.2.13.10

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Mögliche Werte:

Nein
Ja

Slave-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.13.12

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Master-Tx-Limit

Zeigt die maximale Übertragungsbandbreite, die für die generierte P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt (in kBit/s). Der Wert `0` bedeutet 'unlimitiert'.

SNMP-ID:

1.73.2.13.13

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Link-Verlust-Timeout

Zeigt die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

SNMP-ID:

1.73.2.13.14

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Weiterbetrieb

Zeigt die Weiterbetriebszeit der automatisch generierten P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

1.73.2.13.16

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

generiert

Zeigt an, ob die P2P-Konfiguration automatisch vom WLC generiert oder vom Netzadmin manuell im WLC determiniert wurde.

SNMP-ID:

1.73.2.13.17

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Auto-Topology**

Mögliche Werte:

Nein
Ja

Status

Zeigt den Status der betreffenden P2P-Strecke an.

SNMP-ID:

1.73.2.13.18

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Keiner
Der Status der betreffenden P2P-Partner konnte nicht erkannt werden ('Unbekannt').

Aktiv
Die betreffenden P2P-Partner sind miteinander verbunden.

Inaktiv

Die betreffenden P2P-Partner sind nicht miteinander verbunden.

AutoWDS-Prof.-Errors

Diese Tabelle enthält die Fehlermeldungen, die beim Zuweisen eines AutoWDS-Profils aufgetreten sind.

SNMP-ID:

1.73.2.14

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.14.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Prof.-Errors**

Name

Name des AutoWDS-Profils, unter dem der Fehler aufgetreten ist.

SNMP-ID:

1.73.2.14.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Prof.-Errors**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.14.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Prof.-Errors**

Netz/AP-Parameter

Parameter des WLANs und des AP, in deren Zusammenhang der Fehler aufgetreten ist.

SNMP-ID:

1.73.2.14.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Prof.-Errors**

AutoWDS-Topo.-Errors

Diese Tabelle enthält die Fehlermeldungen, die beim Zuweisen einer P2P-Konfiguration für AutoWDS aufgetreten sind.

SNMP-ID:

1.73.2.15

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.15.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

AutoWDS-Profil

Name des AutoWDS-Profils, unter dem der Fehler aufgetreten ist.

SNMP-ID:

1.73.2.15.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Priorität

Zeigt die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

SNMP-ID:

1.73.2.15.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Slave-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Slaves einnimmt.

SNMP-ID:

1.73.2.15.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Slave-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

SNMP-ID:

1.73.2.15.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Slave-AP-WLAN-MAC

MAC-Adresse des Slave-AP.

SNMP-ID:

1.73.2.15.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Master-AP-Name

Name des AP in der WLC-Konfiguration, der die Rolle des Masters einnimmt.

SNMP-ID:

1.73.2.15.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Master-AP-WLAN-Ifc.

Zeigt die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

SNMP-ID:

1.73.2.15.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Master-AP-WLAN-MAC

MAC-Adresse des Master-AP.

SNMP-ID:

1.73.2.15.

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.15.

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topo.-Errors**

AutoWDS-Integration

Zeigt an, ob der hinzukommende AP die CAPWAP-Verbindung über LAN oder WLAN zum WLC aufgebaut hat und welchen Integrationsmodus er verwendet.

SNMP-ID:

1.73.9.3.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Status** > **Neue-AP**

Mögliche Werte:

Keine
CAPWAP über LAN

Express
CAPWAP über WLAN

Preconfigured
CAPWAP über WLAN

8.1.9 Ergänzungen im Setup-Menü

AutoWDS

Diese Tabelle enthält die lokalen Werkseinstellungen Ihres Gerätes für die Suche nach und Authentifikation an einem AutoWDS-Basisnetz. Über die Timeout-Zeiten legen Sie fest, ob Ihr Gerät dabei die vorkonfigurierte Integration, die Express-Integration oder eine abgestufte Kombination aus beidem verfolgt.

Solange Ihr Gerät noch keine AutoWDS-Einstellungen von einem WLC erhalten hat, benutzt das Gerät die hier hinterlegten Voreinstellungen. Sobald Ihr Gerät jedoch ein AutoWDS-Profil von einem WLC erhält, genießt dessen Konfiguration die höhere Priorität, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

Die hier festgelegten Parameter betreffen ausschließlich die initiale Anmeldung eines hinzukommenden Slave-AP an einem Master-AP zur Suche nach einem WLC. Sie betreffen nicht die später aufgebauten P2P-Strecke zu einem Master-AP; hierzu verwendet Ihr Gerät dann die erhaltene WLC-Konfiguration.

Ob das Gerät vom WLC eine AutoWDS-Konfiguration erhalten hat, lässt sich anhand der Status-Tabelle **AutoWDS-Profil** (SNMP-ID 1.59.106) überprüfen.

SNMP-ID:
2.59.4

Pfad Telnet:
Setup > **WLAN-Management**

Aktiv

Schalten Sie die AutoWDS-Funktion auf Ihrem Gerät ein- oder aus. Im deaktivierten Zustand versucht das Gerät nicht selbstständig, sich in ein gemanagtes WLAN zu integrierten, und führt auch keine Scans nach aktiven AutoWDS-Netzen durch.

SNMP-ID:
2.59.4.1

Pfad Telnet:
Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Preconf-SSID

Tragen Sie die SSID des AutoWDS-Basisnetzes ein, nach dem Ihr Gerät im Sinne einer vorkonfigurierten Integration sucht. Dazu müssen Sie AutoWDS aktiviert und die *Wartezeit bis zur vorkonfigurierten Suche* größer `0` gesetzt haben.

Nach Ablauf der Wartezeit schaltet das Gerät sämtliche physikalischen WLAN-Schnittstellen in den Client-Modus und beginnt mit der Suche nach der eingetragenen SSID. Findet das Gerät eine übereinstimmende SSID, versucht es daraufhin, sich mit der eingetragenen WPA2-Passphrase am betreffenden WLAN zu authentisieren.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

SNMP-ID:

2.59.4.2

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

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

Default-Wert:

leer

Preconf-Key

Geben Sie die WPA2-Passphrase an, die Ihr Gerät für die Authentifikation am vorkonfigurierten AutoWDS-Basisnetz benutzt.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

SNMP-ID:

2.59.4.3

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

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

Default-Wert:

leer

Zeit-bis-Preconf-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der lokal hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, sofern noch keine Konfigurationsbestandteile von einem WLC vorliegen. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Konfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

SNMP-ID:

2.59.4.4

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit und den Prozess zur vorkonfigurierte Integration. Das Gerät beginnt sofort damit, die Wartezeit für den Beginn der Express-Integration herabzuzählen.

Default-Wert:

0

Zeit-bis-Express-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, sofern noch keine Konfigurationsbestandteile von einem WLC vorliegen und die *Wartezeit für den Beginn der vorkonfigurierten Integration* (sofern gesetzt) abgelaufen ist. Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

SNMP-ID:

2.59.4.5

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit und den Prozess zur vorkonfigurierte Integration.

Default-Wert:

1

Konfigurationsverzoegerung

Über diesen Parameter definieren Sie die Verzögerungszeit, nach der ein AP ein vom WLC unmittelbar ausgerolltes Konfigurationsupdate ausführt.

Die Verzögerungszeit ist primär für APs relevant, die Sie ausschließlich über eine Funkstrecke (z. B. mittels AutoWDS) in Ihr gemanagtes WLAN integrieren. Dabei reduzieren Sie die Wahrscheinlichkeit, dass durch nicht zugestellte Konfigurationsupdates lediglich eine Teilkonfiguration Ihres Netzes erfolgt und die übrigen APs ggf. unerreichbar werden. Je höher Sie die Verzögerungszeit einstellen, desto wahrscheinlicher ist, dass sämtliche hinzukommenden APs das vom WLC ausgerollte Konfigurationsupdate auch tatsächlich erhalten.

Empfehlenswert ist ein Wert von mindestens 1 Sekunde pro (AutoWDS-)Hop.

SNMP-ID:

2.37.1.3.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert das verzögerte Konfigurationsupdate.

Default-Wert:

0

AutoWDS-Profile

Diese Tabelle enthält die Parameter für das AutoWDS-Profil, welches Sie über das WLAN-Profil den einzelnen Access Points zuweisen, um den Aufbau vermaschter Netze zu realisieren. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

SNMP-ID:

2.37.1.15

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Name

Name des AutoWDS-Profils, auf das Sie aus anderen Tabellen referenzieren.

SNMP-ID:

2.37.1.15.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

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

Default-Wert:

leer

Gesamtprofil

Geben Sie den Namen des WLAN-Profils an, dem das AutoWDS-Basisnetz zugewiesen ist. Alle APs, denen Sie das betreffende WLAN-Profil zugewiesen haben, spannen so gleichzeitig das dazugehörige AutoWDS-Basisnetz auf.

SNMP-ID:

2.37.1.15.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

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

Default-Wert:

leer

SSID

Geben Sie den Namen des logischen WLAN-Netzs (SSID) an, das ein gemanagter AP zum Aufspannen des AutoWDS-Basisnetzes heranzieht. Hinzukommende APs im Client-Modus nutzen die hier angegebene SSID außerdem, um eine Konfiguration vom WLC beziehen.

Die betreffende SSID ist exklusiv für AutoWDS reserviert. Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb Ihrer WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

SNMP-ID:

2.37.1.15.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

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

Default-Wert:

AutoWDS-Control

Key

Geben Sie die WPA2-Passphrase für das AutoWDS-Basisnetz an, das ein gemanagter AP aufspannt. Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

SNMP-ID:

2.37.1.15.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

min. 8 Zeichen; max. 63 Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default-Wert:

leer

Aktiv

Legen Sie fest, ob AutoWDS für das gewählte Profil aktiv oder inaktiv ist. Inaktive Profile überträgt das WLC nicht zu einem AP.

SNMP-ID:

2.37.1.15.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Erlaube-Express-Integration

Geben Sie an, ob die APs des betreffenden WLAN-Profils über das AutoWDS-Basisnetz die Express-Integration für hinzukommende APs erlauben. Wenn Sie diese Einstellung aktivieren, senden die betreffenden Master-APs in ihren Beacons eine zusätzliche herstellerspezifische Kennung aus, die hinzukommenden APs die Verfügbarkeit dieser Integrationsvariante signalisiert.

Sofern Sie AutoWDS aktivieren und die Express-Integration verbieten, erlaubt das AutoWDS-Basisnetz ausschließlich die vorkonfigurierte Integration hinzukommender oder eingebundener APs im Client-Modus.

SNMP-ID:

2.37.1.15.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

nein

Das AutoWDS-Basisnetz erlaubt ausschließlich die vorkonfigurierte Integration hinzukommender APs.

ja

Das AutoWDS-Basisnetz erlaubt sowohl die vorkonfigurierte als auch die Express-Integration hinzukommender APs .

Default-Wert:

nein

Topology-Management

Geben Sie an, welche Art des Topologie-Managements der WLC für das betreffende AutoWDS-Profil verfolgt.

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie die Topologie des vermaschten Netzes aufgebaut ist. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Die beiden betreffenden WLAN-Schnittstellen bilden dazu ein P2P-Paar: Die physikalische WLAN-Schnittstelle des hinzukommenden AP wird zum P2P-Slave; die des gewählten Zugangs-AP zum P2P-Master.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology** (SNMP-ID 1.73.2.13). Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest.

Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

SNMP-ID:

2.37.1.15.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

automatisch

Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.

semi-automatisch

Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.

manuell

Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Default-Wert:

automatisch

Slave-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat.

SNMP-ID:

2.37.1.15.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

Master-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat.

SNMP-ID:

2.37.1.15.11

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

Link-Verlust-Timeout

Definieren Sie die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

Der Link-Verlust-Timeout ist unabhängig von den übrigen Timeouts. Es ist empfehlenswert, den voreingestellten Wert nicht weiter zu verringern, um die Gesamtkonnektivität des AutoWDS-Basisnetzes stabil zu halten.

SNMP-ID:

2.37.1.15.12

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

4

Weiterbetrieb

Definieren Sie die Weiterbetriebszeit der automatisch generierten P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

2.37.1.15.14

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 9999 Minuten

Besondere Werte:

0

Der AP schaltet seine physikalische(n) WLAN-Schnittstelle(n) unverzüglich ab, sobald der Kontakt zum WLC verloren geht. Dabei löscht das Gerät umgehend seine Konfigurations-Parameter, sodass der WLC sie beim Wiederaufbau der Verbindung erneut übertragen muss.

Wählen Sie diese Einstellung, um die sicherheitsrelevanten Konfigurations-Parameter vor unbefugtem Zugriff und Missbrauch (z. B. im Fall eines Diebstahls des AP) zu schützen.

9999

Die Konfigurations-Parameter bleiben dauerhaft im Gerät gespeichert. Der AP arbeitet weiter; unabhängig davon, wie lange der Kontakt zum WLC verloren geht.

Default-Wert:

0

Zeit-bis-Preconf-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der im AutoWDS-Profil hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten abgelaufen sind. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

SNMP-ID:

2.37.1.15.15

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die vorkonfigurierte Integration auf dem betreffenden AP.

Default-Wert:

60

Zeit-bis-Express-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten sowie die *Wartezeit für den Beginn der vorkonfigurierten Integration* abgelaufen sind (sofern gesetzt). Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

SNMP-ID:

2.37.1.15.16

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Express-Integration auf dem betreffenden AP.

Default-Wert:

0

Schnittstellen-Paarung

Legen Sie fest, welche Art der Schnittstellen-Paarung ein Zugangs-AP anhand des ihm zugewiesenen AutoWDS-Profils erlaubt. Die Einstellung ist hauptsächlich für Geräte mit mehr als einer physikalischen WLAN-Schnittstelle relevant.

Die Schnittstellung-Paarung beeinflusst die Suche eines AP im Client-Modus nach geeigneten Zugangs-APs unter Beachtung der beteiligten WLAN-Schnittstellen. Sie legt fest, ob sich der hinzukommende AP für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden muss (mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder auch Paarungen mit anderen physikalischen WLAN-Schnittstellen eingehen darf. Die Definition der Schnittstellen-Paarung erlaubt, schon im Vorfeld ungültige Paarungen auszuschließen, die sich evtl. ansonsten durch die Zuweisung unterschiedlicher Frequenzbänder im Rahmen der WLC-Konfiguration ergeben würden.

Arbeiten die Zugangs-APs Ihres AutoWDS-Basisnetzes beispielsweise mit den physikalischen WLAN-Schnittstellen WLAN-1 fest im 2,4 GHz-Band und WLAN-2 fest im 5 GHz-Band, so vorhindert die Schnittstellen-Paarung **Strikt**, dass ein hinzukommender AP, der auf einer physikalischen WLAN-Schnittstelle beide Frequenzbänder durchsucht, für z. B. WLAN-1 das 5-GHz-Band wählt, um sich mit WLAN-2 des Zugangs-AP zu verbinden. Eine solche Verbindung wäre zwar für den Bezug der WLC-Konfiguration legitim. Der anschließende P2P-Verbindungsaufbau wäre aufgrund der unterschiedlichen Radio-Einstellungen jedoch nicht möglich. Der hinzukommende AP würde die Verbindung verlieren und müsste einen Rekonfigurationsprozess starten.

Funken hingegen beide physikalischen WLAN-Schnittstellen auf demselben Band, ist auch die Schnittstellen-Paarung **Gemischt** zulässig, da die oben beschriebene Problemkonfiguration so nicht auftreten kann.

SNMP-ID:

2.37.1.15.17

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Automatisch

Der WLC prüft, ob eine Problemkonfiguration auftreten kann. Tritt keine Problemkonfiguration auf, akzeptiert er die betreffende Schnittstellen-Paarung über den Zugangs-AP. Andernfalls lehnt der WLC diese ab und der hinzukommende AP muss sich neu verbinden.

Strikt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X ausschließlich mit der äquivalenten WLAN-Schnittstelle eines Zugangs-AP verbinden.

Gemischt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X mit einer beliebigen WLAN-Schnittstelle eines Zugangs-AP verbinden.

Default-Wert:

Automatisch

Slave-Radio-Multi-Hop

Über diesen Parameter legen Sie fest, ob die Zugangs-APs Ihres AutoWDS-Basisnetzes Verbindungsanfragen hinzukommender APs auf jener physikalischen WLAN-Schnittstelle akzeptieren, mit der sie selber als Slave zum Master verbunden sind.

Ein Deaktivieren dieses Parameters kann die Stabilität und die Lastverteilung innerhalb Ihres AutoWDS-Basisnetzes verbessern. In Folge dessen sind Single-Radio-APs dann jedoch nicht mehr als Zugangs-APs für die Erweiterung Ihres AutoWDS-Basisnetzes verfügbar und stellen das Ende eines Hierarchie-Zweigs dar.

SNMP-ID:

2.37.1.15.18

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Nein

Ein Zugangs-AP nimmt Verbindungsanfragen hinzukommender APs niemals auf der gleichen physikalischen WLAN-Schnittstelle an, mit der er bereits als Slave mit dem AutoWDS-Basisnetz verbunden ist. WLAN-Multihops sind ausschließlich auf Geräten mit zwei gemanagten physikalischen WLAN-Schnittstellen möglich.

Ja

Ein Zugangs-AP nimmt Verbindungsanfragen hinzukommender APs auch auf der gleichen physikalischen WLAN-Schnittstelle an, mit der er bereits als Slave mit dem AutoWDS-Basisnetz verbunden ist. WLAN-Multihops sind sowohl auf Geräten mit zwei als auch einer gemanagten physikalischen WLAN-Schnittstelle möglich.

Nur-Single-Radio-AP

Fallabhängige Einstellung:

Für Geräte mit einer physikalischen WLAN-Schnittstelle gilt die Einstellung **Ja**.

Für Geräte mit mehr als einer physikalischen WLAN-Schnittstelle gilt die Einstellung **Nein**.

Default-Wert:

Nein

Band

Geben Sie an, welches Frequenzband die einzelnen P2P-Partner für den Verbindungsaufbau zueinander verwenden.

SNMP-ID:

2.37.1.15.19

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

2,4GHz/5GHz
Für die Kommunikation der P2P-Partner untereinander ist sowohl das 2,4-GHz-Band als auch das 5-GHz-Band zugelassen.

2,4GHz
Für die Kommunikation der P2P-Partner untereinander ist ausschließlich das 2,4-GHz-Band zugelassen.

5GHz
Für die Kommunikation der P2P-Partner untereinander ist ausschließlich das 5-GHz-Band zugelassen.

Default-Wert:

2,4GHz/5GHz

AutoWDS-Topology

In dieser Tabelle legen Sie die manuellen Bestandteile der AutoWDS-Topologie fest; genauer gesagt: die P2P-Strecken zwischen den einzelnen Slave-APs und Master-APs. Das Gerät wertet diese Tabelle nur dann aus, wenn sie das manuelle oder semi-automatische *Topologie-Management* aktiviert haben.

SNMP-ID:

2.37.1.16

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

AutoWDS-Topology

Name des AutoWDS-Profils, für das diese manuelle P2P-Konfiguration gilt.

SNMP-ID:

2.37.1.16.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profil**

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

Default-Wert:

leer

Priorität

Geben Sie die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

Diese Einstellung ist zum gegenwärtigen Zeitpunkt lediglich ein Platzhalter; die Auswertung von Prioritäten ist noch nicht implementiert. Bitte tragen Sie für die Priorität stets den Wert `0` ein.

SNMP-ID:

2.37.1.16.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295

Default-Wert:

leer

Slave-AP-Name

Geben Sie den Namen des AP an, der die Rolle des Slaves einnimmt.

SNMP-ID:

2.37.1.16.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

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

Default-Wert:

leer

Slave-AP-WLAN-Ifc.

Definieren Sie die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

SNMP-ID:

2.37.1.16.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen

Default-Wert:

WLAN-1

Master-AP-Name

Geben Sie den Namen des AP an, der die Rolle des Masters einnimmt.

SNMP-ID:

2.37.1.16.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

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

Default-Wert:

leer

Master-AP-WLAN-Ifc.

Definieren Sie die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

SNMP-ID:

2.37.1.16.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen

Default-Wert:

WLAN-1

Schluessel

Geben Sie optional eine individuelle WPA2-Passphrase für die P2P-Verbindung an. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.

SNMP-ID:

2.37.1.16.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

min. 8 Zeichen; max. 63 Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Aktiv

Legen Sie fest, ob die P2P-Konfiguration für das gewählte AutoWDS-Profil aktiv oder inaktiv ist.

Der WLC überträgt keine inaktiven P2P-Konfigurationen zum AP und ignoriert inaktive Einträge bei der Auswertung der manuellen AutoWDS-Topology-Tabelle im halbautomatischen Modus.

SNMP-ID:

2.37.1.16.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Slave-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen.

SNMP-ID:

2.37.1.16.12

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

Master-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen.

SNMP-ID:

2.37.1.16.13

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

Link-Verlust-Timeout

Definieren Sie die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

Der Link-Verlust-Timeout ist unabhängig von den übrigen Timeouts. Es ist empfehlenswert, den Timeout auf mindestens 4 Sekunden zu setzen, um die Gesamtkonnektivität des AutoWDS-Basisnetzes stabil zu halten.

SNMP-ID:

2.37.1.16.14

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Bei diesem Wert übernimmt der WLC den festgelegten Wert für **Link-Verlust-Timeout** aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.

Default-Wert:

0

Weiterbetrieb

Definieren Sie die Weiterbetriebszeit der manuellen P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

SNMP-ID:

2.37.1.16.16

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 9999 Minuten

Besondere Werte:

0

Der AP schaltet seine physikalische(n) WLAN-Schnittstelle(n) unverzüglich ab, sobald der Kontakt zum WLC verloren geht. Dabei löscht das Gerät umgehend seine Konfigurations-Parameter, sodass der WLC sie beim Wiederaufbau der Verbindung erneut übertragen muss.

Wählen Sie diese Einstellung, um die sicherheitsrelevanten Konfigurations-Parameter vor unbefugtem Zugriff und Missbrauch (z. B. im Fall eines Diebstahls des AP) zu schützen.

9999

Die Konfigurations-Parameter bleiben dauerhaft im Gerät gespeichert. Der AP arbeitet weiter; unabhängig davon, wie lange der Kontakt zum WLC verloren geht.

Default-Wert:

0

8.2 IP-abhängige Autokonfiguration und Tagging von APs

Sämtliche APs, die Sie einem gemanagten Netz hinzufügen, verwalten Sie im einfachsten Falle in einer flachen Hierarchie. In größeren Installationen mit Hunderten von APs über mehrere Standorte hinweg wird diese Form der Organisation jedoch schnell unübersichtlich und erzeugt einen hohen Administrationsaufwand. Über die Einrichtung von **Zuweisungs-Gruppen** haben Sie daher die Möglichkeit, das Management verteilter APs zu vereinfachen. Hierbei lassen Sie neue APs in Abhängigkeit von der erhaltenen IP-Adresse automatisch vom WLC konfigurieren. Dadurch entfällt die manuelle Zuweisung eines IP-Parameter-Profils, eines WLAN-Profils und eines Client-Steering-Profils durch einen Administrator.

Die Anwendung einer Zuweisungs-Gruppe bei Anmeldung eines neuen APs an einem zentralen WLC läuft nach folgendem Schema ab: Nachdem die neuen APs am gewünschten Einsatzort (z. B. einem Firmen- bzw. Filialnetz) installiert sind, versuchen diese, eine Verbindung zum eingetragenen WLC aufzubauen und via CAPWAP eine Konfiguration zu beziehen. Der WLC erkennt die Verbindungsanfragen und prüft für jeden neuen AP, ob in der Access-Point-Tabelle ein geeignetes AP-Profil (z. B. das Default-Profil) vorliegt oder/und eine geeignete Zuweisungs-Gruppe definiert ist. Liegen eine oder mehrere Konfigurationsmöglichkeiten vor, prüft der WLC diese auf folgende Zustände:

1. Für einen neuen AP existiert eine Zuweisungs-Gruppe, jedoch kein AP-Profil. In diesem Fall weist der WLC dem neuen AP die innerhalb der Zuweisungs-Gruppe definierten Profile zu.
2. Für einen neuen AP existiert sowohl eine Zuweisungs-Gruppe als auch ein AP-Profil. In diesem Fall ignoriert der WLC die Zuweisungs-Gruppe und weist dem neuen AP die innerhalb des AP-Profils definierten Profile zu.
3. Für einen neuen AP existiert ein AP-Profil, aber keine Zuweisungs-Gruppe. Das Verhalten entspricht dem von Punkt (2).

Existieren für einen neuen AP weder ein AP-Profil, noch eine Zuweisungs-Gruppe, gibt der WLC eine Warnung aus, welche den Administrator auf die Fehlkonfiguration hinweist.

Nach der erfolgreichen Gruppenzuweisung legt der WLC in der Access-Point-Tabelle automatisch ein AP-Profil für jeden neuen AP an. Im Feld **Gruppen** referenziert der WLC die Zuweisungs-Gruppen, die er beim Hinzufügen des neuen AP angewandt hat.

Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt LCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

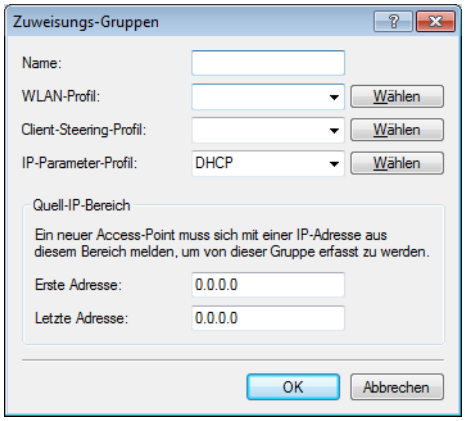
Über das Gruppen-Feld haben Sie ebenfalls die Möglichkeit, einen AP mit individuell definierbaren Tags zu versehen. Diese **Tag-Gruppen** lassen sich z. B. beim Ausführen von Aktionen auf dem WLC als Filterkriterien einsetzen, um eine Aktion auf eine Auswahl von APs zu beschränken.

8.2.1 Einrichten von Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration

Das nachfolgende Tutorial zeigt Ihnen, wie Sie auf einem WLC Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration neuer APs einrichten.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Zuweisungs-Gruppen**.

2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie als **Name** eine eindeutige Bezeichnung für die Zuweisungs-Gruppe an, z. B. `Filiale_Berlin`.
4. Wählen Sie das **WLAN-Profil** aus, welches der WLC einem neuen AP automatisch zuweist, wenn die IP-Adresse des neuen APs innerhalb des Quell-IP-Bereichs liegt.
5. Geben Sie ein **IP-Parameter-Profil** an, sofern der neue AP eine manuelle Netzkonfiguration erhalten soll. Andernfalls belassen Sie den Einzelwert **DHCP**; hierbei erhält der AP eine automatische Netzkonfiguration vom DHCP-Server. Der DHCP-Server muss dazu entsprechend konfiguriert sein.

   Sofern Sie eine manuelle Netzkonfiguration zuweisen wollen, bei der ein neuer AP eine abweichende IP-Adresse erhält, so geben Sie den entsprechenden Adressbereich im **IP-Parameter-Profil** unter **Address-Zuweisungs-Pool** an.
6. **Optional**: Geben Sie ein **Client-Steering-Profil** an, um bei mehreren neuen APs die sich im Sendebereich befindlichen, künftigen WLAN-Clients auf den für sie idealen AP umzuleiten.

   Sofern Sie Client-Steering aktivieren, muss dieses innerhalb der zu managenden Infrastruktur für jeden AP aktiviert sein. Weitere Informationen dazu finden Sie im Abschnitt *Client-Steering über den WLC* auf Seite 254.
7. Geben Sie den Anfang und das Ende des **Quell-IP-Bereich**s an, für den die Zuweisungs-Gruppe gilt.
   Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.
8. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

Der WLC weist fortan allen neuen APs die in den Zuweisungs-Gruppen referenzierten Profile zu. Über die LCOS-Konsole haben Sie dann die Möglichkeit, Informationen zur Kategorisierung abzurufen, siehe *Übersicht der capwap-Parameter im show-Befehl* auf Seite 224.

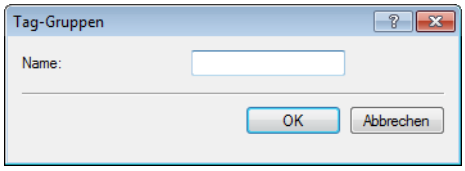
Achten Sie darauf, dass in der Access-Point-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

8.2.2 Einrichten von Tag-Gruppen für die selektive Auswahl von APs

Das nachfolgende Tutorial zeigt Ihnen, wie Sie eine AP-Konfiguration auf einem WLC um eine Tag-Gruppe erweitern. Dazu legen Sie zunächst eine Tag-Gruppe an und weisen diese Gruppe anschließend einem WLAN-Profil zu.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Tag-Gruppen**.

2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie unter **Name** den zu definierenden Tag ein und speichern Sie den Eintrag mit **OK**.
4. Wechseln Sie in den Dialog **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**.
5. Wählen Sie ein bestehendes Access-Point-Profil über **Bearbeiten** aus oder fügen Sie ggf. ein neues hinzu.
6. Wählen Sie unter **Gruppen** die zuvor anlegte(n) Tag-Gruppe(n) aus.
   Mehrere Tag-Gruppen trennen Sie durch eine kommaseparierte Liste.

   Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat gemäß der unter *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 211 beschriebenen Zustandsprüfung keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

   Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.
7. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

Der WLC versieht fortan alle APs, die das bearbeitete WLAN-Profil erhalten, mit den darin referenzierten Tags.

8.2.3 Ergänzungen im Status-Menü

Netz.-Prof.-Fehler

Diese Tabelle enthält die Fehlermeldungen, die beim Zuweisen von Netz-Profilen aufgetreten sind.

SNMP-ID:

1.73.2.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.5.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Netz.-Prof.-Fehler**

Name

Name des Netz-Profils.

SNMP-ID:

1.73.2.5.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Netz.-Prof.-Fehler**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.20.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Netz.-Prof.-Fehler**

AP-Konf.-Fehler

Diese Tabelle enthält die Meldungen zu Konfigurationsfehlern, die in der Access-Point-Tabelle unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen** aufgetreten sind.

SNMP-ID:

1.73.2.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.8.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

Name

Names des APs, für den die Fehlermeldung gilt.

SNMP-ID:

1.73.2.8.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.8.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

Profil

Name des WLAN-Profils, unter dem der Fehler aufgetreten ist.

SNMP-ID:

1.73.2.8.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

MAC-Adresse

MAC-Adresse des betreffenden APs.

SNMP-ID:

1.73.2.8.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

Gruppe

Name der Zuweisungs-Gruppe, unter welcher der Fehler aufgetreten ist.

SNMP-ID:

1.73.2.8.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Konf.-Fehler**

AP-Intranet-Errors

Diese Tabelle enthält die Fehlermeldungen, die beim Zuweisen von IP-Parameter-Profilen aufgetreten sind.

SNMP-ID:

1.73.2.10

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.10

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranet-Errors**

Name

Name des IP-Parameter-Profils.

SNMP-ID:

1.73.2.10.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranet-Errors**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.10.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranet-Errors**

Konfig-Zuweisungs-Gruppen

Diese Tabelle zeigt die Zuweisungs-Gruppen, die der WLC an die einzelnen Access Points übermittelt hat.

SNMP-ID:

1.73.2.19

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Name

Name der Zuweisungs-Gruppe.

SNMP-ID:

1.73.2.19.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Profil

Name des WLAN-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zugewiesen hat.

SNMP-ID:

1.73.2.19.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

AP-Intranet

Name des IP-Parameter-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zugewiesen hat.

SNMP-ID:

1.73.2.19.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

IPv4-Referenz-Pool-Start

Anfang des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

SNMP-ID:

1.73.2.19.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

IPv4-Referenz-Pool-Ende

Ende des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

SNMP-ID:

1.73.2.19.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Gruppen-Konfig-Fehler

Diese Tabelle enthält die Meldungen zu Konfigurationsfehlern, die innerhalb der definierten Zuweisungs-Gruppen unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen** aufgetreten sind.

SNMP-ID:

1.73.2.20

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Indexnummer für den Tabelleneintrag.

SNMP-ID:

1.73.2.20.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Gruppen-Konfig-Fehler**

Gruppe

Name der Zuweisungs-Gruppe.

SNMP-ID:

1.73.2.20.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Gruppen-Konfig-Fehler**

Fehler

Inhalt der Fehlermeldung.

SNMP-ID:

1.73.2.20.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Gruppen-Konfig-Fehler**

Tag-Gruppen

Diese Tabelle zeigt die Tag-Gruppen, die der WLC an die einzelnen Access Points übermittelt hat.

SNMP-ID:

1.73.2.21

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Name

Name der Tag-Gruppe.

SNMP-ID:

1.73.2.21.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Tag-Gruppen**

8.2.4 Ergänzungen im Setup-Menü

Gruppen

Über diesen Parameter ordnen Sie dem betreffenden AP-Profil optional eine oder mehrere Tag-Gruppen zu. Sofern Sie ein AP-Profil bearbeiten, kann dieser Parameter darüber hinaus auch jene Zuweisungs-Gruppen enthalten, die der WLC

dem betreffenden AP im Rahmen der IP-abhängigen Autokonfiguration zugewiesen hat. Weiterführende Informationen hierzu erhalten Sie im Referenzhandbuch.

Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.

SNMP-ID:

2.37.1.4.24

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**. Mehrere Einträge trennen Sie durch eine kommaseparierte Liste.

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Tag-Gruppen**. Mehrere Einträge trennen Sie durch eine kommaseparierte Liste.

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

Default-Wert:

leer

IPv4-konfig-Pool-Start

Anfang des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der Access-Point-Tabelle keine konkrete IP-Adresse definiert haben.

SNMP-ID:

2.37.1.9.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranets**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

IPv4-konfig-Pool-Ende

Ende des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der Access-Point-Tabelle keine konkrete IP-Adresse definiert haben.

SNMP-ID:

2.37.1.9.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranets**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

Konfig-Zuweisungs-Gruppen

Diese Tabelle enthält die Zuweisungs-Gruppen, anhand derer der WLC hinzukommenden APs automatisch eine Netzkonfiguration, ein WLAN-Profil und ein Client-Steering-Profil zuweist. Dazu definieren Sie für die einzelnen Zuweisungs-Gruppen je einen IP-Adressbereich, in dem die betreffende Gruppe greift. Auf diese Weise haben Sie z. B. in einem zentral gemanagten WLAN die Möglichkeit, anhand des Adressbereiches hinzukommenden APs automatisch eine standortspezifische Konfiguration (z. B. Filiale-A, Filiale-B, etc.) zuzuweisen.

Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt LCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

Achten Sie darauf, dass in der Access-Point-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

SNMP-ID:

2.37.1.18

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Name

Name der Zuweisungs-Gruppe, auf die Sie aus anderen Tabellen referenzieren.

SNMP-ID:

2.37.1.18.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

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

Default-Wert:

leer

Profil

Name des WLAN-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zuweist.

SNMP-ID:

2.37.1.18.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

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

Default-Wert:

leer

AP-Intranet

Name des IP-Parameter-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zuweist.

SNMP-ID:

2.37.1.18.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranets**

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

Besondere Werte:

DHCP

Der AP bezieht seine Netzkonfiguration über DHCP.

Default-Wert:

leer

IPv4-Referenz-Pool-Start

Anfang des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

SNMP-ID:

2.37.1.18.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

IPv4-Referenz-Pool-Ende

Ende des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

SNMP-ID:

2.37.1.18.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

Client-Steering-Profil

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

SNMP-ID:

2.37.1.18.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **Client-Steering** > **Profile**

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

Default-Wert:

leer

Tag-Gruppen

Diese Tabelle enthält die Tag-Gruppen, die der WLC automatisch den einem WLAN-Profil angehörigen APs zuweist. Anhand von Tag-Gruppen haben Sie die Möglichkeit, z. B. Aktionen, die Sie auf dem WLC ausführen, auf eine bestimmte Auswahl von APs zu beschränken.

SNMP-ID:

2.37.1.20

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Name

Über diesen Parameter definieren Sie den Namen des anzulegenden des Tags.

SNMP-ID:

2.37.1.20.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Tag-Gruppen**

Mögliche Werte:

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

Default-Wert:

leer

8.2.5 Ergänzungen der Kommandozeilenbefehle

Übersicht der capwap-Parameter im show-Befehl

Über die Kommandozeile lassen sich folgende Informationen zum CAPWAP-Dienst aufrufen:

Tabelle 3: Übersicht aller capwap-Parameter im show-Befehl

Parameter	Bedeutung
-addresses [<IfcNum>]	Zeigt die Adresstabellen eines einzelnen oder aller WLC-Tunnel. Im Falle eines einzelnen WLC-Tunnels geben Sie für `<IfcNum>` die Nummer der logischen WLC-Tunnel-Schnittstelle an, z. B. `10`.
-groups	Zeigt Informationen zu einzelnen oder allen vorhandenen Zuweisungs-/Tag-Gruppen.

Den Befehl `show capwap groups` erweitern Sie um die nachfolgend gelisteten Parameter, wodurch sich der Umfang der angezeigten Informationen regulieren lässt:

Tabelle 4: Übersicht aller 'capwap group'-Parameter im show-Befehl

Parameter	Bedeutung
all	Zeigt die im Setup-Menü konfigurierten Namen und die geräteinternen Namen sämtlicher eingerichteten Zuweisungs-/Tag-Gruppen sowie der Default-Gruppe. Die Default-Gruppe stellt eine interne Gruppe dar, die sämtliche APs enthält.
<group1> <group2> <…>	Zeigt alle APs der betreffenden Zuweisungs-/Tag-Gruppen.
-l <location>	Zeigt alle APs des betreffenden Standorts.
-c <country>	Zeigt alle APs des betreffenden Landes.
-i <city>	Zeigt alle APs der betreffenden Stadt.
-s <street>	Zeigt alle APs des betreffenden Straßen.
-b <building>	Zeigt alle APs des betreffenden Gebäudes.
-f <floor>	Zeigt alle APs der betreffenden Etage.
-r <room>	Zeigt alle APs der betreffenden Raumbezeichnung.
-d <device>	Zeigt alle APs, die den angegebenen Gerätenamen tragen.
-a <antenne>	Zeigt alle APs, welche die angegebene Antennennummer besitzen.
-v <firmware>	Zeigt alle APs, welche die angegebene Firmware besitzen. Geben Sie dazu für `<firmware>` die Versionsnummer gefolgt von der Build-Nummer an, z. B. `9.00.0001`.
-x <firmware>	Zeigt alle APs, deren Firmware-Version kleiner ist als die auf dem aktuellen Gerät installierte.
-y <firmware>	Zeigt alle APs, deren Firmware-Version gleich groß oder kleiner ist als die auf dem aktuellen Gerät installierte.
-z <firmware>	Zeigt alle APs, deren Firmware-Version größer ist als die auf dem aktuellen Gerät installierte.
-t <firmware>	Zeigt alle APs, deren Firmware-Version gleich groß oder größer ist als die auf dem aktuellen Gerät installierte.
-n <intranet>	Zeigt alle APs, deren IP zur angegebenen Intranet-Adresse gehört.
-p <profile>	Zeigt alle APs, denen das angegebene WLAN-Profil zugeordnet ist.
rmgrp <group1 intern_name> <group2 intern_name> …	Löscht die Gruppe(n) mit dem angegebenen internen Namen aus dem Arbeitsspeicher des Gerätes. Nutzen Sie diesen Befehl, um die Arbeitsspeicher freizugeben, falls eine zu hohe Zahl von Gruppen die Perfomanz des Gerätes verschlechtert. Der Eintrag im Setup-Menü bleibt von dieser Aktion unberührt.
resetgrps	Löscht alle Gruppen bis auf die Default-Gruppe.

Für die Standort-Informationen wertet das Gerät die in der Access-Point-Tabelle unter **Standort** eingetragenen Informationen aus. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

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

Der Standort-Eintrag `co=Deutschland,ci=Aachen` z. B. ermöglicht Ihnen, über den Befehl `+show capwap group -i Aachen` an der Konsole alle vom WLC verwalteten APs in Aachen aufzulisten.

Weitere Befehls-Beispiele

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

8.3 Automatische Wahl des 2,4/5-GHz-Modus

Ab LCOS 9.00 haben Sie sowohl auf einem WLC als auch einem AP die Möglichkeit, in der Konfiguration der physikalischen WLAN-Parameter die Wahl eines geeigneten 2,4/5-GHz-Modus dem AP zu überlassen.

- 2,4-GHz-Modus / 5-GHz-Modus

  Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN.Client unterstützt.

  Sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband existieren inzwischen unterschiedliche Funk-Standards, nach denen ein AP senden kann. Im 2,4-GHz-Frequenzband umfasst dies bislang die Standards IEEE 802.11b, IEEE 802.11g und IEEE 802.11n; im 5-GHz-Frequenzband die Standards IEEE 802.11a, IEEE 802.11n und IEEE 802.11ac. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

  Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

  Sofern sich in Ihrem WLAN z. B. ausschließlich 802.11n-fähige WLAN-Clients befinden, empfiehlt sich die Wahl des Greenfield-Modus (**Nur 802.11n**): Hierdurch unterbinden Sie die Anmeldung langsamerer Clients, welche das Netz andernfalls ausbremsen würden.

  Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere WLAN-Clients nicht auszuschließen, empfiehlt sich die Wahl eines Kompatibilitätsmodus (bei 2,4 GHz z. B. **802.11g/b/n (gemischt)**; bei 5 GHz **802.11a/n (gemischt)**). Im Kompatibilitätsmodus arbeitet eine physikalische WLAN-Schnittstelle grundsätzlich nach dem schnellsten Standard, fällt aber auf einen langsameren Standard zurück, wenn sich ein entsprechender WLAN-Client im Netz anmeldet. Im Rahmen von 802.11b können Sie dabei auswählen, ob die physikalische WLAN-Schnittstelle ausschließlich den 11-MBit-Modus oder auch den älteren 2-MBit-Modus unterstützten soll (**… (2Mbit-kompatibel)**).

  Bei APs nach dem 802.11g-Standard haben Sie darüber hinaus die Möglichkeit, die Übertragungsgeschwindigkeit auf bis zu 108MBit/s zu steigern. Im sogenannten Turbo-Modus nutzt ein AP gleichzeitig zwei benachbarte freie Kanäle für die Funkübertragung. Wenn Sie einen AP in den 108Mbit/s-Turbo-Modus schalten, können ausschließlich noch diejenigen WLAN-Clients eine Verbindung zu dem AP aufbauen, welche ebenfalls im Turbo-Modus betrieben werden.

  Der Turbo-Modus wird dem 802.11g-Standard zugeordnet, entspricht jedoch keinem offiziellen IEEE-Standard. Die Technik repräsentiert eigene Erweiterungen unterschiedlicher Chipsatz-Hersteller, die diese Technik auch unter der Bezeichnung „802.11g+" oder „802.11g++" vermarkten. Der Turbo-Modus ist daher ausschließlich auf APs mit reiner 802.11g-Hardware verfügbar.

  Sofern Sie über die Einstellung **Automatisch** die Wahl des 2,4-/5-GHz-Modus dem Gerät überlassen, ist die Wahl des besten Modus vom verwendeten Frequenzband und den Fähigkeiten der Geräte-Hardware abhängig:

- Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **802.11g/b/n (gemischt)** oder zu **802.11g/b (gemischt)**.
- Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **802.11a/n/ac (gemischt)**, **802.11a/n (gemischt)** oder **54Mbit/s-Modus**.

APs nach 802.11n sind im 2,4-GHz-Frequenzband prinzipiell abwärtskompatibel zu den vorhergehenden Standards IEEE 802.11b und IEEE 802.11g. Für im 802.11b- oder 802.11g-Modus betriebene 802.11n-Hardware sind lediglich die 802.11n-spezifischen Funktionen nicht verfügbar. Im 5-GHz-Frequenzband hingegen besteht diese Abwärtskompatibilität nicht: Die betreffenden 802.11n-Geräte müssen 802.11a explizit unterstützen.

8.3.1 Ergänzungen im Status-Menü

2.4GHz-Modus

Dieser Status-Wert zeigt an, in welchem 2,4-GHz-Modus die gemanagten APs das WLAN-Modul betreiben.

SNMP-ID:

1.73.2.2.6

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

11bg-gemischt
802.11g/b (gemischt)

nur-11b
Nur 802.11b (11Mbit)

nur-11g
Nur 802.11g (54Mbit)

108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)

11bgn-gemischt
802.11g/b/n

11gn-gemischt
802.11g/n

Greenfield
Nur 802.11n (Greenfield-Modus)

Auto
Automatisch

5GHz-Modus

Dieser Status-Wert zeigt an, in welchem 5-GHz-Modus die gemanagten APs das WLAN-Modul betreiben.

SNMP-ID:

1.73.2.2.7

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

normal
802.11g (54Mbit/s-Modus)
108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)
11an-gemischt
802.11a/n (gemischt)
Greenfield
Nur 802.11n (Greenfield-Modus)
11anac-gemischt
802.11a/n/ac (gemischt)
11nac-gemischt
802.11n/ac (gemischt)
nur-11ac
Nur 802.11ac
Auto
Automatisch

8.3.2 Ergänzungen im Setup-Menü

2.4GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN.Client im 2,4-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

SNMP-ID:

2.37.1.2.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

11bg-gemischt
802.11g/b (gemischt)
nur-11b
Nur 802.11b (11Mbit)
nur-11g
Nur 802.11g (54Mbit)

108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)
11bgn-gemischt
802.11g/b/n
11gn-gemischt
802.11g/n
Greenfield
Nur 802.11n (Greenfield-Modus)
Auto
Automatisch. Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **11bgn-gemischt** oder zu **11bg-gemischt**.

Default-Wert:

Auto

5GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN.Client im 5-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

SNMP-ID:
2.37.1.2.7

Pfad Telnet:
Setup > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

Mögliche Werte:

normal
802.11g (54Mbit/s-Modus)
108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)
11an-gemischt
802.11a/n (gemischt)
Greenfield
Nur 802.11n (Greenfield-Modus)
11anac-gemischt
802.11a/n/ac (gemischt)
11nac-gemischt
802.11n/ac (gemischt)

nur-11ac

Nur 802.11ac

Auto

Automatisch. Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **11anac-gemischt**, **11an-gemischt** oder **normal**.

Default-Wert:

Auto

8.4 WLC-Cluster

Sofern Sie in Ihrem Netz mehrere WLCs einsetzen, haben Sie die Möglichkeit, diese Geräte zu einem geschlossenen Verbund (Cluster) zusammenfassen. Die APs eines gemanagten WLANs werden dann nicht mehr von einem einzigen, zentralen WLC verwaltetet, sondern von mehreren miteinander synchronisierten WLCs. Ein solcher WLC-Cluster bietet Ihnen vor allem in größeren Netzen diverse Vorteile:

- Automatische Verteilung der Netzlast zwischen den einzelnen APs und WLCs („Load-Balancing").
- Erhöhte Ausfallsicherheit durch die Bereitstellung von Backup-WLCs („Hot Standby") und automatische Neuverteilung der APs im Falle eines WLC-Ausfalls.
- Aufbau einer Zertifikatshierarchie: Verwaltung der Zertifikate durch eine zentrale Zertifizierungsstelle (CA), dargestellt wahlweise durch einen Master-WLC oder eine externe Stelle (z. B. einen Server).

In LCOS-Versionen vor 9.00 erlaubt die Cluster-Funktionalität ausschließlich ein statisch konfiguriertes Load-Balancing. Ab LCOS 9.00 erhält die Funktion oben angeführten Verbesserungen, die im Folgenden näher beschrieben sind.

8.4.1 CAPWAP im WLC gezielt (de)aktivieren

Ab LCOS 9.00 haben Sie auf einem WLC die Möglichkeit, den CAPWAP-Dienst gezielt zu (de)aktivieren.

Um mehrere WLAN-Controller in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile (wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen Controller spiegeln lässt.

Ergänzungen im Setup-Menü

Capwap-Aktiv

Aktiviert oder deaktiviert den CAPWAP-Dienst auf Ihrem Gerät.

Um mehrere WLAN-Controller in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile (wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen Controller spiegeln lässt.

SNMP-ID:

2.37.36

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

nein
ja

Default-Wert:

ja

8.4.2 WLC-Tunnel für die interne Kommunikation

Der Einsatz von WLC-Tunneln ist ein essentieller Bestandteil eines WLC-Clusters. Die am WLC-Cluster beteiligten WLCs nutzen diese Tunnel zur Kommunikation untereinander. Im Rahmen der Funktionserweiterungen ab LCOS 9.00 verbessert sich daher auch der LCOS-interne Umgang mit WLC-Tunneln:

- Aufgebaute WLC-Tunnel bleiben auch beim Zurückschreiben einer Konfiguration bestehen.
- Statisch konfigurierte WLC-Tunnel sind generell robuster. Im Falle eines Verbindungsabbruchs versucht das Gerät, den betreffenden automatisch wieder aufzubauen.
- Ein WLC trennt einen WLC-Tunnel erst nach Ablauf eines Timeouts.
- WLC-Tunnel lassen sich global ein- oder ausschalten.

Die Einstellungen für die WLC-Tunnel und die weiteren WLCs (Remote-WLCs) nehmen Sie in LANconfig im Abschnitt **WLAN-Controller** > **Allgemein** > **WLC-Cluster** vor. Über die Einstellung **WLC-Tunnel aktiv** deaktivieren Sie den Einsatz von WLC-Tunneln, was de facto ein Abschalten der Clustering-Funktion bewirkt.

Ergänzungen im Setup-Menü

WLC-Cluster

Dieses Menü enthält die Einstellungen für die Datenverbindungen und Statusverbindungen zwischen mehreren WLCs (WLC-Cluster).

SNMP-ID:

2.37.34

Pfad Telnet:

Setup > **WLAN-Management**

WLC-Tunnel-aktiv

Über diesen Parameter aktivieren oder deaktivieren Sie die für das WLC-Clustering verwendeten WLC-Tunnel. Der Vorgang schaltet damit indirekt auch die Cluster-Funktionalität für den betreffenden WLC ein oder aus.

SNMP-ID:

2.37.34.6

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Werte:

nein
WLC-Cluster-Tunnel sind auf dem Gerät deaktiviert.

ja
WLC-Cluster-Tunnel sind auf dem Gerät aktiviert.

Default-Wert:

nein

WLC-Discovery

Über diese Tabelle schalten Sie für einzelne IPv4-Netze die automatische Suche nach WLCs, die sich im selben lokalen Netz befinden, ein oder aus.

Die Adressen der WLCs, die nicht im lokalen Netz stehen (Remote-WLCs), tragen Sie in der statischen WLC-Liste fest ein (SNMP-ID *2.37.34.3*). Die automatische Suche findet keine Remote-WLCs.

SNMP-ID:

2.37.34.4

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Netz

Geben Sie den Namen des IPv4-Netzes an, in dem der WLC automatisch nach Remote-WLCs sucht.

SNMP-ID:

2.37.34.4.1

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

Netzname aus **Setup** > **TCP-IP** > **Netzliste**

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

Default-Wert:

leer

Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie für das gewählte Netz die automatische Suche nach Remote-WLCs.

Die automatische Suche nach Remote-WLCs ist eine Möglichkeit für den Aufbau des Daten-Tunnels zwischen zwei WLCs. Wenn Sie diese Option deaktivieren, kann der WLC über das betreffende Netz keinen Datenkanal zu einem anderen WLC automatisch aufbauen, auch wenn Sie die Nutzung der Daten-Tunnel generell aktiviert haben. Alternativ können Sie die gewünschten Gegenstellen in der statischen WLC-Liste definieren.

SNMP-ID:

2.37.34.4.2

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

ja
nein

Default-Wert:

nein

Port

Definieren Sie den Port, über den die automatische Suche nach Remote-WLCs stattfindet.

SNMP-ID:

2.37.34.4.3

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Das Gerät verwendet Default-Port 1027.

Default-Wert:

0

WLC-Daten-Tunnel-aktiviert

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von Daten-Tunneln (L3-Tunneln) zwischen mehreren WLCs. Dies erlaubt Ihnen, ein L3-Overlay-Netz über die Remote-WLCs auszudehnen.

Achten Sie darauf, die betreffenden WLC-Tunnel niemals zu bridgen, wenn sich die einzelnen WLCs in der selben Broadcastdomäne befinden. Andernfalls erzeugen Sie eine Schleife (Switching-Loop), die Ihr Netz in kürzester Zeit durch Überlastung lahmlegt.

SNMP-ID:

2.37.34.2

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Werte:

ja

Ihr WLC ist dazu in der Lage, die Verbindung zu Remote-WLCs auch als L3-Tunnel zu benutzen.

nein

Ihr WLC ist nicht dazu in der Lage, die Verbindung zu Remote-WLCs als L3-Tunnel zu benutzen.

Default-Wert:

nein

Statische WLC Liste

In dieser Tabelle hinterlegen Sie die statischen IPv4-Adressen der Remote-WLCs, zu denen Ihr WLC eine Verbindung aufbaut. Alternativ lässt sich die Tabelle auch dazu nutzen, um die von der **WLC-Discovery**-Tabelle praktizierte Suche im lokalen Netz zu umgehen.

Wenn Sie einen Remote-WLC über eine statische IPv4-Adresse an Ihren WLC anbinden, baut Ihr WLC zunächst einen Kontroll-Tunnel zu dieser Gegenstelle auf. Wenn Sie die Option für den Daten-Tunnel aktiviert haben, baut Ihr WLC anschließend automatisch einen Daten-Tunnel zu dieser Gegenstelle auf.

Die betreffenden WLCs können nur dann einen Daten-Tunnel zueinander aufbauen, wenn die Geräte über ein Zertifikat aus der gleichen Zertifikatshierarchie verfügen.

SNMP-ID:

2.37.34.3

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

IP-Adresse

Definieren Sie hier die IPv4-Adresse des Remote-WLCs, zu dem Ihr WLC einen Daten-Tunnel aufbaut.

SNMP-ID:

2.37.34.3.1

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische WLC Liste**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem Remote-WLC als Absender auftritt.

Standardmäßig verwendet Ihr Gerät seine Adresse aus dem jeweiligen ARF-Kontext, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der Ihr Gerät die Gegenstelle anspricht. Dies kann z. B. dann sinnvoll sein, falls Ihr Gerät über verschiedene Wege erreichbar ist und die Gegenstelle einen bestimmten Weg für ihre Antwort-Nachrichten wählen soll.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet!

SNMP-ID:

2.37.34.3.2

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische WLC Liste**

Mögliche Werte:

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

Besondere Werte:

Name des IP-Netzs (ARF-Netz), dessen Adresse eingesetzt werden soll
`INT` für die Adresse des ersten Intranets
`DMZ` für die Adresse der ersten DMZ

Wenn in der Liste der IP-Netze oder in der Liste der Loopback-Adressen eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen die zugehörige IP-Adresse!

`LB0`...`LBF` für eine der 16 Loopback-Adressen oder deren Name
Beliebige IPv4-Adresse

Default-Wert:

leer

Port

Definieren Sie den Port, über den Ihr WLC einen Daten-Tunnel zum Remote-WLC aufbaut.

SNMP-ID:

2.37.34.3.3

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische-WLC-Liste**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Das Gerät verwendet Default-Port 1027.

Default-Wert:

0

8.4.3 Ermittlung des idealen WLC

Die im LCOS implementierten Algorithmen ermöglichen die intelligente Verteilung von APs auf einzelne WLCs, um innerhalb von WLC-Clustern die Netzlast gleichmäßig auf alle Geräte aufzuteilen oder nach Ausfall eines Geräts einen alternativen WLC zu wählen. Hierzu sendet ein AP zunächst einen Discovery Request ins Netz, um sämtliche verfügbaren WLCs zu ermitteln. Die WLCs antworten ihrerseits mit einem Discovery Response, anhand dessen ein AP eine Liste von WLCs erstellt, die er anhand der folgenden Kritieren priorisiert:

- **Spezifität der AP-Konfiguration**: Ein AP wertet aus, ob ein WLC für den AP eine Konfiguration bereithält und ob diese ein spezifisches AP-Profil oder ein Default-Profil umfasst. Ein spezifisches AP-Profil priorisiert der AP am höchsten, gefolgt von einem Default-Profil. Ein fehlendes Profil erhält die niedrigste Priorität.
- **Höhe des Prioritätswerts**: Ein AP wertet aus, welchen Prioritätswert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

Sofern die Ermittlung des idealen WLC erstmalig erfolgt oder Sie dies manuell bewirken (siehe *Ideale AP-Verteilung manuell initiieren* auf Seite 237), priorisiert ein AP zusätzlich nach folgendem Kriterium:

- **Lizenzkontingent**: Bei der erstmaligen Ermittlung sorgt ein zufallsgesteuerter Algorithmus dafür, dass die APs die im Netz verfügbaren Lizenzkontingente möglichst gleichmäßig ausnutzen. Bei der manuell ausgelösten Ermittlung hingegen bildet jeder AP für jeden WLC einen gewichteten Wert aus der Zahl der verbundenen sowie der maximal möglichen APs. Hat ein WLC die maximal mögliche Anzahl von AP-Verbindungen erreicht (Lizenzkontingent erschöpft), berücksichtigt ein AP den betreffenden WLC nicht mehr für den aktuellen Auswahlprozess.

Ein AP wählt jenen WLC aus, der im Rahmen der o. g. Priorisierung in der Liste der WLCs schließlich an oberster Stelle steht.

Ergänzungen im Setup-Menü

Praeferenz

Über diesen Parameter geben Sie den Prioritätswert an, nach dem ein AP innerhalb von WLC-Clustern die Priorität eines WLC bestimmt. Der AP wertet aus, welchen Prioritätswert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

SNMP-ID:

2.37.37

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

0 … 255

Default-Wert:

0

8.4.4 Ermittlung der idealen AP-Verteilung

Die Ermittlung der idealen AP-Verteilung in einem WLC-Cluster und eine dadurch ggf. ausgelöste Umverteilung erfolgt grundsätzlich automatisch. Dazu durchläuft ein jeder AP in unregelmäßigen Abständen von 30 bis 60 Minuten den Prozess zur *Ermittlung des idealen WLC*. Gewinnt bei diesem Vorgang der WLC, zu dem bereits eine Verbindung besteht, erfolgt keine Umverteilung. Weist jedoch ein anderer WLC eine höhere Priorisierung auf, so versucht der AP, sich mit diesem WLC zu verbinden.

Sie haben aber auch als Administrator die Möglichkeit, via LANmonitor die Ermittlung der idealen AP-Verteilung und eine ggf. daraus resultierende Umverteilung der APs manuell auszulösen (siehe *Ideale AP-Verteilung manuell initiieren* auf Seite 237).

8.4.5 Ideale AP-Verteilung manuell initiieren

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Berechnung der idealen Verteilung manuell starten und dadurch ggf. eine Neuverteilung auslösen.

1. Starten Sie LANmonitor und wählen Sie einen WLC aus.
2. Wechseln Sie in den Menüzweig **Wireless LAN** > **Aktive APs**.
3. Öffnen Sie das Kontextmenü auf einem AP und wählen Sie den Eintrag **Starte WLC suche auf AP's**.

Der betreffende AP berechnet daraufhin für die sich die ideale Verteilung und assoziiert sich bei Bedarf mit einem besseren WLC.

Ergänzungen im Setup-Menü

WLC-Suche-auf-WTPs-anstossen

Über diese Aktion starten Sie auf sämtlichen gemanagten APs die Berechnung der idealen Verteilung der APs im WLC-Cluster. Das Ergebnis dieser Berechnung löst ggf. eine Neuverteilung der APs aus.

SNMP-ID:

2.37.34.5

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Argumente:

keine

8.4.6 Einrichten einer CA-Hierarchie

Um mehrere WLAN-Controller im Verbund zu betreiben (WLC-Cluster), müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies umfasst auch die innerhalb des WLC-Clusters eingesetzten Zertifikate. Die Lösung liegt in dem Aufbau einer Zertifikats- bzw. CA-Hierarchie: Hierbei definieren Sie die CA eines WLC als Root-CA, von welcher die übrigen WLCs das Zertifikat für ihre (Sub-)CA beziehen.

Das nachfolgende Szenario zeigt Ihnen, welche Konfigurationsschritte für den Aufbau einer CA-Hierarchie notwendig sind. Die Konfiguration erfolgt exemplarisch anhand zweier WLCs:

- WLC-MAIN stellt das Gerät mit der Root-CA dar;
- WLC-SUB stellt das Gerät dar, welches bei der Root-CA ein Zertifikat bezieht, um als Sub-CA weitere Zertifikate ausstellen zu können.

Konfiguration der Root-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Root-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Kommandozeile am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`
3. Wechsel Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **Ja**.

Damit haben Sie die Konfiguration der Root-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat.

Konfiguration der Sub-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Sub-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Kommandozeile am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Root-CA** auf **Nein**.
3. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE`
4. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Sub-CA** und tragen Sie für den Parameter **CADN** den Distinguished Name der Root-CA ein.

   Beispiel: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`
5. Tragen Sie für den Parameter **Challenge-Pwd** das Challenge-Passwort ein, das auf WLC-MAIN unter **Setup** > **Zertifikate** > **SCEP-CA** hinterlegt ist.
6. Hinterlegen im Parameter **CA-Url-Adresse** die URL zur Root-CA.
   Stellt ein anderer WLC mit LCOS-Betriebssystem die Root-CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist. Beispiel: `http://192.168.1.1/cgi/bin/pkiclient.exe`.
7. Optional: Spezifizieren Sie die **Ext-Key_Usage** und **Cert-Key-Usage**, um die Funktionen der Sub-CA einzuschränken. Weitere Informationen hierzu finden Sie in der Menüreferenz.
8. Setzten Sie den Parameter **Auto-generiert-Request** auf **ja**, um die Sub-CA zu aktivieren..
9. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **ja**, um den CA-Server mit SCEP zu aktivieren.

Damit haben Sie die Konfiguration der Sub-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat. Die Hierarchie der Zertifikate muss hierbei sichtbar sein: Als erstes zeigt der WLC das Zertifikat der Root-CA an, dann das Zertifikat der Sub-CA.

Ergänzungen im Setup-Menü

Root-CA

Über diesen Parameter legen Sie fest, ob die CA des betreffenden WLC die Root-CA darstellt oder nicht.

SNMP-ID:

2.39.2.11

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

nein
ja

Default-Wert:

ja

CA-Pfad-Laenge

Über diesen Parameter legen Sie fest, wie lang die Hierarchie der Sub-CAs unterhalb der Root-CA maximal sein darf (Länge der „Chain of Trust").

Ein Wert von `1` z. B. bewirkt, dass nur die Root-CA Zertifikate für Sub-CAs austellen kann. Die betreffenden Sub-CAs sind ihrerseits nicht mehr dazu in der Lage, an andere Sub-CAs Zertifikate auszustellen und die „Chain of Trust" auf diese Weise zu verlängern. Bei einem Wert von `0` hingegen ist auch die Root-CA nicht dazu in der Lage, Zertifikate für Sub-CAs auszustellen. In diesem Fall kann die Root-CA nur noch Endbenutzer-Zertifikate signieren.

SNMP-ID:

2.39.2.12

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

0 … 65535

Default-Wert:

1

Sub-CA

In diesem Menü nehmen Sie sämtliche Einstellungen vor, die für den Bezug eines Zertifikats für die Sub-CA notwendig sind.

SNMP-ID:

2.39.2.13

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Auto-generiert-Request

Über diesen Parameter legen Sie fest, ob der WLC den Request nach einem Zertifikat für die Sub-CA automatisch an die Root-CA stellt.

SNMP-ID:

2.39.2.13.1

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

nein
ja

Default-Wert:

nein

CADN

Geben Sie den Certificate Authority Distinguished Name (CADN) der übergeordneten CA (z. B. der Root-CA) an, von welcher der WLC das Zertifikat für die Sub-CA bezieht.

SNMP-ID:

2.39.2.13.2

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Challenge-Pwd

Geben Sie das Challenge-Passwort an, mit dem die Sub-CA das Zertifikat von der übergeordneten CA (z. B. der Root-CA) bezieht. Das Challenge-Passwort für die übergeordnete CA setzen Sie unter LCOS im Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate**.

SNMP-ID:

2.39.2.13.3

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Ext-Key_Usage

Definieren Sie weitere Verwendungs-Zwecke für die Schlüssel-Benutzung. Die erweiterte Schlüssel-Benutzung besteht aus einer kommaseparierten Liste von Verwendungs-Zwecken, für die der öffentliche Zertifikats-Schlüssel verwendbar ist.

Die Verwendungs-Zwecke können entweder deren Kurznamen oder die punktseparierte Form der OIDs sein. Obwohl jede beliebige OID verwendet werden kann, machen nur bestimmte Sinn (siehe unten). Speziell die folgenden PKIX-, NS- und MS-Werte sind von Bedeutung und können in jeder beliebigen Kombination aufgezählt werden:

Tabelle 5: Erweiterte Verwendungs-Zwecke: Bedeutsame Kurznamen

Wert	Bedeutung
serverAuth	SSL/TLS-Web-Server-Authentifizierung
clientAuth	SSL/TLS-Web-Client-Authentifizierung
codeSigning	Code-Signierung
emailProtection	E-Mail-Schutz (S/MIME)
timeStamping	Vertrauenswürdiges Zeitstempeln (Trusted Timestamping)
msCodeInd	Microsoft persönliche Code-Signierung (Authenticode)
msCodeCom	Microsoft kommerzielle Code-Signierung (Authenticode)
msCTLSign	Microsoft vertrauenswürdige Listen-Signierung (Trust List Signing)
msSGC	Microsoft Server-gestützte Verschlüsselung (Server Gated Crypto)
msEFS	Microsoft verschlüsseltes Dateisystem (Encrypted File System)
nsSGC	Netscape Server-gestützte Verschlüsselung (Server Gated Crypto)
critical	Ist diese Einschränkung gesetzt, muss die Schlüssel-Verwendungs-Erweiterung immer beachtet werden. Wenn die Erweiterung nicht unterstützt wird, wird das Zertifikat als nicht gültig abgelehnt.

Tabelle 6: Erweiterte Verwendungs-Zwecke: Sinnvolle OIDs für WLAN-Switching

Gerät	OID
WLAN-Controller	1.3.6.1.5.5.7.3.18
Verwalteter AP (Managed AP)	1.3.6.1.5.5.7.3.19

Beispieleingabe: `critical,clientAuth,1.3.6.1.5.5.7.3.19`

SNMP-ID:

2.39.2.13.4

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

Kommaseparierte Liste aus den o. g. Kurznamen und/oder OIDs. Max. 100 Zeichen aus
`#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Cert-Key-Usage

Geben Sie den Verwendungszweck der eingetragenen Zertifikate an (Schlüssel-Benutzung. Der WLC fragt die Zertifikate für die Sub-CA dann ausschließlich für den entsprechenden Verwendungszweck ab.

Tabelle 7: Verwendungs-Zwecke: Kurznamen

Wert	Bedeutung
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
encipherOnly	
decipherOnly	
critical	Ist diese Einschränkung gesetzt, muss die Schlüssel-Verwendungs-Erweiterung immer beachtet werden. Wenn die Erweiterung nicht unterstützt wird, wird das Zertifikat als nicht gültig abgelehnt.

Beispieleingabe: `digitalSignature, nonRepudiation`

SNMP-ID:

2.39.2.13.5

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

Kommaseparierte Liste aus den o. g. Kurznamen. Max. 100 Zeichen aus
`#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

CA-Url-Adresse

Geben Sie die URL an, unter der die Adresse der die übergeordnete CA zu finden ist. Stellt ein anderer WLC mit LCOS-Betriebssystem die CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist.

SNMP-ID:

2.39.2.13.8

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 256 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

http://127.0.0.1/cgi-bin/pkiclient.exe

Neustart

Diese Aktion bewirkt einen Neustart der Sub-CA. Führen Sie diese Aktion nach Konfigurationsänderungen an der Sub-CA durch.

SNMP-ID:

2.39.2.13.9

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Argumente:

keine

8.5 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im LCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem LCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das LCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des LCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch

mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA - One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B.erfolgt dies über die Auswahl **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA - One Click Backup**.

8.6 Automatischer Neustart verwalteter APs nach Firmware-Update

Ab LCOS 9.00 haben Sie unter dem WEBconfig-Menüpunkt **Extras** > **Firmware in verwalteten AP laden** die Möglichkeit, die APs nach dem manuellen Upload einer neuen Firmware automatisch neu zu starten.

8.6.1 Firmware in verwalteten AP laden

Dieser Menüpunkt nur auf WLAN-Controllern (WLCs) verfügbar.

Auf dieser Seite haben Sie die Möglichkeit, per Fernzugriff die Firmware auf einem vom WLC verwalteten AP manuell zu aktualisieren. Dies kann z. B. sinnvoll sein, um auf ausgewählten APs den Produktiveinsatz einer Firmware vorab zu testen. Wählen Sie dazu einen AP anhand seiner MAC-Adresse aus und wählen Sie die entsptechende Firmware-Datei. Klicken Sie anschließend auf **Starte Upload**, um die Firmware in den AP zu laden.

Beachten Sie, dass dieser Vorgang die Firmwareverwaltung in der AP-Tabelle für den ausgewählten AP deaktiviert. Dies verhindert, dass der WLC ggf. automatisch eine andere Firmware einspielt. Die Firmware-Verwaltung lässt sich im Setup-Menü unter **WLAN-Management** > **AP-Konfiguration** > **Verwalte-Firmware** jederzeit wieder aktivieren.

Damit der Access Points die geladene Firmware auch verwendet, müssen Sie anschließend einen Neustart des Gerätes durchführen. Durch Aktivieren der Einstellung **AP nach Aktualisierung der Firmware neustarten** veranlassen Sie einen automatischen Neustart, sobald der Firmware-Upload abgeschlossen ist.

8.7 Automatische Suche nach alternativen WLCs

Ab LCOS 9.00 versucht ein AP nicht mehr, sich bei einem Verbindungsabbruch mit dem zuletzt bekannten WLC neu zu verbinden. Stattdessen sucht der AP im Netz nach einem erreichbaren WLC, der den Kriterien für die *Ermittlung des idealen WLC* entspricht.

8.8 U-APSD per WLC konfigurierbar

Ab LCOS 9.00 haben Sie die Möglichkeit, den Stromsparmechanismus (U-)APSD für einzelne SSIDs auch über einen WLC zu konfigurieren.

8.8.1 Ergänzungen im Status-Menü

APSD

Zeigt an, ob der Stromsparmodus APSD für das betreffende logische WLAN-Netz aktiviert ist.

SNMP-ID:

1.73.2.1.42

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Netzprofile**

Mögliche Werte:

ja
nein

APSD

Zeigt an, ob der Stromsparmodus APSD für das betreffende logische WLAN-Netz aktiviert ist.

SNMP-ID:

1.53.103.42

Pfad Telnet:

Status > **WLAN-Management** > **Netzprofile**

Mögliche Werte:

ja
nein

8.8.2 Ergänzungen im Setup-Menü

APSD

Aktiviert den Stromsparmodus APSD für das betreffende logische WLAN-Netz.

Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

SNMP-ID:

2.37.1.1.42

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzprofile**

Mögliche Werte:

ja
nein

Default-Wert:

ja

8.9 Gruppenbezogene Funkfeldoptimierung

Die LANCOM WLAN-Controller ermöglichen eine Gruppierung von Access Points anhand von Standortinformationen, Geräteeigenschaften oder Netzgliederung. Auf Basis dieser Gruppenzugehörigkeit lässt sich auch eine Funkfeldoptimierung durchführen. Statt also entweder für alle oder nur für einen Access Point eine Funkfeldoptimierung durchzuführen, kann man z. B. alle Access Points innerhalb eines Gebäudetrakts, mit einer speziellen Bezeichnung oder mit einer bestimmten Firmware-Version adressieren.

Sowohl im WEBconfig wie auch im LANmonitor und über die Kommandozeile können Sie die entsprechende Gruppe über den Gruppen-Parameter ansprechen:

```
do /Setup/WLAN-Management/start optimization <Gruppe>
```

Die Access Points sind über folgende Optionen des Gruppen-Parameters filterbar:

`-g <Gruppenname>`

Access Points, die der Gruppe angehören. Mehrere Gruppennamen sind durch Komma getrennt möglich.

`-l <Standort>`

Access Points, deren Standort entsprechend festgelegt ist.

> Die Kombination von `-l` und einer der Standort-Optionen `-c` bis `-r` ist nicht sinnvoll.

`-c <Land>`

Access Points mit der entsprechenden Landesangabe.

`-i <Stadt>`

Access Points mit der entsprechenden Stadtangabe.

`-s <Straße>`

Access Points mit der entsprechenden Straßenangabe.

`-b <Gebäude>`

Access Points mit der entsprechenden Gebäudeangabe.

`-f <Etage>`

Access Points mit der entsprechenden Etagenangabe.

`-r <Raum>`

Access Points mit der entsprechenden Raumangabe.

`-d <Gerätename>`

Access Points mit den entsprechenden Gerätenamen.

`-a <Antennen>`

Access Points mit der entsprechenden Anzahl an Antennen.

> Eine Kombination aus den Optionen `-d` und `-a` ist nicht sinnvoll.

`-v <Firmware>`

Access Points, die genau diese Firmwareversion besitzen.

`-x <Firmware>`

Access Points, deren Firmwareversion niedriger als die angegebene Version ist.

`-y <Firmware>`

Access Points, deren Firmwareversion niedriger oder gleich der angegebenen Version ist.

`-z <Firmware>`

Access Points, der Firmwareversion höher als die angegebene Version ist.

`-t <Firmware>`

Access Points, deren Firmwareversion höher oder gleich der angegebenen Version ist.

Kombinationen sind möglich, um z. B. Access Points mit einer Firmwareversion zwischen zwei Versionsständen zu adressieren.

`-n <Intranet-Adresse>`

Access Points, die sich im Intranet mit der angegebenen Adresse befinden.

`-p <Profilname>`

Access Points, die sich im angegebenen WLAN-Profil befinden.

8.10 Neue APs über den WEBconfig Setup-Wizard hinzufügen

Ab LCOS 9.00 verfügen WLCs über einen überarbeiteten Setup-Wizard **Neue Access Points zu Profilen zuordnen**, der Ihnen das Hinzufügen neuer APs über WEBconfig erleichtert. Der neue Setup-Wizard erlaubt Ihnen, mit wenigen Mausklicks

- gezielt nach einem neuen AP zu suchen;
- ein oder mehrere neue APs gleichzeitig zu akzeptieren;
- einem neuen AP ein WLAN-Profil oder eine Kanalliste zuzuweisen;
- die Konfiguration eines bereits akzeptierten AP an einen neuen AP zu vererben;
- die Konfiguration eines akzeptierten fehlenden AP mit der eines neuen AP zu wechseln. Beim Wechseln einer Konfiguration erhält der neue AP die vollständige Konfiguration des akzeptierten fehlenden AP (mit Ausnahme der MAC-Adresse). Beim Einbinden des neuen AP löscht der WLC anschließend die Konfiguration des akzeptierten fehlenden AP.

Um einen neuen AP mit den getätigten Einstellungen zu akzeptieren, klicken Sie abschließend auf **AP-einbinden**.

Sofern ein Sie einen AP über Zuweisungs-Gruppen konfigurieren lassen, brauchen Sie für den betreffenden AP keine Einstellungen in diesem Setup-Wizard vornehmen. Der WLC weist dem AP automatisch beim Einbinden die Einstellungen aus den entsprechenden Gruppen zu.

8.10.1 Ergänzungen im Status-Menü

AP-einbinden

Über diese Aktion veranlassen Sie die Einbindung eines neuen APs. Je nach Firmware-Stand Ihres Gerätes akzeptiert die Aktion unterschiedliche Argumente. Die Angabe einer MAC-Adresse ist in jedem Fall erforderlich; die Angabe weiterer Argumente hingegen ist optional.

Syntax in Versionen vor LCOS 9.00

```
[-c] <WTP-MAC> [<Profile>] [<Name>] [<IP>] [<Netmask>] [<Gateway>]
```

Syntax in Versionen nach LCOS 9.00

```
<WTP-MAC> [<WTP-MAC-2> … <WTP-MAC-n> ] [-c] [-l <Location>] [-p <Profile>] [-i
<IP>]
[-n <Name>] [-m <Netmask>] [-g <Gateway>] [-1 <Wlan1Channels>] [-2 <Wlan2Channels>]
```

Sofern Sie mehrere MAC-Adressen definieren, ignoriert das Gerät die Argumente `[-i <IP>]` und `[-n <Name>]`.

SNMP-ID:

2.37.7

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Argumente:

-c

Der WLC generiert keinen Konfigurationseintrag für den AP.

-l <Location>

Der WLC ergänzt die AP-Konfiguration um den angegeben Standort.

Es wird empfohlen, die Ortsangaben als eindeutiges Feld-Werte-Paar im Gerät zu hinterlegen, um z. B. an der Konsole die Filterfunktion im LCOS nutzen zu können. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

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

-p <Profile>

Der WLC ergänzt die AP-Konfiguration um das angegebene WLAN-Profil.

-i <IP>

Der WLC ergänzt die AP-Konfiguration um die angegeben IPv4-Adresse.

-n <Name>

Der WLC ergänzt die AP-Konfiguration um die angegebene Gerätebezeichnung.

-m <Netmask>

Der WLC ergänzt die AP-Konfiguration um die angegeben Netzmaske.

-g <Gateway>

Der WLC ergänzt die AP-Konfiguration um die angegeben Gateway-Adresse (IPv4).

-1 <Wlan1Channels>

Der WLC ergänzt die AP-Konfiguration um die 1. Kanalliste.

-2 <Wlan2Channels>

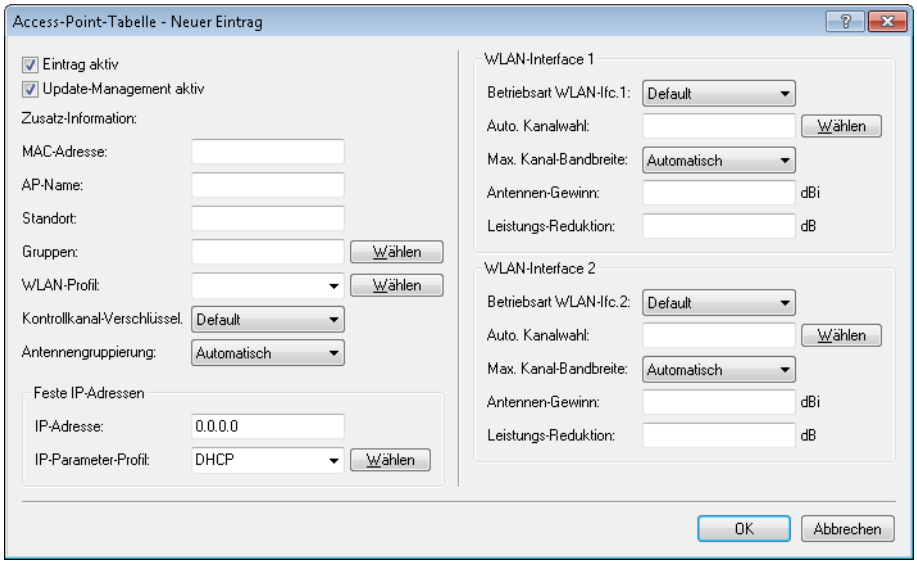
Der WLC ergänzt die AP-Konfiguration um die 2. Kanalliste.

8.11 Maximale Kanalbandbreite je WLAN-Modul einstellbar

Ab LCOS 9.00 lässt sich die maximale Kanal-Bandbreite je WLAN-Modul festlegen.

Die Möglichkeit, eine 40MHz-Kanalbündelung fest vorzugeben, besteht nicht mehr.

Änderungen auf WLCs



Max. Kanal-Bandbreite

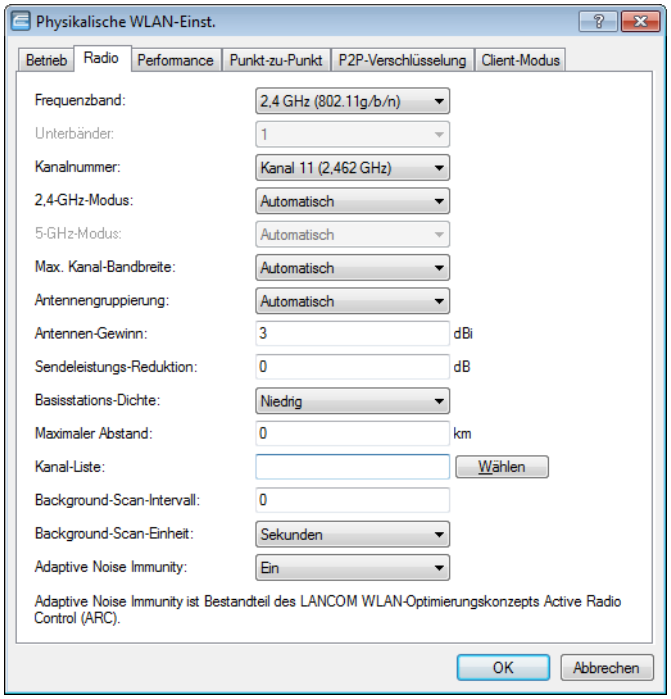
Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Folgende Werte sind möglich:

- **Automatisch**: Der Access Point ermittelt automatisch die maximale Kanal-Bandbreite (Default).
- **20MHz**: Der Access Point benutzt auf 20MHz gebündelte Kanäle.
- **40MHz**: Der Access Point benutzt auf 40MHz gebündelte Kanäle.
- **80MHz**: Der Access Point benutzt auf 80MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Änderungen auf Standalone-APs



8.11.1 Ergänzungen im Status-Menü

Kanal-Bandbreiten

Zeigt an, welche Kanalbreiten der betreffende WLAN-Client unterstützt.

SNMP-ID:

1.3.32.66

Pfad Telnet:

Status > WLAN > Stationstabelle

Mögliche Werte:

20MHz
Auf 20MHz gebündelte Kanäle.

40MHz
Auf 40MHz gebündelte Kanäle.

80MHz
Auf 80MHz gebündelte Kanäle.

160MHz
Auf 160MHz gebündelte Kanäle.

80+80MHz
160MHz Kanalbreite mit zwei disjunkten 80MHz-Kanälen (nur 802.11ac-Geräte).

T-40MHz
Auf 40MHz gebündelte Kanäle im 108Mbit-Turbo-Modus (nur reine 802.11g-Geräte)

Kanal-Bandbreiten

Zeigt an, welche Kanalbreiten die betreffende Gegenstelle unterstützt.

SNMP-ID:

1.3.34.44

Pfad Telnet:

Status > **WLAN** > **Scan-Resultate**

Mögliche Werte:

20MHz
Auf 20MHz gebündelte Kanäle.

40MHz
Auf 40MHz gebündelte Kanäle.

80MHz
Auf 80MHz gebündelte Kanäle.

160MHz
Auf 160MHz gebündelte Kanäle.

80+80MHz
160MHz Kanalbreite mit zwei disjunkten 80MHz-Kanälen (nur 802.11ac-Geräte).

T-40MHz
Auf 40MHz gebündelte Kanäle im 108Mbit-Turbo-Modus (nur reine 802.11g-Geräte)

Kanal-Bandbreite

Zeigt an, welche Kanalbreite die betreffende Gegenstelle aktuell verwendet.

SNMP-ID:

1.3.34.45

Pfad Telnet:

Status > **WLAN** > **Scan-Resultate**

Mögliche Werte:

20MHz
Auf 20MHz gebündelte Kanäle.

40MHz
Auf 40MHz gebündelte Kanäle.

80MHz
Auf 80MHz gebündelte Kanäle.

160MHz
Auf 160MHz gebündelte Kanäle.

80+80MHz
160MHz Kanalbreite mit zwei disjunkten 80MHz-Kanälen (nur 802.11ac-Geräte).

T-40MHz
Auf 40MHz gebündelte Kanäle im 108Mbit-Turbo-Modus (nur reine 802.11g-Geräte)

Kanal-Bandbreiten

Zeigt an, welche die Kanalbreiten der AP für die P2P-Verbindung unterstützt.

SNMP-ID:
1.3.36.1.46

Pfad Telnet:
Status > **WLAN** > **Interpoints** > **Accesspoint-Liste**

Mögliche Werte:

20MHz
Auf 20MHz gebündelte Kanäle.
40MHz
Auf 40MHz gebündelte Kanäle.
80MHz
Auf 80MHz gebündelte Kanäle.
160MHz
Auf 160MHz gebündelte Kanäle.
80+80MHz
160MHz Kanalbreite mit zwei disjunkten 80MHz-Kanälen (nur 802.11ac-Geräte).
T-40MHz
Auf 40MHz gebündelte Kanäle im 108Mbit-Turbo-Modus (nur reine 802.11g-Geräte)

8.11.2 Ergänzungen im Setup-Menü

Max.-Kanal-Bandbreite

Geben Sie den maximalen Frequenzbereich an, in dem die physikalische WLAN-Schnittstelle die zu übertragenen Daten auf die Trägersignale aufmoduliert (Kanal-Bandbreite).

In der Einstellung **Auto** stellt der AP die Kanal-Bandbreite optimal ein. Sie haben aber auch die Möglichkeit, die Automatik abzuschalten, um die Kanal-Bandbreite bewusst zu begrenzen. Die verfügbaren möglichen Werte sind abhängig von den unterstützten WLAN-Standards des Geräts.

SNMP-ID:
2.23.20.8.24

Pfad Telnet:
Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

Auto
Der AP stellt die Kanal-Bandbreite optimal ein. Dabei lässt der AP die maximal verfügbare Bandbreite zu, sofern die momentanen Betriebsbedingungen dies erlauben. Andernfalls begrenzt der AP die Kanal-Bandbreite auf 20MHz.

20MHz
40MHz
80MHz

Default-Wert:

Auto

Modul-2-Max.-Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 2. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

SNMP-ID:

2.37.1.4.25

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

Automatisch
Der AP erkennt automatisch die maximale Kanal-Bandbreite.

20MHz
Der AP benutzt auf 20MHz gebündelte Kanäle.

40MHz
Der AP benutzt auf 40MHz gebündelte Kanäle.

80MHz
Der AP benutzt auf 80MHz gebündelte Kanäle.

Default-Wert:

Automatisch

Modul-1-Max.-Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 1. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

SNMP-ID:

2.37.1.4.26

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

Automatisch

Der AP erkennt automatisch die maximale Kanal-Bandbreite.

20MHz

Der AP benutzt auf 20MHz gebündelte Kanäle.

40MHz

Der AP benutzt auf 40MHz gebündelte Kanäle.

80MHz

Der AP benutzt auf 80MHz gebündelte Kanäle.

Default-Wert:

Automatisch

8.12 Client-Steering über den WLC

Das Client-Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLAN-Controller definiert. Die verwalteten Access Point melden ständig die aktuellen Werte an den WLAN-Controller, der aufgrund der Kriterien entscheidet, welche Access Points die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client-Steering auch nur mit Access Points möglich, die ein WLAN-Controller zentral verwaltet.

In gemanagten Netzen zentralisiert ein WLC das Client-Steering aller angeschlossenen APs. Das Client-Steering läuft in diesem Fall wie folgt ab:

1. Der WLC sammelt die Daten über die angemeldeten WLAN-Clients von den angeschlossenen APs. Aus diesen Daten erstellt der WLC die Bewertung für das Client-Steering.
2. Alle APs sind so konfiguriert, dass das Client-Steering über den WLC erfolgt.
3. Ein hinzukommender WLAN-Client sendet einen Probe-Request an die APs in seiner Reichweite.
4. Die APs übermitteln diese Anfrage zusammen mit der Signalstärke des WLAN-Clients via CAPWAP an den WLC.
5. Der WLC berechnet für jeden AP im Bereich des WLAN-Clients einen Wert, der sich aus drei Bestandteilen zusammensetzt:

- Signalstärke-Wert
- Wert aus der Anzahl der am AP angemeldeten Clients
- Frequenzband-Wert

Zusammen mit der jeweiligen Gewichtung, mit der der WLC jeden einzelnen Wert multipliziert, ergibt sich der endgültige Wert.

6. Der WLC sendet den APs mit dem höchsten oder einem maximal um ein Toleranz-Level davon abweichenden Wert die Nachricht, dass dieser den WLAN-Client beim nächsten Anmeldeversuch annehmen darf.
7. Versucht der WLAN-Client, sich noch vor der Antwort des WLC mit einem AP zu verbinden, weist ihn dieser zurück, solange die Antwort vom WLC aussteht.
8. Versucht ein WLAN-Client nicht, sich trotz einer bestehenden Verbindung mit niedriger Qualität an einem anderen AP mit höherer Verbindungsqualität zu verbinden ("Sticky Client"), kann der WLC den aktuellen AP dazu veranlassen, den WLAN-Client abzumelden. Der WLAN-Client ist daraufhin gezwungen, sich mit dem AP zu verbinden, der die bessere Verbindung anbietet.

Wenn ein AP die Verbindung zu dem WLC verliert, der für das Client-Steering verantwortlich ist, lässt der AP alle Verbindungen von berechtigten WLAN-Clients zu.

8.12.1 Konfiguration

Mit LANconfig konfigurieren Sie das Client-Steering wie folgt:

1. Aktivieren Sie zunächst im WLC das Client-Steering für einen AP unter **WLAN-Controller** > **Profile** in der Ansicht **Physikalische WLAN-Parameter**.

Client-Steering

Folgende Werte sind möglich:

- **Aus**: Das Client-Steering ist deaktiviert.
- **AP-basiertes Band-Steering**: Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.
- **Ein**: Der AP lässt das Client-Steering vom WLC durchführen (Default).

2. Erstellen Sie nun unter **WLAN-Controller** > **AP-Konfiguration** ein Client-Steering-Profil.

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

Die Einträge haben folgende Bedeutung:

Name

Bezeichnung des Profils

Toleranzschwelle

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

Bevorzugt. Frequenzband

Gibt das Frequenzband vor, auf welches der WLC den AP leitet. Mögliche Werte sind:

- **2,4GHz**: Der WLC leitet den AP auf das Frequenzband 2,4GHz.
- **5GHz**: Das WLC leitet den AP auf das Frequenzband 5GHz.

Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

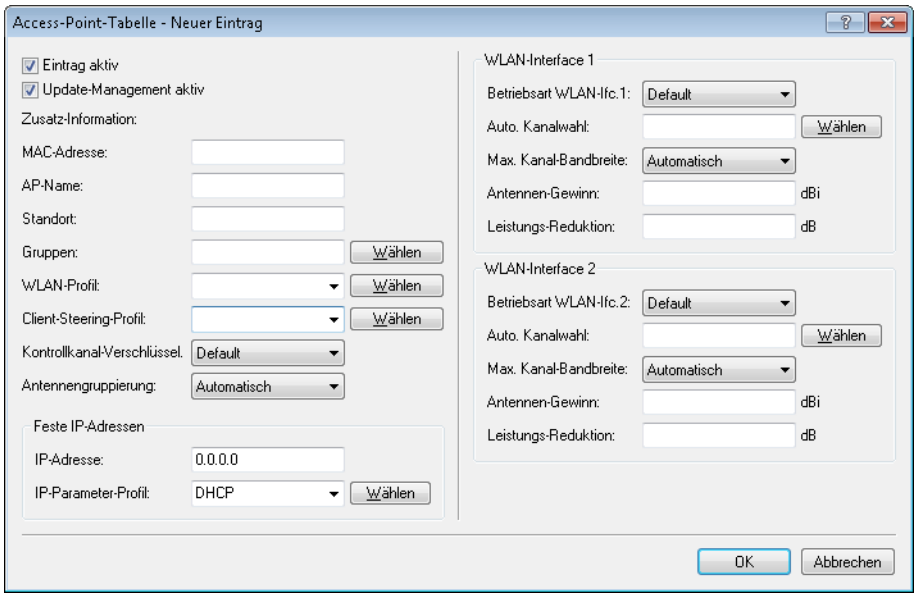
Auslastungs-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

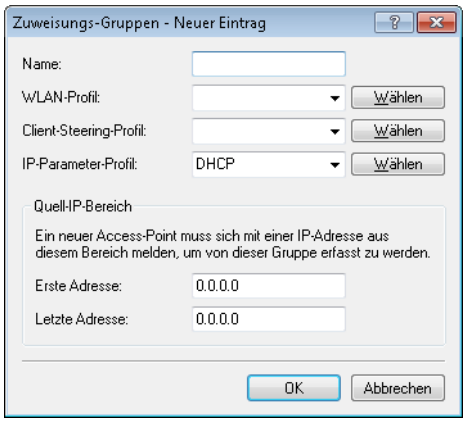
Frequenzband-Gewichtung

Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

3. Weisen Sie jetzt unter **WLAN-Controller** > **AP-Konfiguration** in der AP-Tabelle dem entsprechenden AP eines der Client-Steering-Profile zu.



4. Ordnen Sie ggf. auch den Zuweisungs-Gruppen ein entsprechendes Client-Steering-Profil zu.



8.12.2 Ergänzungen im Status-Menü

Client-Steering

In diesem Verzeichnis finden Sie die Client-Steering-Statistiken.

SNMP-ID:

1.73.123

Pfad Telnet:

Status > **WLAN-Management**

Aktiv

Zeigt an, ob das Client-Steering über den WLC aktiv ist.

SNMP-ID:

1.73.123.1

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering**

Client-Steering-Erfolgsrate

Der Wert zeigt das Verhältnis von erfolgreich gesteuerten Clients zu allen angemeldeten Clients an. Erfolgreich heißt dabei, dass der Client bei einem AP angemeldet ist, der vom WLC die Erlaubnis dazu bekommen hat.

SNMP-ID:

1.73.123.3

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering**

Client-Info

Diese Tabelle enthält die Daten aller WLAN-Clients, die sich erfolgreich mit den angeschlossenen APs verbunden haben.

SNMP-ID:

1.73.123.4

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering**

Client-MAC

Diese Spalte zeigt die MAC-Adresse des verbundenen WLAN-Clients.

SNMP-ID:

1.73.123.4.1

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering** > **Client-Steering**

Anzahl-positiver-Antworten

zeigt die Anzahl der APs an, die aktuell vom WLC die Erlaubnis bekommen haben, den Client anzunehmen.

SNMP-ID:

1.73.123.4.2

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering** > **Client-Steering**

Status

Diese Spalte zeigt den Status des WLAN-Clients an.

SNMP-ID:

1.73.123.4.3

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering** > **Client-Steering**

Mögliche Werte:

Steering OK

Zeigt an, ob der Client sich bei einem AP angemeldet hat, der vom WLC die Erlaubnis dazu bekommen hat.

Steering NOK

Zeigt an, ob der Client sich bei einem AP angemeldet hat, der vom WLC nicht die Erlaubnis dazu bekommen hat.

Pending

Der Controller hat für diesen Client eine Nachricht mit "OK" oder "NOK" gesendet. Der Status bleibt solange erhalten, bis der Controller von einem AP die Information erhalten hat, dass der Client sich bei ihm assoziiert hat. Der Controller prüft, ob dieser AP zuvor ein "OK" erhalten hat. In diesem Fall setzt er den Status auf "OK", anderenfalls setzt er ihn auf "NOK".

8.12.3 Ergänzungen im Setup-Menü

Kriterium

.

SNMP-ID:

2.12.87.2

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

Radio-Band

Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.

Controller

Der AP lässt das Client-Steering vom WLC durchführen.

Default-Wert:

Radio-Band

Deassoziierungs-Signalstaerke-Schwelle

SNMP-ID:

2.12.87.6

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

0 … 255

Default-Wert:

30

Deassoziierungs-Timeout-Schwelle

SNMP-ID:

2.12.87.7

Pfad Telnet:

Setup > **WLAN** > **Client-Steering**

Mögliche Werte:

0 … 65535

Default-Wert:

3600

Client-Steering-Profil

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

SNMP-ID:

2.37.1.4.27

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

Mögliche Werte:

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

Default-Wert:

leer

Client-Steering-Profil

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

SNMP-ID:

2.37.1.18.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **Client-Steering** > **Profile**

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

Default-Wert:

leer

Client-Steering

In diesem Verzeichnis konfigurieren Sie das Client-Steering über den WLC.

SNMP-ID:

2.37.40

Pfad Telnet:

Setup > **WLAN-Management**

Trace-Mac

Um die Fehlersuche zu erleichtern, erscheint bei aktiviertem Trace (`trace # wlc-steering`) nur die hier eingetragene MAC-Adresse.

SNMP-ID:

2.37.40.11

Pfad Telnet:

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

Mögliche Werte:

16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

Check-Aktiv

SNMP-ID:

2.37.40.13

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

ja

Berechnung-Aktiv

SNMP-ID:

2.37.40.14

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

ja

Statistiken-anzeigen

Aktivieren bzw. deaktivieren Sie hier die Anzeige der Statistiken. Die Statistiken können Sie unter **Status** > **WLAN-Management** > **Client-Steering** einsehen.

Die Statistikanzeige erhöht die Last auf dem WLC. Deshalb ist es nicht ratsam, die Statistikanzeige dauerhaft zu aktivieren.

SNMP-ID:

2.37.40.17

Pfad Telnet:

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

Mögliche Werte:

ja
Aktiviert die Anzeige von Client-Steering-Statistiken.

nein
Deaktiviert die Anzeige von Client-Steering-Statistiken.

Default-Wert:

nein

Profile

In dieser Tabelle verwalten Sie die Profile für das Client-Steering.

SNMP-ID:

2.37.40.19

Pfad Telnet:

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

Name

Bezeichnung des Client-Steering-Profils. Dieses Profil legt die Bedingungen fest, unter denen der WLC einen Client-Steering-Vorgang auslöst.

SNMP-ID:

2.37.40.19.1

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

Rating-Schwellwert

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

SNMP-ID:

2.37.40.19.2

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 100 Prozent

Default-Wert:

0

Signal-Schwellwert

SNMP-ID:

2.37.40.19.3

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

0

Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

SNMP-ID:

2.37.40.19.4

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 100 Prozent

Default-Wert:

0

Auslastungs-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

SNMP-ID:

2.37.40.19.5

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 100 Prozent

Default-Wert:

0

Radio-Gewichtung

Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

SNMP-ID:

2.37.40.19.6

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 100 Prozent

Default-Wert:

0

8.13 Automatische Wahl des Frequenzbands

Ab LCOS 9.00 haben Sie die Möglichkeit, einen gemanagten AP das bevorzugte Frequenzband für die physikalische WLAN-Schnittstelle selbst wählen zu lassen. In LANconfig erfolgt die Konfiguration im Dialog **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**:

Betriebsart WLAN-Ifc. 1

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 1. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der AP das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 2,4GHz-Band bevorzugt, sofern dieses verfügbar ist.

Betriebsart WLAN-Ifc. 2

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 2. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der AP das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 5GHz-Band bevorzugt, sofern dieses verfügbar ist.

Sofern ein verwalteter AP lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der AP die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

8.13.1 Ergänzungen im Setup-Menü

WLAN-Modul-1-Default

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 1. physikalische WLAN-Schnittstelle betreibt.

SNMP-ID:

2.37.1.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Mögliche Werte:

Auto
Der AP wählt das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 2,4GHz-Band bevorzugt, sofern dieses verfügbar ist.

2,4GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 2,4Ghz-Band.

5GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 5Ghz-Band.

Aus
Der AP deaktiviert die physikalische WLAN-Schnittstelle.

Default-Wert:

Auto

WLAN-Modul-2-Default

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 2. physikalische WLAN-Schnittstelle betreibt.

Sofern ein verwalteter AP lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der AP die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

SNMP-ID:

2.37.1.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Mögliche Werte:

Auto

Der AP wählt das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 5GHz-Band bevorzugt, sofern dieses verfügbar ist.

2,4GHz

Der AP betreibt die physikalische WLAN-Schnittstelle im 2,4Ghz-Band.

5GHz

Der AP betreibt die physikalische WLAN-Schnittstelle im 5Ghz-Band.

Aus

Der AP deaktiviert die physikalische WLAN-Schnittstelle.

Default-Wert:

Auto

9 VPN

9.1 VPN-Einwahl-Wizard in WEBconfig

Ab LCOS 9.00 haben Sie die Möglichkeit, VPN-Client-Einwahlzugänge über den LANCOM Advanced-VPN-Client oder einen alternativen VPN-Client auch über WEBconfig anzulegen. Dazu wird der bisherige Setup-Wizard **Einwahl-Zugang bereitstellen** um die VPN-Möglichkeit erweitert. Die Einrichtungsschritte entsprechen denen von LANconfig.

Die 1-Click-VPN-Konfiguration ist in WEBconfig durch die Beschränkungen des Browserzugriffs nicht verfügbar.

9.2 L2TPv2 (Layer 2 Tunneling Protocol Version 2)

Ein L2TP Access Concentrator (LAC) tunnelt die PPP-Anfrage eines Clients über eine öffentliche Verbindung (Internet, ATM, Frame Relay) zu einem L2TP Network Server (LNS). Der LNS dient als Gateway zum entfernten Netzwerk. Ggf. authentifiziert dort zunächst ein angeschlossener RADIUS-Server den Client. Anschließend sendet der LNS die zu verwendende IP-Adresse an den LAC und startet den L2TP-Tunnel. Der LAC gibt die IP-Adresse an den Client weiter. Ab diesem Zeitpunkt ist der Client über eine L2TP-Verbindung Teil des entfernten Netzwerkes.

L2TP verwendet zwei Arten 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 PPP-Frames, die der LAC und der LNS über den Tunnel austauschen.

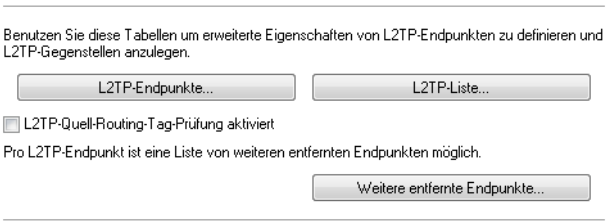
Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

Im Gegensatz zu PPTP, das Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Daten nur UDP. Es ist auch möglich, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

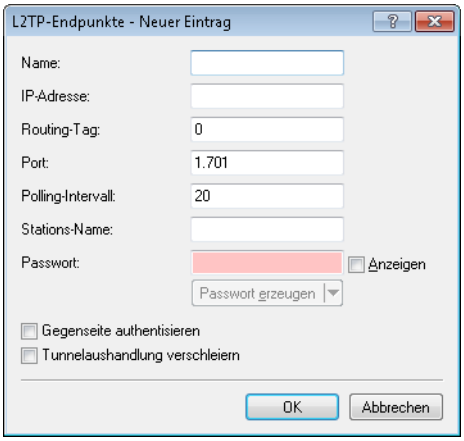
Das LANCOM ist sowohl als LAC als auch als LNS einsetzbar.

9.2.1 Konfiguration der L2TP-Tunnel

Mit LANconfig konfigurieren Sie L2TP unter **Kommunikation** > **Gegenstellen**.



Die Tunnel-Konfiguration für der Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt erfolgt unter **L2TP-Endpunkte**.



Name

Namen des Tunnelendpunktes

IP-Adresse

IP-Adresse des Tunnelendpunktes (IPv4, IPv6, FQDN).

Routing-Tag

Routing-Tag der Route zum Tunnelendpunkt

Port

UDP-Port

Polling-Intervall

Poll-Intervall in Sekunden

Stations-Name

Name, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

Passwort

Passwort, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

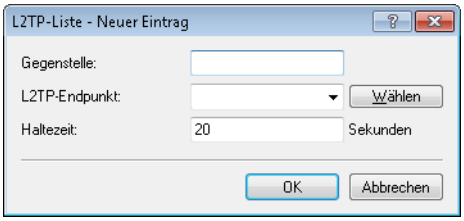
Gegenseite authentisieren

Wenn zwei Tunnelendpunkte (LAC und LNS) sich gegenseitig authentifizieren sollen, um einen Tunnel aufzubauen, ist diese Option aktiv. In diesem Fall sind im Tunnelendpunkt Stations-Name und Passwort dieses Gerätes als Tunnelendpunkt konfiguriert und ebenfalls die Option **Gegenseite authentisieren** aktiv.

Tunnelaushandlung verschleiern

Wenn bereits die Aushandlung eines Tunnels zwischen LAC und LNS verschlüsselt erfolgen soll, ist diese Option aktiv. Hierbei ver- und entschlüsseln beide L2TP-Partner mit Hilfe eines gemeinsamen "preshared Secrets" bestimmte AVPs (Attribute Value Pair) der L2TP-Nachrichten.

Unter **L2TP-Liste** verknüpfen Sie die L2TP-Gegenstellen mit einem zuvor konfigurierten Tunnelendpunkt.



Ein Eintrag in dieser Tabelle ist nur für die folgenden Bedingungen notwendig:

- abgehende Verbindungen,
- ankommende Verbindungen mit einem Idle-Timeout ungleich "20" oder
- wenn ankommende Verbindungen nur einen bestimmten Tunnel nutzen sollen.

Gegenstelle

Name der L2TP-Gegenstelle

L2TP-Endpunkt

Name des Tunnelendpunktes, den diese Gegenstelle verwendet.

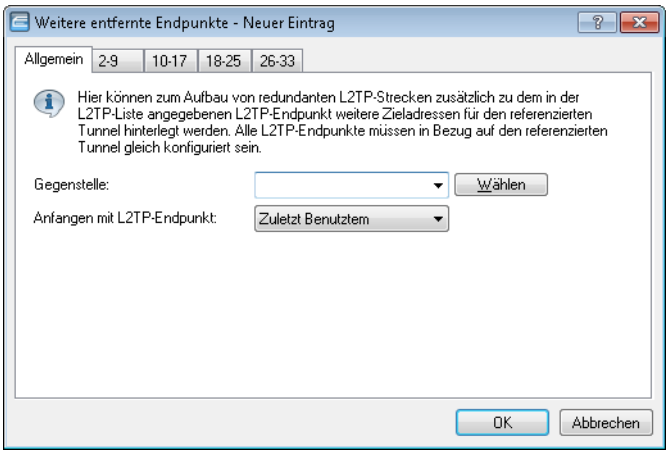
Haltezeit

Bestimmt, wie lange der L2TP-Tunnelendpunkt den Tunnel bei Inaktivität offen hält.

Bei ankommenden Tunnel-Anfragen erfolgt eine Prüfung entweder über RADIUS oder über einen Eintrag des anfragenden Hostes in der L2TP-Endpunkte-Tabelle. Existiert ein Tabellen-Eintrag mit identischer IP-Adresse (oder ist für diesen Eintrag keine IP-Adresse definiert), lässt das Gerät diesen Host für einen Tunnelaufbau zu.

Als zusätzliche Sicherung, um z. B. eine Verschlüsselung der L2TP-Sessions über IPSec zu ermöglichen, kann das Gerät darüber hinaus auch das Routing-Tag der Gegenstelle prüfen, über die es die Daten empfangen hat. Diese Option aktivieren Sie unter **L2TP-Quell-Routing-Tag-Prüfung aktiviert**.

Um bis zu 32 zusätzliche Gateways je Tunnelendpunkt zu konfigurieren, klicken Sie auf **Weitere entfernte Endpunkte**.



Achten Sie darauf, dass alle zusätzlich angegebenen L2TP-Endpunkte identisch zum referenzierten Tunnel-Endpunkt konfiguriert sind.

Gegenstelle

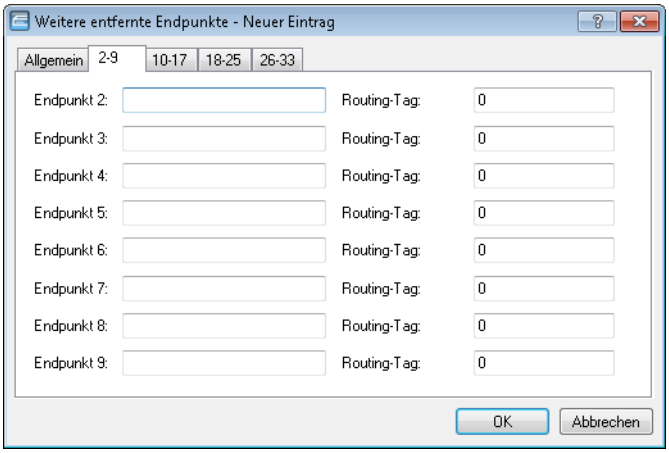
Name des Tunnelendpunktes, wie er in der Tabelle **L2TP-Endpunkte** konfiguriert ist.

Anfangen mit L2TP-Endpunkt

Option zur Auswahl des nächsten Gateways. Folgende Auswahl ist möglich:

- **Zuletzt Benutztem**: Auswahl der zuletzt erfolgreichen Adresse
- **Erstem**: Auswahl des ersten Gateways in der Liste
- **Zufall**: Zufällige Auswahl eines Gateways aus der Liste

Auf den folgenden Reitern konfigurieren Sie die Namen sowie die jeweiligen Routing-Tags der alternativen Gateways.



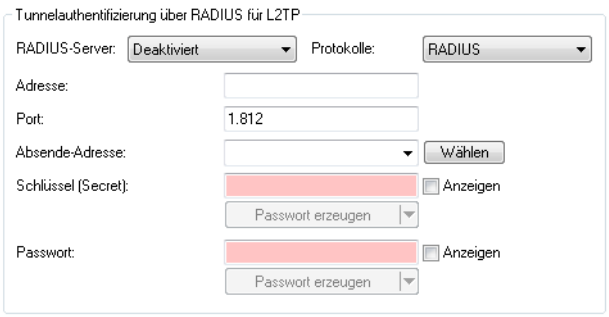
9.2.2 Authentifizierung über RADIUS

Eine RADIUS-Authentifizierung ist bei L2TP in zwei Anwendungsfällen möglich:

- Tunnel-Authentifizierung: Der RADIUS-Server prüft, ob ein LAC eine L2TP-Verbindung aufbauen darf.
- PPP-Session: Der RADIUS-Server prüft die Benutzerdaten der jeweiligen PPP-Session.

Deshalb erfolgt die Konfiguration des RADIUS-Servers für die Authentifizierung des L2TP-Tunnels und der PPP-Benutzerdaten unabhängig voneinander.

Bei einer Tunnel-Authentifizierung über RADIUS konfigurieren Sie die Einstellungen im LANconfig unter **Kommunikation** > **RADIUS** im Abschnitt **Tunnel-Authentifizierung**.



RADIUS-Server

Aktiviert bzw. deaktiviert den RADIUS-Server für die Authentifizierung des Tunnelendpunktes, unabhängig von einer Authentifizierung einer PPP-Session. Die folgende Auswahl ist möglich:

- **Deaktiviert**: Der RADIUS-Server ist nicht aktiv für die Authentifizierung eines Tunnelendpunktes.
- **Aktiviert**: Der RADIUS-Server übernimmt die Authentifizierung eines Tunnelendpunktes.

- **Exklusiv**: Aktiviert die Nutzung des externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

Protokolle

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Tunnelendpunkt.

Adresse

IP-Adresse oder DNS-Name des RADIUS-Servers.

Port

Port des RADIUS-Servers

Absende-Adresse

Optionale Absende-Adresse des Gerätes. Falls Sie z. B. Loopback-Adressen konfiguriert haben, ist deren Eingabe hier ebenfalls möglich. Folgende Eingabeformate sind erlaubt:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse stattdessen zu verwenden ist
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Schlüssel (Secret)

Shared-Secret zwischen dem RADIUS-Server und dem LANCOM

Passwort

Dummy-Passwort für die Tunnel-Authentifizierung

Trifft von einem entfernten Host eine L2TP-Tunnelanfrage ein (Start Control Connection Request), schickt das LANCOM eine Anfrage an den für L2TP aktivierten RADIUS-Server. Diese Anfrage enthält u. a. den Namen des Hostes, das Dummy-Passwort, die IP-Adresse des Gerätes sowie den Service-Typ "Outbound-User". Der RADIUS-Server authentifiziert den Host und schickt ein "RADIUS-Accept" an das LANCOM zusammen mit dem zu verwendenden Tunnel-Passwort, dem Tunnel-Typ "L2TP" mit dem Tag "0" sowie der Tunnel-Client-Auth-ID, die dem zuvor vom LANCOM übermittelten Stationsnamen entsprechen muss. Das LANCOM prüft diese Daten und übernimmt bei positivem Ergebnis das Tunnel-Passwort, um den einwählenden Client zu authentifizieren und ggf. die L2TP-Tunnelaushandlung zu verschleiern.

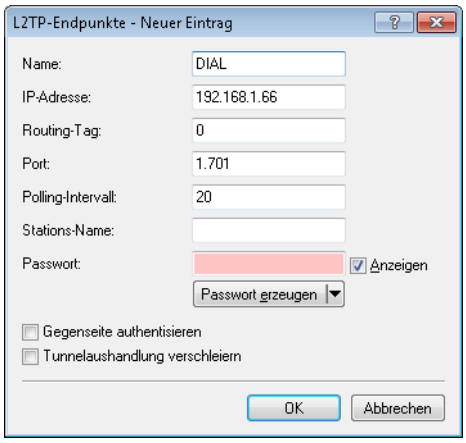
Die Konfiguration des RADIUS-Servers zur Authentifizierung von PPP-Sessions erfolgt, wie es im Abschnitt **Weitere Dienste** > **RADIUS** > **Konfiguration von RADIUS als Authenticator bzw. NAS** > **Einwahl über PPP und RADIUS** beschrieben ist.

9.2.3 Betrieb als L2TP Access Concentrator (LAC)

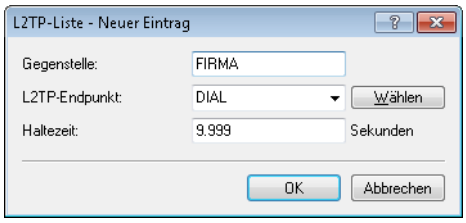
Im folgenden Beispiel baut der LANCOM als L2TP Access Concentrator (LAC) einen L2TP-Tunnel zu einem L2TP Network Server (LNS) mit der IP-Adresse 192.168.1.66 auf.

Um der LANCOM als LAC zu konfigurieren, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** einen Eintrag für einen LNS als entferntes L2TP-Gateway.

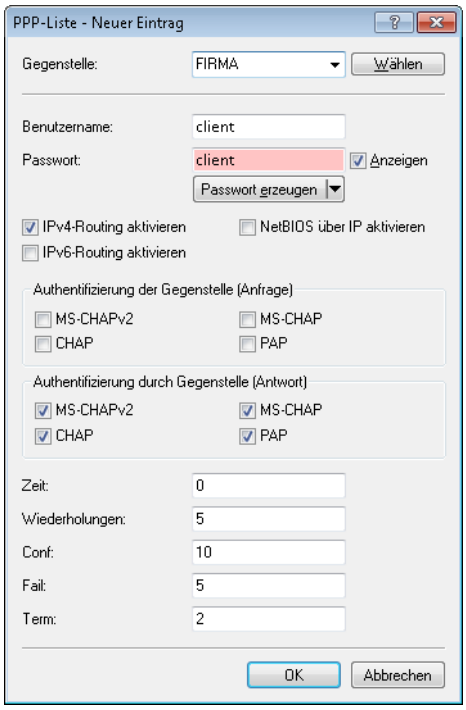


2. Vergeben Sie unter **Kommunikation** > **Protokolle** in der Tabelle **L2TP-Liste** einen Namen für diese Gegenstelle und verbinden Sie sie mit dem zuvor angelegten L2TP-Endpunkt.

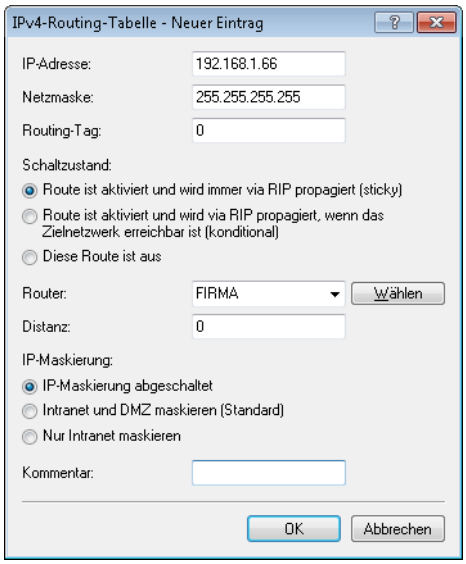


Es ist möglich, mehrere Gegenstellen mit einem L2TP-Tunnel zu verbinden. Dadurch lassen sich mehrere PPP-Sessions durch einen L2TP-Tunnel transportieren. Konfigurieren Sie hierfür in dieser Tabelle mehrere Gegenstellen mit dem gleichen L2TP-Endpunkt.

3. Erstellen Sie unter **Kommunikation** > **Protokolle** in der Tabelle **PPP-Liste** einen Eintrag für den L2TP-Tunnel.



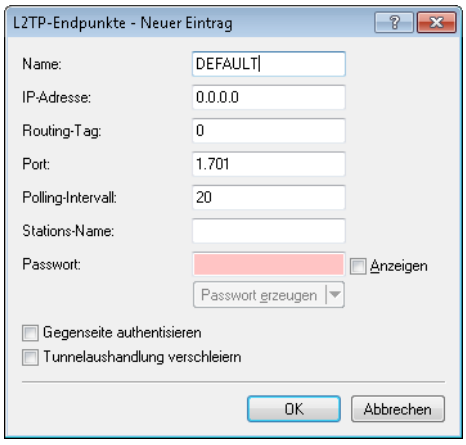
4. Legen Sie unter **Konfiguration** > **IP-Router** > **Routing** in der entsprechenden IPv4- oder IPv6-Routing-Tabelle einen Eintrag für diese Gegenstelle an.



9.2.4 Betrieb als L2TP Network Server (LNS) für RAS-Clients

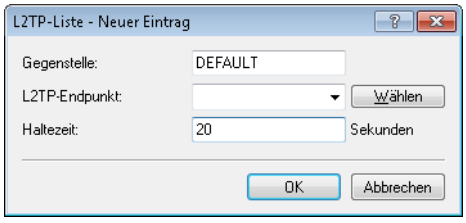
Um das LANCOM als L2TP Network Server (LNS) für die Anmeldung von RAS-Clients zu konfigurieren, ohne einen RADIUS-Server im LANCOM zu konfigurieren, haben Sie zwei Möglichkeiten:

1. Erstellen Sie unter **Kommunikation** > **Gegenstelle** in der Tabelle **L2TP-Endpunkte** einen Eintrag "DEFAULT".



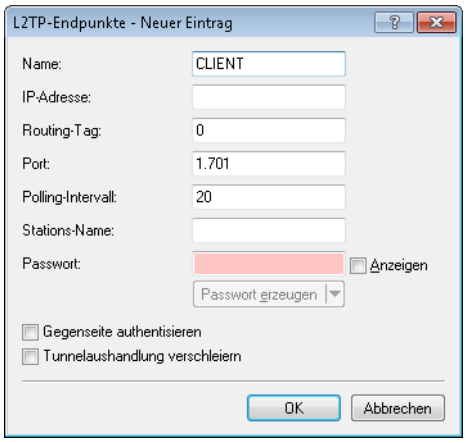
Der Eintrag für die IP-Adresse lautet "0.0.0.0", da die IP-Adresse des L2TP-LACs dem LANCOM unbekannt ist.

2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Liste** einen Eintrag "DEFAULT".

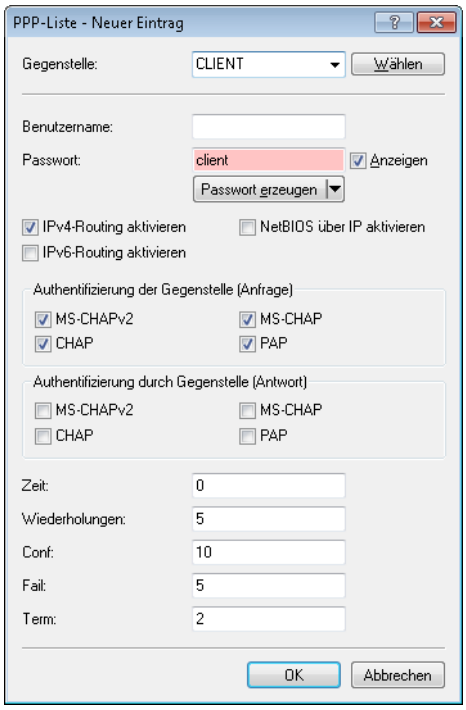


Soll der L2TP-Tunnel dauerhaft verbunden sein, setzen Sie die Haltezeit auf "9999".

3. Alternativ legen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** für den RAS-Client einen separaten Eintrag (z. B. "CLIENT") an.



4. Anschließend konfigurieren Sie unter **Kommunikation** > **Protokolle** in der **PPP-Liste** für den Client einen neuen Eintrag.

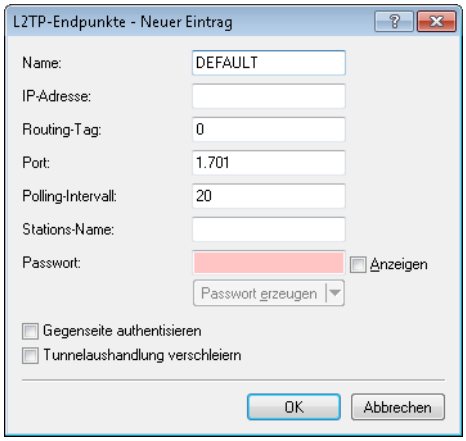


9.2.5 Betrieb als L2TP Network Server (LNS) mit Authentifizierung über RADIUS

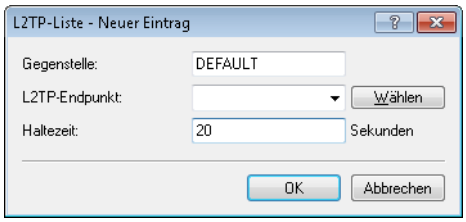
Im folgenden Beispiel arbeitet der LANCOM als L2TP Network Server (LNS). Die Authentifizierung der eingehenden L2TP-Tunnel sowie der PPP-Sessions erfolgt über RADIUS.

Um das LANCOM als LNS zu konfigurieren, gehen Sie wie folgt vor:

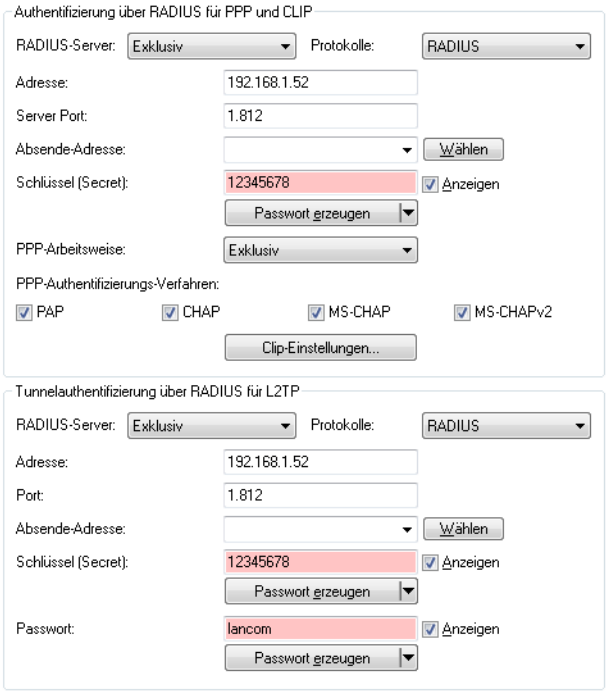
1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** einen Eintrag "DEFAULT".



2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Liste** einen Eintrag "DEFAULT".



3. Konfigurieren Sie unter **Kommunikation** > **RADIUS** den RADIUS-Server.



> Den unteren Abschnitt **RADIUS-Server-Einstellungen für L2TP** konfigurieren Sie nur, wenn eine L2TP-Tunnel-Authentifizierung über den RADIUS-Server erfolgen soll.

4. Konfigurieren Sie den RADIUS-Server entsprechend, damit er die Authentifizierung des L2TP-Tunnels und der PPP-Sessions durchführen kann.

Möchte sich ein LAC mit dem Stationsnamen "router1" und dem Passwort "abcde" für den L2TP-Tunnel authentifizieren lassen, konfigurieren Sie den entsprechenden Eintrag im RADIUS-Server (z. B. FreeRADIUS) wie folgt:

```
router1 Cleartext-Password := "lancom"
        Service-Type = Outbound-User,
        Tunnel-Type  = L2TP,
        Tunnel-Password = "abcde",
        Tunnel-Client-Auth-ID = "router1"
```

Für die Authentifizierung der PPP-Session eines Benutzers mit dem Benutzernamen "test" und dem Passwort "test" lautet der entsprechende Eintrag im RADIUS-Server wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type = Framed-User,
     Framed-Protocol = PPP
```

9.2.6 Ergänzungen im Status-Menü

L2TP

Layer 2 Tunneling Protocol

SNMP-ID:

1.84

Pfad Telnet:

Status

Rx-Pakete

Anzahl der empfangenen Pakete.

SNMP-ID:

1.84.1

Pfad Telnet:

Status > **L2TP**

Tx-Pakete

Anzahl der gesendeten Pakete.

SNMP-ID:

1.84.2

Pfad Telnet:

Status > **L2TP**

Tx-Wiederholungen

Wiederholungen im Kontrollkanal.

SNMP-ID:

1.84.3

Pfad Telnet:

Status > **L2TP**

Ruffehler

Anzahl der gescheiterten Versuche, eine Session aufzubauen.

SNMP-ID:

1.84.4

Pfad Telnet:

Status > **L2TP**

Endpunkte

In dieser Tabelle werden Informationen über die aktuell aktiven Tunnel nachgehalten. Nachdem ein Tunnel abgebaut wurde, wird dieser sofort aus der Tabelle gelöscht, falls kein Fehler aufgetreten ist. Der Fehler wird automatisch gelöscht, wenn der Tunnel erneut aufgebaut wird, er kann aber auch manuell gelöscht werden. Die Syntax hierfür lautet: set <Gegenstelle> {letzter-fehler} (none)

SNMP-ID:

1.84.5

Pfad Telnet:

Status > **L2TP**

L2TP-Endpunkt

Name des Tunnel-Endpunkts.

SNMP-ID:

1.84.5.1

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Status

Aktueller Zustand des Tunnel-Endpunkts.

SNMP-ID:

1.84.5.2

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Letzter-Fehler

Der letzte erkannte Fehler.

SNMP-ID:

1.84.5.3

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Mögliche Werte:

(none)
Kein Fehler

Dns-resolution-failed
DNS-Auflösung fehlgeschlagen

No-route-to-gateway
Es existiert keine Route zum Gateway

Invalid-gateway-address
Die IP-Adresse des Gateway ist ungültig

No-response
Es wurde keine Antwort vom Gateway empfangen

Message-timeout
Eine Kontrollnachricht wurde nicht beantwortet

Tunnel-already-exists
Es existiert bereits ein Tunnel mit diesem Gateway

Authorization-failed
Die Authentifizierung ist fehlgeschlagen

Bad-protocol-version
Eine falsche Version des L2TP wird genutzt

Shutting-down
Das Gerät bootet momentan

State-machine-error
Allgemeiner Fehler

No-tunnel-exists
Unbekannte Tunnel-ID

Invalid-length
Ungültige Länge eines Parameters

Invalid-value
Ungültiger Wert eines Parameters
No-ressources
Keine Ressourcen verfügbar
Invalid-session-id
Ungültige Session-ID
Vendor-specific-error
Hersteller-spezifischer Fehler
Try-another
Ein anderes Gateway versuchen
Unkown-mandatory-attribute
Unbekanntes notwendiges Attribut
Unknown
Unbekannter Fehler

Mode

Aktiver (LAC) oder passiver (LNS) Aufbau.

SNMP-ID:
1.84.5.4

Pfad Telnet:
Status > **L2TP** > **Endpunkte**

Phys.-Verbindung

Name der genutzten physikalischen Verbindung.

SNMP-ID:
1.84.5.5

Pfad Telnet:
Status > **L2TP** > **Endpunkte**

Gateway

Aufgelöste IP-Adresse des aktuellen Gateways.

SNMP-ID:
1.84.5.6

Pfad Telnet:
Status > **L2TP** > **Endpunkte**

Verbindungen

Anzahl der Verbindungen, die den Tunnel nutzen.

SNMP-ID:

1.84.5.7

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Verb.-Zeit

Dauer der Verbindung in Sekunden.

SNMP-ID:

1.84.5.8

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Eingebettete-Fehler-Meldung

Fehlermeldung im Klartext.

SNMP-ID:

1.84.5.9

Pfad Telnet:

Status > **L2TP** > **Endpunkte**

Anzahl-Endpunkte

Anzahl bestehender Tunnel.

SNMP-ID:

1.84.6

Pfad Telnet:

Status > **L2TP**

Verbindungen

In dieser Tabelle werden Informationen über die aktuell aktiven Sessions nachgehalten. Etwaige IPv6-Parameter werden in der Tabelle nicht angezeigt, können aber den verschiedenen IPv6-Statistiken schnittstellenbezogen entnommen werden. Nachdem eine Session abgebaut wurde, wird diese sofort aus der Tabelle gelöscht, falls kein Fehler aufgetreten ist. Der

Fehler wird automatisch gelöscht, wenn die Session erneut aufgebaut wird, er kann aber auch manuell gelöscht werden. Die Syntax hierfür lautet: set <Gegenstelle> {letzter-fehler} (none)

SNMP-ID:

1.84.7

Pfad Telnet:

Status > **L2TP**

Gegenstelle

Name der Gegenstelle/Session.

SNMP-ID:

1.84.7.1

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Status

Aktueller Verbindungszustand der Session.

SNMP-ID:

1.84.7.2

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Letzter-Fehler

Der letzte erfasste Fehler.

SNMP-ID:

1.84.7.3

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Mode

Angabe, ob der Aufbau der Session aktiv oder passiv erfolgt ist.

SNMP-ID:

1.84.7.4

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

SH-Zeit

Der Idle-Timeout der Session.

SNMP-ID:

1.84.7.5

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

L2TP-Endpunkt

Angabe des genutzten Tunnels.

SNMP-ID:

1.84.7.6

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Adresse-Gegenstelle

IPv4-Adresse der Gegenstelle.

SNMP-ID:

1.84.7.7

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

IP-Adresse

Eigene IPv4-Adresse.

SNMP-ID:

1.84.7.8

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

DNS-Default

IPv4-Adresse des ersten DNS-Servers.

SNMP-ID:

1.84.7.9

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

DNS-Backup

IPv4-Adresse des zweiten DNS-Servers.

SNMP-ID:

1.84.7.10

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

NBNS-Default

IPv4-Adresse des ersten NBNS-Servers.

SNMP-ID:

1.84.7.11

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

NBNS-Backup

IPv4-Adresse des zweiten NBNS-Servers.

SNMP-ID:

1.84.7.12

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Verb.-Zeit

Dauer der Session in Sekunden.

SNMP-ID:

1.84.7.13

Pfad Telnet:

Status > **L2TP** > **Verbindungen**

Anzahl-Verbindungen

Anzahl bestehender Verbindungen.

SNMP-ID:

1.84.8

Pfad Telnet:

Status > **L2TP**

Werte-loeschen

Aktion, um die Zähler zurückzusetzen. Syntax: do werte-loeschen

SNMP-ID:

1.84.9

Pfad Telnet:

Status > **L2TP**

9.2.7 Ergänzungen im Setup-Menü

L2TP-Aktiv

Hier kann eingestellt werden, ob eine Authentifizierung des Tunnel-Endpunktes über RADIUS erfolgen soll.

SNMP-ID:

2.2.22.20

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

nein

Es findet keine RADIUS-Authentifizierung statt.

ja

Eine RADIUS-Authentifizierung findet statt, wenn in der Tabelle 'L2TP-Endpunkte' das Feld 'Auth-Peer' auf 'ja' steht, aber kein Passwort hinterlegt wurde.

Exclusiv

Es findet immer eine RADIUS-Authentifizierung statt, wenn in der Tabelle 'L2TP-Endpunkte' das Feld 'Auth-Peer' auf 'ja' steht, unabhängig davon, ob ein Passwort angegeben wurde.

Default-Wert:

nein

L2TP-Server-Hostname

IP-Adresse des RADIUS-Servers.

Der interne RADIUS-Server des Geräts unterstützt nicht die Tunnel-Authentifizierung. Hierzu wird ein externer RADIUS-Server benötigt.

SNMP-ID:

2.2.22.21

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

L2TP-Auth.-Port

Der UDP-Port des RADIUS-Servers.

SNMP-ID:

2.2.22.22

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

0 … 65535

L2TP-Loopback-Adresse

Die Absender-Adresse, die bei RADIUS-Anfragen genutzt wird.

SNMP-ID:

2.2.22.23

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

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

L2TP-Protokoll

Das zu nutzende Protokoll.

SNMP-ID:

2.2.22.24

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

L2TP-Schluessel

Das Shared Secret zwischen Router und RADIUS-Server.

SNMP-ID:

2.2.22.25

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

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

L2TP-Password

Das Passwort, welches zusammen mit dem Host im RADIUS-Server hinterlegt ist. Nach der Authentifizierung wird vom RADIUS-Server das zu nutzende Passwort für den Tunnel übermittelt.

SNMP-ID:

2.2.22.26

Pfad Telnet:

Setup > **WAN** > **RADIUS**

Mögliche Werte:

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

L2TP-Endpunkte

In dieser Tabelle werden die grundsätzlichen Einstellungen zur Konfiguration eines L2TP-Tunnels vorgenommen.

Sollen RAS-Verbindungen ohne Konfiguration in einem Router über RADIUS authentifiziert werden, muss in dieser Tabelle ein Default-Eintrag mit folgenden Werten angelegt werden:

Identifier: DEFAULT

Poll: 20

Auth-Peer: ja

Verschleiern: nein

Alle anderen Werte müssen leer bleiben. Wird 'Auth-Peer' im DEFAULT-Eintrag auf 'nein' gesetzt, werden alle Hosts ungeprüft angenommen und nur die PPP-Sessions authentifiziert.

SNMP-ID:

2.2.35

Pfad Telnet:

Setup > **WAN**

Identifier

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge 'Identifier' und 'Hostname' überkreuz übereinstimmen.

SNMP-ID:

2.2.35.1

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts. Anstelle einer IP-Adresse (IPv4 oder IPv6) kann auch ein FQDN angegeben werden.

SNMP-ID:

2.2.35.2

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag

Hier muss das Tag angegeben werden, welches der Route zum Tunnel-Endpunkt zugewiesen ist.

SNMP-ID:

2.2.35.3

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

Port

Der zu nutzende UDP-Port.

SNMP-ID:

2.2.35.4

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

Default-Wert:

1701

Poll

Das Polling-Intervall in Sekunden.

SNMP-ID:

2.2.35.5

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

Default-Wert:

20

Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge 'Identifier' und 'Hostname' überkreuz übereinstimmen.

SNMP-ID:

2.2.35.6

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

Passwort

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

SNMP-ID:

2.2.35.7

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

SNMP-ID:

2.2.35.8

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Verschleiern

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

SNMP-ID:

2.2.35.9

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

nein
ja

Default-Wert:

nein

L2TP-Zusaetzliche-Gateways

In dieser Tabelle können bis zu 32 redundante Gateways je L2TP-Tunnel angegeben werden.

SNMP-ID:

2.2.36

Pfad Telnet:

Setup > **WAN**

Identifier

Die Bezeichnung des Tunnel-Endpunkts, welche auch in der Tabelle L2TP-Endpunkte verwendet wurde.

SNMP-ID:

2.2.36.1

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

Anfangen-mit

Mit dieser Einstellung wird festgelegt, welcher redundante Gateway zuerst verwendet wird.

SNMP-ID:

2.2.36.2

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

zuletzt-verwendetem

Es wird der zuletzt erfolgreich verwendete Gateway gewählt.

erstem

Es wird immer mit dem ersten Gateways begonnen.

zufaelligem

Bei jedem Versuch wird ein zufälliger Gateway ausgewählt.

Default-Wert:

zuletzt-verwendetem

Gateway-1

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.3

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-1

Das Routing-Tag der Route, über welche Gateway-1 erreicht werden kann.

SNMP-ID:

2.2.36.4

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-2

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.5

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-2

Das Routing-Tag der Route, über welche Gateway-2 erreicht werden kann.

SNMP-ID:

2.2.36.6

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-3

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.7

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-3

Das Routing-Tag der Route, über welche Gateway-3 erreicht werden kann.

SNMP-ID:

2.2.36.8

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-4

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.9

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-4

Das Routing-Tag der Route, über welche Gateway-4 erreicht werden kann.

SNMP-ID:

2.2.36.10

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-5

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.11

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-5

Das Routing-Tag der Route, über welche Gateway-5 erreicht werden kann.

SNMP-ID:

2.2.36.12

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-6

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.13

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-6

Das Routing-Tag der Route, über welche Gateway-6 erreicht werden kann.

SNMP-ID:

2.2.36.14

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-7

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.15

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-7

Das Routing-Tag der Route, über welche Gateway-7 erreicht werden kann.

SNMP-ID:

2.2.36.16

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-8

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.17

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-8

Das Routing-Tag der Route, über welche Gateway-8 erreicht werden kann.

SNMP-ID:

2.2.36.18

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-9

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.19

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-9

Das Routing-Tag der Route, über welche Gateway-9 erreicht werden kann.

SNMP-ID:

2.2.36.20

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-10

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.21

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-10

Das Routing-Tag der Route, über welche Gateway-10 erreicht werden kann.

SNMP-ID:

2.2.36.22

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-11

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.23

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-11

Das Routing-Tag der Route, über welche Gateway-11 erreicht werden kann.

SNMP-ID:

2.2.36.24

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-12

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.25

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-12

Das Routing-Tag der Route, über welche Gateway-12 erreicht werden kann.

SNMP-ID:

2.2.36.26

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-13

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.27

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-13

Das Routing-Tag der Route, über welche Gateway-13 erreicht werden kann.

SNMP-ID:

2.2.36.28

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-14

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.29

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-14

Das Routing-Tag der Route, über welche Gateway-14 erreicht werden kann.

SNMP-ID:

2.2.36.30

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-15

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.31

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-15

Das Routing-Tag der Route, über welche Gateway-15 erreicht werden kann.

SNMP-ID:

2.2.36.32

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-16

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.33

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-16

Das Routing-Tag der Route, über welche Gateway-16 erreicht werden kann.

SNMP-ID:

2.2.36.34

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-17

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.35

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-17

Das Routing-Tag der Route, über welche Gateway-17 erreicht werden kann.

SNMP-ID:

2.2.36.36

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-18

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.37

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-18

Das Routing-Tag der Route, über welche Gateway-18 erreicht werden kann.

SNMP-ID:

2.2.36.38

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-19

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.39

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-19

Das Routing-Tag der Route, über welche Gateway-19 erreicht werden kann.

SNMP-ID:

2.2.36.40

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-20

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.41

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-20

Das Routing-Tag der Route, über welche Gateway-20 erreicht werden kann.

SNMP-ID:

2.2.36.42

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-21

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.43

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-21

Das Routing-Tag der Route, über welche Gateway-21 erreicht werden kann.

SNMP-ID:

2.2.36.44

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-22

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.45

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-22

Das Routing-Tag der Route, über welche Gateway-22 erreicht werden kann.

SNMP-ID:

2.2.36.46

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-23

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.47

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-23

Das Routing-Tag der Route, über welche Gateway-23 erreicht werden kann.

SNMP-ID:

2.2.36.48

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-24

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.49

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-24

Das Routing-Tag der Route, über welche Gateway-24 erreicht werden kann.

SNMP-ID:

2.2.36.50

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-25

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.51

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-25

Das Routing-Tag der Route, über welche Gateway-25 erreicht werden kann.

SNMP-ID:

2.2.36.52

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-26

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.53

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-26

Das Routing-Tag der Route, über welche Gateway-26 erreicht werden kann.

SNMP-ID:

2.2.36.54

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-27

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.55

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-27

Das Routing-Tag der Route, über welche Gateway-27 erreicht werden kann.

SNMP-ID:

2.2.36.56

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-28

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.57

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-28

Das Routing-Tag der Route, über welche Gateway-28 erreicht werden kann.

SNMP-ID:

2.2.36.58

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-29

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.59

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-29

Das Routing-Tag der Route, über welche Gateway-29 erreicht werden kann.

SNMP-ID:

2.2.36.60

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-30

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.61

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-30

Das Routing-Tag der Route, über welche Gateway-30 erreicht werden kann.

SNMP-ID:

2.2.36.62

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-31

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.63

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-31

Das Routing-Tag der Route, über welche Gateway-31 erreicht werden kann.

SNMP-ID:

2.2.36.64

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

Gateway-32

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

SNMP-ID:

2.2.36.65

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9].-:%`

Rtg-Tag-32

Das Routing-Tag der Route, über welche Gateway-32 erreicht werden kann.

SNMP-ID:

2.2.36.66

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

L2TP-Gegenstellen

In dieser Tabelle werden die Tunnel-Endpunkte mit den L2TP-Gegenstellen verknüpft, die in der Routing-Tabelle verwendet werden. Ein Eintrag in dieser Tabelle wird für abgehende Verbindungen benötigt, wenn einer eingehenden Session ein Idle-Timeout ungleich 0 zugeordnet oder die Nutzung eines bestimmten Tunnels erzwungen werden soll.

SNMP-ID:

2.2.37

Pfad Telnet:

Setup > **WAN**

Gegenstelle

Name der L2TP-Gegenstelle.

SNMP-ID:

2.2.37.1

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

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

L2TP-Endpunkt

Name des Tunnel-Endpunkts.

SNMP-ID:

2.2.37.2

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

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

SH-Zeit

Idle-Timeout in Sekunden.

SNMP-ID:

2.2.37.3

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

0 … 9999

L2TP-Quell-Pruefung

In der Voreinstellung wird die Absenderadresse eines eingehenden Tunnels geprüft. Ist sie Teil der konfigurierten Gateways für den Tunnel oder wurden keine Gateways konfiguriert, so wird der Tunnel zugelassen. Zusätzlich kann auch das Routing-Tag geprüft werden, über das entsprechende Pakete eingehen. Hierbei ist zu beachten, dass nur auf Routing-Tags ungleich 0 geprüft wird.

SNMP-ID:

2.2.38

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

Adresse
Tag+Adresse

Default-Wert:

Adresse

9.3 Unterstützung der DH-Gruppen 15 und 16

Ab Version 9.00 bietet Ihnen LANconfig bei der Verschlüsselung von VPN-Verbindungen verbesserte Möglichkeiten des Schlüsselaustauschs nach dem Diffie-Hellman-Verfahren. Bei kombatiblen Geräten können dafür die DH-Gruppen 15 und 16 verwendet werden. Die entsprechenden Einstellungen befinden sich im Konfigurationsmenü unter **VPN** > **Allgemein** > **Verbindungsparameter** > **Hinzufügen** sowie **VPN** > **Defaults**.

9.3.1 Ergänzungen im Setup-Menü

IKE-Auth-Alg

Hash-Verfahren zur Abbildung der Verschlüsselung. Die zur Verfügung stehenden Werte sind abhängig von dem zu konfigurierenden Gerät.

SNMP-ID:

2.19.4.11.4

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IKE**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384
SHA2-512

Default-Wert:

MD5

DH-Gruppe

Dieser Wert zeigt die jeweilige DH-Gruppe an.

SNMP-ID:

2.19.3.29.2.1

Pfad Telnet:

Setup > **VPN** > **Isakmp** > **DH-Gruppen** > **Gruppenkonfig**

Mögliche Werte:

Auswahl aus der Liste vorgegebener DH-Gruppen

PFS-Grp

Perfect Forward Secrecy (PFS) ist ein Sicherheitsmerkmal von Verschlüsselungsverfahren. Die PFS-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

SNMP-ID:

2.19.7.3

Pfad Telnet:

Setup > **VPN** > **Layer**

Mögliche Werte:

0
Kein PFS
1
MODP-768
2
MODP-1024
5
MODP-1536

14
MODP-2048
15
MODP-3072
16
MODP-4096

Default-Wert:

0

IKE-Grp

Die IKE-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

SNMP-ID:

2.19.7.4

Pfad Telnet:

Setup > **VPN** > **Layer**

Mögliche Werte:

1
MODP-768
2
MODP-1024
5
MODP-1536
14
MODP-2048
15
MODP-3072
16
MODP-4096

Default-Wert:

1

AggrMode-IKE-Group-Default

Diese IKE-Gruppe wird für Aggressive-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

SNMP-ID:

2.19.11

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

1
MODP-768
2
MODP-1024
5
MODP-1536
14
MODP-2048
15
MODP-3072
16
MODP-4096

Default-Wert:

2

MainMode-IKE-Group-Default

Diese IKE-Gruppe wird für Main-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

SNMP-ID:

2.19.14

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

1
MODP-768
2
MODP-1024
5
MODP-1536
14
MODP-2048
15
MODP-3072

16
MODP-4096

Default-Wert:

2

QuickMode-PFS-Group-Default

Diese IPSec-Gruppe wird bei der vereinfachten Einwahl mit Zertifikaten genutzt.

SNMP-ID:

2.19.20

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

0
Kein PFS
1
MODP-768
2
MODP-1024
5
MODP-1536
14
MODP-2048
15
MODP-3072
16
MODP-4096

Default-Wert:

2

10 Routing und WAN-Verbindungen

10.1 Überarbeitete Flusssteuerung

Bisher war nur der Flow-Control-Status zweier Netz-Partner einsehbar. Ab LCOS 9.00 lässt sich Flow-Control in gewissem Rahmen konfigurieren und im Statusbereich der Modus (symmetrisch, asymmetrisch) einsehen.

10.1.1 Ergänzungen im Status-Menü

Flusssteuerung

Zeigt den aktuellen Flow-Control-Status an. Mögliche Werte sind:

SNMP-ID:

1.5.51.6

Pfad Telnet:

Status > **LAN** > **Schnittstellen**

Mögliche Werte:

Nein
Flow-Control ist deaktiviert.

Ja
Flow-Control ist aktiviert (symmetrischer Betrieb).

Nur-Tx
Flow-Control ist aktiviert (asymmetrischer Betrieb, nur Senden)

Nur-Rx
Flow-Control ist aktiviert (asymmetrischer Betrieb, nur Empfangen)

Flusssteuerung

Zeigt den aktuellen Flow-Control-Status an. Mögliche Werte sind:

SNMP-ID:

1.51.1.8

Pfad Telnet:

Status > **Ethernet-Ports** > **Ports**

Mögliche Werte:

Nein
Flow-Control ist deaktiviert.

Ja
Flow-Control ist aktiviert (symmetrischer Betrieb).

Nur-Tx
Flow-Control ist aktiviert (asymmetrischer Betrieb, nur Senden)

Nur-Rx
Flow-Control ist aktiviert (asymmetrischer Betrieb, nur Empfangen)

10.1.2 Ergänzungen im Setup-Menü

Flusssteuerung

Mit der Flusssteuerung können Sie dem Verlust von Datenpaketen vorbeugen, wenn ein Netzpartner zeitweise z. B. aufgrund eines Speicherüberlaufs die ankommenden Datenpakete nicht verarbeiten kann. In diesem Fall signalisiert der Empfänger dem Sender, mit der Datenübertragung für einen bestimmten Zeitraum zu pausieren.

SNMP-ID:
2.23.21.11

Pfad Telnet:
Setup > **Schnittstellen** > **Ethernet-Ports**

Mögliche Werte:

Auto
Ist die automatische Verbindungsverhandlung aktiviert, erfolgt auch die Flusssteuerung automatisch, je nach Fähigkeit der Partner (symmetrisch, asymmetrisch).

Ist die automatische Verbindungsverhandlung deaktiviert, findet auch keine Flusssteuerung statt.

an
Aktiviert die symmetrische Flusssteuerung, wenn die automatische Verbindungsverhandlung deaktiviert ist.

aus
Deaktiviert die Flusssteuerung, wenn die automatische Verbindungsverhandlung aktiviert ist.

Flusssteuerung

Mit der Flusssteuerung können Sie dem Verlust von Datenpaketen vorbeugen, wenn ein Netzpartner zeitweise z. B. aufgrund eines Speicherüberlaufs die ankommenden Datenpakete nicht verarbeiten kann. In diesem Fall signalisiert der Empfänger dem Sender, mit der Datenübertragung für einen bestimmten Zeitraum zu pausieren.

SNMP-ID:
2.23.30.9

Pfad Telnet:

Setup > **Schnittstellen** > **LAN-Schnittstellen**

Mögliche Werte:

Auto

Ist die automatische Verbindungsverhandlung aktiviert, erfolgt auch die Flusssteuerung automatisch, je nach Fähigkeit der Partner (symmetrisch, asymmetrisch).

Ist die automatische Verbindungsverhandlung deaktiviert, findet auch keine Flusssteuerung statt.

an

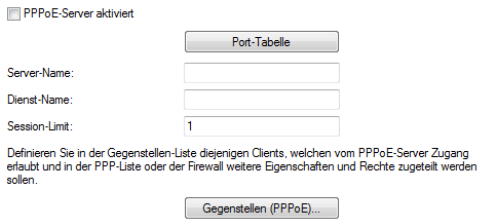
Aktiviert die symmetrische Flusssteuerung, wenn die automatische Verbindungsverhandlung deaktiviert ist.

aus

Deaktiviert die Flusssteuerung, wenn die automatische Verbindungsverhandlung aktiviert ist.

10.2 AC-Name für PPPoE-Server konfigurierbar

Ab LCOS 9.00 haben Sie die Möglichkeit, einem PPPoE-Server einen AC-Namen (Access Concentrator Name) zuzuweisen.



Server-Name

Über dieses Eingabefeld haben Sie optional die Möglichkeit, dem PPPoE-Server einen eigenen Namen unabhängig vom Gerätenamen zuzuweisen (AC-Name = Access Concentrator Name). Sofern Sie dieses Feld leer lassen, verwendet der PPPoE-Server den Gerätenamen als Server-Namen.

10.2.1 Ergänzungen im Setup-Menü

AC-Name

Über dieses Eingabefeld haben Sie optional die Möglichkeit, dem PPPoE-Server einen eigenen Namen unabhängig vom Gerätenamen zuzuweisen (AC-Name = Access Concentrator Name).

SNMP-ID:

2.31.6

Pfad Telnet:

Setup > **PPPoE-Server**

Mögliche Werte:

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

Besondere Werte:

leer

Sofern Sie dieses Feld leer lassen, verwendet der PPPoE-Server den Gerätenamen als Server-Namen.

Default-Wert:

leer

11 Weitere Dienste

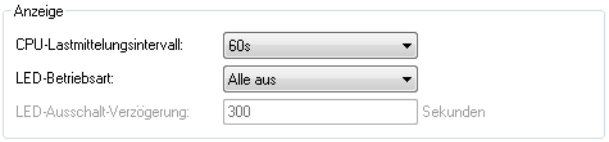
Ein LANCOM bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzen mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Bürokommunikations-Funktionen mit LANCAPI
- Zeit-Server

11.1 Geräte-LEDs bootpersistent ausschalten

Um einen Access Point unauffällig zu betreiben, können Sie die Betriebs- und Status-LEDs am Gerät deaktivieren. Auch nach einem Neustart bleiben die LEDs ausgeschaltet. Sie können allerdings auch festlegen, dass die LEDs kurz nach einem Neustart für eine bestimmte Zeit leuchten sollen, bevor das Gerät sie deaktiviert. Das ist z. bei von WLAN-Controllern verwalteten Access Points hilfreich, um den Verbindungsaufbau zum WLAN-Controller verfolgen zu können.

Die LED-Betriebsart können Sie unter **Management** > **Erweitert** im Abschnitt **Anzeige** festlegen.



In der Auswahlliste **LED-Betriebsart** stehen drei Optionen zur Auswahl:

Normal

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Alle aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Verzögert aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

Die Funktion "LED-Test" lässt sich trotz deaktivierter LEDs ausführen.

Wenn Sie diesen Wert innerhalb der zuvor eingestellten Dauer ändern und speichern, starten Sie den Timer neu.

11.1.1 Ergänzungen im Setup-Menü

LED-Modus

Bestimmen Sie die Betriebsart der Geräte-LEDs.

Die Funktion "LED-Test" lässt sich trotz deaktivierter LEDs ausführen.

SNMP-ID:

2.11.90

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

An

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Zeitgesteuert-Aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

Default-Wert:

An

LED-Ausschalten-Sekunden

Bestimmen Sie die Dauer in Sekunden, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

Wenn Sie diesen Wert innerhalb der zuvor eingestellten Dauer ändern und speichern, starten Sie den Timer neu.

SNMP-ID:

2.11.91

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen `0123456789`

Default-Wert:

300

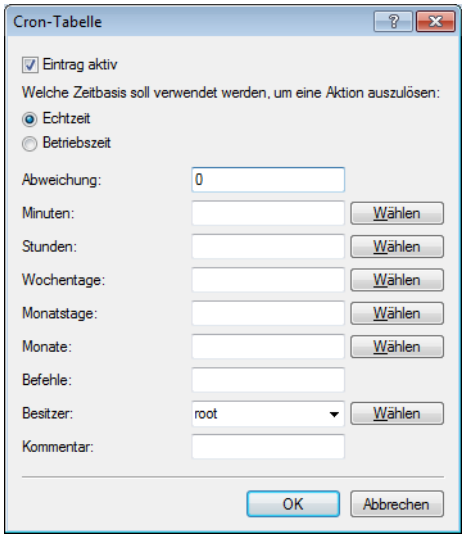
11.2 Kommentarfeld für CRON-Jobs

Ab LCOS 9.00 haben Sie die Möglichkeit, CRON-Jobs mit Kommentaren zu versehen.

11.2.1 Konfiguration der Zeitautomatik

Das folgende Tutorial zeigt Ihnen, wie Sie einen neuen CRON-Job anlegen und welche Parameter Ihnen dabei zur Verfügung stehen.

1. Öffnen Sie in LANconfig die manuelle Konfiguration für Ihr Gerät.
2. Öffnen Sie die **Cron-Tabelle** im Dialog **Datum/Zeit** > **Allgemein** und klicken Sie **Hinzufügen**, um einen neuen CRON-Job zu erstellen.



3. Geben Sie eine Zeitbasis an.
   Die Zeitbasis bestimmt, ob LCOS die zeitliche Steuerung der künftigen Aktion auf Grundlage der Echtzeit oder der Systemlaufzeit des Gerätes ausführt. In der Einstellung **Echtzeit** wertet das System sämtliche Zeit- und Datumsangaben aus. In der Einstellung **Betriebszeit** wertet das System nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.
4. Geben Sie unter **Abweichung** eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der festgelegten Startzeit maximal verzögert wird.
   Die tatsächliche Verzögerungszeit erkennt das Gerät zufällig; sie liegt zwischen Null und der hier eingetragenen Zeit. Bei einer Variation von Null wird der CRON-Job exakt zur festgelegten Zeit ausgeführt.

   Echtzeit-basierte Regeln sind ausschließlich dann ausführbar, wenn Ihr Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.
5. Geben Sie den/die Minute(n), Stunde(n), Wochentag(e), Monatstag(e) und Monat(e), an denen Ihr Gerät das festgelegte Kommando ausführt.
   Wenn Sie keinen Wert eingeben, zieht Ihr Gerät den betreffenden Zeitwert auch nicht in die Steuerung mit ein. Für jeden Parameter haben Sie optional auch die Möglichkeit, eine kommaseparierte Liste von Werten oder einen Wertebereich (in Form von als `<Min.>-<Max.>`) anzugeben.

   Die Syntax des Feldes **Wochentage** entspricht dabei der üblichen CRON-Interpretation:

Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag
0	1	2	3	4	5	6

Das Wochentagsfeld ist auch für Regeln bedeutend, die auf die Betriebszeit bezogen sind. Das ist sinnvoll für Aktionen, die Sie nur einmal beim Start des Gerätes (also bei Null Tagen Betriebszeit) ausführen. So gleichen Sie z. B. den Wochentag gegen die Tage der Betriebszeit ab.

6. Geben Sie unter **Befehle** das auszuführende Kommando oder eine kommaseparierte Liste von Kommandos ein. Ausgeführt werden kann **jede** beliebige Kommandozeilenfunktion.
7. Geben Sie den **Besitzer** des CRON-Jobs an.
   Als Besitzer lässt sich ein im Gerät definierter Administrator auswählen. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.
8. Geben Sie im Feld **Kommentar** eine kurze Beschreibung zu dem CRON-Job ein.
9. Klicken Sie **OK**, um den Eintrag zu speichern. Schreiben Sie anschließend die Konfiguration zurück auf das Gerät.

Weitere Konfigurationsbeispiele:

Zeitbasis	Min.	Std.	W.-Tage	M.-Tage	Monate	Befehl
Echtzeit	0	4	0-6	1-31	1-12	do /so/man/abbau internet
Echtzeit	59	3	0-6	1-31	1-12	mailto:admin@mylancom.de?subject=Zwangstrennung?body=Manuelles Trennen der Internetverbindung
Echtzeit	0	0		1		do /setup/accounting/loeschen
Echtzeit	0	18	1,2,3,4,5			do /so/man/aufbau ZENTRALE

- Der erste Eintrag trennt jeden Morgen um 4:00 Uhr die Verbindung zum Internetprovider (Zwangstrennung).
- Der zweite Eintrag sendet jeden Morgen um 3:59 Uhr, also kurz vor der Zwangstrennung, eine Info-Mail an den Admin.
- Der dritte Eintrag löscht an jedem 1. eines Monats die Accounting-Tabelle.
- Der vierte Eintrag baut an jedem Werktag um 18:00 Uhr eine Verbindung zur Zentrale auf.

Das Gerät führt zeitgesteuerte Regeln mit einer Genauigkeit von einer Minute aus. Bitte achten Sie darauf, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da das Gerät ansonsten die Kommandos der Zeitautomatik ignoriert.

11.2.2 Ergänzungen im Setup-Menü

Kommentar

Über diesen Parameter lässt sich zu dem Eintrag in der CRON-Tabelle ein Kommentar hinterlegen.

SNMP-ID:

2.11.20.12

Pfad Telnet:

Setup > **Config** > **Cron-Tabelle**

Mögliche Werte:

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

Default-Wert:

leer

11.3 LANCAPI standardmäßig deaktiviert

Ab LCOS 9.00 ist LANCAPI für die einzelnen Interfaces per Default deaktiviert.

11.3.1 Ergänzungen im Setup-Menü

Aktiv

Wählen Sie aus, ob und wie dieses Interface für LANCAPI-Clients verfügbar ist.

SNMP-ID:

2.13.6.2

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

Mögliche Werte:

ja

Das Gerät lässt über das ausgewählte Interface sämtliche Rufe zu.

nein

Das Gerät lässt über das ausgewählte Interface keine Rufe zu.

Abgehend

Das Gerät lässt über das ausgewählte Interface ausschließlich abgehende Rufe zu.

Ankommend

Das Gerät lässt über das ausgewählte Interface ausschließlich ankommende Rufe zu.

Default-Wert:

nein

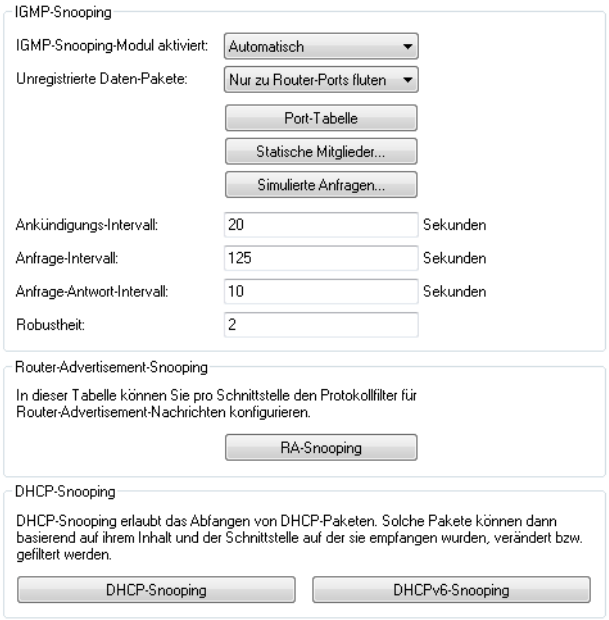
11.4 DHCP-Snooping und DHCP-Option 82

DHCP verfügt ursprünglich über keine Sicherheitsmechanismen zum Schutz von Angriffen auf die Zuweisung der Netzkonfiguration. Sendet z. B. ein Client ein DHCP-Discover-Paket ins Netz, um von einem DHCP-Server eine gültige Netzkonfiguration zu erhalten, kann ein Angreifer gefälschte DHCP-Offer-Pakete an diesen Client senden und ihm so z. B. ein präpariertes Default-Gateway vorsetzen (DHCP-Spoofing).

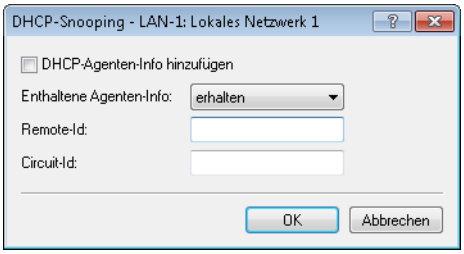
Das DHCP-Snooping ermöglicht Geräten, die DHCP-Pakete empfangen und weiterleiten, diese Datenpakete zu analysieren, zu verändern und anhand bestimmter Kriterien zu filtern. Die zusätzlich eingefügten Informationen über die Herkunft von DHCP-Paketen ermöglichen es einem DHCP-Server einerseits, umfangreiche Netzen besser zu verwalten. Anderseits kann ein Angreifer, in dessen DHCP-Paketen diese Zusatzinformationen fehlen, nicht mehr einfach in DHCP-Verhandlungen zwischen DHCP-Server, DHCP-Relay-Agent und DHCP-Client stören.

Der Access Point unterstützt DHCP-Snooping auf Layer-2. Damit ist es ihm z. B. möglich, Informationen (z. B. die SSID) in die empfangenen DHCP-Pakete des Clients auf dem WLAN einzufügen, bevor er sie anschließend in das LAN weiterleitet. Der Access Point fügt dazu die DHCP Relay Agent Information Option (Option 82) nach RFC 3046 ein.

Im LANconfig können Sie das DHCP-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCP-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



DHCP-Agenten-Info hinzufügen

Bestimmen Sie hier, ob der DHCP-Relay-Agent den ankommenden DHCP-Paketen die DHCP-Option "Relay Agent Info" (Option 82) anfügen bzw. eine vorhandene "Relay Agent Info" bearbeiten soll, bevor er die Anfrage an einen DHCP-Server weiterleitet.

Die "Relay Agent Info" setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Erhaltene Agenten-Info

Bestimmen Sie hier, wie der DHCP-Relay-Agent mit der "Relay Agent Info" in ankommenden DHCP-Datenpaketen umgehen soll. Folgende Einstellungen sind möglich:

- erhalten: In dieser Einstellung leitet der DHCP-Relay-Agent ein DHCP-Paket mit vorhandener "Relay Agent Info" ohne Veränderung an den DHCP-Server weiter.
- ersetzen: In dieser Einstellung ersetzt der DHCP-Relay-Agent eine vorhandene "Relay Agent Info" durch die in den Feldern **Remote-Id** und **Circuit-Id** vorgegebenen Werte.
- Paket verwerfen: In dieser Einstellung löscht der DHCP-Relay-Agent ein DHCP-Paket, das eine "Relay Agent Info" enthält.

Remote-Id

Die Remote-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig den Client, der einen DHCP-Request stellt.

Circuit-Id

Die Circuit-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen DHCP-Request stellt.

Sie können die folgenden Variablen für **Remote-Id** und **Circuit-Id** verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- %n: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- %v: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.
- %s: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

11.4.1 Ergänzungen im Setup-Menü

DHCP-Snooping

Hier können Sie das DHCP-Snooping je Schnittstelle konfigurieren.

SNMP-ID:

2.20.40

Pfad Telnet:

Setup > **LAN-Bridge**

Port

Zeigt das physikalische oder logische Interface an, für das die DHCP-Snooping-Konfiguration gültig ist.

SNMP-ID:

2.20.40.1

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

LAN-x

Alle physikalischen LAN-Schnittstellen

WLAN-x

Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen
P2P-x-x
Alle logischen P2P-Schnittstellen
WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

Agent-Info-hinzufuegen

Bestimmen Sie hier, ob der DHCP-Relay-Agent den ankommenden DHCP-Paketen die DHCP-Option "Relay Agent Info" (Option 82) anfügen bzw. eine vorhandene "Relay Agent Info" bearbeiten soll, bevor er die Anfrage an einen DHCP-Server weiterleitet.

Mit dieser Option übermittelt der Relay-Agent dem DHCP-Server zusätzliche Informationen über die Schnittstelle, über die der Client die Anfrage gestellt hat.

Die "Relay Agent Info" setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Sollten diese beiden Felder leer sein, fügt der DHCP-Relay-Agent auch keine "Relay Agent Info" in die Datenpakete ein.

SNMP-ID:
2.20.40.2

Pfad Telnet:
Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

Ja
Fügt den DHCP-Paketen die "Relay Agent Info" an.
Nein
Diese Einstellung deaktiviert das DHCP-Snooping für diese Schnittstelle.

Default-Wert:

Nein

Behandle-existierendes-Agent-Info

Bestimmen Sie hier, wie der DHCP-Relay-Agent mit der "Relay Agent Info" in ankommenden DHCP-Datenpaketen umgehen soll.

SNMP-ID:
2.20.40.3

Pfad Telnet:
Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

beibehalten

In dieser Einstellung leitet der DHCP-Relay-Agent ein DHCP-Paket mit vorhandener "Relay Agent Info" ohne Veränderung an den DHCP-Server weiter.

ersetzen

In dieser Einstellung ersetzt der DHCP-Relay-Agent eine vorhandene "Relay Agent Info" durch die in den Feldern **Remote-Id** und **Circuit-Id** vorgegebenen Werte.

verwerfen

In dieser Einstellung löscht der DHCP-Relay-Agent ein DHCP-Paket, das eine "Relay Agent Info" enthält.

Default-Wert:

beibehalten

Remote-Id

Die Remote-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig den Client, der einen DHCP-Request stellt.

Sie können die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- `%v`: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- `%p`: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind `%p` und `%i` identisch.
- `%s`: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- `%e`: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.40.4

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

max. 30 Zeichen `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Circuit-Id

Die Circuit-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen DHCP-Request stellt.

Sie können die folgenden Variablen verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- %n: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- %v: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.
- %s: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.40.5

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

max. 30 Zeichen `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

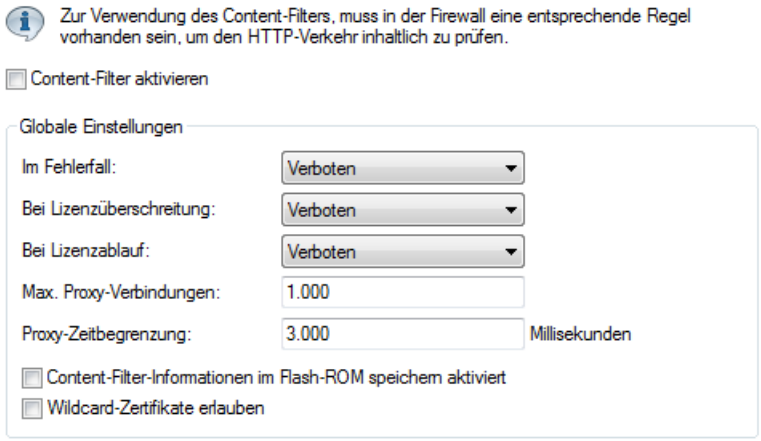
11.5 LLDP über LANconfig aktivieren

Ab LCOS 9.00 lässt sich LLDP auch über LANconfig aktivieren.

Die Aktivierung von LLDP mittels LANconfig erfolgt unter **Schnittstellen** > **LAN**.

11.6 Wildcard-Zertifikate im LANCOM Content Filter

Ab LCOS 9.00 haben Sie die Möglichkeit, im LANCOM Content Filter Wildcard-Zertifikate zu verwenden.



Wildcard-Zertifikate erlauben

Bei Webseiten mit Wildcard-Zertifikaten (bestehend aus CN-Einträgen wie z. B. `*.mydomain.de`) wird durch das Einschalten dieser Funktion die Haupt-Domain (`mydomain.de`) zur Prüfung herangezogen. Die Prüfung erfolgt dabei in dieser Reihenfolge:

- Prüfung des Servernamens im „Client Hello" (abhängig vom verwendeten Webbrowser)
- Prüfung des CN im empfangenen SSL-Zertifikat
- Einträge mit Wildcards werden dabei ignoriert
- Ist der CN nicht verwertbar, wird das Feld „Alternative Name" ausgewertet
- DNS Reverse Lookup der zugehörigen IP-Adresse und Prüfung des so erlangten Hostnamens
- Sind im Zertifikat Wildcards enthalten, wird stattdessen die Haupt-Domain geprüft (entspricht der oben beschriebenen Funktion)
- Prüfung der IP-Adresse

11.6.1 Ergänzungen im Setup-Menü

Wildcard

Bei Webseiten mit Wildcard-Zertifikaten (bestehend aus CN-Einträgen wie z. B. `*.mydomain.de`) wird durch das Einschalten dieser Funktion die Haupt-Domain (`mydomain.de`) zur Prüfung herangezogen. Die Prüfung erfolgt dabei in dieser Reihenfolge:

- Prüfung des Servernamens im „Client Hello" (abhängig vom verwendeten Webbrowser)
- Prüfung des CN im empfangenen SSL-Zertifikat
- Einträge mit Wildcards werden dabei ignoriert
- Ist der CN nicht verwertbar, wird das Feld „Alternative Name" ausgewertet
- DNS Reverse Lookup der zugehörigen IP-Adresse und Prüfung des so erlangten Hostnamens
- Sind im Zertifikat Wildcards enthalten, wird stattdessen die Haupt-Domain geprüft (entspricht der oben beschriebenen Funktion)
- Prüfung der IP-Adresse

SNMP-ID:

2.41.2.2.29

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Mögliche Werte:

nein
ja

Default-Wert:

nein