connecting your business

Addendum

LCOS 9.20 RC2

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 9.20

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 9.20 gegenüber der vorherigen Version.

2 Übersicht über die Neuerungen der LCOS-Version 9.20

In der LCOS-Version 9.20 wurde eine Vielzahl neuer Features umgesetzt.

Tabelle 1: Neue Features der LCOS-Version 9.20

Voice over Secure IP (VoSIP) - Verschlüsselte IP-Telefonie	Ein echtes Plus an Sicherheit im Bereich Telefonie! Der in der LANCOM All-IP Option integrierte Voice Call Manager mit Session Border Controller-Funktionalität unterstützt ab sofort Voice over Secure IP (VoSIP). Die Verschlüsselung von Signalisierungs- und Sprachdaten (SIPS/SRTP) ermöglicht abhörsichere Telefonie an IP-basierten Amtsanschlüssen.
SNMPv3	Ab sofort profitieren alle LANCOM Kunden von mehr Sicherheit bei der Netzwerküberwachung durch die Unterstützung von SNMPv3 (Simple Network Management Protocol Version 3). Dieses Protokoll vereint komfortables Geräte-Monitoring mit hoher Sicherheit dank verschlüsselter Datenkommunikation - ganz ohne Konfigurationsänderungen, da automatisch aktiviert!
Maximale WLAN-Qualität	Spürbar mehr Performance, Robustheit und Reichweite für LANCOM Access Points, WLAN-Router und WLAN-Controller: Ab LCOS 9.20 unterstützen alle WLAN-Geräte die Highlight-Features Airtime Fairness, Adaptive RF Optimization, Wireless Intrusion Detection System und viele weitere Funktionen. Darüber hinaus genießen LANCOM User und Administratoren dank umfangreicher Qualitätsverbesserungen das beste WLAN-Erlebnis aller Zeiten!
IKEv2	IKEv2 ermöglicht einen schnelleren und sichereren Verbindungsaufbau von VPN-Tunneln. Erstmals wird darüber hinaus die VPN-verschlüsselte Vernetzung von IPv6-basierten Standorten möglich - auch im Mischbetrieb mit IPv4.
IKEv1 mit IPv6-Unterstützung	Neben der Unterstützung von IKEv2 lassen sich ab LCOS 9.20 auch über IKEv1 VPN-Verbindungen zwischen IPv6-Netzwerken aushandeln.
BGP	Effiziente VPN-Vernetzung von Standortorten dank dynamischem Routing in mittleren bis großen Netzen. BGP (Border Gateway Protocol) sorgt für eine optimale Wegwahl aller vernetzten Router durch den Austausch ihrer besten Pfade aus ihrer Routing-Tabelle.

Erweiterte Telefonie-Funktionen

Der in der LANCOM All-IP Option integrierte Voice Call Manager (VCM) unterstützt zahlreiche zusätzliche Funktionen wie gleichzeitige Anrufsignalisierung über mehrere interne ISDN-Busse, integrierte DTMF-Umwandlung für eine zuverlässige Übertragung von Wähltönen über All-IP-Leitungen sowie die Unterstützung von SIP-Paketen über TCP-Verbindungen.

Logging von DNS-Anfragen

Client-seitige DNS-Anfragen können zur Protokollierung und Auswertung an einen externen SYSLOG-Server gesendet werden.

Performance-Messung über iPerf

Mit dem im LCOS integrierten Tool "iPerf" messen Sie exakt den maximalen, sowie den aktuellen TCP- und UDP-Durchsatz zwischen zwei Geräten im Netzwerk. Daraus ableitbare Bandbreitenverluste können so als Engpass im Netzwerk aufgedeckt und behoben werden.

Höhere Komplexität bei Gerätepasswörtern

Höhere Sicherheit bei der Verwendung von Passwörtern durch neue Vergaberichtlinie für mindestens acht Zeichen bestehend aus Buchstaben, Ziffern und Sonderzeichen.

Adaptive RF Optimization

Dynamische Auswahl des besten WLAN-Kanals

Höherer WLAN-Durchsatz im Funkfeld dank dynamischer Auswahl des besten WLAN-Kanals durch den Access Point bei Kanalstörungen.

Airtime Fairness

Verbesserte Ausnutzung der WLAN-Bandbreite

Bessere WLAN-Performance durch effiziente Ausnutzung der zur Verfügung stehenden Bandbreite dank einer fairen Aufteilung der WLAN-Übertragungszeiten unter den aktiven Clients.

Wireless IDS

Erkennung von Angriffen oder auffälligem Verhalten von Clients in der WLAN-Infrastruktur durch dauerhafte Überwachung des Funkfeldes. Tritt ein angriffähnliches Ereignis mit einer bestimmten Häufigkeit in einem definierten Zeitraum auf, wird eine Warnung via E-Mail, SYSLOG-Nachricht, SNMP oder LANmonitor ausgegeben.

Adaptive Transmission Power

Ideal für professionelle Backup-Szenarien in WLAN-Umgebungen: Bei Ausfall eines Access Points wird die Sendeleistung der verbleibenden Access Points automatisch erhöht, sodass eine vollständige WLAN-Abdeckung stets sichergestellt ist.

Konfigurierbare Datenraten je SSID

Die für die Kommunikation zwischen Access Point und WLAN Clients vorgegebenen Datenraten stehen nun detaillierte Konfigurationsmöglichkeiten zur Verfügung - ein echter Zugewinn an Flexibilität. So können z. B. Datenraten, die aufgrund der Umgebungsbedingungen nicht sinnvoll nutzbar sind, von der Verwendung ausgeschlossen werden.

Flexible Gültigkeit von Public Spot-Zugängen

Ab LCOS 9.20 kann die gebuchte Bandbreite auf den Public Spot Vouchern dargestellt werden. Zudem kann die Gültigkeit (Ablaufzeitpunkt) von Vouchern mit kürzeren Zeiteinheiten (Tage, Stunden, Minuten) gestaltet werden - ideal für Szenarien mit hoher Kundenfrequenz bei gleichzeitig kurzer Verweildauer.

Controller-less WLAN-Management

Die LANCOM Management Cloud sowie das Management-System LANCOM Large Scale Rollout & Management (LSR) ermöglichen die automatische Inbetriebnahme und Konfigurationsvergabe ("Zero-touch Deployment") sowie das Management von LANCOM Access.

3 Konfiguration

3.1 Speicherung von Passwort-Formularfeldern im Browser verhindern

Ab LCOS-Version 9.20 besteht die Möglichkeit, im Webbrowser die Speicherung von Passwörten im Login-Formularfeld von WEBconfig zu unterdrücken.

3.1.1 Speicherung von Passwort-Formularfeldern im Browser verhindern

Eingabe-Dialoge auf Webseiten bieten den Webbrowsern die Möglichkeit, eingegebene Passwörter zu speichern, um sie bei einem erneuten Seitenaufruf komfortabel abzurufen. Diese Funktion der Webbrowser erleichtert Schadsoftware das Auslesen der vertraulichen Formulardaten.

Um die manuelle Eingabe des Login-Passwortes bei jedem erneuten Seitenaufruf zu erzwingen, deaktivieren Sie im WEBconfig unter **Setup** > **HTTP** > **Verhindere-Passwort-Vervollstaendigung** die Speicherung von Formularfeld-Inhalten mit der Einstellung „Ja“.

3.1.2 Ergänzungen im Setup-Menü

Verhindere-Passwort-Vervollstaendigung

Dieser Schalter legt fest, ob der WEBconfig-Login-Dialog dem Browser des Anwenders erlaubt, den Inhalt des Passwort-Formularfeldes zur späteren Autovervollständigung zu speichern.

SNMP-ID:

2.21.22

Pfad Telnet:

Setup > **HTTP**

Mögliche Werte:

nein

Der Browser darf den Inhalt des Passwort-Formularfeldes nicht speichern. Die Eingabe-Maske von WEBconfig erzwingt somit die manuelle Eingabe des Passwortes durch den Anwender.

ja

Der Browser speichert die Eingabe des Passwort-Formularfeldes und füllt das Feld bei einem erneuten Aufruf des Login-Dialoges automatisch.

Default-Wert:

nein

3.2 DHCP Rollout-Agent

Ab LCOS-Version 9.20 fragt ein Gerät im unkonfigurierten Zustand die Vendor-spezifische DHCP-Option 43 beim DHCP-Server an. Der DHCP-Server kann daraufhin weiterführende Informationen zur Kontaktaufnahme mit dem LSR oder einem anderen Rollout-Server an das Gerät senden.

Folgende LANCOM-Geräte unterstützen diese Funktion: L-3xx, L-4xx, L-13xx, L-151 LN-830, L-822, 178x-Serie, OAPs, IAPs, WLCs, 7100(+), 9100(+), 831A, 1631E, E-Serie.

3.2.1 LSR-Informationen über DHCP-Server erhalten (Zero-Touch-Rollout)

Ein unkonfiguriertes LANCOM-Gerät startet mit einem aktivierten DHCP-Client und bezieht dadurch IP-Adresse, Netzmaske, DNS-Adresse und Gateway-Adresse vom DHCP-Server im Netzwerk.

Über die Vendor-spezifische DHCP-Option 43 sendet ein entsprechend konfigurierter DHCP-Server u. a. auch Informationen darüber, wie ein LSR-Server (Large Scale Rollout) zu erreichen ist. Der Rollout-Agent des LANCOM-Gerätes wertet diese Informationen aus, kontaktiert den LSR-Server und bezieht anschließend im Rahmen der bestehenden Rollout-Strategie seine Konfiguration oder aktualisiert seine Firmware.

Diese Funktion erleichtert den Rollout-Prozess, da keine Vorkonfiguration der Geräte mehr notwendig ist.

Die Verbindung zum LSR-Server erfolgt über HTTP, HTTPS oder TFTP, wobei im LANCOM-Gerät für eine sichere Verbindung ein entsprechendes SSL-Zertifikat gespeichert sein muss.

Eine (auch partielle) Vorkonfiguration des Rollout-Agents ist ebenfalls möglich. So kann z. B. die vom DHCP-Server gesendete Rollout-Server-URL übernommen, eine Projektnummer im Gerät allerdings vorkonfiguriert werden.

Konfiguration des Zero-Touch-Rollouts

Ausgangslage

In einem Filial-Rollout ist es auf Grund der hohen Zahl an Geräten erforderlich, die LANCOM-Geräte nicht vorkonfigurieren zu müssen. Sie sollen stattdessen in Betrieb gehen, nachdem sie die Konfiguration von einem zentralen LSR-Server erhalten haben, vergleichbar dem „Zero-Touch-Management" bei einem WLC.

Rahmenbedingungen

Damit dieser „Zero-Touch-Rollout" über den Rollout-Agenten des Gerätes funktioniert, sind einige Rahmenbedingungen zu erfüllen:

- Es muss ein zentraler Rollout-Server verfügbar und für die Zero-Touch-Geräte über HTTP/HTTPS erreichbar sein.
- Im Filial-Netz muss DHCP aktiv sein. D. h.,
  - ein filialnetz-eigener DHCP-Server ist erreichbar oder
  - ein DHCP-Relay-Server im Filialnetz vermittelt die DHCP-Datenpakete zwischen den Geräten im Filialnetz und einem DHCP-Server in der Zentrale.
- Der DHCP-Server muss die DHCP-Option 43 ausliefern können.

Der DHCP-Server überträgt sensitive Daten wie z. B. das Rollout-Passwort ungesichert als DHCP-Nachricht. Es ist also darauf zu achten, die Daten nur über entsprechend abgesicherte Verbindungen zu transportieren.

Ablauf

Der Konfigurations-Rollout läuft wie folgt ab:

1. Das unkonfigurierte Gerät wird an das Filial-Netz angeschlossen.

2. Über den DHCP-Server bezieht das Gerät die erforderlichen Verbindungsdaten wie IP-Adresse, Gateway, Netzmaske, DNS-Adresse und die DHCP-Option 43.
3. Aus der DHCP-Option 43 dekodiert das Gerät die URL des Rollout-Servers sowie zusätzliche Informationen und konfiguriert damit den Rollout-Agenten des Gerätes.
4. Der Rollout-Agent kontaktiert daraufhin den Rollout-Server und führt den Rollout nacheinander in zwei Schritten durch:
   - Firmware-Update
   - Konfigurations-Update

Der Rollout-Agent erwartet, dass der unter der konfigurierten Firmware-Server-URL erreichbare Rollout-Server eine Firmware im `.upx`-Format ausliefert, die er anschließend in das Gerät einspielt.

Nach dem Firmware-Update startet das Gerät neu und kontaktiert den Rollout-Server erneut. Der Rollout-Agent prüft, ob die vom Rollout-Server ausgelieferte Firmware bereits installiert ist. Diese Prüfung ist erfolgreich, da das Gerät im ersten Schritt die aktuelle Firmware erhalten hat. Der Rollout-Agent fährt mit dem Update der Konfiguration bzw. dem Download von Skriptdateien fort. Er erwartet, dass der unter der konfigurierten Config-Server-URL erreichbare Rollout-Server ein Skript im `.lcs`-Format ausliefert, das er anschließend auf in das Gerät einspielt.

Die DHCP-Option 43

Die DHCP-Option 43 ist vendorspezifisch, d. h., jeder Vendor kann selbst entscheiden, wie er diese Option strukturiert und welche Informationen er darin kodiert. Die Option kann mehrere sogenannter Sub-Typen enthalten, die die Daten detaillierter strukturieren.

Für den Rollout-Agenten des Gerätes sind die folgenden Sub-Typen spezifiziert:

Sub-Type 1: Config-Server-URL

Die Angabe der Server-Adresse ist in den folgenden Formaten möglich:

- HTTP, HTTPS, TFTP
- IP-Adresse, FQDN

Beispiele:

- https://rollout:443/
- tftp://10.1.1.1
- http://10.1.1.2/test

Auch die Angabe von LCOS-Variablen ist möglich

Der Rollout-Agent erwartet, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin ein Konfigurations-Skript mit der Erweiterung `.lcs` sendet.

Handelt es sich beim Rollout-Server um einen LSR, muss der Adresse das Präfix `lsr:` vorangestellt sein, z. B. `lsr:https://rollout:443/`. Anschließend baut der Rollout-Agent die korrekte LSR-Rollout-URL aus den Sub-Types 5 und folgende zusammen. Entsprechend sind die Sub-Types ab 5 nur bei der Verwendung dieses Präfixes von Bedeutung.

Handelt es sich beim Rollout-Server um keinen LSR, ist die Angabe der URLs für Config-Server und Firmware-Server von Hand und unter Verwendung von Variablen notwendig.

Sub-Type 2: Firmware-Server-URL

Wie bei Sub-Type 1, allerdings erwartet der Rollout-Agent, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin eine Firmware-Datei mit der Erweiterung `.upx` sendet.

Sub-Type 3: HTTP-Username

Enthält den Usernamen für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 4: HTTP-Password

Enthält das Passwort für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 5: LSR-Projektnummer

Enthält die im Rollout-Server für das erforderliche Rollout-Projekt gespeicherte Projektnummer.

Sub-Type 6: Zusätzliche URL-Parameter für LSR-Keyword

Der Rollout-Agent fügt diesen Inhalt an die konstruierte LSR-URL an (z. B. `?approval=yes`).

Sub-Type 7: Reboot-Time

Gibt die Wartezeit in Minuten für den Restart des Gerätes nach dem Update durch den Rollout-Server an.

Sub-Type 8: Request-Interval

Gibt den Intervall in Minuten an, in dem der Rollout-Agent seine Anfragen an den Rollout-Server sendet.

Sub-Type 9: TAN

Dieser Eintrag enthält die Rollout-TAN.

Sub-Type 10: Gerätenummer

Enthält die Gerätenummer des zu aktualisierenden Gerätes.

Sub-Type 11: Request-Delay

Enthält die Zeit in Minuten, die der Rollout-Agent zwischen Request 1 und Request 2 wartet.

Sub Type 12: Request-Random

Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern. Die folgenden Angaben sind möglich:

0

Die Anfragen erfolgen immer mit fest eingestellten Zeitangaben.

1

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt.

Sub-Type 13: Omit-Certificate-Check

Dieser Wert legt fest, ob der Rollout-Agent die Überprüfung des Rollout-Server-Zertifikats überspringen soll.

Fehlt dieser Sub-Type oder ist sein Inhalt leer, nimmt der Rollout-Agent den Wert „0“ an und prüft somit das Server-Zertifikat.

Beachten Sie bitte, dass die vom Rollout-Server erhaltene Konfiguration den Rollout-Agent zum Abschluss abschalten sollte **(`Operating: no`)**, da das Gerät sonst nach der Reboot-Time rebootet.

Variablen

In den URLs sind alle Variablen verwendbar, die die LCOS-Konsole beinhaltet. Diese Variablen lassen sich in der Konsole über den Befehl `printenv` ausgeben.

Die Angabe der Variablen in den URLs erfolgt mit vorangestelltem „$“ (z. B. `$__SERIALNO`).

Erzeugung der DHCP-Option 43

Die Erzeugung der DHCP-Option 43 erfolgt auf Grundlage der *RFC 2132, Abschnitt 8.4*.

Bei Verwendung eines ISC DHCPd DHCP-Server kann die Option 43 passend mit dem folgenden Konfigurationsabschnitt beispielhaft erzeugt werden:

Innerhalb der allgemeinen Konfiguration

```
option space Rollout;
option Rollout.config-server code 1 = text;
option Rollout.firmware-server code 2 = text;
option Rollout.HTTP-Username code 3 = text;
option Rollout.HTTP-Password code 4 = text;
option Rollout.Projectnumber code 5 = text;
option Rollout.AdditionalParams code 6 = text;
option Rollout.RebootTime code 7 = text;
option Rollout.RequestInterval code 8 = text;
option Rollout.Tan code 9 = text;
option Rollout.Devicenumber code 10 = text;
option Rollout.RequestDelay code 11 = text;
option Rollout.RequestRandom code 12 = text;
option Rollout.OmitCertCheck code 13 = text;
```

Innerhalb der Subnetz-spezifischen Konfiguration

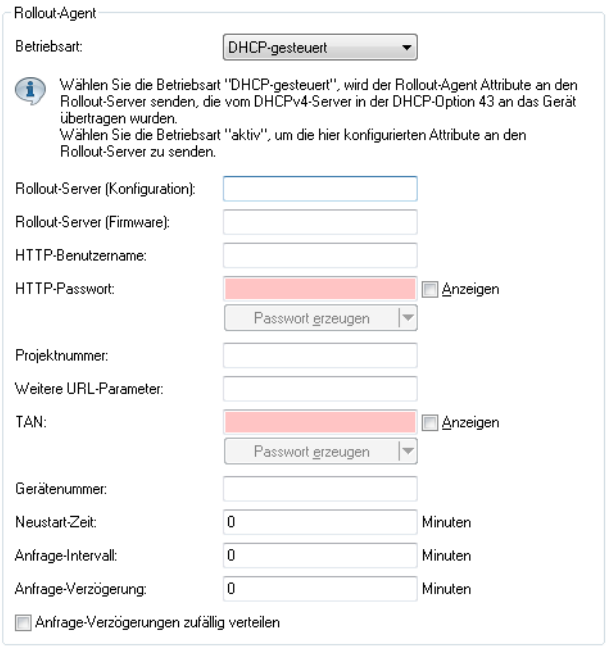
```
vendor-option-space Rollout;
 option Rollout.config-server "LSR:https://10.200.50.1:443";
 option Rollout.firmware-server "LSR:https:// 10.200.50.1:443";
 option Rollout.HTTP-Username "RolloutUser";
 option Rollout.HTTP-Password "Secret";
 option Rollout.Projectnumber "1";
 option Rollout.RebootTime "300";
 option Rollout.RequestDelay "20";
 option Rollout.RequestRandom "0";
 option Rollout.OmitCertCheck "2";
```

Andere DHCP-Server (z. B. der Microsoft DHCP-Server) lassen keine Definition der Option 43 in der Konfiguration zu. Hier muss die vom Server als Option 43 auszuliefernde Bytefolge vorgefertigt in die Konfiguration eingefügt werden.

Um die Bytefolge nicht manuell erzeugen zu müssen, kann dies auch mit dem auf der folgenden Seite verlinkten Python-Skript erfolgen: *wiki.snom.com/Category:HowTo:Option_43*.

Konfiguration mit LANconfig

Mit LANconfig konfigurieren Sie den Rollout-Agent über **Management** > **Rollout-Agent**.



Betriebsart

Wählen Sie die Betriebsart „DHCP-gesteuert“, wenn der Rollout-Agent des Gerätes die Attribute an den Rollout-Server übertragen soll, die er zuvor über die Vendor-spezifische DHCP-Option 43 vom DHCP-Server erhalten hat. In der Betriebsart „Aktiv“ überträgt das Gerät die in diesem Dialog konfigurierten Attribute (z. B., wenn im Netzwerk kein DHCP verfügbar ist). Die Betriebsart „Aus“ deaktiviert den Rollout-Agenten.

Die Betriebsart „DHCP-gesteuert“ überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

Rollout-Server (Konfiguration)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

Rollout-Server (Firmware)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

HTTP-Benutzername

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

HTTP-Passwort

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

Projektnummer

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

Weitere URL-Parameter

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

Gerätenummer

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

Neustart-Zeit

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

Anfrage-Intervall

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.

Bei einem Wert „0“ startet der erneute Versuch in 1 Minute.

Anfrage-Verzögerung

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

Anfrage-Verzögerung zufällig verteilen

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

3.2.2 Ergänzungen im Setup-Menü

Rollout-Agent

In diesem Menü konfigurieren Sie die Einstellungen des Rollout-Agenten.

SNMP-ID:

2.11.92

Pfad Telnet:

Setup > **Config**

Aktiviert

Mit diesem Eintrag legen Sie die Funktionsweise des Rollout-Agenten fest.

SNMP-ID:

2.11.92.1

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

Nein

Der Rollout-Agent ist deaktiviert.

Ja

Der Rollout-Agent ist aktiviert und überträgt die im Gerät konfigurierten Rollout-Daten an den Rollout-Server.

DHCP-initiiert

Der Rollout-Agent ist aktiviert. Er wertet die Informationen aus, die er über den DHCP-Server in der DHCP-Option 43 erhalten hat.

Die Betriebsart „DHCP-initiiert" überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

Default-Wert:

DHCP-initiiert

Konfigurations-Server

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

SNMP-ID:

2.11.92.2

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Firmware-Server

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

SNMP-ID:

2.11.92.3

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Username

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

SNMP-ID:

2.11.92.4

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Passwort

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

SNMP-ID:

2.11.92.5

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Projekt-Nummer

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

SNMP-ID:

2.11.92.6

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Zusaetzliche-Parameter

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

SNMP-ID:

2.11.92.7

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Reboot-Zeit

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

SNMP-ID:

2.11.92.8

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

0

Request-Interval

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.

SNMP-ID:

2.11.92.9

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Der erneute Versuch startet nach 1 Minute.

TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

SNMP-ID:

2.11.92.10

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Geraete-Nummer

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

SNMP-ID:

2.11.92.11

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

leer

Request-Verzoegerung

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

SNMP-ID:

2.11.92.12

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

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

Default-Wert:

0

Request-Zeit-Verteilung

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

SNMP-ID:

2.11.92.13

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Zertifikats-Check-unterlassen

Legt fest, ob bei HTTPS-Verbindungen eine Überprüfung des Server-Zertifikates erfolgen soll.

SNMP-ID:

2.11.92.14

Pfad Telnet:

Setup > **Config** > **Rollout-Agent**

Mögliche Werte:

Nein

Ein Zertifikats-Check wird durchgeführt.

Ja

Es wird kein Zertifikats-Check durchgeführt.

Default-Wert:

Nein

3.3 Unterstützung ChaCha20/Poly1305 für SSH-Zugriff

Ab Version 9.20 unterstützt LCOS zusätzlich die folgenden Cipher-Algorithmen für Zugriff über SSH:

- chacha20-poly1305
- aes128-gcm
- aes256-gcm

3.3.1 Ergänzungen im Setup-Menü

Cipher-Algorithmen

Die Cipher-Algorithmen dienen zum Verschlüsseln und Entschlüsseln von Daten. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

SNMP-ID:

2.11.28.1

Pfad Telnet:

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

Mögliche Werte:

3des-cbc
3des-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
blowfish-ctr
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
chacha20-poly1305
aes128-gcm
aes256-gcm

Default-Wert:

3des-cbc

3des-ctr

arcfour

arcfour128

arcfour256

blowfish-cbc

blowfish-ctr

aes128-cbc

aes192-cbc

aes256-cbc

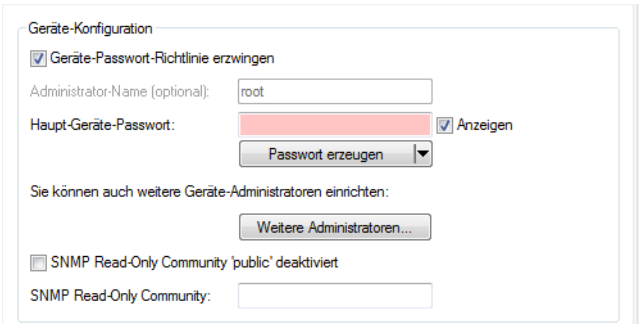
aes128-ctr

aes192-ctr

aes256-ctr

3.4 Passwortkomplexität bei Gerätepasswort erzwingen

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, bei der Vergabe von Gerätekennwörtern eine vordefinierte Passwortrichtlinie zu erzwingen.



Der Schalter **Geräte-Passwort-Richtlinie erzwingen** legt die folgenden Richtlinien für das Hauptgeräte- und die Administrator-Passwörter fest:

- Die Passwortlänge beträgt mindestens 8 Zeichen.
- Das Passwort beinhaltet mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

Beachten Sie bitte, dass sich die Aktivierung dieser Funktion nicht auf aktuelle Passwörter auswirkt. Nur bei Änderungen der Passwörter werden diese auf ihre Richtlinienkonformität überprüft.

3.4.1 Ergänzungen im Setup-Menü

Password-Regeln-Erzwingen

Mit diesem Eintrag haben Sie die Möglichkeit, das Erzwingen von Passwort-Regeln zu aktivieren oder zu deaktivieren.

SNMP-ID:

2.11.93

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

nein

Das Erzwingen von Passwort-Regeln ist deaktiviert.

ja

Das Erzwingen von Passwort-Regeln ist aktiviert.

Default-Wert:

ja

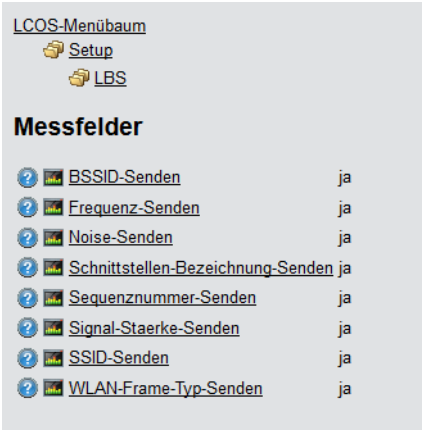
3.5 LBS-Server 1.1: Elemente in LBS-Messfeldern auswählbar machen

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, die zu übertragenden Elemente der LBS-Messfelder über WEBconfig auszuwählen.

Bislang versendete ein AP oder WLC für jeden Management-Frame alle verfügbaren Daten, was ein erhöhtes Overhead-Aufkommen zur Folge hatte.

3.5.1 Elemente in LBS-Messfeldern mit WEBconfig auswählbar machen

Auf einem AP aktivieren oder deaktivieren Sie die einzelnen Elemente der LANCOM Location Based Services Messfelder im LCOS-Menübaum unter **Setup** > **LBS** > **Messfelder**.



Die Elemente **clientid**, **deviceid** und **timestamp** sind daher Pflichtfelder und werden in der Elementauswahl nicht auswählbar.

BSSID-Senden

Legt fest, ob das Gerät die BSSID, die der WLAN-Client in seinen Management-Frames angegeben hat, an den LBS-Server übermittelt.

Frequenz-Senden

Legt fest, ob die Frequenz des Gerätes an den LBS-Server übermittelt wird.

Noise-Senden

Legt fest, ob das Gerät den Rauschwert an den LBS-Server übermittelt.

Schnittstellen-Bezeichnung-Senden

Legt fest, ob das Gerät die Bezeichnung der verwendeten Schnittstelle an den LBS-Server übermittelt.

Sequenznummer-Senden

Legt fest, ob die Sequenznummer gesendet wird.

Signal-Staerke-Senden

Legt fest, ob die Signalstärke, mit der der WLAN-Client gesehen wurde, an den LBS-Server übermittelt wird.

SSID-Senden

Legt fest, ob das Gerät die SSID, die der WLAN-Client in seinen Management-Frames angegeben hat, an den LBS-Server übermittelt.

WLAN-Frame-Typ-Senden

Legt fest, ob das Gerät den WLAN-Frame-Typ an den LBS-Server sendet.

Auf einem WLC finden Sie die LBS-Messfelder im LCOS-Menübaum unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**.

3.5.2 Ergänzungen im Setup-Menü

Messfelder

Dieses Menü beinhaltet die Einstellungen der LBS-Messfelder.

SNMP-ID:

2.100.16

Pfad Telnet:

Setup > **LBS**

Sequenznummer-Senden

Dieser Eintrag legt fest, ob die Sequenznummer gesendet wird.

SNMP-ID:

2.100.16.1

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

SSID-Senden

Legt fest, ob das Gerät die SSID, die der WLAN-Client in seinen Management-Frames angegeben hat, an den LBS-Server übermittelt.

SNMP-ID:

2.100.16.2

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Schnittstellen-Bezeichnung-Senden

Dieser Eintrag legt fest, ob das Gerät die Bezeichnung der verwendeten Schnittstelle an den LBS-Server übermittelt.

SNMP-ID:

2.100.16.3

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

BSSID-Senden

Legt fest, ob das Gerät die BSSID, die der WLAN-Client in seinen Management-Frames angegeben hat, an den LBS-Server übermittelt.

SNMP-ID:

2.100.16.4

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Signal-Staerke-Senden

Legt fest, ob die Signalstärke, mit der der WLAN-Client gesehen wurde, an den LBS-Server übermittelt wird.

SNMP-ID:

2.100.16.5

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Frequenz-Senden

Dieser Eintrag legt fest, ob die Frequenz des Gerätes an den LBS-Server übermittelt wird.

SNMP-ID:

2.100.16.6

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Noise-Senden

Legt fest, ob das Gerät den Rauschwert an den LBS-Server übermittelt.

SNMP-ID:

2.100.16.7

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

WLAN-Frame-Typ-Senden

Legt fest, ob das Gerät den WLAN-Frame-Typ an den LBS-Server sendet.

SNMP-ID:

2.100.16.8

Pfad Telnet:

Setup > **LBS** > **Messfelder**

Mögliche Werte:

ja
nein

Default-Wert:

ja

3.6 Verhinderung der Speicherung von WEBconfig-Passwort-Formularfeldern

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, die Autovervollständigung von Passwortfeldern zu deaktivieren.

3.6.1 Ergänzungen im Setup-Menü

Verhindere-Passwort-Vervollstaendigung

Dieser Schalter legt fest, ob der WEBconfig-Login-Dialog dem Browser des Anwenders erlaubt, den Inhalt des Passwort-Formularfeldes zur späteren Autovervollständigung zu speichern.

SNMP-ID:

2.21.22

Pfad Telnet:

Setup > **HTTP**

Mögliche Werte:

nein

Der Browser darf den Inhalt des Passwort-Formularfeldes nicht speichern. Die Eingabe-Maske von WEBconfig erzwingt somit die manuelle Eingabe des Passwortes durch den Anwender.

ja

Der Browser speichert die Eingabe des Passwort-Formularfeldes und füllt das Feld bei einem erneuten Aufruf des Login-Dialoges automatisch.

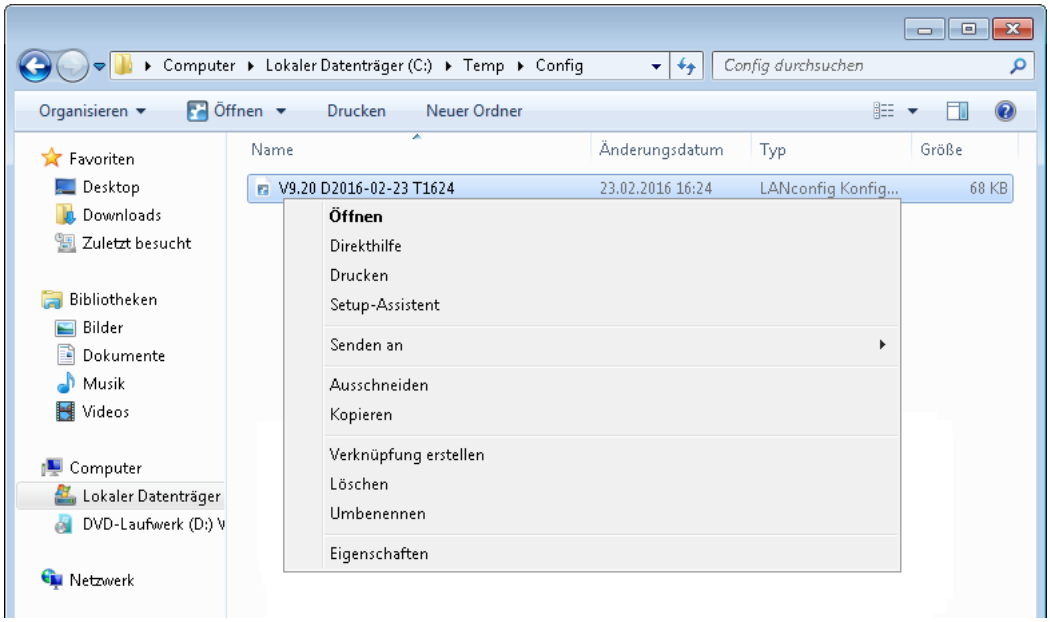
Default-Wert:

nein

3.7 LANconfig: Icon für *.LCS-Dateien im Windows-Explorer

Ab LCOS-Version 9.20 zeigt der Windows-Explorer für *.LCS-Dateien ein entsprechendes Icon an. Über den Kontextdialog oder über einen Doppelklick auf die Datei öffnet sich die LANconfig-Direkthilfe.

Über den Kontextdialog des Windows-Explorers können Sie die folgenden Funktionen ausführen:



Öffnen

Dieser Menüpunkt öffnet die Konfiguration der Datei über LANconfig.

Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

Direkthilfe

Dieser Menüpunkt öffnet einen Hilfetext, der Benutzerinformationen über den Umgang mit dieser Datei gibt.

Drucken

Mit diesem Menüpunkt drucken Sie die Datei aus.

Setup-Assistent

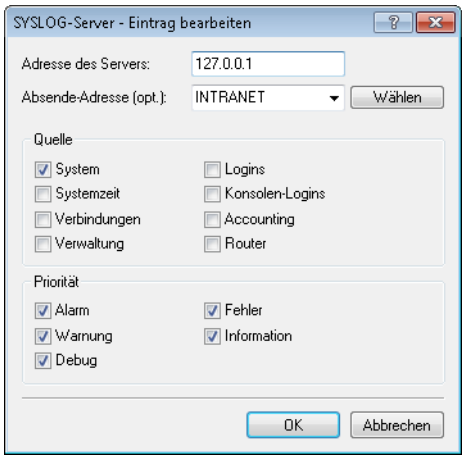
Dieser Menüpunkt startet den LANconfig-Setup-Assistenten.

Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

4 Diagnose

4.1 Angabe der SYSLOG-Serveradresse als IPv6-Adresse oder DNS-Name

Ab LCOS-Version 9.20 ist die Adressangabe eines SYSLOG-Servers zusätzlich in Form einer IPv6-Adresse oder eines DNS-Namens möglich.



Adresse des Servers

Legen Sie die IP-Adresse des SYSLOG-Servers fest. Die Angabe ist möglich in Form einer IPv4-/IPv6-Adresse oder eines Hostnamens.

4.2 IPv6-Unterstützung für LCOScap

Ab LCOS-Version 9.20 unterstützt LCOScap auch IPv6-Verbindungen.

Der LCOScap-Client kann sich somit sowohl über IPv4 als auch über IPv6 mit dem Gerät verbinden.

5 Routing und WAN-Verbindungen

5.1 Border Gateway Protokoll Version 4 (BGPv4)

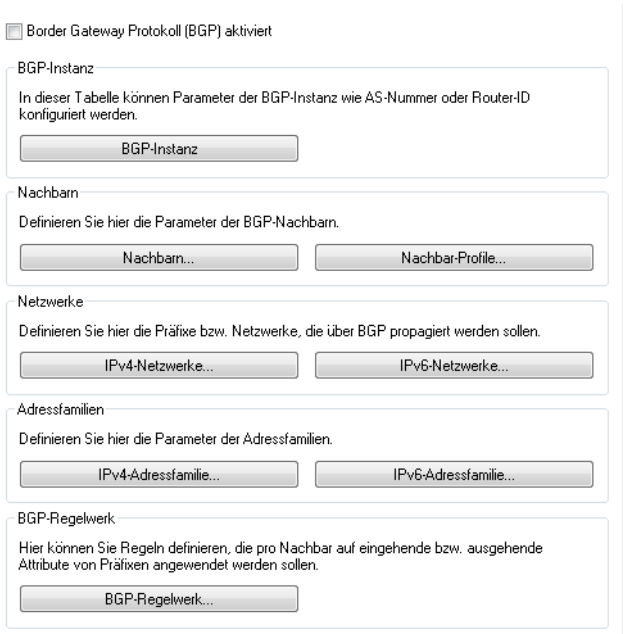
Ab LCOS-Version 9.20 ist die Verwendung des Border Gateway Protokolls Version 4 möglich.

5.1.1 Border Gateway Protokoll Version 4 (BGPv4)

Das Netzwerk eines Netzproviders bezeichnet man auch als „Autonomes System“ (AS). Das Border Gateway Protokoll Version 4 (BGPv4) dient dazu, Routinginformationen zwischen autonomen Systemen auszutauschen (eBGP: External BGP) und diese Informationen an die Router des eigenen AS zu verteilen (iBGP: Internal BGP).

BGPv4 mit LANconfig konfigurieren

Um BGPv4 mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Routing Protokolle** > **BGP**.



BGP aktivieren

Um die BGP-Funktion zu aktivieren, markieren Sie die Option **Border Gateway Protokoll (BGP) aktiviert**.

BGP-Instanz

LCOS ordnet die BGP-Konfiguration des BGP-Routers einer sogenannten **BGP-Instanz** zu. Diese BGP-Instanz enthält z. B. die AS-Nummer und die Router-ID des Routers.

Aktuell unterstützt LCOS nur eine BGP-Instanz gleichzeitig.

Nachbarn

Als **Nachbarn** gelten die BGP-Gateways anderer autonomer Systeme. Die autonomen Systeme müssen dabei nicht direkt benachbart, aber mindestens einem benachbarten BGP-Gateway bekannt sein.

Zur komfortablen Konfiguration der BGP-Nachbarn erfolgt die Verwaltung über **Nachbar-Profile**.

Netzwerke

Der BGP-Router propagiert an die BGP-Nachbarn, welche Netzwerke er verwaltet.

Adressfamilien

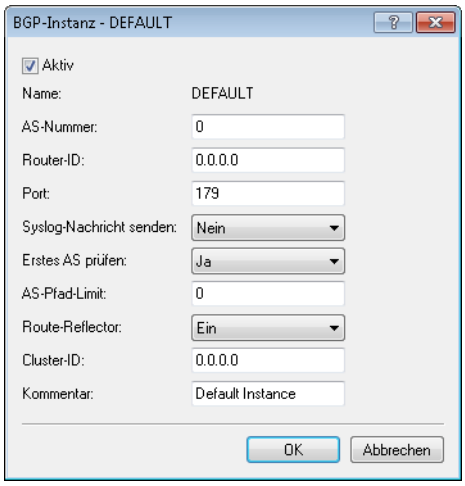
Der BGP-Router ordnet die BGP-Nachbarn Adressfamilien zu, um die Kommunikation mit diesen Nachbarn komfortabel zu verwalten.

BGP-Regelwerk

Filterregeln ermöglichen dem BGP-Router zu entscheiden, wie er ausgehende und ankommende BGP-Nachrichten behandeln soll.

BGP-Instanz

Die BGP-Instanz des Gerätes konfigurieren Sie unter **BGP-Instanz**.



Aktiv

Aktiviert oder deaktiviert diese BGP-Instanz.

Diese Einstellung ist nur wirksam, wenn BGP im Gerät aktiv ist.

Name

Enthält den Namen der BGP-Instanz.

Da das Gerät nur eine BGP-Instanz gleichzeitig unterstützt, ist bereits ein Eintrag „DEFAULT" vorgegeben.

AS-Nummer

Die AS-Nummer, die dieser BGP-Instanz zugeordnet ist.

Ein Verbindungsaufbau zu einem BGP-Router, der keine 32Bit-großen AS-Nummern unterstützt, ist nur dann möglich, wenn Sie hier eine 16Bit-AS-Nummer eintragen (kleiner 65536).

Router-ID

Die Router-ID (IPv4-Adresse), die dieser BGP-Instanz zugeordnet ist.

Die Router-ID muss unter allen Nachbarn eines BGP-Routers eindeutig sein.

Bei Verwendung von IPv6-Verbindungen vergeben Sie hier eine fiktive IPv4-Adresse oder eine beliebige IPv4-Adresse des Routers.

Port

Enthält den Port, auf dem die BGP-Instanz auf ankommende Verbindungen von Nachbarn reagiert.

Syslog-Nachricht senden

Das Gerät kann Ereignisse wie Verbindungsabbrüche von Nachbarn, die mit dieser BGP-Instanz verbunden sind, im Syslog speichern. Mit dieser Option aktivieren oder deaktivieren Sie diese Funktion.

Erstes AS prüfen

Prüft, ob die erste AS-Nummer im AS-Pfad bei empfangenen Update-Nachrichten der AS-Nummer des Nachbarn entspricht. Falls dies nicht der Fall ist, wird diese Route verworfen.

Diese Prüfung muss deaktiviert werden, wenn der Router mit einem BGP-Route-Server verbunden ist, der zwar Routen verteilt, aber nicht selbst im Routing-Pfad liegt bzw. sein eigenes AS in den AS-Pfad einfügt.

AS-Pfad-Limit

Maximale Anzahl von erlaubten AS-Nummern im AS-Pfad bei empfangenen Update-Nachrichten. Wird das Limit überschritten, verwirft das Gerät die entsprechende Route. Ein AS-Pfad-Limit kann vor Nachrichten von fehlerhaft konfigurierten Routern schützen, die zu lange AS-Pfade ankündigen.

Route-Reflector

Definiert, ob der Router die Funktion eines Route-Reflectors übernehmen soll.

Beim Einsatz von iBGP müssen normalerweise alle BGP-Router voll vermascht sein, d. h., jeder BGP-Router muss zu jedem BGP-Router eine BGP-Verbindung aufgebaut haben. Ein Route-Reflector hebt diese Anforderung auf und ermöglicht es, dass iBGP-Router z. B. eine sternförmige Topologie aufbauen können. Der Route-Reflector leitet dann iBGP-Routen an alle Route-Reflector-Clients weiter.

Ein Route-Reflector kann sowohl Route-Reflector-Clients als auch normale BGP-Clients bedienen. Auf dem Client muss in beiden Fällen keine gesonderte Konfiguration erfolgen.

Cluster-ID

Cluster-ID des Routers, falls dieser als Route-Reflector konfiguriert wird. Die Eingabe erfolgt im Format einer IPv4-Adresse.

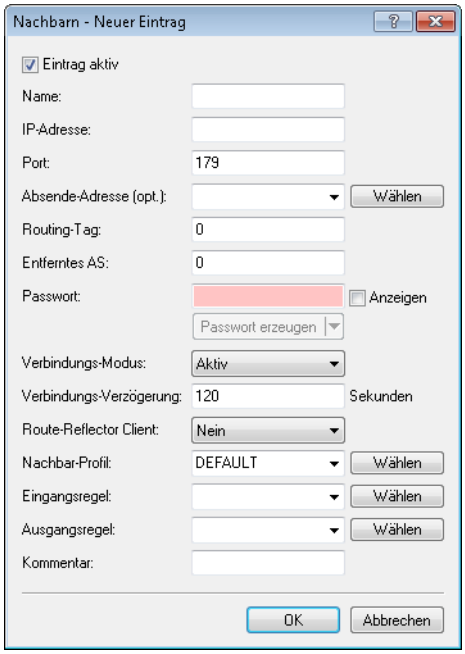
Kommentar

Kommentar zu dieser BGP-Instanz.

Nachbarn

BGP-Nachbarn

Die BGP-Nachbarn des Gerätes konfigurieren Sie unter **Nachbarn**.



Eintrag aktiv

Aktiviert oder deaktiviert den Eintrag für diesen BGP-Nachbarn.

Die Aktivierung des BGP-Nachbarn startet ggf. einen BGP-Verbindungsaufbau.

Bei deaktiviertem BGP-Nachbarn ist eine Verbindung zu ihm nicht möglich.

Name

Enthält den Namen des BGP-Nachbarn.

IP-Adresse

Enthält die IP-Adresse (IPv4 oder IPv6) des BGP-Nachbarn, zu dem das Gerät in den Verbindungsarten „Aktiv" oder „Verzögert" eine BGP-Verbindung aufbaut.

Alternativ haben Sie die Möglichkeit, ein gesamtes IPv4-Subnetz zu konfigurieren, z. B. 192.168.1.0/24. In diesem Fall akzeptiert der Router BGP-Verbindungen anderer Router aus dem Subnetz 192.168.1.0 mit der Subnetzmaske 255.255.255.0. Dafür ist es erforderlich, den Verbindungs-Modus als "Passiv" zu definieren.

IPv6-Subnetze werden nicht unterstützt.

Dieser Eintrag muss identisch zu der IP-Adresse (z. B. physikalische Interface-Adresse, Loopback-Adresse) sein, die dieser Nachbar bei einer ankommenden Verbindung meldet.

Port

Enthält den Port, auf dem der BGP-Nachbar einkommende BGP-Nachrichten erwartet und den das Gerät entsprechend für ausgehende Verbindungen in den Verbindungsarten „Aktiv" oder „Verzögert" verwendet.

Ankommende Verbindungen nimmt das Gerät auf jedem vom Sender verwendeten Quell-Port an.

Absende-Adresse (opt.)

Enthält die Absender-Adresse (IPv4 oder IPv6), die das Gerät dem BGP-Nachbarn bei einem Verbindungsaufbau mitteilt.

Die Angabe ist optional und nur in den Verbindungsarten „Aktiv“ oder „Verzögert“ relevant.

Routing-Tag

Enthält das Routing-Tag. Stimmt das Routing-Tag nicht mit dem der ankommenden Verbindung überein, verweigert das Gerät den Verbindungsaufbau.

Entferntes AS

Enthält die AS-Nummer des BGP-Nachbarn.

Ist die AS-Nummer des BGP-Nachbarn identisch zur AS-Nummer der eigenen BGP-Instanz des Gerätes, handelt es sich bei dem Nachbarn um einen iBGP-Peer (Internal BGP) innerhalb des eigenen AS.

Passwort

Gerät und BGP-Nachbar übertragen dieses Passwort als MD5-Signatur in den TCP-Paketen, um sich zu authentifizieren.

Ohne die Angabe eines Passwortes ist die Authentifizierung deaktiviert.

Verbindungs-Modus

Bestimmt den Modus, mit dem eine Verbindung vom Gerät zu diesem BGP-Nachbarn zustande kommt. Folgende Modi sind möglich:

- **Aktiv**: In diesem Modus versucht das Gerät eine Verbindung zum BGP-Nachbarn aufzubauen, sobald u. a. eine der folgenden Bedingungen erfüllt ist:
  - Die Konfiguration des BGP-Nachbarn ist komplett.
  - Sie führen im WEBconfig oder über die Konsole die Aktion **Manueller-Start** aus.
  - Sie starten das Gerät.
  - Sie aktivieren die BGP-Instanz unter **Routing-Protokolle** > **BGP** > **BGP-Instanz**.
  - Sie aktivieren diesen BGP-Nachbarn unter **Eintrag aktiv**.
- **Passiv**: In diesem Modus baut das Gerät nicht aktiv eine Verbindung zum BGP-Nachbarn auf, sondern wartet auf eine entsprechende Verbindungsanfrage vom BGP-Nachbarn.
- **Verzögert**: In diesem Modus baut das Gerät eine Verbindung zum BGP-Nachbarn erst nach Ablauf einer Verzögerungszeit auf. Die Bedingungen zum Aufbau einer Verbindung sind identisch zum Modus „Aktiv“.

Verbindungs-Verzögerung

Gibt die Zeit in Sekunden an, die das Gerät in der Verbindungsart „Verzögert“ wartet, bis es eine Verbindung zu einem BGP-Nachbarn aufbaut.

Route-Reflector Client

Definiert, ob der entsprechende Nachbar als Route-Reflector-Client behandelt werden soll, so dass das Gerät iBGP-Routen zu diesem Client reflektiert.

Dieser Schalter ist nur dann wirksam, falls

- das Gerät in der BGP-Instanz als Route-Reflector konfiguriert wurde, d. h. selbst Route-Reflector ist und
- die entfernte AS-Nummer der eigenen AS-Nummer entspricht (iBGP).

Nachbar-Profil

Enthält den Namen des BGP-Nachbar-Profils aus **Routing-Protokolle** > **BGP** > **Nachbar-Profile**.

Bei fehlendem oder falschem Eintrag gilt der BGP-Nachbar als nicht vollständig konfiguriert und eine Verbindung zu ihm ist nicht möglich.

Eingangsregel

Gibt an, nach welchen Regeln das Gerät die eingehenden Verbindungen von diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter**.

Wenn Sie dieses Feld leer lassen, filtert das Gerät die ankommenden Verbindungen entsprechend der Default-Regel unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Standard**.

Ausgangsregel

Gibt an, nach welchen Regeln das Gerät die ausgehenden Verbindungen von diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter**.

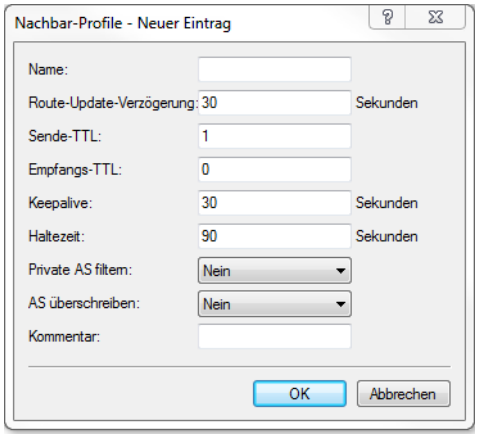
Wenn Sie dieses Feld leer lassen, filtert das Gerät die ankommenden Verbindungen entsprechend der Default-Regel unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Standard**.

Kommentar

Enthält einen Kommentar zu diesem BGP-Nachbarn.

BGP-Nachbar-Profile

Die Profile der BGP-Nachbarn des Gerätes konfigurieren Sie unter **BGP-Instanz**.



Name

Enthält den Namen des Profils.

Dieser Name ist u. a. für die Angabe in folgenden Tabellen vorgesehen:

- **Nachbar-Profil** unter **Routing-Protokolle** > **BGP** > **Nachbarn**
- **Nachbar-Profil** unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie**
- **Nachbar-Profil** unter **Setup** > **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie**

Route-Update-Verzögerung

Enthält die Zeit in Sekunden, die das Gerät mindestens zwischen dem Versenden von BGP-Update-Nachrichten an die BGP-Nachbarn mit diesem Profil wartet.

Sende-TTL

Bestimmt die TTL (time to live), die das Gerät den TCP-Paketen an die BGP-Nachbarn dieses Profils hinzufügt.

Bei direkt verbundenen Nachbarn beträgt dieser Wert „1". Für eBGP-Umgebungen erhöhen Sie diesen Wert für jeden Hop um 1.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert und verwendet stattdessen standardmäßig den maximalen TTL-Wert.

Dieser Wert muss „0" betragen, wenn **Empfangs-TTL** einen Wert ungleich „0" besitzt. Das Gerät verwendet automatisch den Wert „1", wenn sowohl **Sende-TTL** als auch **Empfangs-TTL** den Wert „0" besitzen.

Empfangs-TTL

Bestimmt die TTL (time to live), die die ankommenden TCP-Pakete von BGP-Nachbarn dieses Profils mindestens beinhalten müssen. Ankommende TCP-Pakete mit geringerer TTL nimmt das Gerät nicht an.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert.

Wenn dieser Wert ungleich „0" ist, setzt das Gerät den Wert für **Sende-TTL** intern auf „255".

Dieser Wert muss „0" betragen, wenn **Sende-TTL** einen Wert ungleich „0" besitzt.

Keepalive

Bestimmt die Zeit für den Keepalive-Timer in Sekunden. Nach Ablauf dieser Zeit sendet das Gerät eine Keepalive-Meldung an die Nachbarn dieses Profils, um die BGP-Verbindung aufrecht zu erhalten.

Das Gerät muss mindestens dreimal pro Holdtime eine Keepalive-Nachricht schicken. Der Wert darf deshalb max. ein Drittel der Haltezeit betragen. Bei einem höheren Wert oder einem Wert gleich „0" verwendet LCOS intern automatisch ein Drittel der Haltezeit.

Haltezeit

Bestimmt die Zeit in Sekunden, für die das Gerät eine BGP-Verbindung ohne Datenverkehr als gültig anerkennt.

Das Gerät verhandelt diesen Wert mit dem BGP-Nachbarn bei einem Verbindungsaufbau. Der niedrigere der beiden Werte gilt danach als gültig.

Ist das Resultat dieser Verhandlung ein Wert von „0", setzt das Gerät diese Verbindung solange auf gültig, bis es eine Verbindungsfehlermeldung erhält oder die Verbindung zusammenbricht. In dieser Zeit sendet es keine Keepalive-Nachrichten an die BGP-Nachbarn, selbst wenn der Keepalive-Timer eine Zeitdauer enthält.

Die Werte „1" und „2" sind gemäß RFC nicht erlaubt.

Private AS filtern

Kontrolliert die Behandlung von privaten AS-Einträgen (64512 - 65535, 4200000000 - 4294967294) aus der AS_PATH-Liste von ausgehenden Network Layer Reachability Information-Nachrichten (NLRI) zum Update der BGP-Nachbarn dieses Profils.

Bei iBGP-Verbindungen hat diese Option keine Funktion.

AS überschreiben

Aktiviert oder deaktiviert das Überschreiben von AS-Nummern im AS_PATH ausgehender Network Layer Reachability Information (NLRI).

Bei aktivierter Option überschreibt das Gerät alle AS-Nummern des BGP-Nachbarn mit der eigenen AS-Nummer.

Kommentar

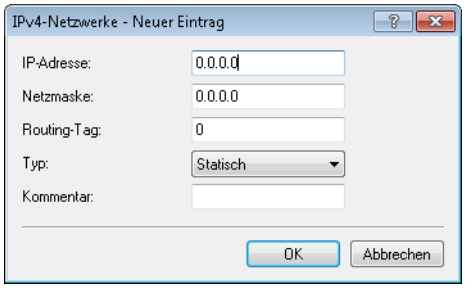
Kommentar zu diesem Eintrag.

IPv4-Netzwerke

In dieser Tabelle konfigurieren Sie die IPv4-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie**.

Die Mindestangabe für einen neuen gültigen Eintrag ist eine **IP-Adresse**.



IP-Adresse

Beinhaltet die IPv4-Adresse oder das Präfix des Netzwerkes.

Netzmaske

Beinhaltet die IPv4-Netzmaske des Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0.0.0.0` besitzt.

Routing-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Routing-Protokolle** > **BGP** > **IPv4-Adressfamilie** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell für Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

- In der Einstellung „Statisch“ ist das Netzwerk immer für Ankündigungen ausgewählt.
- In der Einstellung „Dynamisch“ ist das Netzwerk nur für Ankündigungen ausgewählt, wenn es in der aktiven Routing-Tabelle erscheint.

Kommentar

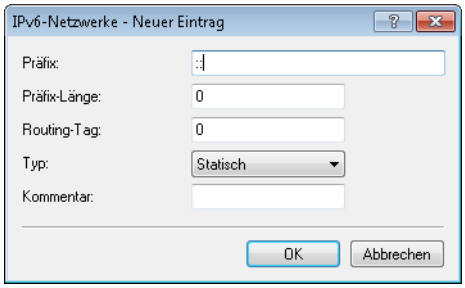
Kommentar zu diesem Eintrag.

IPv6-Netzwerke

In dieser Tabelle konfigurieren Sie die IPv6-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie**.

Die Mindestangabe für einen neuen gültigen Eintrag ist ein **Präfix**.



Präfix

Beinhaltet das Präfix (IPv6-Adressteil) des Netzwerkes.

Präfix-Länge

Beinhaltet die Präfix-Länge des IPv6-Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0` besitzt.

Routing-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Routing-Protokolle** > **BGP** > **IPv6-Adressfamilie** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell für Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

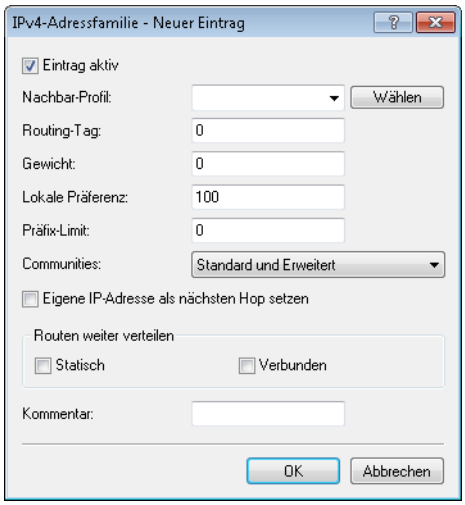
- In der Einstellung „Statisch“ ist das Netzwerk immer für Ankündigungen ausgewählt.
- In der Einstellung „Dynamisch“ ist das Netzwerk nur für Ankündigungen ausgewählt, wenn es in der aktiven Routing-Tabelle erscheint.

Kommentar

Kommentar zu diesem Eintrag.

IPv4-Adressfamilie

In dieser Tabelle konfigurieren Sie die Einstellungen der IPv4-Parameter, die für alle Geräte eines BGP-Nachbar-Profils gelten.



Eintrag aktiv

Aktiviert oder deaktiviert den Versand von IPv4-NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

Routing-Tag

Legt fest, dass das Gerät Routen nur dann weiter verteilt, wenn diese das konfigurierte Routing-Tag aus der Routing-Tabelle verwenden. Empfangene Routen des Nachbarn speichert das Gerät für dieses Routing-Tag in der Routing-Tabelle ab.

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht" ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

Lokale Präferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Lokale Präferenz" ist ein BGP-Standard-Attribut (LOCAL_PREF), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz" von 100.

Präfix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard“ als auch die Option „Erweitert“ deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

Eigene IP-Adresse als nächsten Hop setzen

Aktiviert oder deaktiviert den Austausch des Nexthops durch die eigene IP-Adresse in den NLRI.

Mögliche Werte:

Ja

Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein

Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer

Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Routen weiter verteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

- Statisch: Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- Verbunden: Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

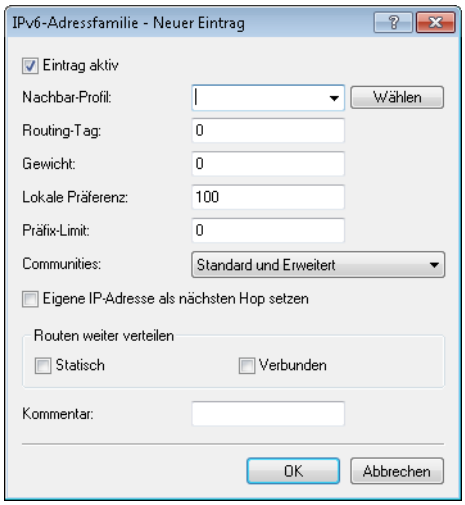
Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

Kommentar

Kommentar zu diesem Eintrag.

IPv6-Adressfamilie

In dieser Tabelle konfigurieren Sie die Einstellungen der IPv6-Parameter, die für alle Geräte eines BGP-Nachbar-Profils gelten.



Eintrag aktiv

Aktiviert oder deaktiviert den Versand von IPv6-NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

Routing-Tag

Legt fest, dass das Gerät Routen nur dann weiter verteilt, wenn diese das konfigurierte Routing-Tag aus der Routing-Tabelle verwenden. Empfangene Routen des Nachbarn speichert das Gerät für dieses Routing-Tag in der Routing-Tabelle ab.

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht“ ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

Lokale Präferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Lokale Präferenz“ ist ein BGP-Standard-Attribut (LOCAL_PREF), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz“ von 100.

Präfix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard“ als auch die Option „Erweitert“ deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

Eigene IP-Adresse als nächsten Hop setzen

Aktiviert oder deaktiviert den Austausch des Nexthops durch die eigene IP-Adresse in den NLRI.

Mögliche Werte:

Ja

Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein

Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer

Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Routen weiter verteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

- Statisch: Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.
- Verbunden: Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

Kommentar

Kommentar zu diesem Eintrag.

BGP-Regelwerk

In diesem Abschnitt konfigurieren Sie die Filter-Einstellungen für ausgehende und ankommende NLRI.

Standard

Das Gerät wendet für einen BGP-Nachbarn diese Standardregel an, wenn unklar ist, ob es dessen Präfix akzeptieren oder ablehnen soll. Die Ursache dafür kann sein:

- Für diesen BGP-Nachbarn ist keine Regel konfiguriert.
- Der angegebene Filter existiert nicht.
- Kein Filter unter **Filter** trifft zu.

Filter

Definieren Sie hier die Filter, die pro Nachbar zur Verfügung stehen sollen.

Trefferlisten

Definieren Sie hier die Trefferlisten für Filter.

Präfix- und Attribut-Listen

Definieren Sie hier Listen von Präfixen und Attributen, die das Gerät als Treffer erkennen soll.

Aktionen

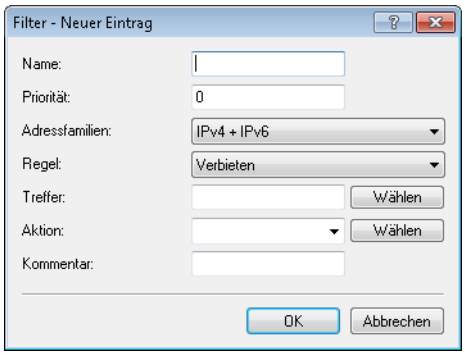
Definieren Sie hier Aktionen, die das Gerät im Falle eines Treffers ausführen soll.

Anpassungen

Definieren Sie hier Anpassungen, die das Gerät auf Präfix-Attribute anwenden soll.

Filter

Diese Tabelle enthält Filter, die eine NLRI von einem oder an einen BGP-Nachbarn durchlaufen muss, wenn dieser Nachbar entsprechend konfiguriert ist.



Name

Enthält den Namen für diesen Eintrag.

Bei mehreren Filtereinträgen mit identischem Namen bearbeitet das Gerät diese Filter gemäß der konfigurierten Priorität, bis ein Filter auf die NLRI zutrifft. Danach beendet das Gerät den Filterdurchlauf.

Priorität

Gibt die Priorität dieses Eintrages an.

Falls Einträge mit einem identischen Namen existieren, gehören diese Einträge zur selben Filterkette. Das Gerät arbeitet die Einträge dieser Filterkette entsprechend ihrer jeweiligen Priorität ab. Ein höherer Wert bedeutet eine höhere Priorität.

Adressfamilien

Gibt an, für welche Adressfamilie dieser Filter gilt.

Ohne ausgewählte Option ist dieser Eintrag deaktiviert.

Regel

Gibt an, ob das Gerät die gefilterte NLRI weiter verarbeiten soll, wenn dieser Filter für diese NLRI gültig ist.

- Ablehnen: Es erfolgt keine weitere Verarbeitung.
- Erlauben: Das Gerät verarbeitet die NLRI weiter.

Treffer

Gibt den Namen eines Eintrages aus der Tabelle **Treffer** an.

Das Gerät wendet diesen Filter an, wenn die NLRI mit den Kriterien übereinstimmt.

Wenn dieses Feld auf einen ungültigen Namen verweist, verweigert das Gerät die NLRI und führt keine weiteren Filter in der aktuellen Filterkette aus.

Aktion

Gibt an, welche Aktion aus der Tabelle **Aktion** das Gerät auf die NLRI anwenden soll.

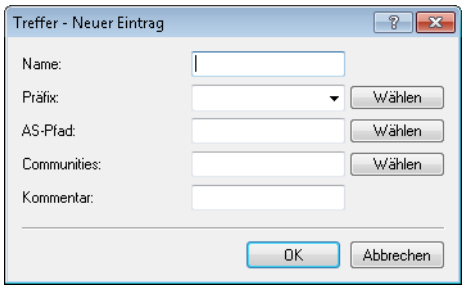
Wenn dieses Feld leer ist oder auf einen ungültigen Namen verweist, führt das Gerät keine Aktion aus.

Kommentar

Kommentar zu diesem Eintrag.

Treffer

Diese Tabelle kombiniert Präfix- und Attribut-Listen, um mehrere Listeneinträge auf Übereinstimmungen mit NLRI abzugleichen.



Name

Enthält den Namen für diesen Eintrag.

Präfix

Enthält den entsprechenden Eintrag der Liste unter **Präfix**.

AS-Pfad

Enthält den entsprechenden Eintrag der Liste unter **AS-Pfad** im Abschnitt „Präfix- und Attribut-Listen“.

Communities

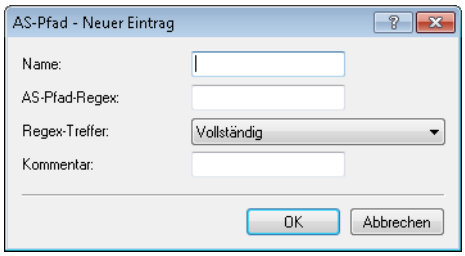
Enthält den entsprechenden Eintrag der Liste unter **Communities** im Abschnitt „Präfix- und Attribut-Listen“.

Kommentar

Kommentar zu diesem Eintrag.

AS-Pfad (Attribut-Liste)

Diese Tabelle enthält AS-Pfad-Listen, um NLRIs anhand ihres AS_PATH-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

AS-Pfad-Regex

Enthält einen regulären Ausdruck, der das AS_PATH-Attribut der NLRI überprüft. Beispiele:

- `.*_100`: filtert alle NLRIs, die in „AS100“ ihren Ursprung haben.
- `.*_(100|200)`: filtert alle NLRIs,die in „AS100“ oder „AS200“ ihren Ursprung haben.
- `100_(.*_)?(500|400)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die vorher zusätzlich den Weg über Netzwerke mit den AS-Nummern „AS500“ oder „AS400“ (oder beide) genommen haben.

- `100_(500|400|123)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die dieser vorher direkt von BGP-Nachbarn mit den AS-Nummern „AS500“, „AS400“ oder „AS123“ erhalten hat.
- `100_(100_)*(300_)*300`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die dieser vorher von seinem BGP-Nachbarn mit der AS-Nummer „AS300“ erhalten hat. Dieser Ausdruck berücksichtigt auch AS-Prepend Pfade.
- `100_.*_200`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“ und die im Netzwerk mit der AS-Nummer „AS200“ gestartet sind. Die Route, die die NLRIs vom „AS200“ bis zum „AS100“ genommen haben, ist hierbei unwichtig.

Regex-Treffer

Bestimmt, wie detailliert der reguläre Ausdruck unter **AS-Pfad-Regex** mit dem AS_PATH-Attribut der NLRI übereinstimmen muss, damit der Listeneintrag gültig ist.

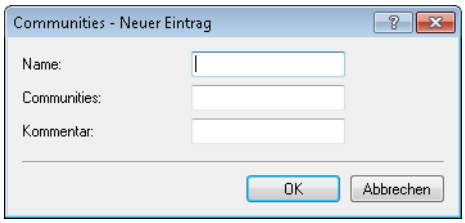
- Vollständig: Der reguläre Ausdruck beschreibt das gesamte AS_PATH-Attribut der NLRI.
- Teilweise: Der reguläre Ausdruck beschreibt nur Abschnitte des AS_PATH-Attributes.

Kommentar

Kommentar zu diesem Eintrag.

Communities (Attribut-Liste)

Diese Tabelle enthält Community-Listen, um NLRIs anhand ihres Community-Attributes zu erkennen.



Name

Enthält den Namen für diesen Eintrag.

Communities

Enthält Communities, die dem Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

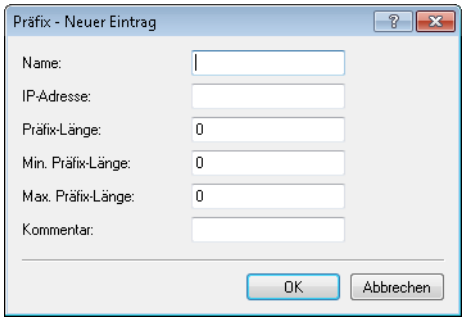
Kommentar

Kommentar zu diesem Eintrag.

Präfix (Attribut-Liste)

Diese Tabelle enthält Präfix-Listen, um NLRIs anhand ihres Netzwerkes (Präfix) und ihrer Netzmaske (Präfix-Länge) zu erkennen.

Ein Eintrag kann mehrere Präfixe enthalten.



Name

Enthält den Namen für diesen Eintrag.

IP-Adresse

Enthält die IPv4- oder IPv6-Adresse des Netzwerkes.

Präfix-Länge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes.

Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

Die Präfix-Länge der NLRI muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für „Min. Präfix-Länge“ und „Max. Präfix-Länge“ andere Werte vorgegeben sind.

Beim Wert „0“ stimmt das Netzwerk der NLRI dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter „IP-Adresse“ vorgegeben ist.

Min. Präfix-Länge

Enthält die minimale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

Max. Präfix-Länge

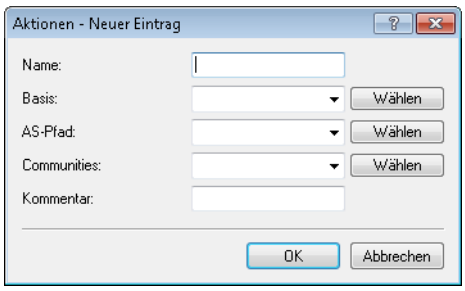
Enthält die maximale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

Kommentar

Kommentar zu diesem Eintrag.

Aktion

Diese Tabelle kombiniert Anpassungs-Listen, um mehrere Anpassungen auf NLRI mit einer Aktion durchzuführen.



Name

Enthält den Namen für diesen Eintrag.

Basis

Enthält den Namen für die Manipulation von Basis-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter **Basis**.

AS-Pfad

Enthält den Namen für die Manipulation von AS_PATH-Attributen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter **AS-Pfad**.

Communities

Enthält den Namen für die Manipulation von Community-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Anpassungs-Tabelle unter **Communities**.

Kommentar

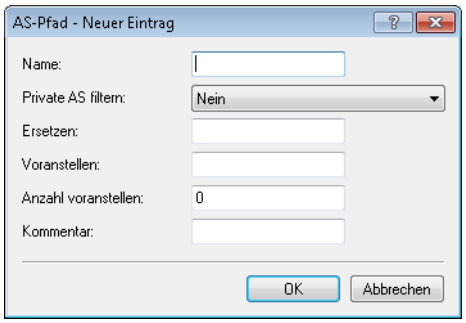
Kommentar zu diesem Eintrag.

AS-Pfad (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der AS_PATH-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. „Private AS Filtern“
2. „Ersetzen“
3. Gemeinsam „Anzahl voranstellen“ und „Voranstellen“



Name

Enthält den Namen für diesen Eintrag.

Private AS filtern

Wenn konfiguriert, ändert das Gerät die Angabe der privaten AS-Nummern im AS_PATH-Attribut einer NLRI gemäß dieser Einstellung.

- Nein: Das Gerät behält die vorhandenen privaten AS-Nummern der NLRI.
- Entfernen: Das Gerät entfernt alle privaten AS-Nummern.
- Ersetzen: Das Gerät tauscht die vorhandenen privaten AS-Nummern gegen die AS-Nummer der aktuellen BGP-Instanz.

Ersetzen

Wenn konfiguriert, ändert das Gerät das AS_PATH-Attribut der NLRI auf den hier angegebenen Wert.

Voranstellen

Wenn konfiguriert, stellt das Gerät dem AS_PATH-Attribut der NLRI so oft den hier angegebenen Wert voran, wie unter „Anzahl voranstellen“ konfiguriert. Besondere Werte:

- `self`: Das Gerät stellt dem AS_PATH-Attribut der NLRI seine eigene AS-Nummer voran.
- `last`: Das Gerät stellt dem AS_PATH-Attribut der NLRI die zuletzt vorangestellte AS-Nummer voran.

Anzahl voranstellen

Bestimmt, wie oft das Gerät dem AS_PATH-Attribut der NLRI eine AS-Nummer voranstellen soll.

Kommentar

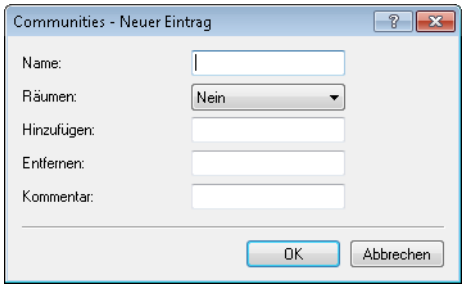
Kommentar zu diesem Eintrag.

Communities (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. „Räumen“
2. „Hinzufügen“
3. „Entfernen“



Name

Enthält den Namen für diesen Eintrag.

Räumen

Legt fest, ob das Gerät unbekannte Communities aus der NLRI löscht.

Bekannte Communities bleiben auch dann bestehen, wenn diese Option auf „Ja“ steht.

Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`

Mehr Informationen hierzu finden Sie unter *RFC 1997* und *RFC 3765*.

Hinzufügen

Legt fest, welche Communities das Gerät einer NLRI hinzufügt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

Entfernen

Legt fest, welche Communities das Gerät aus einer NLRI entfernt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

Bekannte Communities lassen sich nicht aus NLRI entfernen. Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`

Folgende Eingabeformate sind für Communities möglich:

Eingabeformat	Community
1:2	Standard Community
1.2.3.4:1	IPv4 spezifische Extended Community
roc:1.2.3.4:1	IPv4 spezifische Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4 spezifische Route Target Extended Community
ext2:1:2	zwei Byte AS Extended Community
ext4:1:2	vier Byte AS Extended Community
roc:1:2	zwei Byte AS Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1:2	zwei Byte AS Route Origin Extended Community
roc:ext4:1:2	vier Byte AS Route Origin Extended Community (Site-of-Origin (SoO))

Kommentar

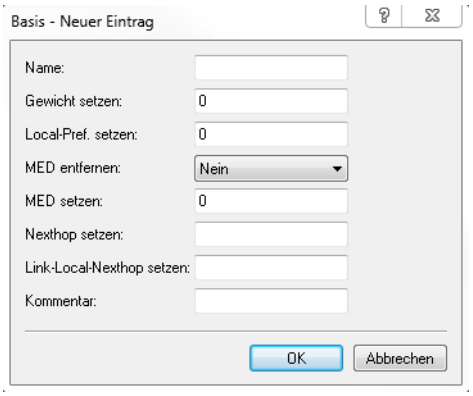
Kommentar zu diesem Eintrag.

Basis (Anpassungs-Liste)

Diese Tabelle enthält Manipulationen der Basis-Attribute von NLRIs.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen durch.

Die Angabe von Basis-Attributen ist optional. Wenn die Aktion nur ein Basis-Attribut ändern soll, geben Sie an der entsprechenden Stelle den zu ändernden Wert ein und lassen Sie die übrigen Attribute in der jeweiligen Standardeinstellung.



Name

Enthält den Namen für diesen Eintrag.

Gewicht setzen

Das Gerät ändert die Gewichtung einer NLRI auf den hier angegebenen Wert.

Lokale Präferenz

Das Gerät ändert den lokalen Präferenz-Wert einer NLRI auf den hier angegebenen Wert.

MED entfernen

Das Gerät löscht bei der Einstellung „Ja“ den Multi Exit Discriminator (MED) einer NLRI, bevor es die Einstellung unter „MED setzen“ verarbeitet.

MED setzen

Das Gerät ändert den Multi Exit Discriminator (MED) einer NLRI auf den hier angegebenen Wert. Falls die NLRI keinen MED beinhaltet, erzeugt das Gerät dieses Attribut.

Nexthop setzen

Das Gerät ändert die Nexthop-IP-Adresse einer NLRI auf den hier angegebenen Wert. Mögliche Werte sind eine IPv4-Adresse oder eine globale IPv6-Adresse.

Link-Local-Nexthop setzen

Das Gerät ändert den IPv6 Link-Local-Nexthop einer NLRI auf den hier angegebenen Wert. Ist nur wirksam bei IPv6-Präfixen.

Kommentar

Kommentar zu diesem Eintrag.

5.1.2 Algorithmus für die Auswahl des besten Pfades

Der folgende Algorithmus wird zur Auswahl des besten Pfades angewendet:

1. Der Next-Hop aus der BGP-Update-Nachricht ist erreichbar.
2. Das eigene AS kommt nicht im `AS-Path` vor.
3. Der Next-Hop ist keine eigene Adresse.
4. Höchstes Gewicht
5. Höchste Lokale Präferenz
6. Kürzester `AS_PATH` (`AS_SET` zählt als Länge 1)

7. Niedrigster Origin (IGP < EGP < Incomplete)
8. Niedrigster MED

   Gilt nur, wenn die verglichenen Routen aus dem gleichen Nachbar-AS stammen.

9. eBGP wird vor iBGP bevorzugt.
10. Niedrigste Router ID
11. Nachbar mit niedrigster IP-Adresse
12. Nachbar mit niedrigstem RTG-Tag
13. Der älteste Pfad wird gegenüber einem neu gelernten Pfad bevorzugt.

Beeinflussung des Routing-Algorithmus durch Attribute

Sie haben die Möglichkeit, die Auswahl des besten Pfades zu einem Ziel mittels folgender Attribute zu beeinflussen:

Gewicht

Gewicht ist ein proprietäres Attribut, welches nicht in BGP-Update-Nachrichten an Nachbarn propagiert wird. „Gewicht" ist somit nur auf dem lokalen Router gültig. Sie haben die Möglichkeit, das Attribut lokal entweder pro Adressfamilie oder durch Filterregeln zu setzen.

Lokale Präferenz

Lokale Präferenz ist ein BGP-Standard-Attribut (`LOCAL_PREF`) und wird per iBGP an Nachbarn propagiert. Alle Pfade besitzen standardmäßig eine lokale Präferenz von 100 (Default). Das Attribut wird in der Praxis z. B. dazu verwendet, bestimmte Präfixe zu bevorzugen. Das Attribut kann entweder pro Adressfamilie oder durch Filterregeln gesetzt werden.

AS_PATH

Der AS-Pfad (AS-Path) gibt den zurückgelegten Pfad einer Route an. Durch Filterregeln kann der AS-Pfad manipuliert werden, indem z. B. die eigene AS-Nummer mehrfach vorangestellt wird. Dadurch erscheint der AS-Path bei einem Nachbarn länger.

Origin

Origin ist ein BGP-Standard-Attribut, das an alle Nachbarn propagiert wird. Dieses Attribut definiert den Ursprung einer Route. Dies kann ein Interior Gateway Protokoll (IGP), das Exterior Gateway-Protokoll (EGP, RFC 904) oder „Incomplete" sein. Dabei steht „Incomplete" für die Redistribution durch ein anderes Routing-Protokoll. Das Attribut **Origin** wird automatisch vom Router gesetzt. Routen, die in BGP durch einen Eintrag in der IPv4- / IPv6-Netzwerktabelle hinzugefügt werden, erhalten den Ursprung IGP. Routen, die in den Adressfamilien zum Weiterverteilen konfiguriert werden, erhalten den Ursprung „Incomplete".

MED

MED (`MULTI_EXIT_DISC`) ist ein optionales BGP-Attribut, um mehrere Eingänge oder Ausgänge zum gleichen Nachbar-AS zu unterscheiden. Das Attribut kann durch Filterregeln gesetzt werden.

Router ID

Die Router ID, auch als BGP-Identifier bezeichnet, ist die eindeutige Identifikation eines Routers. Diese besteht aus der IPv4-Adresse des Routers. Die Router ID können Sie unter **BGP-Instanz** > **Router ID** manuell konfigurieren.

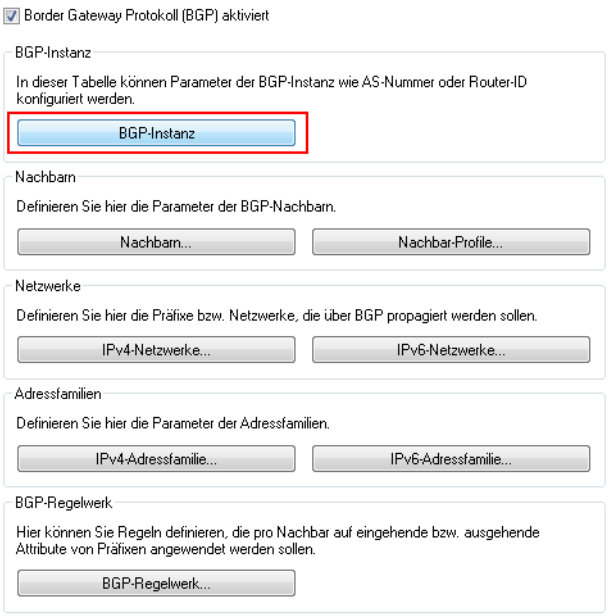
5.1.3 Tutorial: Einrichtung von BGPv4 unter LANconfig

Zwei LANCOM-Router sind über eine WAN-Verbindung miteinander verbunden und sollen über BGP bestimmte IPv4-Netzwerke propagieren. Bei den Routern handelt es sich um einen LANCOM 1781AW in der Zentrale und einen LANCOM 1781VA-4G in der Filiale.

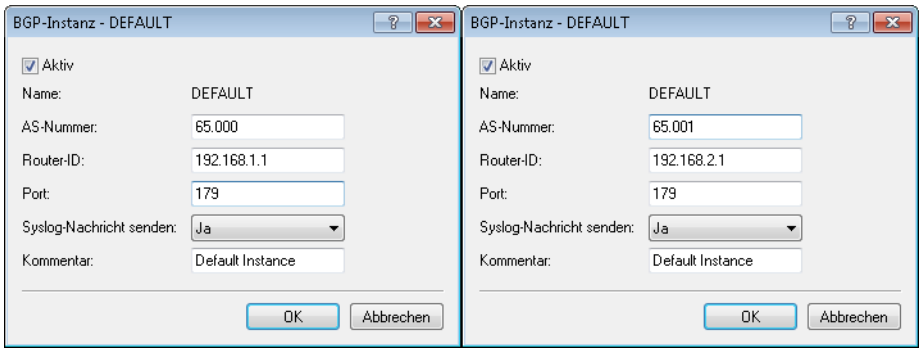
Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

1. **Aktivieren von BGP**: Öffnen Sie den Menüpunkt **Routing-Protokolle** > **BGP** in der Konfiguration der beiden Router und setzen Sie den Haken in der Checkbox **Border Gateway Protokoll (BGP) aktiviert**. Hiermit haben Sie BGP auf dem jeweiligen Gerät aktiviert. In den nächsten Schritten konfigurieren Sie die einzelnen BGP-Instanzen, die zugehörigen Nachbarn und die zu propagierenden Netze konfiguriert.

2. **Konfiguration der einzelnen BGP-Instanzen**: Um die BGP-Instanz des jeweiligen Routers zu konfigurieren, klicken Sie auf die Schaltfläche **BGP-Instanz**.



3. Bestimmen Sie im Konfigurationsfenster die allgemeinen Informationen zu der BGP-Instanz des jeweiligen Routers. Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt.



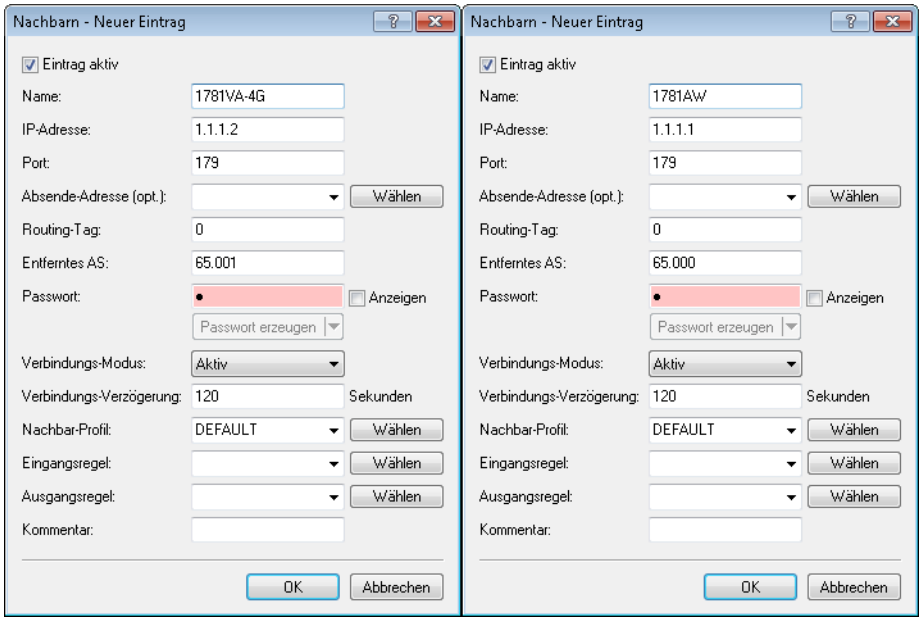
In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

Parameter	Beschreibung
Checkbox **Aktiv**	Aktivieren Sie die BGP-Instanz des Routers. Dies ist notwendig, damit eine Kommunikation zwischen den beiden Routern möglich ist.
AS-Nummer	Die AS-Nummer (Nummer des **A**utonomen **S**ystems) fasst Router unter der gleichen Administration zusammen. Geben Sie hier unterschiedliche Nummern ein, handelt es sich um eBGP-Peers. Bei identischen Nummern handelt es sich um Peers im selben AS (iBGP). Welche Einträge gültig sind, erfahren Sie unter *http://www.iana.org/assignments/as-numbers/as-numbers.xhtml*.
Router-ID	Hinterlegen Sie eine IP-Adresse des Routers. Tragen Sie `0.0.0.0` ein, wird die IP-Adresse automatisch ermittelt. Die Router-ID muss unter allen Nachbarn eines BGP-Routers eindeutig sein. Hier sind unterschiedliche Einträge notwendig.
Port	Konfigurieren Sie den TCP-IP-Port, den der Router für eingehende BGP-Verbindungen nutzt. Der Default-Wert ist 179.
Syslog-Nachrichten senden	Geben Sie an, ob das Gerät Syslog-Nachrichten erzeugen soll. Diese können Sie bequem über WEBconfig einsehen.
Kommentar	Tragen Sie einen Kommentar ein, der das spätere Nachvollziehen der Konfiguration erleichtert.

4. **Konfiguration der BGP-Nachbarn**: Nachdem die Konfiguration der BGP-Instanz abgeschlossen ist, ist es notwendig, die zugehörigen Nachbarn zu definieren, mit denen die Informationen der zu propagierenden Netze ausgetauscht werden. Klicken Sie dazu auf die Schaltfläche **Nachbarn**.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen neuen BGP-Nachbarn zu konfigurieren. Bestimmen Sie im Konfigurationsfenster die Informationen zu den BGP-Nachbarn der einzelnen Router.

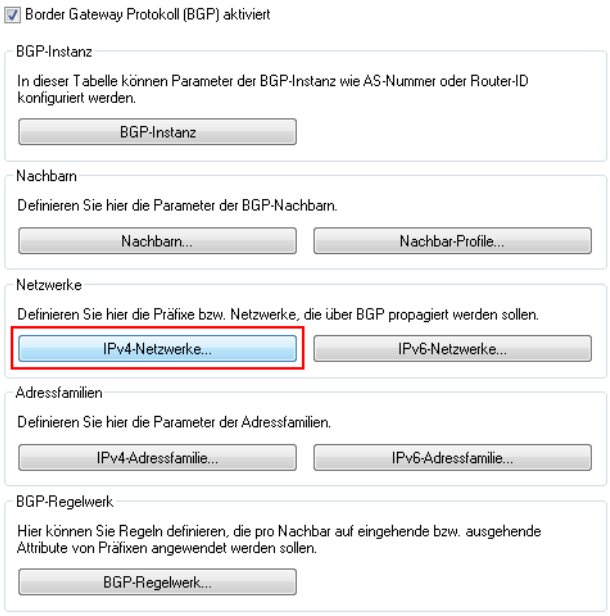
Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

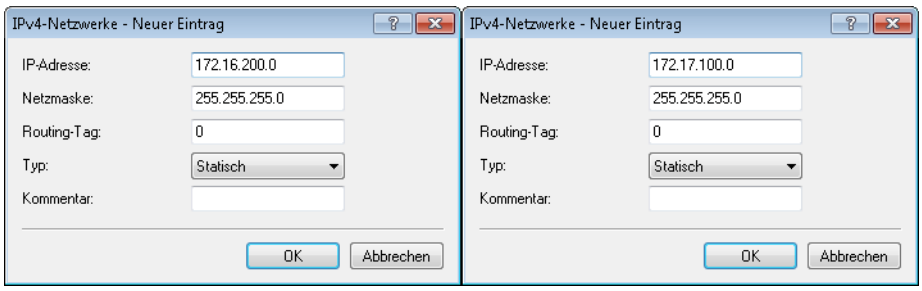
Parameter	Beschreibung
Eintrag aktiv	Aktivieren Sie den Eintrag für den entsprechenden Nachbarn.
Name	Weisen Sie dem Nachbarn einen Namen zu. In diesem Beispiel wird eine abgekürzte Version der Gerätebezeichnung zur einfachen Identifizierung in der Konfiguration verwendet.
IP-Adresse	Tragen Sie die IP-Adresse ein, unter der der Nachbar zu erreichen ist. In diesem Beispiel ist die WAN-Adresse des 1781AW `1.1.1.1` und die des 1781VA-4G `1.1.1.2`.
Entferntes AS	Tragen Sie die in **Schritt 2** definierten AS-Nummern der entsprechenden Nachbarn ein.
Passwort	Tragen Sie ein Passwort ein, mit dem die Kommunikation zwischen den beiden BGP-Nachbarn durch einen MD5-Hash verschleiert wird. Das Passwort muss auf beiden Seiten identisch sein.

6. **Konfiguration der zu propagierenden IPv4-Netzwerke**: Konfigurieren Sie die Netzwerke, die die einzelnen BGP-Instanzen propagieren. Klicken Sie dazu auf die Schaltfläche **IPv4-Netzwerke**.



7. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues IPv4-Netzwerk zu definieren, welches propagiert werden soll.

Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

Parameter	Beschreibung
IP-Adresse	Der IPv4-Adressbereich des zu propagierenden Netzwerkes.
Netzmaske	Die zum definierten Netzwerk gehörige Netzmaske.
Typ	Der Typ, mit dem die Propagierung erfolgen soll. In diesem Beispiel statisch, um eine möglichst einfache Konfiguration zu zeigen.

8. Schreiben Sie die Konfiguration in beide Geräte zurück.
9. Die Überprüfung der BGP-Verbindung erfolgt einfach über die Kommandozeile. Der Befehl `show bgp-neighbors` zeigt alle aktiven Nachbarn und deren Status an.

```
> show bgp-neighbors
BGP-Neighbors:

1.1.1.2, Rtg-Tag 0
 BGP-State: ESTABLISHED, up for 00:09:23
 remote AS 65001, remote router id 192.168.1.161, eBGP
 Neighbor capabilities:
  Four-octets ASN capability: advertised and received
  Address family IPv4 NLRI used for unicast forwarding: advertised and received
> _
```

5.1.4 Tutorial: Präferenz von Präfixen einrichten

„Präferenz“ ist ein optionales BGP-Attribut, mit dessen Hilfe Sie Pfade zu einem entsprechenden Präfix bevorzugen können. Das Gerät bevorzugt einen Pfad mit einer höheren Präferenz gegenüber einem Pfad mit einer niedrigeren Präferenz.

Innerhalb eines AS übertragen die iBGP-Nachbarn untereinander das BGP-Attribut LOCAL_PREFERENCE. Zwischen benachbarten AS übertragen die eBGP-Nachbarn dieses Attribut nicht.

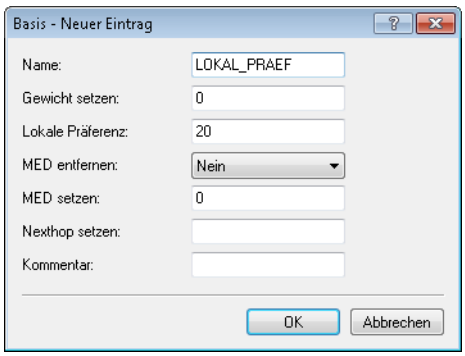
Es gibt zwei Methoden, um Präferenzen zu konfigurieren:

- Pro Adressfamilie
- Durch Regeln

Dieses Beispiel erläutert die Konfiguration, um das Präfix eines BGP-Nachbarn mit der Präferenz „200“gegenüber dem Präfix eines anderen BGP-Nachbarn mit der Präferenz „100“zu priorisieren.

Die Defaulteinstellung für Präferenzen ist „100“. Dementsprechend genügt es, nur den zu bevorzugenden Nachbarn mit der Präferenz „200“ zu konfigurieren.

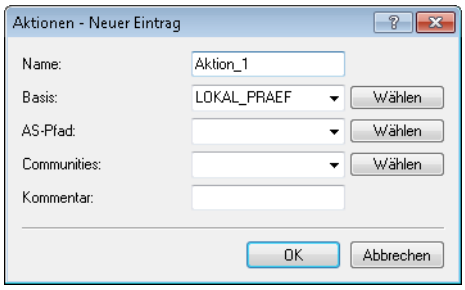
1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Basis** einen neuen Eintrag zur Manipulation von Basis-Attributen der NLRI (in diesem Fall das Basis-Attribut LOCAL_PREFERENCE).



Vergeben Sie dem Eintrag einen aussagekräftigen Namen.

Unter **Lokale Präferenz** geben Sie den Wert „200“ für die neue lokale Präferenz ein.

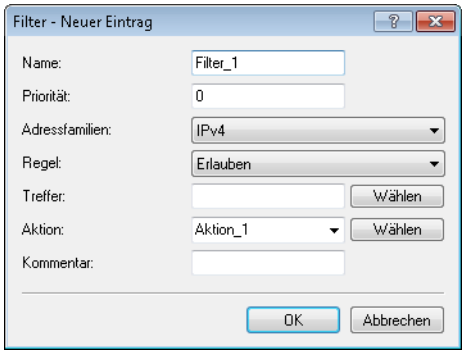
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **Aktionen** eine neue Aktion.



Vergeben Sie der Aktion einen aussagekräftigen Namen.

Wählen Sie unter **Basis** den zuvor erstellten Basis-Eintrag aus.

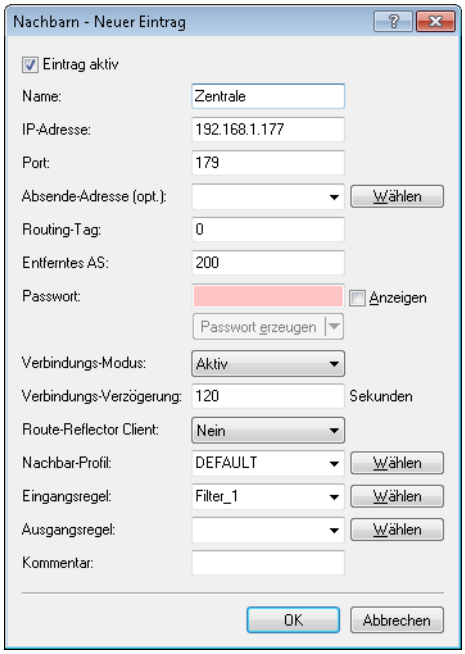
3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Erlauben“ im Feld **Regel** bestimmen Sie, dass das Gerät die abgehende NLRI verändern soll. Wählen Sie unter **Aktion** die zuvor erstellte Aktion aus.

4. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **Nachbarn** einen neuen Eintrag für einen BGP-Nachbarn.



Vergeben Sie dem Nachbarn einen aussagekräftigen Namen und konfigurieren Sie seine IP-Adresse sowie die Nummer des entfernten AS, in dem er sich befindet.

Wenn Sie für diesen BGP-Nachbarn kein eigenes Nachbar-Profil erstellt haben, verwenden Sie das „Default"-Profil.

Wählen Sie unter **Eingangsregel** den zuvor erstellten Filter aus.

5. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

Der Befehl `show bgp-policy Filter_1` zeigt die aktuelle Einstellung der Regel „Filter_1" an.

```
> show bgp-policy Filter_1
Traverse chain "Filter_1"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Aktion_1"
         No AS-path override configured
         Apply basic override "LOKAL_PRAEF"
            Set local preference to 200
         No community override configured
      Permit route
> _
```

Der Befehl `show bgp-v4-adj-rib-in` zeigt die Routing Information Base (RIB) an.

```
> show bgp-v4-adj-rib-in
IPv4 Unicast Adj-RIB-In

 192.168.1.177, Rtg-Tag 0

  Prefix            Next Hop       Local-Pref  Weight  MED AS Path
  ------------------------------------------------------------------
  192.168.210.0/24  192.168.1.177         200       0    0 AS sequence: 200
  192.168.211.0/24  192.168.1.177         200       0    0 AS sequence: 200

> _
```

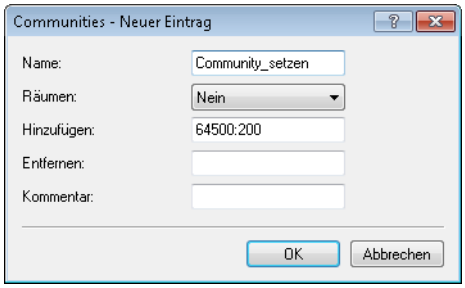
5.1.5 Tutorial: Community-Attribut setzen

„Community“ ist ein optionales BGP-Attribut, mit dessen Hilfe Sie Präfixe in logischen Gruppen zusammenfassen und darüber identifizieren können. Auf diese Gruppen lassen sich Ein- und Ausgangsregeln anwenden. Zu einem Präfix können Sie mehrere Communities definieren.

Neben den bekannten Communities `NO-ADVERTISE` oder `NO-EXPORT` ist die Bedeutung einer Community vom Provider frei definierbar. So definiert z. B. der Provider des AS „64500“, dass Kunden-Routen mit der Community „64500:200“ mit der Präferenz „200” zu behandeln sind und Routen mit der Community „64500:90“ mit der Präferenz „90“.

Das folgende Beispiel erläutert die Erweiterung aller abgehenden Routen mit Community „64500:200“.

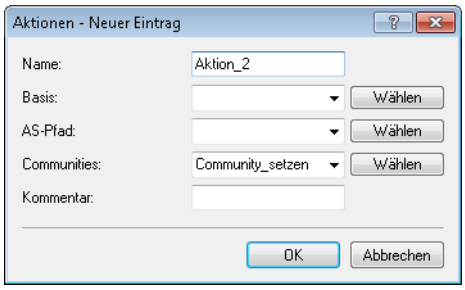
1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Communities (Anpassungen)** einen neuen Community-Eintrag.



   Vergeben Sie der Community einen aussagekräftigen Namen.

   Unter **Hinzufügen** geben Sie den Wert „64500:200“ für das Community-Attribut an. Diesen Wert fügt das Gerät dem Community-Attribut der abgehenden NLRI an.

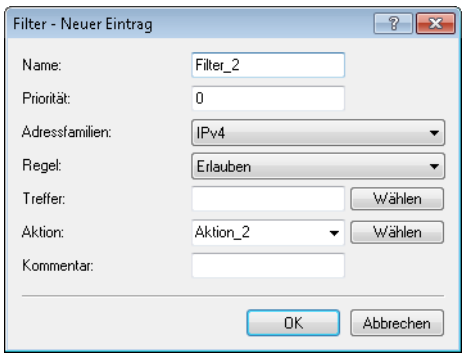
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **Aktionen** eine neue Aktion.



   Vergeben Sie der Aktion einen aussagekräftigen Namen.

   Wählen Sie unter **Communities** die zuvor erstellte Community aus.

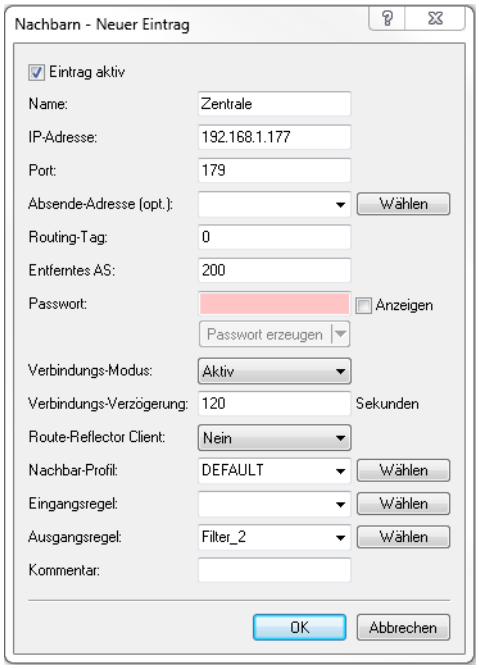
3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Erlauben“ im Feld **Regel** bestimmen Sie, dass das Gerät die abgehende NLRI verändern soll. Wählen Sie unter **Aktion** die zuvor erstellte Aktion aus.

4. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **Nachbarn** einen neuen Eintrag für einen BGP-Nachbarn.



Vergeben Sie dem Nachbarn einen aussagekräftigen Namen und konfigurieren Sie seine IP-Adresse sowie die Nummer des entfernten AS, in dem er sich befindet.

Wenn Sie für diesen BGP-Nachbarn kein eigenes Nachbar-Profil erstellt haben, verwenden Sie das „Default“-Profil.

Wählen Sie unter **Ausgangsregel** den zuvor erstellten Filter aus.

5. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

Der Befehl `show bgp-policy Filter_2` zeigt die aktuelle Einstellung der Regel „Filter_2“ an.

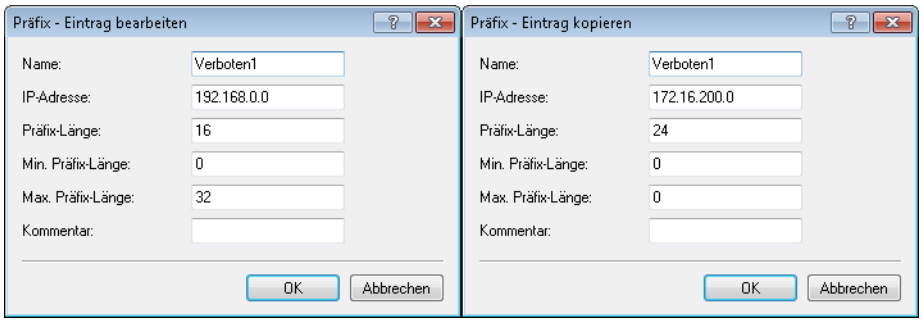
```
> show bgp-policy Filter_2
Traverse chain "Filter_2"
   Inspect filter of priority 0
      Match IPv4 routes
      Execute action "Aktion_2"
         No AS-path override configured
         No basic override configured
         Apply community override "Community_setzen"
            Add community 64500:200
      Permit route
> _
```

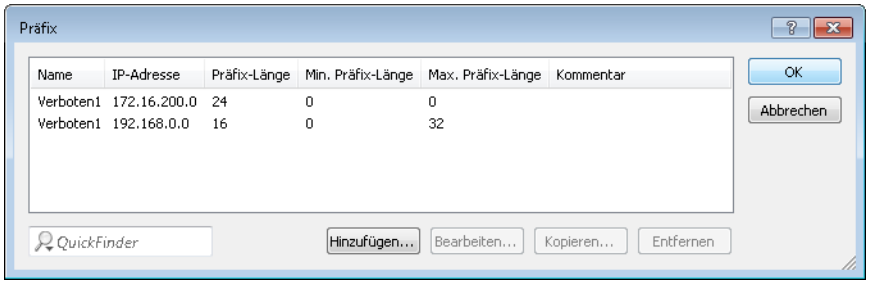
5.1.6 Tutorial: Empfangene Präfixe filtern

Dieses Beispiel erläutert die Konfiguration, um die folgenden ankommenden Präfixe eines BGP-Nachbarn auszufiltern:

- alle Präfixe aus dem Bereich „192.168.0.0/16“
- das einzelne Präfix „172.16.200.0/24“

1. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Präfix** zwei neue Präfix-Einträge mit den zu filternden Präfixen.



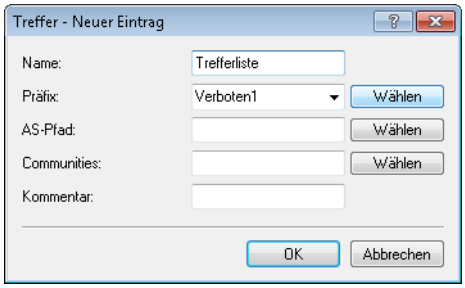


Vergeben Sie den Einträgen jeweils einen aussagekräftigen Namen.

Für jedes zu filternde Präfix geben Sie jeweils einen Eintrag an, der jedoch immer den gleichen Namen besitzt.

Bestimmen Sie je Eintrag die IP-Adresse sowie die benötigte Präfix-Länge.

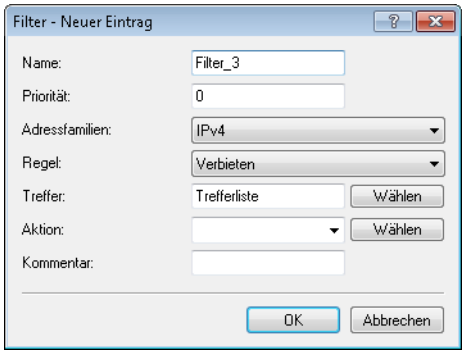
2. Definieren Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Treffer** einen Treffer für den zuvor erstellten Präfix-Eintrag.



Vergeben Sie dem Eintrag einen aussagekräftigen Namen.

Wählen Sie unter **Präfix** die zuvor erstellte Präfix-Bezeichnung aus.

3. Erstellen Sie unter **Routing-Protokolle** > **BGP** > **BGP-Regelwerk** > **Filter** einen neuen Filter.



Vergeben Sie dem Filter einen aussagekräftigen Namen.

Wählen Sie unter **Adressfamilien** das entsprechende Verbindungsprotokoll zum BGP-Nachbarn aus. Mit der Einstellung „Verbieten" im Feld **Regel** bestimmen Sie, dass das Gerät die ankommenden Präfixe herausfiltern soll. Wählen Sie unter **Treffer** den zuvor erstellten Treffer aus.

4. Um die Konfiguration zu prüfen, öffnen Sie eine Terminalverbindung zum Gerät.

Der Befehl `show bgp-policy Filter_3` zeigt die aktuelle Einstellung der Regel „Filter_3" an.

```
> show bgp-policy Filter_3
Traverse chain "Filter_3"
   Inspect filter of priority 0
      Match IPv4 routes
      Assess match "Trefferliste"
         Evaluate prefix list "Verboten1"
            Analyze prefix 172.16.200.0
               Match IPv4 routes
               Match route's 24 MSB
               Match route prefix length in [24, 24]
            Analyze prefix 172.168.0.0
               Match IPv4 routes
               Match route's 16 MSB
               Match route prefix length in [16, 32]
         No AS-path list configured
         No community list configured
      Deny route
> _
```

5.1.7 Ergänzungen im Setup-Menü

Routing-Protokolle

In diesem Verzeichnis konfigurieren Sie die Routing-Protokolle und den Route-Monitor.

SNMP-ID:

2.93

Pfad Telnet:

Setup

BGP

In diesem Verzeichnis konfigurieren Sie das Gerät für das Border Gateway Protokoll Version 4 (BGPv4).

SNMP-ID:

2.93.1

Pfad Telnet:

Setup > **Routing-Protokolle**

BGP-Instanz

In dieser Tabelle konfigurieren Sie die BGP-Instanzen.

Da das Gerät nur eine BGP-Instanz gleichzeitig unterstützt, enthält diese Tabelle nur einen Eintrag.

SNMP-ID:

2.93.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Name

Enthält den Namen der BGP-Instanz.

In der Standardeinstellung ist bereits ein Eintrag „DEFAULT“ vorgegeben.

SNMP-ID:

2.93.1.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Aktiv

Aktiviert oder deaktiviert diese BGP-Instanz.

Diese Einstellung ist nur wirksam, wenn BGP im Gerät aktiv ist.

SNMP-ID:

2.93.1.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

Ja

Die BGP-Instanz ist aktiviert.

Nein

Die BGP-Instanz ist deaktiviert.

Default-Wert:

Nein

AS-Nummer

Die AS-Nummer, die dieser BGP-Instanz zugeordnet ist.

Ein Verbindungsaufbau zu einem BGP-Router, der keine 32Bit-großen AS-Nummern unterstützt, ist nur dann möglich, wenn Sie hier eine 16Bit-AS-Nummer eintragen (kleiner 65536).

SNMP-ID:

2.93.1.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

0

Router-ID

Die Router-ID (IPv4-Adresse), die dieser BGP-Instanz zugeordnet ist.

SNMP-ID:

2.93.1.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

0.0.0.0

Syslog

Das Gerät kann Ereignisse wie Verbindungsabbrüche von Nachbarn, die mit dieser BGP-Instanz verbunden sind, im Syslog speichern. Mit dieser Option aktivieren oder deaktivieren Sie diese Funktion.

SNMP-ID:

2.93.1.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

Ja

Aufzeichnung im Syslog ist aktiviert.

Nein

Aufzeichnung im Syslog ist deaktiviert.

Default-Wert:

Nein

Port

Geben Sie hier an, auf welchem Port die BGP-Instanz auf ankommende Verbindungen von Nachbarn reagiert.

SNMP-ID:

2.93.1.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

179

Kommentar

Kommentar zu dieser BGP-Instanz.

SNMP-ID:

2.93.1.1.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

Default Instance

Erstes-AS-pruefen

Prüft, ob die erste AS-Nummer im AS-Pfad bei empfangenen Update-Nachrichten der AS-Nummer des Nachbarn entspricht. Falls dies nicht der Fall ist, wird diese Route verworfen.

Diese Prüfung muss deaktiviert werden, wenn der Router mit einem BGP-Route-Server verbunden ist, der zwar Routen verteilt, aber nicht selbst im Routing-Pfad liegt bzw. sein eigenes AS in den AS-Pfad einfügt.

SNMP-ID:

2.93.1.1.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

ja
nein

Default-Wert:

ja

AS-Pfad-Limit

Maximale Anzahl von erlaubten AS-Nummern im AS-Pfad bei empfangenen Update-Nachrichten. Wird das Limit überschritten, so verwirft das Gerät die entsprechende Route. Ein AS-Pfad-Limit kann vor Nachrichten von fehlerhaft konfigurierten Routern schützen, die zu lange AS-Pfade ankündigen.

SNMP-ID:

2.93.1.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

0

Cluster-ID

Cluster-ID des Routers, falls dieser als Route-Reflector konfiguriert wird. Die Eingabe erfolgt im Format einer IPv4-Adresse.

SNMP-ID:

2.93.1.1.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

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

Default-Wert:

0.0.0.0

Route-Reflector

Definiert, ob der Router die Funktion eines Route-Reflectors übernehmen soll.

Beim Einsatz von iBGP müssen normalerweise alle BGP-Router voll vermascht sein, d. h., jeder BGP-Router muss zu jedem BGP-Router eine BGP-Verbindung aufgebaut haben. Ein Route-Reflector hebt diese Anforderung auf und ermöglicht es, dass iBGP-Router z. B. eine sternförmige Topologie aufbauen können. Der Route-Reflector leitet dann iBGP-Routen an alle Route-Reflector-Clients weiter.

Ein Route-Reflector kann sowohl Route-Reflector-Clients als auch normale BGP-Clients bedienen. Auf dem Client muss in beiden Fällen keine gesonderte Konfiguration erfolgen.

SNMP-ID:

2.93.1.1.11

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

ja
nein

Default-Wert:

nein

TX-Loop-Erkennung

Die aktivierte Loop-Erkennung beeinflusst das Verhalten der BGP-Instanz wie folgt:

1. Die BGP-Instanz propagiert keine Routen zu Nachbarn, deren AS-Nummer im AS-Pfad der Route existiert.
2. Die BGP-Instanz sendet lokale Routen nur an iBGP-Nachbarn, falls der Nachbar ein Route-Reflector-Client und die lokale BGP-Instanz ein Route-Reflector ist.
3. Die BGP-Instanz verteilt eine Route nicht an Nachbarn, falls dieser Nachbar diese Route bereits gelernt hat.

Diese Maßnahmen dienen der Reduzierung von unnötig gesendeten Nachrichten, die ein Nachbar ggf. auf Grund seiner eigenen Erkennung von Schleifen verwerfen würde.

In bestimmten VPN-/ARF-Szenarien muss die TX-Loop-Erkennung deaktiviert sein.

SNMP-ID:

2.93.1.1.12

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **BGP-Instanz**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Nachbarn

In dieser Tabelle konfigurieren Sie die BGP-Nachbarn.

Für einen neuen Eintrag genügt die Angabe einer **IP-Adresse**, wobei die BGP-Instanz diesen Eintrag solange ignoriert, bis die folgenden Bedingungen erfüllt sind:

- Der Eintrag ist unter **Aktiv** mit „Ja“ aktiviert.
- Der **Instanzname** entspricht dem unter **Setup** > **Routing-Protokolle** > **BGP** > **BGP-Instanz** konfigurierten BGP-Instanznamen.
- Das **Nachbar-Profil** entspricht einem unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile** eingetragenen Profil.

Im Default ist diese Tabelle leer.

SNMP-ID:

2.93.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

IP-Adresse

Enthält die IP-Adresse (IPv4 oder IPv6) des BGP-Nachbarn, zu dem das Gerät in den Verbindungsarten „Aktiv“ oder „Verzögert“ eine BGP-Verbindung aufbaut.

Dieser Eintrag muss identisch zu der IP-Adresse (z. B. physikalische Interface-Adresse, Loopback-Adresse) sein, die dieser Nachbar bei einer ankommenden Verbindung meldet.

SNMP-ID:

2.93.1.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

max. 56 Zeichen aus `[A-F][a-f][0-9].:-%`

Default-Wert:

leer

Port

Enthält den Port, auf dem der BGP-Nachbar eingehende BGP-Nachrichten erwartet und den das Gerät entsprechend für ausgehende Verbindungen in den Verbindungsarten „Aktiv" oder „Verzögert" verwendet.

Ankommende Verbindungen nimmt das Gerät von jedem vom Sender verwendeten Quell-Port an.

SNMP-ID:

2.93.1.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

179

Loopback-Adresse

Enthält die Absender-Adresse (IPv4 oder IPv6), die das Gerät beim Verbindungsaufbau mit dem BGP-Nachbarn nutzt. Das Feld erlaubt die Eingabe von Loopback-Adressen, die unter **Setup** > **TCP-IP** > **Loopback-Liste** und **Setup** > **IPv6** > **Netzwerk** > **Loopback** konfiguriert sind.

Die Angabe ist optional und nur in den Verbindungsarten „Aktiv" oder „Verzögert" relevant.

SNMP-ID:

2.93.1.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

max. 56 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Besondere Werte:

leer

Das Gerät versucht, als Absendeadresse für die TCP-Verbindung eine passende Loopback-Adresse aus dem gleichen Subnetz wie die IP-Adresse des BGP-Nachbarn zu finden.

Rtg-Tag

Enthält das Routing-Tag. Stimmt das Routing-Tag nicht mit dem der ankommenden Verbindung überein, verweigert das Gerät den Verbindungsaufbau.

SNMP-ID:

2.93.1.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

0 … 65536

Default-Wert:

0

Entferntes-AS

Enthält die AS-Nummer des BGP-Nachbarn.

Ist die AS-Nummer des BGP-Nachbarn identisch zur AS-Nummer der eigenen BGP-Instanz des Gerätes, handelt es sich bei dem Nachbarn um einen iBGP-Peer (Internal BGP) innerhalb des AS.

SNMP-ID:

2.93.1.2.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

0

Name

Enthält den Namen des BGP-Nachbarn.

Geben Sie diesen Namen als Parameter bei den folgenden Aktionen an:

- **Manueller-Start** unter **Setup** > **Routing-Protokolle** > **BGP**
- **Manueller-Stop** unter **Setup** > **Routing-Protokolle** > **BGP**
- **Aktiver-Start** unter **Setup** > **Routing-Protokolle** > **BGP**

SNMP-ID:

2.93.1.2.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Aktiviert oder deaktiviert diesen BGP-Nachbarn.

Die Aktivierung des BGP-Nachbarn startet ggf. einen BGP-Verbindungsaufbau.

Bei deaktiviertem BGP-Nachbarn sind abgehende oder ankommende Verbindungen mit ihm nicht möglich.

SNMP-ID:

2.93.1.2.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

Ja

Der BGP-Nachbar ist aktiv. Ein BGP-Verbindungsaufbau mit ihm ist möglich.

Nein

Der BGP-Nachbar ist nicht aktiv. Ein BGP-Verbindungsaufbau (Senden oder Empfangen) ist nicht möglich.

Default-Wert:

Ja

Passwort

Gerät und BGP-Nachbar übertragen dieses Passwort als MD5-Signatur in den TCP-Paketen, um sich zu authentifizieren.

Ohne die Angabe eines Passwortes ist die Authentifizierung deaktiviert.

SNMP-ID:

2.93.1.2.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

leer

Nachbar-Profil

Enthält den Namen des BGP-Nachbar-Profils aus **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**.

Bei fehlendem oder falschem Eintrag gilt der BGP-Nachbar als nicht vollständig konfiguriert und eine Verbindung zu ihm ist nicht möglich.

SNMP-ID:

2.93.1.2.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Verbindungsart

Bestimmt den Modus, mit dem eine Verbindung vom Gerät zu diesem BGP-Nachbarn zustande kommt.

Alle drei Modi ermöglichen einen Verbindungsaufbau bei ankommender Verbindung.

SNMP-ID:

2.93.1.2.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

Aktiv

In diesem Modus versucht das Gerät eine Verbindung zum BGP-Nachbarn aufzubauen, sobald u. a. eine der folgenden Bedingungen erfüllt ist:

- Sie haben die Konfiguration des BGP-Nachbarn komplett abgeschlossen.
- Sie führen die Aktion **Manueller-Start** aus.
- Sie starten das Gerät.
- Sie aktivieren die BGP-Instanz unter **Setup** > **Routing-Protokolle** > **BGP** > **BGP-Instanz** > **Aktiv**.
- Sie aktivieren diesen BGP-Nachbarn unter **Aktiv**.

Passiv

In diesem Modus baut das Gerät nicht aktiv eine Verbindung zum BGP-Nachbarn auf, sondern wartet ausschließlich auf eine entsprechende Verbindungsanfrage vom BGP-Nachbarn.

Verzoegert

In diesem Modus baut das Gerät eine Verbindung zum BGP-Nachbarn erst nach Ablauf einer Verzögerungszeit auf. Die Bedingungen zum Aufbau einer Verbindung sind identisch zum Modus „Aktiv".

Default-Wert:

Aktiv

Verbindungsverzoegerung

Gibt die Zeit in Sekunden an, die das Gerät in der Verbindungsart „Verzoegert" wartet, bis es eine Verbindung zu diesem BGP-Nachbarn aufbaut.

SNMP-ID:

2.93.1.2.11

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

120

Besondere Werte:

0

Entspricht der Verbindungsart „Aktiv" mit sofortigem Verbindungsaufbau.

Instanzname

Gibt den Namen der verknüpften BGP-Instanz aus **Setup** > **Routing-Protokolle** > **BGP** > **BGP-Instanz** an.

Bei fehlendem oder falschem Eintrag gilt der BGP-Nachbar als nicht vollständig konfiguriert und eine Verbindung zu ihm ist nicht möglich.

SNMP-ID:

2.93.1.2.12

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Eingangsregel

Gibt an, nach welchen Regeln das Gerät die ankommenden Präfixe von diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**.

Wenn Sie dieses Feld leer lassen, filtert das Gerät die ankommenden Präfixe entsprechend der Default-Regel unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Standard**.

SNMP-ID:

2.93.1.2.13

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

leer

Ausgangsregel

Gibt an, nach welchen Regeln das Gerät die ausgehenden Präfixe zu diesem BGP-Nachbarn filtert.

Die Regeln konfigurieren Sie unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**.

Wenn Sie dieses Feld leer lassen, filtert das Gerät die ausgehenden Präfixe entsprechend der Default-Regel unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Standard**.

SNMP-ID:

2.93.1.2.14

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Enthält einen Kommentar zu diesem BGP-Nachbarn.

SNMP-ID:

2.93.1.2.15

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

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

Default-Wert:

leer

Route-Reflector-Client

Definiert, ob der entsprechende Nachbar als Route-Reflector-Client behandelt werden soll, so dass das Gerät iBGP-Routen zu diesem Client reflektiert.

Dieser Schalter ist nur dann wirksam, wenn

- das Gerät in der BGP-Instanz als Route-Reflector konfiguriert wurde, d. h. selbst Route-Reflector ist, oder
- die entfernte AS-Nummer der eigenen AS-Nummer entspricht (iBGP).

SNMP-ID:

2.93.1.2.16

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

ja
nein

Default-Wert:

nein

Nachbar-Profile

In dieser Tabelle konfigurieren Sie die BGP-Nachbar-Profile.

Die Nachbar-Profile ermöglichen es, eine allgemeine Konfiguration festzulegen und diese unterschiedlichen BGP-Nachbarn zuzuordnen.

Standardmäßig ist bereits ein Eintrag mit der Bezeichnung „DEFAULT“ und dem Kommentar „Default Entry“ vorgegeben.

SNMP-ID:

2.93.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Name

Enthält den Namen des Profils.

Dieser Name ist u. a. für die Angabe in folgenden Tabellen vorgesehen:

- **Nachbar-Profil** unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**
- **Nachbar-Profil** unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**
- **Nachbar-Profil** unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

SNMP-ID:

2.93.1.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

Default-Wert:

leer

Route-Update-Verzoegerung

Enthält die Zeit in Sekunden, die das Gerät mindestens zwischen dem Versenden von BGP-Update-Nachrichten an die BGP-Nachbarn mit diesem Profil wartet.

SNMP-ID:

2.93.1.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

Default-Wert:

30

Send-TTL

Bestimmt die TTL (time to live), die das Gerät für die TCP-Pakete an die BGP-Nachbarn dieses Profils einstellt.

Bei direkt verbundenen Nachbarn beträgt dieser Wert „1". Für eBGP-Umgebungen erhöhen Sie diesen Wert für jeden Hop um 1.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert und verwendet stattdessen standardmäßig den maximalen TTL-Wert.

Dieser Wert muss „0" betragen, wenn **Recv-TTL** einen Wert ungleich „0" besitzt. Das Gerät verwendet automatisch den Wert „1", wenn sowohl **Send-TTL** als auch **Recv-TTL** den Wert „0" besitzen.

SNMP-ID:

2.93.1.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

1

Recv-TTL

Bestimmt die TTL (time to live), die die ankommenden TCP-Pakete von BGP-Nachbarn dieses Profils mindestens beinhalten müssen. Ankommende TCP-Pakete mit geringerer TTL nimmt das Gerät nicht an.

In iBGP-Sitzungen ignoriert das Gerät diesen Wert.

Wenn dieser Wert ungleich „0“ ist, setzt das Gerät den Wert für **Send-TTL** intern auf „255“.

Dieser Wert muss „0“ betragen, wenn **Send-TTL** einen Wert ungleich „0“ besitzt.

SNMP-ID:

2.93.1.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

1

Besondere Werte:

0

Deaktiviert die TTL-Prüfung der ankommenden TCP-Pakete.

Keepalive

Bestimmt die Zeit für den Keepalive-Timer in Sekunden. Nach Ablauf dieser Zeit sendet das Gerät eine Keepalive-Meldung an die Nachbarn dieses Profils, um die BGP-Verbindung aufrecht zu erhalten.

Das Gerät sollte mindestens dreimal pro Holdtime eine Keepalive-Nachricht schicken. Der Wert darf deshalb max. ein Drittel der Haltezeit betragen. Bei einem höheren Wert oder einem Wert gleich „0“ verwendet LCOS intern automatisch ein Drittel der Haltezeit.

SNMP-ID:

2.93.1.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

Default-Wert:

30

0 … 65536

Haltezeit

Bestimmt die Zeit in Sekunden, für die das Gerät eine BGP-Verbindung ohne Datenverkehr als gültig anerkennt.

Das Gerät verhandelt diesen Wert mit dem BGP-Nachbarn bei einem Verbindungsaufbau. Der niedrigere der beiden Werte gilt danach als gültig.

Ist das Resultat dieser Verhandlung ein Wert von „0", setzt das Gerät diese Verbindung solange auf gültig, bis es eine Verbindungsfehlermeldung erhält oder die Verbindung zusammenbricht. In dieser Zeit sendet es keine Keepalive-Nachrichten an die BGP-Nachbarn, selbst wenn der Keepalive-Timer eine Zeitdauer enthält.

Die Werte „1" und „2" sind gemäß RFC nicht erlaubt.

SNMP-ID:

2.93.1.3.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

Default-Wert:

90

Besondere Werte:

0

Das Gerät setzt diese Verbindung solange auf gültig, bis es eine Verbindungsfehlermeldung erhält oder die Verbindung zusammenbricht. Die Sendung von Keepalive-Nachrichten ist deaktiviert, selbst wenn der Keepalive-Timer eine Zeitdauer enthält.

Private-AS-Filtern

Kontrolliert die Behandlung von privaten AS-Einträgen (64512 - 65535, 4200000000 - 4294967294) aus der AS_PATH-Liste von ausgehenden Präfixen der BGP-Nachbarn dieses Profils.

Bei iBGP-Verbindungen hat diese Option keine Funktion.

SNMP-ID:

2.93.1.3.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

Ersetzen

Ersetzt alle privaten AS-Nummern aus dem AS_PATH durch die AS-Nummer des Gerätes.

Entfernen

Entfernt alle privaten AS-Nummern aus dem AS_PATH.

Nein

Belässt alle privaten AS-Nummern im AS_PATH.

Default-Wert:

Nein

AS-Ueberschreiben

Aktiviert oder deaktiviert das Überschreiben von AS-Nummern im AS_PATH ausgehender Präfixe.

Bei aktivierter Option überschreibt das Gerät alle AS-Nummern des BGP-Nachbarn mit der eigenen AS-Nummer.

SNMP-ID:

2.93.1.3.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

Ja

Ersetzt alle AS-Nummern des BGP-Nachbarn im AS_PATH durch die eigene AS-Nummer.

Nein

Belässt alle AS-Nummern des BGP-Nachbarn im AS_PATH.

Default-Wert:

Nein

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.3.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Nachbar-Profile**

Mögliche Werte:

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

Default-Wert:

leer

Adressfamilie

In diesem Verzeichnis konfigurieren Sie die Einstellungen der IPv4- und IPv6-Parameter, die für alle Geräte eines BGP-Nachbar-Profils gelten.

SNMP-ID:

2.93.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

IPv4

In dieser Tabelle konfigurieren Sie die IPv4-Einstellungen, die für alle Geräte eines BGP-Nachbar-Profils gelten.

Standardmäßig ist bereits ein „aktiver" Eintrag mit der Bezeichnung „DEFAULT" vorgegeben.

SNMP-ID:

2.93.1.4.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie**

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

SNMP-ID:

2.93.1.4.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

Rtg-Tag

Legt fest, dass das Gerät die unter **Setup** > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4** fest konfigurierten IPv4-Routen nur dann an den BGP-Nachbarn ankündigt, wenn deren Routing-Tag dem hier konfigurierten Routing-Tag entspricht.

SNMP-ID:

2.93.1.4.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Aktiviert oder deaktiviert den Versand von IPv4-NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

SNMP-ID:

2.93.1.4.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Ja

Dieser Eintrag ist aktiv. Das Gerät versendet IPv4-Routen an die BGP-Nachbarn.

Nein

Dieser Eintrag ist nicht aktiv. Das Gerät versendet keine IPv4-Routen an die BGP-Nachbarn, je nach Einstellung aber ggf. IPv6-Routen.

Default-Wert:

Nein

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard" als auch die Option „Erweitert" deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

SNMP-ID:

2.93.1.4.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Standard
Wenn aktiviert, erlaubt das Gerät die Standard-Community-Attribute in den NLRI gemäß *RFC 1997*.

Erweitert
Wenn aktiviert, erlaubt das Gerät die erweiterten Community-Attribute in den NLRI gemäß *RFC 4360*.

Default-Wert:

Standard

Erweitert

Nexthop-Self

Aktiviert oder deaktiviert den Austausch des Nexthops durch die eigene IP-Adresse in den NLRI.

SNMP-ID:

2.93.1.4.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Ja
Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein
Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer
Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Default-Wert:

Nein

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht" ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

SNMP-ID:

2.93.1.4.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

0 … 65535

Default-Wert:

0

Lokale-Praeferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Lokale Präferenz" ist ein BGP-Standard-Attribut (LOCAL_PREF), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz" von 100.

SNMP-ID:

2.93.1.4.1.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

0 … 99999

Default-Wert:

100

Praefix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

SNMP-ID:

2.93.1.4.1.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Die Präfix-Beschränkung ist deaktiviert.

Route-Weiterverteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

SNMP-ID:

2.93.1.4.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

Statisch

Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Verbunden

Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.4.1.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**

Mögliche Werte:

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

IPv6

In dieser Tabelle konfigurieren Sie die IPv6-Einstellungen, die für alle Geräte eines BGP-Nachbar-Profils gelten.

Standardmäßig ist bereits ein „inaktiver" Eintrag mit der Bezeichnung „DEFAULT" vorgegeben.

SNMP-ID:

2.93.1.4.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie**

Nachbar-Profil

Enthält den Namen des entsprechenden Nachbar-Profils, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile** gespeichert ist.

SNMP-ID:

2.93.1.4.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

Default-Wert:

leer

Rtg-Tag

Legt fest, dass das Gerät die unter **Setup** > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6** fest konfigurierten IPv6-Routen nur dann an den BGP-Nachbarn ankündigt, wenn deren Routing-Tag dem hier konfigurierten Routing-Tag entspricht.

SNMP-ID:

2.93.1.4.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Aktiviert oder deaktiviert den Versand von NLRI dieser Adressfamilie an die BGP-Nachbarn, die dieses Nachbar-Profil verwenden.

SNMP-ID:

2.93.1.4.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Ja

Dieser Eintrag ist aktiv. Das Gerät versendet IPv6-Routen an die BGP-Nachbarn.

Nein

Dieser Eintrag ist nicht aktiv. Das Gerät versendet keine IPv6-Routen an die BGP-Nachbarn, je nach Einstellung aber ggf. IPv4-Routen.

Default-Wert:

Nein

Communities

Bestimmt, welche Community-Attribute die NLRI dieser Adressfamilie an eBGP-Nachbarn enthalten darf, die das entsprechende Nachbar-Profil verwenden.

Wenn sowohl die Option „Standard" als auch die Option „Erweitert" deaktiviert sind, überträgt das Gerät keine Community-Attribute in den NLRI zu eBGP-Nachbarn.

Diese Option hat keine Funktion bei der Kommunikation mit iBGP-Nachbarn.

SNMP-ID:

2.93.1.4.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Standard

Wenn aktiviert, erlaubt das Gerät die Standard-Community-Attribute in den NLRI gemäß *RFC 1997*.

Erweitert

Wenn aktiviert, erlaubt das Gerät die erweiterten Community-Attribute in den NLRI gemäß *RFC 4360*.

Default-Wert:

Standard

Erweitert

Nexthop-Self

Aktiviert oder deaktiviert den Austausch des Nexthop-Attributes durch die eigene IP-Adresse in den NLRI.

SNMP-ID:

2.93.1.4.2.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Ja

Tauscht in den NLRI die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus.

Nein

Lässt die IP-Adresse des Nexthops in den NLRI unverändert.

Immer

Tauscht in den NLRI immer die IP-Adresse des Nexthops gegen die eigene IP-Adresse aus auch wenn das Gerät als Route Reflector konfiguriert ist.

Default-Wert:

Nein

Gewicht

Gibt die Standard-Gewichtung für NLRI an.

Diese Angabe beeinflusst die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Gewicht" ist ein proprietäres Attribut, das das Gerät nicht in BGP-Update-Nachrichten an andere eBGP-Nachbarn propagiert. Dieses Attribut ist somit nur auf dem lokalen Router gültig.

SNMP-ID:

2.93.1.4.2.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

0 … 65535

Default-Wert:

0

Lokale-Praeferenz

Ähnlich der Einstellung bei **Gewicht** ermöglicht diese Angabe die Bevorzugung von gleichen Präfix-Ankündigungen, die das Gerät von unterschiedlichen BGP-Nachbarn erhalten hat. Das Präfix mit der höheren Gewichtung erhält den Vorzug.

„Lokale Präferenz" ist ein BGP-Standard-Attribut (LOCAL_PREF), das das Gerät per iBGP an Nachbarn propagiert. Alle Pfade besitzen in der Standardeinstellung eine „Lokale Präferenz" von 100.

SNMP-ID:

2.93.1.4.2.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

0 … 99999

Default-Wert:

100

Praefix-Limit

Bestimmt die Anzahl der akzeptierten Präfixe pro BGP-Nachbar des angegebenen Nachbar-Profils.

Alle Präfixe, die über dieses Limit hinausgehen, verwirft das Gerät.

SNMP-ID:

2.93.1.4.2.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Die Präfix-Beschränkung ist deaktiviert.

Route-Weiterverteilen

Bestimmt, ob das Gerät bestimmte Routen an BGP-Nachbarn dieses Profils weiterleiten soll.

Wenn keine Option ausgewählt ist, verteilt das Gerät keine Routen an die BGP-Nachbarn dieses Nachbar-Profils (Default-Einstellung).

SNMP-ID:

2.93.1.4.2.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

Statisch

Das Gerät verteilt statische Routen aus der Routing-Tabelle an die BGP-Nachbarn.

Verbunden

Das Gerät verteilt Routen von direkt angeschlossenen Netzwerken an die BGP-Nachbarn.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.4.2.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**

Mögliche Werte:

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

Regelwerk

In diesem Verzeichnis konfigurieren Sie die Filter-Einstellungen für ausgehende und ankommende NLRI.

SNMP-ID:

2.93.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Standard

Das Gerät wendet für einen BGP-Nachbarn diese Standardregel an, wenn unklar ist, ob es dessen Präfix akzeptieren oder ablehnen soll. Die Ursache dafür kann sein:

- Für diesen BGP-Nachbarn ist keine Regel konfiguriert.
- Der angegebene Filter existiert nicht.
- Kein Filter unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter** trifft zu.

SNMP-ID:

2.93.1.5.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Mögliche Werte:

Erlauben

Das Gerät akzeptiert das Präfix des BGP-Nachbarn.

Ablehnen

Das Gerät lehnt das Präfix des BGP-Nachbarn ab.

Anpassungen

Dieses Verzeichnis enthält die Liste möglicher Anpassungen von NLRI. Die Aktionen der Tabelle **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen** verwenden die hier konfigurierten Anpassungen.

SNMP-ID:

2.93.1.5.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Basis

Diese Tabelle enthält Manipulationen der Basis-Attribute von NLRIs.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen durch.

Die Angabe von Basis-Attributen ist optional. Wenn die Aktion nur ein Basis-Attribut ändern soll, geben Sie an der entsprechenden Stelle den zu ändernden Wert ein und lassen Sie die übrigen Attribute in der jeweiligen Standardeinstellung.

SNMP-ID:

2.93.1.5.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen**

Name

Enthält den Namen für diese Modifikation.

Auf diesen Eintrag beziehen sich die unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen** konfigurierten Aktionen.

SNMP-ID:

2.93.1.5.2.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

Default-Wert:

leer

Gewicht-Setzen

Wenn konfiguriert, ändert das Gerät die Gewichtung einer NLRI auf den hier angegebenen Wert.

SNMP-ID:

2.93.1.5.2.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Das Gerät behält den ursprünglichen Wert der NLRI bei.

Local-Pref.-Setzen

Wenn konfiguriert, ändert das Gerät den lokalen Präferenz-Wert einer NLRI auf den hier angegebenen Wert.

SNMP-ID:

2.93.1.5.2.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Das Gerät behält den ursprünglichen Wert der NLRI bei.

MED-Entfernen

Wenn konfiguriert, löscht das Gerät den Multi Exit Discriminator (MED) einer NLRI, bevor es die Einstellung unter **MED-Setzen** verarbeitet.

SNMP-ID:

2.93.1.5.2.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

Nein

Der MED verbleibt in der NLRI.

Ja

Das Gerät löscht den MED der NLRI.

Default-Wert:

Nein

MED-Setzen

Wenn konfiguriert, ändert das Gerät den Multi Exit Discriminator (MED) einer NLRI auf den hier angegebenen Wert. Falls die NLRI keinen MED beinhaltet, erzeugt das Gerät dieses Attribut.

SNMP-ID:

2.93.1.5.2.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Das Gerät behält den ursprünglichen Wert der NLRI bei.

Nexthop-Setzen

Wenn konfiguriert, ändert das Gerät die Nexthop-IP-Adresse einer NLRI auf den hier angegebenen Wert.

SNMP-ID:

2.93.1.5.2.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

Besondere Werte:

leer

Das Gerät behält den ursprünglichen Wert der NLRI bei.

`self`

Das Gerät ersetzt die Nexthop-IP-Adresse durch seine eigene IP-Adresse.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.2.1.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

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

Default-Wert:

leer

Link-Local-Nexthop-Setzen

Wenn konfiguriert, ändert das Gerät die Nexthop-Link-Lokale IPv6-Adresse einer NLRI auf den hier angegebenen Wert. Ist nur wirksam bei IPv6-Präfixen.

SNMP-ID:

2.93.1.5.2.1.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

AS-Pfad

Diese Tabelle enthält Manipulationen der AS_PATH-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. **Private-Filtern**
2. **Ersetzen**
3. Gemeinsam **Voranstellen-Anzahl** und **Voranstellen**

SNMP-ID:

2.93.1.5.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen**

Name

Enthält den Namen für diese Modifikation.

Auf diesen Eintrag beziehen sich die unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen** konfigurierten Aktionen.

SNMP-ID:

2.93.1.5.2.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

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

Default-Wert:

leer

Private-AS-Filtern

Wenn konfiguriert, ändert das Gerät die Angabe der privaten AS-Nummern im AS_PATH-Attribut einer NLRI gemäß dieser Einstellung.

SNMP-ID:

2.93.1.5.2.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

Ersetzen

Das Gerät tauscht die vorhandenen privaten AS-Nummern gegen die AS-Nummer der aktuellen BGP-Instanz.

Entfernen

Das Gerät entfernt alle privaten AS-Nummern.

Nein

Das Gerät behält die vorhandenen privaten AS-Nummern der NLRI.

Default-Wert:

Nein

Ersetzen

Wenn konfiguriert, ändert das Gerät das AS_PATH-Attribut der NLRI auf den hier angegebenen Wert.

SNMP-ID:

2.93.1.5.2.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

max. 62 Zeichen aus `[0-1],`

Default-Wert:

leer

Besondere Werte:

leer

Das Gerät behält den ursprünglichen Wert der NLRI bei.

Voranstellen

Wenn konfiguriert, stellt das Gerät dem AS_PATH-Attribut der NLRI so oft den hier angegebenen Wert voran, wie unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad** > **Voranstellen-Anzahl** konfiguriert.

SNMP-ID:

2.93.1.5.2.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

max. 10 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Besondere Werte:

leer

Das Gerät behält den ursprünglichen Wert der NLRI bei.

self

Das Gerät stellt dem AS_PATH-Attribut der NLRI seine eigene AS-Nummer voran.

last

Das Gerät stellt dem AS_PATH-Attribut der NLRI die zuletzt vorangestellte AS-Nummer voran.

Voranstellen-Anzahl

Bestimmt, wie oft das Gerät dem AS_PATH-Attribut der NLRI eine AS-Nummer voranstellen soll.

SNMP-ID:

2.93.1.5.2.2.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Das Gerät behält den ursprünglichen Wert der NLRI bei, auch wenn unter **Voranstellen** ein Eintrag konfiguriert sein sollte.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.2.2.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**

Mögliche Werte:

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

Default-Wert:

leer

Communities

Diese Tabelle enthält Manipulationen der Community-Attribute von NLRI.

Wenn eine Aktion auf einen Eintrag dieser Tabelle zugreift, führt das Gerät alle in der entsprechenden Zeile aufgeführten Änderungen in der folgenden Reihenfolge durch:

1. **Loeschen**
2. **Hinzufügen**
3. **Entfernen**

SNMP-ID:

2.93.1.5.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen**

Name

Enthält den Namen für diese Modifikation.

Auf diesen Eintrag beziehen sich die unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen** konfigurierten Aktionen.

SNMP-ID:

2.93.1.5.2.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Raeumen

Legt fest, ob das Gerät unbekannte Communities aus der NLRI löscht.

Bekannte Communities bleiben auch dann bestehen, wenn diese Option auf „Ja“ steht.

Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`

Mehr Informationen hierzu finden Sie unter *RFC 1997* und *RFC 3765*.

SNMP-ID:

2.93.1.5.2.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**

Mögliche Werte:

Ja

Das Gerät löscht unbekannte Communities aus der NLRI.

Nein

Das Gerät ändert die Communities einer NLRI nicht.

Default-Wert:

Nein

Hinzufuegen

Legt fest, welche Communities das Gerät einer NLRI hinzufügt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

SNMP-ID:

2.93.1.5.2.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**

Mögliche Werte:

max. 62 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Entfernen

Legt fest, welche Communities das Gerät aus einer NLRI entfernt.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

Bekannte Communities lassen sich nicht aus NLRI entfernen. Bekannte Communities sind:

- `no-peer`
- `no-export`
- `no-advertise`
- `no-export-subconfed`

Folgende Eingabeformate sind für Communities möglich:

Eingabeformat	Community
1:2	Standard Community
1.2.3.4:1	IPv4-spezifische Extended Community
roc:1.2.3.4:1	IPv4-spezifische Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4-spezifische Route Target Extended Community
ext2:1:2	zwei Byte AS Extended Community
ext4:1:2	vier Byte AS Extended Community
roc:1:2	zwei Byte AS Route Origin Extended Community (Site-of-Origin (SoO))
rtc:1:2	zwei Byte AS Route Origin Extended Community
roc:ext4:1:2	vier Byte AS Route Origin Extended Community (Site-of-Origin (SoO))

SNMP-ID:

2.93.1.5.2.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**

Mögliche Werte:

max. 62 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.2.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Aktionen

Diese Tabelle enthält Aktionen, die die entsprechenden Anpassungen in NLRIs vornehmen.

Die für die jeweilige Aktion angegebenen Anpassungen konfigurieren Sie im Verzeichnis **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen**.

SNMP-ID:

2.93.1.5.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Name

Enthält den Namen für diese Aktion.

Auf diesen Eintrag beziehen sich die unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter** eingetragenen Aktionen.

SNMP-ID:

2.93.1.5.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

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

Default-Wert:

leer

Basis

Enthält den Namen für die Manipulation von Basis-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Tabelle unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Basis**.

SNMP-ID:

2.93.1.5.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

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

Default-Wert:

leer

AS-Pfad

Enthält den Namen für die Manipulation von AS_PATH-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Tabelle unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **AS-Pfad**.

SNMP-ID:

2.93.1.5.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

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

Default-Wert:

leer

Community

Enthält den Namen für die Manipulation von Community-Einträgen der NLRI.

Dieser Eintrag bezieht sich auf die Einträge der Tabelle unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Anpassungen** > **Communities**.

SNMP-ID:

2.93.1.5.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen**

Mögliche Werte:

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

Default-Wert:

leer

Listen

Dieses Verzeichnis enthält Definitionen, anhand derer die BGP-Filter NLRIs identifizieren und die entsprechenden Aktionen ausführen.

SNMP-ID:

2.93.1.5.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Praefix

Diese Tabelle enthält Präfix-Listen, um NLRIs anhand ihres Netzwerkes (Präfix) und ihrer Netzmaske (Präfix-Länge) zu erkennen.

Ein Eintrag kann mehrere Präfixe enthalten.

SNMP-ID:

2.93.1.5.4.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen**

Name

Enthält den Namen für diese Präfix-Liste.

SNMP-ID:

2.93.1.5.4.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

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

Default-Wert:

leer

IP-Adresse

Enthält die IPv4- oder IPv6-Adresse des Netzwerkes.

SNMP-ID:

2.93.1.5.4.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Default-Wert:

leer

Praefix-Laenge

Enthält die Netzmaske oder Präfix-Länge des Netzwerkes.

Dieser Eintrag legt fest, wie viele höchstwertige Bits (Most Significant Bit, MSB) der IP-Adresse für eine Übereinstimmung notwendig sind.

Die Präfix-Länge der NLRI muss für eine Übereinstimmung diesem Wert exakt entsprechen, wenn nicht für **Laenge-Min** und **Laenge-Max** andere Werte vorgegeben sind.

SNMP-ID:

2.93.1.5.4.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Das Netzwerk der NLRI stimmt dann überein, wenn es aus derselben IP-Adressfamilie stammt, die unter **IP-Adresse** vorgegeben ist.

Laenge-Min

Enthält die minimale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

SNMP-ID:

2.93.1.5.4.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Laenge-Max

Enthält die maximale Präfix-Länge, die das Netzwerk der NLRI für eine Übereinstimmung aufweisen darf.

Ist dieser Eintrag kleiner als der Wert bei **Praefix-Min**, gilt ein Wert von „0“.

SNMP-ID:

2.93.1.5.4.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Keine maximale Präfix-Länge vorgesehen.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.4.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**

Mögliche Werte:

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

Default-Wert:

leer

AS-Pfad

Diese Tabelle enthält AS-Pfad-Listen, um NLRIs anhand ihres AS_PATH-Attributes zu erkennen.

SNMP-ID:

2.93.1.5.4.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen**

Name

Enthält den Namen für diese AS-Pfad-Liste.

SNMP-ID:

2.93.1.5.4.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **AS-Pfade**

Mögliche Werte:

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

Default-Wert:

leer

AS-Pfad-Regex

Enthält einen regulären Ausdruck, der das AS_PATH-Attribut der NLRI überprüft. Beispiele:

- `.*_100`: filtert alle NLRIs, die in „AS100“ ihren Ursprung haben.
- `.*_(100|200)`: filtert alle NLRIs, die in „AS100“ oder „AS200“ ihren Ursprung haben.
- `100_(.*_)?(500|400)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“, die vorher zusätzlich den Weg über Netzwerke mit den AS-Nummern „AS500“ oder „AS400“ (oder beide) genommen haben.
- `100_(500|400|123)_.*`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“, die dieser vorher direkt von BGP-Nachbarn mit den AS-Nummern „AS500“, „AS400“ oder „AS123“ erhalten hat.
- `100_(100_)*(300_)*300`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100“, die dieser vorher von seinem BGP-Nachbarn mit der AS-Nummer „AS300“ erhalten hat. Der Ausdruck berücksichtigt auch AS-Prepend Pfade.

- `100_.*_200`: filtert alle NLRIs vom BGP-Nachbarn mit der AS-Nummer „AS100", die im Netzwerk mit der AS-Nummer „AS200" gestartet sind. Die Route, die die NLRIs vom „AS200" bis zum „AS100" genommen haben, ist hierbei unwichtig.

Der Ausdruck muss in PERL-Syntax konstruiert sein.

SNMP-ID:

2.93.1.5.4.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **AS-Pfade**

Mögliche Werte:

max. 62 Zeichen aus `[0-9]$()*+-.?[\]^_{|}`

Default-Wert:

leer

Besondere Werte:

leer

Dieser Listeneintrag ist für alle AS_PATH-Attribute der NLRI gültig.

Regex-Treffer

Bestimmt, wie detailliert der reguläre Ausdruck unter **AS-Pfad-Regex** mit dem AS_PATH-Attribut der NLRI übereinstimmen muss, damit der Listeneintrag gültig ist.

SNMP-ID:

2.93.1.5.4.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **AS-Pfade**

Mögliche Werte:

Vollständig

Der reguläre Ausdruck beschreibt das gesamte AS_PATH-Attribut der NLRI.

Teilweise

Der reguläre Ausdruck beschreibt nur Abschnitte des AS_PATH-Attributes.

Default-Wert:

Vollständig

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.4.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **AS-Pfade**

Mögliche Werte:

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

Default-Wert:

leer

Communities

Diese Tabelle enthält Community-Listen, um NLRIs anhand ihres Community-Attributes zu erkennen.

SNMP-ID:

2.93.1.5.4.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen**

Name

Enthält den Namen für diese Community-Liste.

SNMP-ID:

2.93.1.5.4.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Communities

Enthält Communities, die dem Community-Attribut der NLRI für eine Übereinstimmung entsprechen müssen.

Die Angabe der Communities erfolgt als kommaseparierte Liste (`<AS-Nummer1>:<Wert1>,<AS-Nummer2>:<Wert2>,<AS-Nummer3>:<Wert3>`).

SNMP-ID:

2.93.1.5.4.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Communities**

Mögliche Werte:

max. 62 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.4.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

Treffer

Diese Tabelle kombiniert Listeneinträge aus dem Verzeichnis **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen**, um mehrere Listeneinträge auf Übereinstimmungen mit NLRI abzugleichen.

SNMP-ID:

2.93.1.5.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.93.1.5.5.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

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

Default-Wert:

leer

Praefix

Enthält den entsprechenden Eintrag einer Präfix-Liste unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Praefixe**.

SNMP-ID:

2.93.1.5.5.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

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

Default-Wert:

leer

Besondere Werte:

leer

Behandelt die NLRI, als würde eine Übereinstimmung mit der Präfix-Liste bestehen.

AS-Pfad

Enthält den entsprechenden Eintrag einer AS-Pfad-Liste unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **AS-Pfade**.

SNMP-ID:

2.93.1.5.5.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

max. 80 Zeichen aus `[A-Z][a-z][0-9]-_,`

Default-Wert:

leer

Besondere Werte:

leer

Behandelt die NLRI, als würde eine Übereinstimmung mit der AS-Pfad-Liste bestehen.

Communities

Enthält den entsprechenden Eintrag einer Community-Liste unter **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Listen** > **Communities**.

SNMP-ID:

2.93.1.5.5.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

max. 80 Zeichen aus `[A-Z][a-z][0-9]-_,`

Default-Wert:

leer

Besondere Werte:

leer

Behandelt die NLRI, als würde eine Übereinstimmung mit der Community-Liste bestehen.

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.5.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer**

Mögliche Werte:

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

Default-Wert:

leer

Filter

Diese Tabelle enthält Filter, die eine NLRI von einem oder an einen BGP-Nachbarn durchlaufen muss, wenn dieser Nachbar entsprechend konfiguriert ist.

Bei mehreren Filtereinträgen mit identischem Namen bearbeitet das Gerät diese Filter gemäß der konfigurierten Priorität, bis ein Filter auf die NLRI zutrifft. Danach beendet das Gerät den Filterdurchlauf.

SNMP-ID:

2.93.1.5.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk**

Name

Enthält den Namen für diesen Eintrag.

Falls Einträge mit einem identischen Namen existieren, gehören diese Einträge zur selben Filterkette. Das Gerät arbeitet die Einträge dieser Filterkette entsprechend ihrer jeweiligen Priorität ab.

SNMP-ID:

2.93.1.5.6.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

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

Default-Wert:

leer

Prioritaet

Gibt die Priorität dieses Eintrages an.

Falls Einträge mit einem identischen Namen existieren, gehören diese Einträge zur selben Filterkette. Das Gerät arbeitet die Einträge dieser Filterkette entsprechend ihrer jeweiligen Priorität ab. Ein höherer Wert bedeutet eine höhere Priorität.

SNMP-ID:

2.93.1.5.6.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

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

Default-Wert:

0

Adressfamilie

Gibt an, für welche Adressfamilie dieser Filter gilt.

Ohne ausgewählte Option ist dieser Eintrag deaktiviert.

SNMP-ID:

2.93.1.5.6.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

IPv4
IPv6

Default-Wert:

IPv4

IPv6

Treffer

Gibt den Namen eines Eintrages aus der Tabelle **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Treffer** an.

Das Gerät wendet diesen Filter an, wenn die NLRI mit den Kriterien übereinstimmt.

Wenn dieses Feld auf einen ungültigen Namen verweist, verweigert das Gerät die NLRI und führt keine weiteren Filter in der aktuellen Filterkette aus.

SNMP-ID:

2.93.1.5.6.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

max. 80 Zeichen aus `[0-9][A-Z][a-z]-_,!`

Default-Wert:

leer

Besondere Werte:

leer

Das Gerät behandelt die NLRI, als ob sie mit den Kriterien übereinstimmt.

Regel

Gibt an, ob das Gerät die gefilterte NLRI weiter verarbeiten soll, wenn dieser Filter für diese NLRI gültig ist.

SNMP-ID:

2.93.1.5.6.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

Ablehnen

Es erfolgt keine weitere Verarbeitung.

Erlauben

Das Gerät verarbeitet die NLRI weiter.

Default-Wert:

Ablehnen

Aktion

Gibt an, welche Aktion aus der Tabelle **Setup** > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Aktionen** das Gerät auf die NLRI anwenden soll.

Wenn dieses Feld leer ist oder auf einen ungültigen Namen verweist, führt das Gerät keine Aktion aus.

SNMP-ID:

2.93.1.5.6.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.5.6.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Regelwerk** > **Filter**

Mögliche Werte:

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

Default-Wert:

leer

Netzwerke

In diesem Verzeichnis konfigurieren Sie die Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von der Einstellung unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4/IPv6** > **Aktiv**.

SNMP-ID:

2.93.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

IPv4

In diesem Verzeichnis konfigurieren Sie die IPv4-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4**.

Die Mindestangabe für einen neuen gültigen Eintrag ist eine **IP-Adresse**.

SNMP-ID:

2.93.1.6.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke**

IP-Adresse

Beinhaltet die IPv4-Adresse oder das Präfix des Netzwerkes.

SNMP-ID:

2.93.1.6.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

Netzmaske

Beinhaltet die IPv4-Netzmaske des Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0.0.0.0` besitzt.

SNMP-ID:

2.93.1.6.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4**

Mögliche Werte:

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

Default-Wert:

0.0.0.0

Rtg-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv4** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

SNMP-ID:

2.93.1.6.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4**

Mögliche Werte:

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

Default-Wert:

0

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell für Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

SNMP-ID:

2.93.1.6.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4**

Mögliche Werte:

Statisch

Das Netzwerk ist immer für Ankündigungen ausgewählt.

Dynamisch

Das Netzwerk ist nur für Ankündigungen ausgewählt, wenn es in der aktiven Routing-Tabelle erscheint.

Default-Wert:

Statisch

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.6.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv4**

Mögliche Werte:

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

IPv6

In diesem Verzeichnis konfigurieren Sie die IPv6-Netzwerke, die das Gerät an die BGP-Nachbarn verteilt.

Die Verteilung dieser Netzwerke ist abhängig von den Einschränkungen unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6**.

Die Mindestangabe für einen neuen gültigen Eintrag ist ein **Praefix**.

SNMP-ID:

2.93.1.6.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke**

Praefix

Beinhaltet das Präfix (IPv6-Adressteil) des Netzwerkes.

SNMP-ID:

2.93.1.6.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Default-Wert:

leer

Praefix-Laenge

Beinhaltet die Präfix-Länge des IPv6-Netzwerkes.

Die Route wird zur Default-Route dieser Adressfamilie, wenn dieser Eintrag die Default-Einstellung `0` besitzt.

SNMP-ID:

2.93.1.6.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Rtg-Tag

Enthält das Routing-Tag für dieses Netzwerk.

Die Tabelle unter **Setup** > **Routing-Protokolle** > **BGP** > **Adressfamilie** > **IPv6** nutzt diesen Eintrag zur Filterung der Kommunikation mit den BGP-Nachbarn.

SNMP-ID:

2.93.1.6.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6**

Mögliche Werte:

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

Default-Wert:

0

Typ

Bestimmt, ob das Gerät dieses Netzwerk generell in Ankündigungen nutzt oder nur, wenn dieses Netzwerk in der aktiven Routing-Tabelle erscheint.

SNMP-ID:

2.93.1.6.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6**

Mögliche Werte:

Statisch

Das Gerät verwendet dieses Netzwerk immer in Ankündigungen.

Dynamisch

Das Gerät verwendet dieses Netzwerk nur in Ankündigungen, wenn es in der aktiven Routing-Tabelle erscheint.

Default-Wert:

Statisch

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.1.6.2.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP** > **Netzwerke** > **IPv6**

Mögliche Werte:

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

Aktiv

Aktiviert oder deaktiviert die BGP-Funktion im Gerät.

Bei deaktivierter BGP-Funktion haben die BGP-spezifischen show-Kommandozeilen-Befehle keine Funktion.

SNMP-ID:

2.93.1.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Mögliche Werte:

Ja

BGP ist im Gerät aktiv.

Nein

BGP ist im Gerät nicht aktiv.

Default-Wert:

Nein

Auto-Neustart

Gibt an, ob ein BGP-Nachbar automatisch nach einem Fehler neu gestartet werden soll.

SNMP-ID:

2.93.1.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Mögliche Werte:

Ja

Der automatische Neustart ist aktiviert.

Nein

Der automatische Neustart ist deaktiviert.

Default-Wert:

Ja

Manueller-Start

Mit dieser Aktion starten Sie einen BGP-Nachbarn, falls dieser zuvor manuell durch einen manuellen Stopp angehalten wurde.

Geben Sie als Parameter den Namen des Nachbarn an, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** im Feld **Name** eingetragen ist (max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`).

Trifft die Angabe des Parameters auf mehrere Nachbarn zu, baut das Gerät zu allen Nachbarn jeweils eine Verbindung auf.

Die angegebenen Nachbarn müssen folgende Voraussetzungen erfüllen:

- Sie müssen komplett für BGP konfiguriert sein.
- Ihre **Verbindungsart** unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** darf nicht auf „Passiv" eingestellt sein.

SNMP-ID:

2.93.1.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Manueller-Stopp

Mit dieser Aktion stoppen Sie einen BGP-Nachbarn manuell.

Geben Sie als Parameter den Namen des Nachbarn an, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** im Feld **Name** eingetragen ist (max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`).

Trifft die Angabe des Parameters auf mehrere Nachbarn zu, beendet das Gerät zu allen Nachbarn die Verbindung.

Bestehen mehrere offene Verbindungen zum Nachbarn, beendet das Gerät alle diese Verbindungen.

SNMP-ID:

2.93.1.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Aktiver-Start

Startet einen BGP-Nachbarn manuell.

Funktion und Rahmenbedingungen sind identisch zu **Manueller-Start**, allerdings funktioniert der Verbindungsaufbau in diesem Fall auch mit Nachbarn, deren **Verbindungsart** unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** auf „Passiv" eingestellt ist.

SNMP-ID:

2.93.1.11

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Neustart

Mit dieser Aktion starten Sie einen BGP-Nachbarn neu.

Geben Sie als Parameter den Namen des Nachbarn an, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** im Feld **Name** eingetragen ist (max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`).

SNMP-ID:

2.93.1.12

Pfad Telnet:

Setup > **Routing-Protocols** > **BGP**

Global-Read-Only-Timer

Zeit in Sekunden, die das Gerät nach dem Start im Read-Only-Modus bleibt. Solange das Gerät im Read-Only-Modus arbeitet, empfängt es Routen von BGP-Nachbarn, führt jedoch keinen „kürzester-Pfad-Algorithmus" zur Routen-Berechnung aus. Damit versendet es auch keine Routen an BGP-Nachbarn. Dieser Schalter dient der Performance-Optimierung für zentralseitige Geräte, wenn viele mögliche Routen vorhanden sind. Das hat zur Folge, dass das Gerät erst dann eine Routen-Berechnung ausführt, wenn es alle möglichen Routen empfangen hat.

SNMP-ID:

2.93.1.13

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Der Timer ist deaktiviert.

Peer-Read-Only-Timer

Zeit in Sekunden, die das Gerät für pro individuellen Nachbar nach dem Start im Read-Only-Modus bleibt. Solange das Gerät im Read-Only-Modus arbeitet, empfängt es Routen von diesem BGP-Nachbarn, führt jedoch keinen „kürzester-Pfad-Algorithmus" zur Routen-Berechnung aus. Damit versendet es auch keine Routen an diesen BGP-Nachbarn. Sobald ein BGP-Nachbar nach dem Senden seiner Routen einen `End-Of-RIB`-Marker sendet, verlässt das empfangene Gerät automatisch den Read-Only-Modus und startet die Routen-Berechnung. LANCOM-Router senden nach erfolgreichem Senden aller Routen an einen Nachbarn automatisch einen `End-Of-RIB`-Marker.

SNMP-ID:

2.93.1.14

Pfad Telnet:

Setup > **Routing-Protokolle** > **BGP**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Der Timer ist deaktiviert.

Refresh-Anforderung-Senden

Diese Aktion sendet eine `BGP-Route-Refresh`-Nachricht an einen BGP-Nachbarn. Falls dieser Nachbar die Option `Route-Refresh` unterstützt, so sendet dieser Nachbar (erneut) seine Routen. Durch `Route-Refresh` können die Routen eines Nachbarn erneut empfangen werden, ohne die BGP-Verbindung neu zu starten.

Geben Sie als Parameter den Namen des Nachbarn an, wie er unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn** im Feld **Name** eingetragen ist (max. 16 Zeichen aus `[A-Z][a-z][0-9]-_`). Geben Sie optional die Adressfamilie (IPv4 oder IPv6) mit an.

SNMP-ID:

2.93.1.15

Pfad Telnet:

Setup > **Routing-Protocols** > **BGP**

5.1.8 Ergänzungen im Status-Menü

Routing-Protokolle

Dieses Verzeichnis zeigt die Statistiken für BGP-Verbindungen und den Route-Monitor an.

SNMP-ID:

1.93

Pfad Telnet:

Status

BGP

Dieses Verzeichnis zeigt die Statistiken für BGP-Verbindungen an.

SNMP-ID:

1.93.1

Pfad Telnet:

Status > **Routing-Protokolle**

Nachbarn

Diese Tabelle enthält die Statistiken für Verbindungen zu konfigurierten BGP-Nachbarn.

Die Tabelle behält ihre Einträge, wenn Sie BGP deaktivieren.

SNMP-ID:

1.93.1.1

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP**

IP-Adresse

Enthält die IPv4- oder IPv6-Adresse des BGP-Nachbarn.

Die IP-Adresse ist konfiguriert unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**.

SNMP-ID:

1.93.1.1.1

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Port

Enthält den Port, auf dem der BGP-Nachbar einkommende BGP-Nachrichten erwartet und den das Gerät entsprechend für ausgehende Verbindungen in den Verbindungsarten „Aktiv“ oder „Verzögert“ verwendet.

Der Port ist konfiguriert unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**.

SNMP-ID:

1.93.1.1.2

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Loopback-Adresse

Enthält die Absender-Adresse (IPv4 oder IPv6), die das Gerät für den Verbindungsaufbau mit dem BGP-Nachbarn nutzt.

Die Loopback-Adresse ist konfiguriert unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**.

Wenn keine Loopback-Adresse konfiguriert ist, enthält dieses Feld die verwendete Absender-Adresse.

SNMP-ID:

1.93.1.1.3

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Rtg-Tag

Enthält das Routing-Tag. Stimmt das Routing-Tag nicht mit dem der ankommenden Verbindung überein, verweigert das Gerät den Verbindungsaufbau.

Das Routing-Tag ist konfiguriert unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**.

SNMP-ID:

1.93.1.1.4

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Entferntes-AS

Enthält die AS-Nummer des BGP-Nachbarn.

Ist die AS-Nummer des BGP-Nachbarn identisch zur AS-Nummer der eigenen BGP-Instanz des Gerätes, handelt es sich bei dem Nachbarn um einen iBGP-Peer (Internal BGP) innerhalb des AS.

Das entfernte AS ist konfiguriert unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbarn**.

SNMP-ID:

1.93.1.1.5

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Router-ID

Enthält die Router-ID (IPv4-Adresse), die dem BGP-Nachbarn zugeordnet ist. Der BGP-Nachbar teilt seine Router-ID beim Verbindungsaufbau in der OPEN-Nachricht mit. Soll eine BGP-Verbindung über IPv6 verwendet werden, ist es erforderlich, als Router-ID ebenfalls eine eindeutige 32-Bit Zahl zu verwenden (z. B. eine fiktive IPv4-Adresse). Die Router-ID muss zwischen BGP-Nachbarn pro Gerät eindeutig sein.

SNMP-ID:

1.93.1.1.6

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Zustand

Enthält den aktuellen Zustand der Verbindung zum BGP-Nachbarn.

SNMP-ID:

1.93.1.1.7

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

ruhend

In diesem Zustand werden keine Verbindungen zum Nachbarn aufgebaut oder vom Nachbarn akzeptiert. Es sind noch keine Ressourcen bereitgestellt, um eine Verbindung aufzubauen.

verbinden

Das Gerät baut aktiv eine Verbindung zum Nachbarn auf und wartet auf die Vollendung des TCP-Handshakes.

aktiv

Das Gerät akzeptiert eingehende Verbindungen des Nachbarn.

open-gesendet

Das Gerät hat eine OPEN-Nachricht an den Nachbarn gesendet und wartet auf dessen OPEN-Nachricht.

open-bestaetigt

Das Gerät hat die OPEN-Nachricht des Nachbarn akzeptiert, eine Keepalive-Nachricht an den Nachbarn gesendet und wartet auf dessen Keepalive-Nachricht.

aufgebaut

Gerät und BGP-Nachbar tauschen BGP-Nachrichten aus.

Default-Wert:

aktiv

Vorheriger-Zustand

Enthält den vorherigen Zustand der Verbindung zum BGP-Nachbarn.

SNMP-ID:

1.93.1.1.8

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Mögliche Werte:

ruhend
In diesem Zustand werden keine Verbindungen zum Nachbarn aufgebaut oder vom Nachbarn akzeptiert. Es sind noch keine Ressourcen bereitgestellt, um eine Verbindung aufzubauen.

verbinden
Das Gerät baut aktiv eine Verbindung zum Nachbarn auf und wartet auf die Vollendung des TCP-Handshakes.

aktiv
Das Gerät akzeptiert eingehende Verbindungen des Nachbarn.

open-gesendet
Das Gerät hat eine OPEN-Nachricht an den Nachbarn gesendet und wartet auf dessen OPEN-Nachricht.

open-bestaetigt
Das Gerät hat die OPEN-Nachricht des Nachbarn akzeptiert, eine Keepalive-Nachricht an den Nachbarn gesendet und wartet auf dessen Keepalive-Nachricht.

aufgebaut
Gerät und BGP-Nachbar tauschen BGP-Nachrichten aus.

Default-Wert:

aktiv

Eing.-Updates

Enthält die Anzahl der von diesem BGP-Nachbarn gesendeten BGP-UPDATE-Nachrichten.

Auch der Empfang ungültiger sowie leerer BGP-UPDATE-Nachrichten erhöht diesen Zähler.

SNMP-ID:

1.93.1.1.9

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Ausg.-Updates

Enthält die Anzahl der an diesen BGP-Nachbarn gesendeten BGP-UPDATE-Nachrichten.

SNMP-ID:

1.93.1.1.10

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Eing.-Nachrichten

Enthält die Anzahl der von diesem BGP-Nachbarn gesendeten BGP-Nachrichten.

Die Anzeige enthält alle Arten von BGP-Nachrichten.

SNMP-ID:

1.93.1.1.11

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Ausg.-Nachrichten

Enthält die Anzahl der an diesen BGP-Nachbarn gesendeten BGP-Nachrichten.

SNMP-ID:

1.93.1.1.12

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Letzter-Fehler

Enthält die letzte erkannte Fehlermeldung.

SNMP-ID:

1.93.1.1.13

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Verbunden-Transitionen

Dieser Wert zeigt an, wie oft das Gerät eine Verbindung zum BGP-Nachbarn aufgebaut hat. Gründe für einen erneuten Verbindungsaufbau können Verbindungsfehler oder die erneute Konfiguration des BGP-Nachbarn sein.

SNMP-ID:

1.93.1.1.14

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Verbindungsdauer

Enthält die Zeit in Sekunden, die die aktuelle Verbindung zu diesem BGP-Nachbarn bereits besteht (Zustand „verbunden“).

Die Anzeige beginnt von „0“, wenn das Gerät die Verbindung zum BGP-Nachbarn neu aufbaut.

SNMP-ID:

1.93.1.1.15

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Keepalive

Enthält den aktuellen Wert des Keepalive-Timers. Falls Gerät und BGP-Nachbar diesen Wert noch nicht ausgehandelt haben (Verbindungszustand „verbunden“ ist noch nicht erreicht), enthält dieses Feld die für den BGP-Nachbarn unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile** konfigurierte Keepalive-Zeit.

Haben Gerät und BGP-Nachbar den Wert „0“ ausgehandelt, tauschen sie keine regelmäßigen Keepalive-Nachrichten aus.

SNMP-ID:

1.93.1.1.16

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Haltezeit

Enthält den aktuellen Wert des Haltezeit-Timers. Falls Gerät und BGP-Nachbar diesen Wert noch nicht ausgehandelt haben (Verbindungszustand „verbunden“ ist noch nicht erreicht), enthält dieses Feld die für den BGP-Nachbarn unter **Setup** > **Routing-Protokolle** > **BGP** > **Nachbar-Profile** konfigurierte Haltezeit.

Ist dieser Wert „0“, geht das Gerät davon aus, dass sich die Verbindung auch ohne empfangene Nachrichten im Zustand „Established“ befindet.

Hat das Gerät innerhalb der angegebenen Zeit keine Nachrichten empfangen, geht es davon aus, dass die Verbindung gestört ist.

SNMP-ID:

1.93.1.1.17

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Akzeptierte-Praefixe

Enthält die Anzahl der vom Gerät akzeptierten Präfixe dieses BGP-Nachbarn.

Der angezeigte Wert ist unabhängig von der Anzahl der BGP-UPDATE-Nachrichten dieses BGP-Nachbarn, da UPDATE-Nachrichten auch keinen oder mehrere Präfixe übermitteln können.

SNMP-ID:

1.93.1.1.18

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Abgelehnte-Eing.-Praefixe

Enthält die Anzahl der vom Gerät abgelehnten Präfixe dieses BGP-Nachbarn. Präfixe werden abgelehnt, falls das lokale Regelwerk sie ablehnt oder falls das Präfix-Limit erreicht wurde.

SNMP-ID:

1.93.1.1.19

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Eing.-Widerrufene-Praefixe

Enthält die Anzahl der vom BGP-Nachbarn widerrufenen Präfixe.

SNMP-ID:

1.93.1.1.20

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Angekuendigte-Praefixe

Enthält die Anzahl der vom Gerät angekündigten Präfixe.

Der angezeigte Wert ist unabhängig von der Anzahl der BGP-UPDATE-Nachrichten, da eine UPDATE-Meldung auch keinen oder mehrere Präfixe ankündigen kann.

SNMP-ID:

1.93.1.1.21

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Abgelehnte-Ausg.-Praefixe

Enthält die Anzahl der vom Gerät abgelehnten ausgehenden Präfixe an diesen BGP-Nachbarn.

Der angezeigte Wert ist ausschließlich abhängig vom angewendeten Regelwerk für abgehende BGP-Nachrichten.

SNMP-ID:

1.93.1.1.22

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

Ausg.-Widerrufene-Praefixe

Enthält die Anzahl der vom Gerät abgekündigten Präfixe an diesen BGP-Nachbarn.

SNMP-ID:

1.93.1.1.23

Pfad Telnet:

Status > **Routing-Protokolle** > **BGP** > **Nachbarn**

5.2 Route-Monitor

Ab LCOS-Version 9.20 überprüft ein Route-Monitor die Netzwerk-Verbindungen zu einem definierten Präfix. Dieses gelernte Präfix ist z. B. das Ergebnis eines dynamischen Routing-Protokolls wie BGP.

Bei einer fehlerhaften Verbindung startet der Route-Monitor ggf. eine Backup-Verbindung.

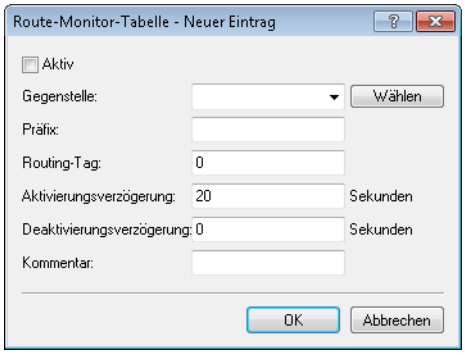
5.2.1 Route-Monitor

Der Route-Monitor überwacht Verbindungen zu Netzwerken verschiedener Provider und stellt im Fehlerfall eine Backup-Verbindung her. Die Überwachung geschieht über ein Trigger-Präfix, das der Provider in seinem Routing-Protokoll zur Verfügung stellt, z. B. beim Border Gateway Protokoll (BGP). Sobald die Route zu einem Provider-Netzwerk unerreichbar ist, erklärt der Route-Monitor das entsprechende Trigger-Präfix im eigenen Netzwerk für ungültig und öffnet eine Backup-Verbindung zum Provider-Netzwerk.

Route-Monitor mit LANconfig konfigurieren

Um den Route-Monitor zu aktivieren, wechseln Sie in die Ansicht **Kommunikation** > **Ruf-Verwaltung** und markieren Sie die Option **Route-Monitor aktiviert**.

Um den Route-Monitor zu konfigurieren, öffnen Sie die **Route-Monitor-Tabelle**.



Aktiv

Gibt an, ob diese Backup-Verbindung aktiv ist.

Gegenstelle

Enthält den Namen der Backup-Gegenstelle.

Präfix

Enthält das Präfix (IPv4- oder IPv6-Adresse), das der Route-Monitor überwachen soll.

Routing-Tag

Enthält das Routing-Tag des zu überwachenden Präfixes.

Aktivierungsverzögerung

Enthält die Verzögerung in Sekunden, die das Gerät nach dem Ausbleiben des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle aufbaut.

Deaktivierungsverzögerung

Definiert die Verzögerung in Sekunden, die das Gerät nach dem Auftauchen des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle wieder abbaut.

Beim Wert „0" beendet das Gerät die Verbindung zur Backup-Gegenstelle sofort beim Auftauchen des Präfixes (keine Verzögerung).

Kommentar

Kommentar zu diesem Eintrag.

5.2.2 Ergänzungen im Setup-Menü

Route-Monitor

In diesem Verzeichnis konfigurieren Sie den Route-Monitor.

SNMP-ID:

2.93.2

Pfad Telnet:

Setup > **Routing-Protokolle**

Monitor-Tabelle

In dieser Tabelle konfigurieren Sie den Route-Monitor.

SNMP-ID:

2.93.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor**

Backup-Gegenstelle

Enthält den Namen der Backup-Gegenstelle.

SNMP-ID:

2.93.2.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

leer

Praefix

Enthält das Präfix (IPv4- oder IPv6-Adresse), das der Route-Monitor überwachen soll.

SNMP-ID:

2.93.2.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

leer

Rtg-Tag

Enthält das Routing-Tag des zu überwachenden Präfixes.

SNMP-ID:

2.93.2.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

0

Aktivierungsverzoegerung

Enthält die Verzögerung in Sekunden, die das Gerät nach dem Ausbleiben des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle aufbaut.

SNMP-ID:

2.93.2.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

20

Deaktivierungsverzoegerung

Definiert die Verzögerung in Sekunden, die das Gerät nach dem Auftauchen des Präfixes wartet, bis es die Verbindung zur Backup-Gegenstelle wieder abbaut.

SNMP-ID:

2.93.2.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Keine Verzögerung: Das Gerät beendet die Verbindung zur Backup-Gegenstelle sofort beim Auftauchen des Präfixes.

Aktiv

Gibt an, ob diese Backup-Verbindung aktiv ist.

SNMP-ID:

2.93.2.1.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

Ja

Die Backup-Verbindung ist aktiv.

Nein

Die Backup-Verbindung ist nicht aktiv.

Default-Wert:

Nein

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.93.2.1.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Mit dieser Aktion aktivieren oder deaktivieren Sie den Route-Monitor.

SNMP-ID:

2.93.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **Route-Monitor**

Mögliche Werte:

nein

Der Route-Monitor ist deaktiviert.

ja

Der Route-Monitor ist aktiviert.

Default-Wert:

nein

5.2.3 Ergänzungen im Status-Menü

Route-Monitor

Dieses Verzeichnis zeigt die Statistiken des Route-Monitors.

SNMP-ID:

1.93.2

Pfad Telnet:

Status > **Routing-Protokolle**

Monitor-Tabelle

Diese Tabelle zeigt die Statistiken des Route-Monitors.

SNMP-ID:

1.93.2.1

Pfad Telnet:

Status > **Routing-Protokolle** > **Route-Monitor**

Backup-Gegenstelle

Enthält den Namen der Backup-Gegenstelle.

SNMP-ID:

1.93.2.1.1

Pfad Telnet:

Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Praefix

Enthält den Präfix (IPv4- oder IPv6-Adresse) der Backup-Gegenstelle.

SNMP-ID:

1.93.2.1.2

Pfad Telnet:

Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Rtg-Tag

Enthält das Routing-Tag für die Backup-Verbindung.

SNMP-ID:

1.93.2.1.3

Pfad Telnet:

Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

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

Default-Wert:

0

Praefix-Status

Enthält den Präfix-Status der Backup-Verbindung.

SNMP-ID:

1.93.2.1.4

Pfad Telnet:

Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

Vorhanden

Das Präfix dieser Backup-Verbindung ist in der Routing-Tabelle gespeichert.

Nicht-vorhanden
Das Präfix dieser Backup-Verbindung ist nicht in der Routing-Tabelle gespeichert.
Unbekannt
Das Präfix dieser Backup-Verbindung ist unbekannt.

Backup-Status

Enthält den Status der Backup-Verbindung.

SNMP-ID:
1.93.2.1.5

Pfad Telnet:
Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

Unbekannt
Der Backup-Status ist unbekannt.
Abgebaut
Es besteht keine Backup-Verbindung.
Aufgebaut
Es besteht eine Backup-Verbindung.
Abbauverzoegerung
Das Gerät beendet die Backup-Verbindung nach Ablauf der eingestellten Verzögerung.
Aufbauverzoegerung
Das Gerät startet die Backup-Verbindung nach Ablauf der eingestellten Verzögerung.

Ggst-Status

Enthält den Status der Backup-Gegenstelle.

SNMP-ID:
1.93.2.1.6

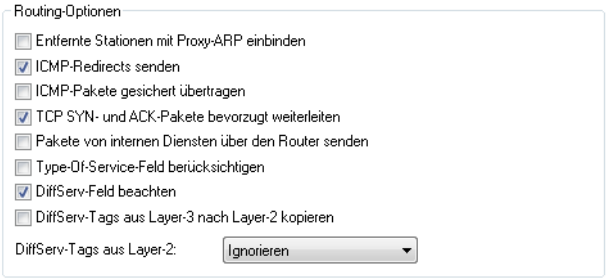
Pfad Telnet:
Status > **Routing-Protokolle** > **Route-Monitor** > **Monitor-Tabelle**

Mögliche Werte:

Verbunden
Die Gegenstelle ist korrekt konfiguriert, die Backup-Verbindung ist hergestellt.
Getrennt/Unbekannt
Entweder ist die Gegenstelle nicht korrekt konfiguriert oder die Backup-Verbindung ist nicht hergestellt.

5.3 DiffServ-Feld per Default aktiviert

Ab LCOS-Version 9.20 beachtet die Routing-Methode standardmäßig das DiffServ-Feld von IP-Paketen.



DiffServ-Feld beachten

Wenn der Router das DiffServ-Feld in IP-Paketen beachtet, dann benutzt er die standardisierten DSCPs (DiffServ Codepoints) AFxx (Assured Forwarding) zur gesicherten Übertragung und EF (Expedited Forwarding) zur bevorzugten Übertragung. Alle abweichend gekennzeichneten IP-Pakete werden normal übertragen. Standardmäßig ist diese Option aktiviert.

Diese Option ist nicht gleichzeitig mit ToS nutzbar, da das DiffServ-Feld innerhalb eines IP- Paketes das ToS-Feld ersetzt.

Mehr Informationen zu DiffServ erhalten Sie im Kapitel *Quality-of-Service*.

5.3.1 Ergänzungen im Setup-Menü

Routing-Methode

Bestimmt die Auswertung der ToS- oder DiffServ-Felder.

SNMP-ID:

2.8.7.1

Pfad Telnet:

Setup > **IP-Router** > **Routing-Methode**

Mögliche Werte:

Normal

Das ToS/DiffServ-Feld wird ignoriert.

TOS

Das ToS/DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits "Low-Delay" und "High-Reliability" ausgewertet.

DiffServ

Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

- **CSx (inklusive CS0 = BE):** normal übertragen
- **AFxx:** gesichert übertragen
- **EF:** bevorzugt übertragen

Default-Wert:

DiffServ

5.4 iPerf-kompatibler Server/Client

Ab LCOS-Version 9.20 ist das Tool "iPerf" zur Performance-Messung von Netzwerkstrecken im LCOS integriert und führt Bandbreitenmessungen (uni- oder bidirektional) durch. iPerf lässt sich direkt über jedes LANCOM-Gerät starten. Dabei kann das LANCOM-Gerät sowohl als Client als auch als Server fungieren (UDP/TCP). Die LCOS-Implementierung basiert auf iPerf2.

Die iPerf-Konfiguration ist sowohl über LANconfig, als auch über die Konsole möglich.

5.4.1 Bandbreiten-Messung mit iPerf

Die Messung der Netzwerkperformance ermittelt Werte wie Datendurchsatz, Verzögerung, Jitter und Fehlerraten einer Netzwerkverbindung. Die gemessenen Werte dienen u. a. der Netzwerkoptimierung, der Fehlererkennung und -beseitigung sowie der Beurteilung der Leistungsfähigkeit einer Netzwerkinfrastruktur.

Als freie Software zur Erzeugung und Auswertung von definierten Datenströmen auf bestimmten Verbindungen hat sich iPerf etabliert. Ein iPerf-Server-Daemon empfängt TCP- und UDP-Streams und misst den Datendurchsatz für die entsprechenden Anwendungen sowie Verzögerung, Jitter, Verlust und Neuanordnung von Datenpaketen bei UDP-Verbindungen.

Zur Bandbreitenmessung zwischen zwei Hosts startet man den iPerf-Server auf dem einen und den iPerf-Client auf dem anderen Gerät. Der iPerf-Client verbindet sich daraufhin mit dem iPerf-Server. Server und Client tauschen für eine bestimmte Zeit oder eine bestimmte Datenmenge Datenpakete untereinander aus und erzeugen darüber eine Statistik. Diese Statistik gibt Auskünft über die Qualität der Verbindung zwischen beiden Gegenstellen.

Bei der Messung der TCP-Verbindungsqualität sendet der iPerf-Client so schnell wie möglich komplett gefüllte TCP-Datenpakete. Die durchschnittliche Datenrate für den erfolgreichen Datentransfer („goodput“) ist das Ergebnis dessen, was der iPerf-Server fehlerfrei empfangen hat.

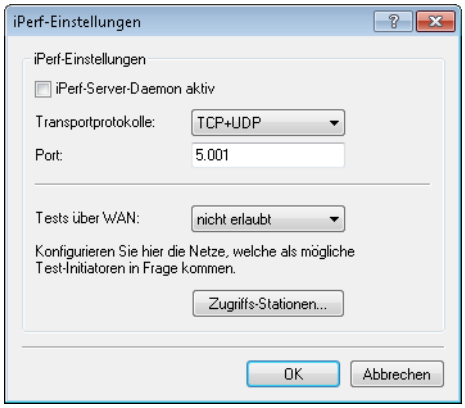
Bei der Messung der UDP-Verbindungsqualität überträgt der iPerf-Client Daten über eine definierte Bandbreite (standardmäßig 1 Mbit/s), allerdings ohne Fluss- oder Leistungskontrolle. Der „goodput“ orientiert sich an der maximalen Bandbreite, bei der der Übertragungspuffer des Clients dauerhaft und ohne den Verlust von Datenpaketen gefüllt ist.

LANCOM-Geräte beinhalten eine iPerf2-kompatible Funktion zur Messung der Netzwerkperformance direkt zwischen den Netzwerkzugangspunkten (z. B. Router, VPN-Gateway, AP). Damit vereinfacht sich die Messung z. B. des Datendurchsatzes über WAN- oder WLAN-Point-to-Point-Verbindungen.

Sowohl die Messung zwischen zwei LANCOM-Geräten als auch die Messung zwischen einem LANCOM-Gerät und einer anderen iPerf2-Instanz ist möglich.

5.4.2 iPerf mit LANconfig einrichten

Mit LANconfig konfigurieren Sie iPerf unter **Meldungen** > **Allgemein** mit einem Klick auf **iPerf-Einstellungen**.



iPerf-Server-Daemon aktiv

Aktiviert bzw. deaktiviert den iPerf-Server-Daemon.

Statt den iPerf-Server an dieser Stelle dauerhaft einzurichten, besteht die Möglichkeit, über die Konsole via SSH-Verbindung für einen einzelnen Test auch nur einen temporären iPerf-Server zu starten.

Transportprotokolle

Bestimmen Sie hier, über welche Übertragungsprotokolle das Gerät die Bandbreite messen soll.

Port

Über diesen Port kommunizieren iPerf-Client und -Server (standardmäßig „5001“).

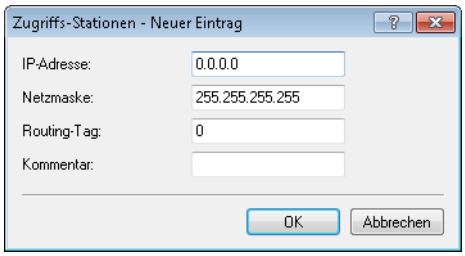
Tests über WAN

Bestimmen Sie, ob die Messung auch über eine WAN-Verbindung erfolgen darf.

Bei Messungen über WAN-Verbindungen können je nach Providervertrag zusätzliche Verbindungskosten entstehen.

Zugriffs-Stationen

Um den iPerf-Zugriff auf bestimmte Stationen zu begrenzen, tragen Sie deren Verbindungsdaten in diese Tabelle ein.



IP-Adresse

Geben Sie die IPv4-Adresse der entfernten Station ein.

Netzmaske

Geben Sie die Netzmaske für die entfernte Station ein.

Routing-Tag

Tragen Sie hier die das Routing-Tag ein, das die Verbindung zur entfernten Station definiert.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

5.4.3 Temporärer iPerf-Server und -Client

Bei der iPerf-Konfiguration über LANconfig ist die iPerf-Funktion dauerhaft aktiv. Es besteht die Möglichkeit, mit der Konsole über eine SSH-Verbindung einen temporären iPerf-Daemon zu starten, der nur für die Dauer eines Tests aktiv ist.

Starten Sie dazu ein Terminalprogramm (z. B. PuTTY) und öffnen Sie die Verbindung zum Gerät, auf dem Sie die iPerf-Funktion aktivieren möchten. Mit dem Konsolenbefehl `iperf` und den entsprechenden Optionsschaltern konfigurieren Sie den temporären iPerf-Daemon. Die folgenden Konsolenbeispiele erläutern einige Standardbefehle.

Mehr Informationen über die Optionsschalter bei `iperf` finden Sie im Abschnitt *Befehle für die Konsole*.

iPerf-Server im TCP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s
[Iperf-TCP-Server|1526] Now listening on port 5001
```

Drücken Sie erneut die Enter-Taste oder schließen Sie das Konsolenfenster, um den iPerf-Server zu beenden.

iPerf-Server im UDP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s -u
[Iperf-UDP-Server|1524] Now listening on port 5001
```

Drücken Sie erneut die Enter-Taste oder schließen Sie das Konsolenfenster, um den iPerf-Server zu beenden.

iPerf-Client im UDP-Modus starten

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -u -c 172.16.30.23
WARN: Using default UPD bandwidth limitation of 1 MBit/s
WARN: Using default UDP payload length of 1472 bytes (for matching Ethernet MTU
via IPv4)
[Iperf-UDP-Client|2100] Connecting to server...
[Iperf-UDP-Client|2100] Connection established to 172.16.30.23:5001

root@device:/
>
```

Drücken Sie die Enter-Taste, um den Test zu beenden.

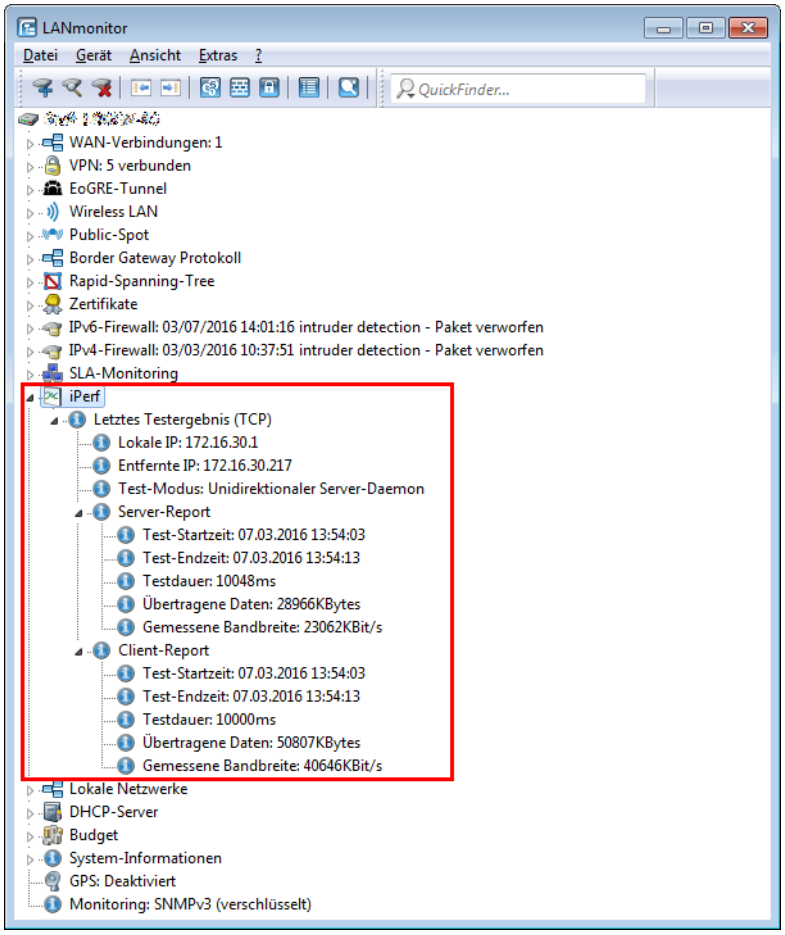
```
[Iperf-UDP-Client|2100] Connection closed actively
[Iperf-UDP-Client|2100] Sent 1249728 bytes within 10s (10000ms) -> 0 Mbit/s (999
 Kbit/s)
[Iperf-UDP-Client|2100] Server reports 1249728 bytes received within 9s (9985ms)
 -> 1 Mbit/s (1001 Kbit/s)
[Iperf-UDP-Client|2100] Server received 849 packets (0 lost / 0 out-of-order) with
 62us jitter

root@device:/
>
```

5.4.4 iPerf-Ergebnisse mit LANmonitor auswerten

LANCOM-Geräte beinhalten eine iPerf2-kompatible Funktion zur Messung der Netzwerkperformance direkt zwischen den Netzwerkzugangspunkten (z. B. Router, VPN-Gateway, AP). Damit vereinfacht sich die Messung z. B. des Datendurchsatzes über WAN- oder WLAN-Point-to-Point-Verbindungen.

Mehr Informationen zu iPerf finden Sie im Abschnitt *Bandbreiten-Messung mit iPerf*.

Das letzte iPerf-Testergebnis lässt sich auch im LANmonitor unter „iPerf" anzeigen. Dabei ist es egal, ob das Gerät eine Verbindung gestartet hat oder sich von extern verbunden hat. Die Verbindungsart „Test-Modus" zeigt den verwendeten Modus entsprechend an:



LANmonitor stellt dabei die im Gerät unter **Status** > **Iperf** > **Last-Results** gespeicherten Testergebnisse dar.

5.4.5 iPerf-Befehle in der Kommandozeile

Tabelle 2: Übersicht über die iPerf-Optionen

Befehl	Beschreibung
`iperf [-s|-c <Host>] [-u] [-p <Port>] [-B <Interface>] [-c] [-b [<Bandw>/]<Bandw>[kKmM]] [-l <Length>] [-t <Time>] [-d] [-r] [-L <Port>] [-h]`	Startet iPerf auf dem Gerät, um eine Bandbreitenmessung mit einer iPerf2-Gegenstelle durchzuführen. Mögliche Optionsschalter sind: ■ **Client/Server** □ `-u, --udp`: Verwendet UDP statt TCP.

Befehl	Beschreibung
	▫ `-p, --port <Port>`: Verbindet mit oder erwartet Datenpakete auf diesem Port (Standard: 5001). ▫ `-B, --bind <Interface>`: Erlaubt die Verbindung nur über die angegebene Schnittstelle (IP-Adresse oder Schnittstellenname). ■ **Server-spezifisch** ▫ `-s, --server`: Startet iPerf im Server-Modus und wartet auf die Kontaktaufnahme durch einen iPerf-Client. ■ **Client-spezifisch** ▫ `-c, --client <Host>`: Startet iPerf im Client-Modus und verbindet mit dem iPerf-Server <Host> (IP-Adresse oder DNS-Name). ▫ `-b, --bandwidth [<Bandw>/]<Bandw>{kKmM}`: Begrenzung der Bandbreite bei der Analyse einer UDP-Verbindung im [Down-]/Up-Stream. Die Angabe erfolgt in Kilo- (kK) oder Megabyte (mM) pro Sekunde (Standard: 1 Mbps). ▫ `-l, --len <Length>`: Bestimmt die Länge der UDP-Datenpakete. ▫ `-t, --time <Time>`: Bestimmt die Dauer der Verbindung in Sekunden (Standard: 10 Sekunden). ▫ `-d, --dualtest`: Der Test erfolgt bidirektional: iPerf-Server und -Client senden und empfangen dabei gleichzeitig. ▫ `-r, --tradeoff`: Der Test erfolgt sequentiell: iPerf-Server und -Client senden und empfangen nacheinander. ▫ `-L, --listenport <Port>`: Gibt den Port an, auf dem das Gerät im bidirektionalen Betrieb Datenpakete vom entfernten iPerf-Server erwartet (Standard: 5001). ■ **Verschiedenes** ▫ `-h, --help`: Gibt den Hilfetext aus.

5.4.6 Ergänzungen im Setup-Menü

Iperf

iPerf misst den Datendurchsatz für TCP- und UDP-Anwendungen ebenso wie Verzögerung, Jitter oder Verlust und Neuanordnung von Datenpaketen bei UDP-Verbindungen.

In diesem Menü konfigurieren Sie die iPerf-Einstellungen.

SNMP-ID:

2.96

Pfad Telnet:

Setup

Server-Daemon

Dieses Menü enthält die Konfiguration für den Iperf-Serverdienst.

SNMP-ID:

2.96.1

Pfad Telnet:

Setup > **Iperf**

Aktiv

Mit diesem Eintrag aktivieren oder deaktivieren Sie den Iperf-Serverdienst.

SNMP-ID:

2.96.1.1

Pfad Telnet:

Setup > **Iperf** > **Server-Daemon**

Mögliche Werte:

nein
Der Iperf Server-Deamon ist nicht aktiv.

ja
Der Iperf Server-Deamon ist aktiv.

Default-Wert:

nein

Transport

Legen Sie mit diesem Eintrag fest, welches Übertragungs-Protokoll der iPerf-Server-Daemon verwenden soll.

SNMP-ID:

2.96.1.2

Pfad Telnet:

Setup > **Iperf** > **Server-Daemon**

Mögliche Werte:

UDP
TCP

Default-Wert:

UDP

Port

Legen Sie einen Port fest, auf dem der iPerf-Server Datenpakete erwarten soll.

SNMP-ID:

2.96.1.3

Pfad Telnet:

Setup > **Iperf** > **Server-Daemon**

Mögliche Werte:

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

Default-Wert:

5001

IPv4-WAN-Access

Bestimmen Sie, ob die Messung auch über eine WAN-Verbindung erfolgen darf.

Bei Messungen über WAN-Verbindungen können je nach Providervertrag zusätzliche Verbindungskosten entstehen.

SNMP-ID:

2.96.2

Pfad Telnet:

Setup > **Iperf**

Mögliche Werte:

nein
Die Bandbreitenmessung darf nicht über eine WAN-Verbindung erfolgen.

VPN
Die Bandbreitenmessung darf zwar über eine WAN-Verbindung erfolgen, allerdings nur geschützt durch einen VPN-Tunnel.

ja
Die Bandbreitenmessung darf auch über eine WAN-Verbindung erfolgen.

Default-Wert:

nein

IPv4-Access-List

Um den iPerf-Zugriff auf bestimmte Stationen zu begrenzen, tragen Sie deren Verbindungsdaten in diese Tabelle ein.

SNMP-ID:

2.96.3

Pfad Telnet:

Setup > **Iperf**

IP-Adresse

Geben Sie die IPv4-Adresse der entfernten Station ein.

SNMP-ID:

2.96.3.1

Pfad Telnet:

Setup > **Iperf** > **IPv4-Access-List**

Mögliche Werte:

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

Default-Wert:

leer

Netzmaske

Geben Sie die Netzmaske für die entfernte Station ein.

SNMP-ID:

2.96.3.2

Pfad Telnet:

Setup > **Iperf** > **IPv4-Access-List**

Mögliche Werte:

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

Default-Wert:

255.255.255.255

Rtg-Tag

Tragen Sie hier die das Routing-Tag ein, das die Verbindung zur entfernten Station definiert.

SNMP-ID:

2.96.3.3

Pfad Telnet:

Setup > **Iperf** > **IPv4-Access-List**

Mögliche Werte:

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

Default-Wert:

0

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

SNMP-ID:

2.96.3.4

Pfad Telnet:

Setup > **Iperf** > **IPv4-Access-List**

Mögliche Werte:

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

Default-Wert:

leer

5.4.7 Ergänzungen im Status-Menü

Iperf

Die Messung der Netzwerkperformance ermittelt Werte wie Datendurchsatz, Verzögerung, Jitter und Fehlerraten einer Netzwerkverbindung. Die gemessenen Werte dienen u. a. der Netzwerkoptimierung, der Fehlererkennung und -beseitigung sowie der Beurteilung der Leistungsfähigkeit einer Netzwerkinfrastruktur. Die Durchführung einer Messung erfolgt dabei entweder automatisiert und regelmäßig oder nach Bedarf manuell.

Als freie Software zur Erzeugung und Auswertung von definierten Datenströmen auf bestimmten Verbindungen hat sich iPerf etabliert. iPerf misst den Datendurchsatz für TCP- und UDP-Anwendungen sowie Verzögerung, Jitter sowie Verlust und Neuanordnung von Datenpaketen bei UDP-Verbindungen.

LANCOM-Geräte beinhalten eine iPerf-kompatible Funktion zur Messung der Netzwerkperformance direkt zwischen den Netzwerkzugangspunkten (z. B. Router, VPN-Gateway, AP). Damit vereinfacht sich die Messung z. B. des Datendurchsatzes über WAN- oder WLAN-Point-to-Point-Verbindungen.

Dieses Verzeichnis enthält eine Übersicht der WAN-Bandbreiten-Messung.

SNMP-ID:

1.96

Pfad Telnet:

Status

Last-Results

Dieses Menü enthält die Tabellen mit den Ergebnissen der WAN-Bandbreiten-Messung für TCP und UDP.

SNMP-ID:

1.96.1

Pfad Telnet:

Status > **Iperf**

UDP

Dieses Menü enthält die Tabelle mit den Ergebnissen der WAN-Bandbreiten-Messung für UDP.

Um auch auf der Client-Seite eine Auswertung der Messergebnisse zu ermöglichen, sendet der iPerf-Server die Messdaten zurück an den iPerf-Client. Diese Daten erscheinen in separaten Tabellenspalten.

SNMP-ID:

1.96.1.1

Pfad Telnet:

Status > **Iperf** > **Last-Results**

Index

Diese Spalte enthält die fortlaufende Nummern der Einträge.

SNMP-ID:

1.96.1.1.1

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Local-IP

Diese Spalte enthält die lokale IP der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.1.2

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-IP

Diese Spalte enthält die entfernte IP der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.1.3

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Mode

Diese Spalte enthält den Modus der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.1.4

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Connections

Diese Spalte enthält die aktuellen Verbindungen der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.1.5

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Start

Diese Spalte enthält den Start-Zeitpunkt des iPerf-Servers.

SNMP-ID:

1.96.1.1.6

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Stop

Diese Spalte enthält den Stop-Zeitpunkt des iPerf-Servers.

SNMP-ID:

1.96.1.1.7

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Duration-ms

Diese Spalte enthält die Übertragungszeit der Datenpakete in Millisekunden vom Server zum Client.

SNMP-ID:

1.96.1.1.8

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Bytes

Diese Spalte enthält die Anzahl Bytes, die der Server während der Verbindung übertragen hat.

SNMP-ID:

1.96.1.1.9

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Bandwidth-kbps

Diese Spalte enthält die Server-Bandbreite während der Verbindung.

SNMP-ID:

1.96.1.1.10

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Packets

Diese Spalte enthält die Anzahl der Datenpakete, die der Server während der Verbindung übertragen hat.

SNMP-ID:

1.96.1.1.11

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Lost-Packets

Um den Verlust oder die Neuanordnung eines Datenpakets zu erkennen, fügt der Client eine Sequenz-ID in den Header jedes empfangenen Datenpakets ein, bevor er es an den Server zurücksendet.

Diese Spalte enthält die Differenz der Datenpakete, die der Server gesendet und der Client als empfangen zurückgemeldet hat.

SNMP-ID:

1.96.1.1.12

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Out-Of-Order-Packets

Um den Verlust oder die Neuanordnung eines Datenpakets zu erkennen, fügt der Client eine Sequenz-ID in den Header jedes empfangenen Datenpakets ein, bevor er es an den Server zurücksendet.

Diese Spalte enthält die Anzahl der Datenpakete, die der Server gesendet und der Client in einer abweichenden Reihenfolge zurückgemeldet hat.

SNMP-ID:

1.96.1.1.13

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Jitter-us

Der Client fügt einen Zeitstempel in den Header jedes gesendeten Datenpakets ein, anhand dessen der Server die Verzögerung dieser Datenübertragung erkennen kann.

Diese Spalte enthält die Verzögerung der Datenpakete in Mikrosekunden.

SNMP-ID:

1.96.1.1.14

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Error

Diese Spalte enthält den Fehler, den der Server während der Verbindung im Fehlerfall gemeldet hat.

SNMP-ID:

1.96.1.1.15

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Start

Diese Spalte enthält den Start-Zeitpunkt des iPerf-Clients.

SNMP-ID:

1.96.1.1.16

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Stop

Diese Spalte enthält den Stop-Zeitpunkt des iPerf-Clients.

SNMP-ID:

1.96.1.1.17

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Duration-ms

Diese Spalte enthält die Übertragungszeit der Datenpakete in Millisekunden vom Client zum Server.

SNMP-ID:

1.96.1.1.18

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Bytes

Diese Spalte enthält die Anzahl der Datenpakete in Bytes, die der Client während der Verbindung empfangen hat.

SNMP-ID:

1.96.1.1.19

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Bandwidth-kbps

Diese Spalte enthält die Client-Bandbreite während der Verbindung.

SNMP-ID:

1.96.1.1.20

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Packets

Diese Spalte enthält die Anzahl der Datenpakete, die der Client während der Verbindung empfangen hat.

SNMP-ID:

1.96.1.1.21

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Error

Diese Spalte enthält den Fehler, den der Client während der Verbindung im Fehlerfall gemeldet hat.

SNMP-ID:

1.96.1.1.22

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Duration-ms

Diese Spalte enthält die Übertragungszeit der Datenpakete in Millisekunden, die der Server an den Client zurückgemeldet hat.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.23

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Bytes

Diese Spalte enthält die Anzahl Bytes, die der Server an den Client zurückgemeldet hat.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.24

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Bandwidth-kbps

Diese Spalte enthält die Server-Bandbreite während der Verbindung, die der Server an den Client zurückgemeldet hat.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.25

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Packets

Diese Spalte enthält die Anzahl der Datenpakete, die der Server dem Client als gesendet meldet.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.26

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Lost-Packets

Um den Verlust oder die Neuanordnung eines Datenpakets zu erkennen, fügt der Client eine Sequenz-ID in den Header jedes empfangenen Datenpakets ein, bevor er es an den Server zurücksendet.

Der Server erstellt daraus die Differenz der Datenpakete, die er gesendet und der Client als empfangen zurückgemeldet hat.

Diese Spalte enthält diesen Wert, den der Server an den Client zurückmeldet.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.27

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Out-Of-Order-Packets

Um den Verlust oder die Neuanordnung eines Datenpakets zu erkennen, fügt der Client eine Sequenz-ID in den Header jedes empfangenen Datenpakets ein, bevor er es an den Server zurücksendet.

Der Server errechnet daraus die Anzahl der Datenpakete, die er gesendet und der Client in einer abweichenden Reihenfolge zurückgemeldet hat.

Diese Spalte enthält diesen Wert, den der Server an den Client zurückmeldet.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.28

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Jitter-us

Der Client fügt einen Zeitstempel in den Header jedes gesendeten Datenpakets ein, anhand dessen der Server die Verzögerung dieser Datenübertragung erkennen kann.

Der Server errechnet daraus die Verzögerung der Datenpakete in Mikrosekunden.

Diese Spalte enthält diesen Wert, den der Server an den Client zurückmeldet.

Dieser Wert erscheint nur, wenn sich das Gerät im iPerf-Client-Modus befindet.

SNMP-ID:

1.96.1.1.29

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **UDP**

TCP

Dieses Menü enthält die Tabelle mit den Ergebnissen der WAN-Bandbreiten-Messung für TCP.

SNMP-ID:

1.96.1.2

Pfad Telnet:

Status > **Iperf** > **Last-Results**

Index

Diese Spalte enthält die fortlaufenden Nummern der Einträge.

SNMP-ID:

1.96.1.2.1

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Local-IP

Diese Spalte enthält die lokale IP der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.2.2

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Remote-IP

Diese Spalte enthält die entfernte IP der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.2.3

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Mode

Diese Spalte enthält den Modus der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.2.4

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Connections

Diese Spalte enthält die aktuellen Verbindungen der gemessenen Schnittstelle.

SNMP-ID:

1.96.1.2.5

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Start

Diese Spalte enthält den Start-Zeitpunkt des iPerf-Servers.

SNMP-ID:

1.96.1.2.6

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Stop

Diese Spalte enthält den Stop-Zeitpunkt des iPerf-Servers.

SNMP-ID:

1.96.1.2.7

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Duration-ms

Diese Spalte enthält die Übertragungszeit der Datenpakete in Millisekunden vom Server zum Client.

SNMP-ID:

1.96.1.2.8

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Bytes

Diese Spalte enthält die Anzahl Bytes, die der Server während der Verbindung übertragen hat.

SNMP-ID:

1.96.1.2.9

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Bandwidth-kbps

Diese Spalte enthält die Server-Bandbreite während der Verbindung.

SNMP-ID:

1.96.1.2.10

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Error

Diese Spalte enthält den Fehler, den der Server während der Verbindung im Fehlerfall gemeldet hat.

SNMP-ID:

1.96.1.2.11

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Start

Diese Spalte enthält den Start-Zeitpunkt des iPerf-Clients.

SNMP-ID:

1.96.1.2.12

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Stop

Diese Spalte enthält den Stop-Zeitpunkt des iPerf-Clients.

SNMP-ID:

1.96.1.2.13

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Duration-ms

Diese Spalte enthält die Übertragungszeit der Datenpakete in Millisekunden vom Client zum Server.

SNMP-ID:

1.96.1.2.14

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Bytes

Diese Spalte enthält die Anzahl der Datenpakete in Bytes, die der Client während der Verbindung empfangen hat.

SNMP-ID:

1.96.1.2.15

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Bandwidth-kbps

Diese Spalte enthält die Client-Bandbreite während der Verbindung.

SNMP-ID:

1.96.1.2.16

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Error

Diese Spalte enthält den Fehler, den der Client während der Verbindung im Fehlerfall gemeldet hat.

SNMP-ID:

1.96.1.2.17

Pfad Telnet:

Status > **Iperf** > **Last-Results** > **TCP**

5.5 SLA-Monitor

Ab LCOS-Version 9.20 überprüft ein SLA-Monitor die Netzwerk-Verbindungen und zur Verfügung stehende Dienste. Dazu versendet das Gerät Datenpakete über das Internet Control Message Protocol (ICMP) und fragt durch Ping-Befehle z. B. die Erreichbarkeit von Gegenstellen ab.

Sie erhalten über Syslog oder LANmonitor Informationen über Paketlaufzeiten und die Anzahl verlorener Datenpakete.

5.5.1 SLA-Monitoring

Das SLA-Monitoring überwacht die Verbindungen zu Gegenstellen innerhalb einer Netzwerkstruktur. Ping-Tests zu definierten Zielen geben Aufschluss über die Verfügbarkeit der Peers und zeigen Paketlaufzeiten sowie die Anzahl verlorener Datenpakete an. Sie haben die Möglichkeit, Warnungen bei der Überschreitung festgelegter Richtwerte zu definieren und über SYSLOG oder LANmonitor ausgegeben zu lassen. Zudem wird die Historie vergangener Überprüfungen gespeichert, sodass Administratoren stets über die Qualität der Verbindungen informiert sind.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

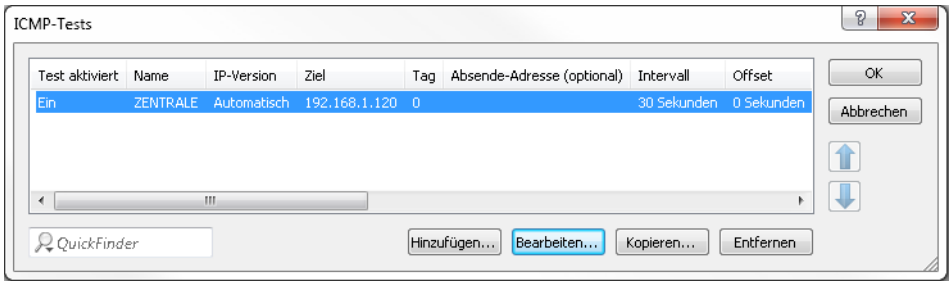
Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

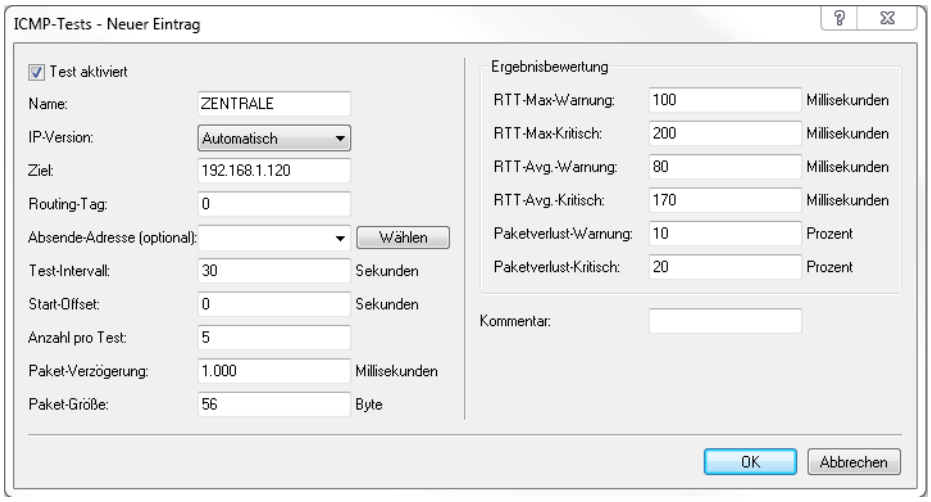
5.5.2 Konfiguration von SLA-Monitoring über LANconfig

Die Parameter zur Konfiguration des SLA-Monitors finden Sie bei LANconfig unter **Meldungen** > **Allgemein** im Abschnitt **SLA-Monitoring**.

Klicken Sie auf die Schaltfläche **ICMP-Tests**, um neue Abfragen hinzuzufügen und Richtwerte für die Verbindungstests zu definieren.



Klicken Sie auf die Schaltfläche **Hinzufügen** oder markieren Sie einen bereits vorhandenen Eintrag und klicken Sie auf **Bearbeiten**.



Test aktiviert

Bei aktivierter Checkbox verwendet das Gerät die definierten Einstellungen für den Verbindungstest.

Name

Name der Verbindung

IP-Version

Legt fest, ob IPv4 oder IPv6 verwendet wird.

Per Default ist die Einstellung "Automatisch" ausgewählt.

Ziel

Definiert das Ziel der Überprüfung (ICMP / PING Ziel).

Routing-Tag

Geben Sie ein Routing-Tag an, falls eine bestimmte Route verwendet werden soll.

Absende-Adresse (opt.)

Konfigurieren Sie optional eine Absende-Adresse, falls Sie ein bestimmtes Netzwerk als Absende-Schnittstelle verwenden möchten.

Test-Intervall

Definiert das Zeitintervall, in dem das Gerät ICMP Pakete verschickt (**Default: 30 Sekunden**).

Start-Offset

Legen Sie eine Verzögerungszeit für den Versand von ICMP-Paketen fest.

Anzahl pro Test

Gibt an, wie viele ICMP Pakete pro Durchlauf verschickt werden (**Default: 5**).

Paket-Verzögerung

Legen Sie eine Verzögerung für den Versand von Paketen fest.

Paket-Größe

Definiert die Paketgröße der ICMP Nachricht.

Ergebnisbewertung

In diesem Abschnitt definieren Sie Grenzwerte für die Paketbehandlung.

RTT-Max-Warnung

Definieren Sie eine maximale Paketumlaufzeit (**R**ound **T**rip **T**ime). Sollte eines der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Warnmeldung generiert.

RTT-Max-Kritisch

Definieren Sie eine maximale Paketumlaufzeit, nach der eine Fehlermeldung generiert wird, falls eines der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigt.

RTT-Avg.-Warnung

Definieren Sie eine durchschnittliche Paketumlaufzeit. Sollte die durchschnittliche Anzahl der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Warnmeldung generiert.

RTT-Avg.-Kritisch

Definieren Sie eine durchschnittliche Paketumlaufzeit. Sollte die durchschnittliche Anzahl der ICMP-Pakete eine längere Umlaufzeit als die hier festgelegte benötigen, wird eine Fehlermeldung generiert.

Paketverlust-Warnung

Wenn der Prozentsatz der verloren gegangenen Pakete diesen definierten Wert erreicht, wird eine entsprechende Warnmeldung generiert.

Paketverlust-Kritisch

Wenn der Prozentsatz der verloren gegangenen Pakete diesen definierten Wert erreicht, wird eine entsprechende Fehlermeldung generiert.

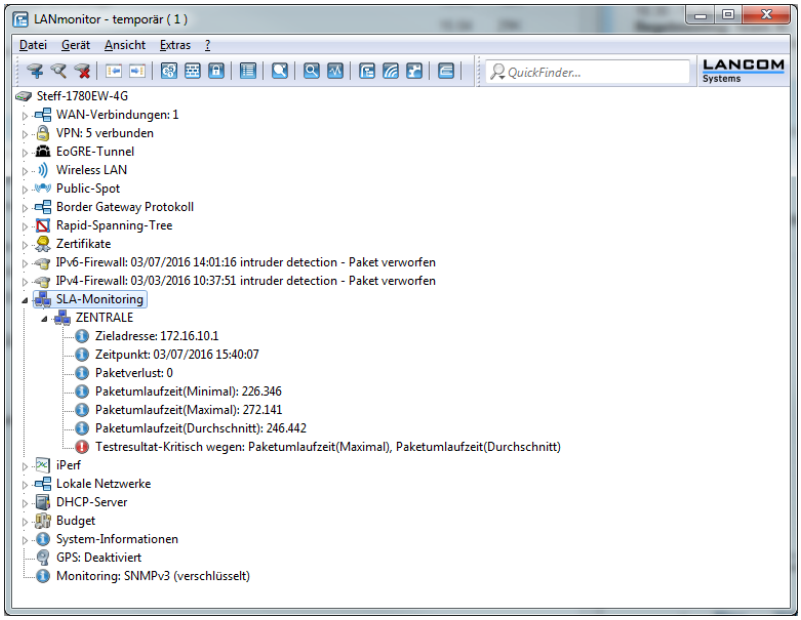
Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

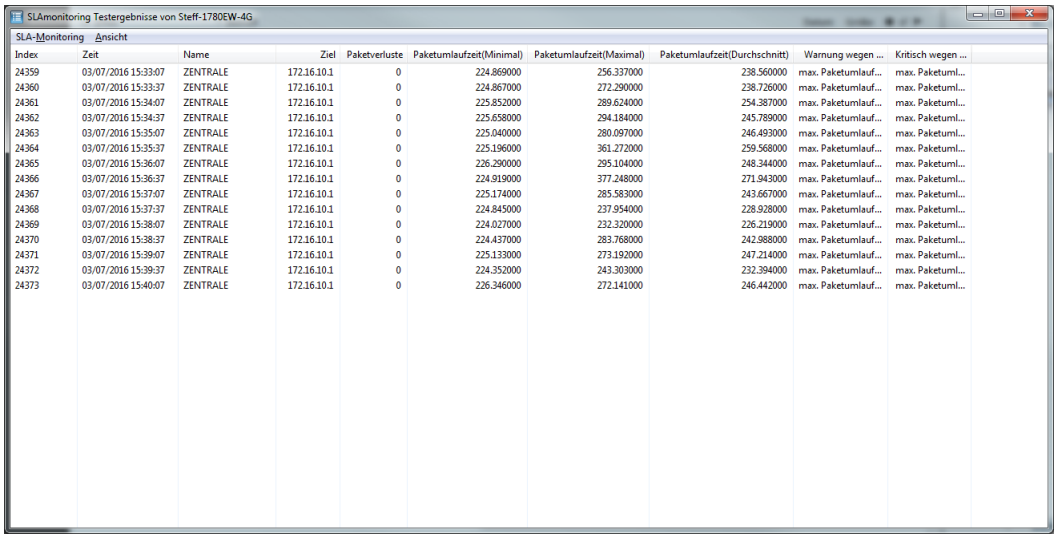
5.5.3 Anzeigen der SLA-Monitoring Ergebnisse in LANmonitor

In LANmonitor sind die Ergebnisse der konfigurierten Tests unter **SLA-Monitoring** ersichtlich.

Angezeigt werden die zuletzt gesammelten Informationen des Verbindungstests.



Sie haben zudem die Möglichkeit, sich die Historie der Verbindungsprüfungen anzeigen zu lassen. Klicken Sie dazu mit der rechten Maustaste auf den Eintrag **SLA-Monitoring**. Wählen Sie im folgenden Dialog den Eintrag **SLA-Monitoring Historie** aus.



Index	Zeit	Name	Ziel	Paketverluste	Paketumlaufzeit(Minimal)	Paketumlaufzeit(Maximal)	Paketumlaufzeit(Durchschnitt)	Warnung wegen ...	Kritisch wegen ...
24359	03/07/2016 15:33:07	ZENTRALE	172.16.10.1	0	224.869000	256.337000	238.560000	max. Paketumlauf...	max. Paketuml...
24360	03/07/2016 15:33:37	ZENTRALE	172.16.10.1	0	224.867000	272.290000	238.726000	max. Paketumlauf...	max. Paketuml...
24361	03/07/2016 15:34:07	ZENTRALE	172.16.10.1	0	225.852000	289.624000	254.387000	max. Paketumlauf...	max. Paketuml...
24362	03/07/2016 15:34:37	ZENTRALE	172.16.10.1	0	225.658000	294.184000	245.789000	max. Paketumlauf...	max. Paketuml...
24363	03/07/2016 15:35:07	ZENTRALE	172.16.10.1	0	225.040000	280.097000	246.493000	max. Paketumlauf...	max. Paketuml...
24364	03/07/2016 15:35:37	ZENTRALE	172.16.10.1	0	225.196000	361.272000	259.568000	max. Paketumlauf...	max. Paketuml...
24365	03/07/2016 15:36:07	ZENTRALE	172.16.10.1	0	226.290000	295.104000	248.344000	max. Paketumlauf...	max. Paketuml...
24366	03/07/2016 15:36:37	ZENTRALE	172.16.10.1	0	224.919000	377.248000	271.943000	max. Paketumlauf...	max. Paketuml...
24367	03/07/2016 15:37:07	ZENTRALE	172.16.10.1	0	225.174000	285.583000	243.667000	max. Paketumlauf...	max. Paketuml...
24368	03/07/2016 15:37:37	ZENTRALE	172.16.10.1	0	224.845000	237.954000	228.928000	max. Paketumlauf...	max. Paketuml...
24369	03/07/2016 15:38:07	ZENTRALE	172.16.10.1	0	224.027000	232.320000	226.219000	max. Paketumlauf...	max. Paketuml...
24370	03/07/2016 15:38:37	ZENTRALE	172.16.10.1	0	224.437000	283.768000	242.988000	max. Paketumlauf...	max. Paketuml...
24371	03/07/2016 15:39:07	ZENTRALE	172.16.10.1	0	225.133000	273.192000	247.214000	max. Paketumlauf...	max. Paketuml...
24372	03/07/2016 15:39:37	ZENTRALE	172.16.10.1	0	224.352000	243.303000	232.394000	max. Paketumlauf...	max. Paketuml...
24373	03/07/2016 15:40:07	ZENTRALE	172.16.10.1	0	226.346000	272.141000	246.442000	max. Paketumlauf...	max. Paketuml...

5.5.4 Ergänzungen im Status-Menü

SLA-Monitor

Dieses Menü beinhaltet die Statuswerte für den SLA-Monitor.

SNMP-ID:

1.36

Pfad Telnet:

Status

ICMP

Dieses Menü beinhaltet das Historie-Log und die letzten Ergebnisse des ICMP.

SNMP-ID:

1.36.1

Pfad Telnet:

Status > **SLA-Monitor**

Historie-Log

Dieser Eintrag enthält die Historien-Tabelle.

SNMP-ID:

1.36.1.1

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP**

Index

Fortlaufende Nummerierung der Einträge.

SNMP-ID:

1.36.1.1.1

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Zeitstempel

Genaue Zeitangabe zu dem der Eintrag angelegt wurde.

SNMP-ID:

1.36.1.1.2

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Name

Name der ICMP-Konfiguration.

SNMP-ID:

1.36.1.1.3

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Ziel

Dieser Eintrag enthält Ziel der Überprüfung.

SNMP-ID:

1.36.1.1.4

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Pkt-Loss-Percent

Dieser Eintrag zeigt die Anzahl verloren gegangener Datenpakete in Prozent.

SNMP-ID:

1.36.1.1.5

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

RTT-Min

Dieser Eintrag zeigt die minimale Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.1.6

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

RTT-Max

Dieser Eintrag zeigt die maximale Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.1.7

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

RTT-Avg

Dieser Eintrag zeigt die durchschnittliche Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.1.8

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Warnung

Dieser Eintrag enthält die Anzahl gemeldeter Warnungen.

SNMP-ID:

1.36.1.1.9

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Kritisch

Dieser Eintrag enthält die Anzahl gemeldeter Fehler.

SNMP-ID:

1.36.1.1.10

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Historie-Log**

Letzte-Ergebnisse

Dieser Eintrag enthält die Tabelle mit den Ergebnissen der letzten Überprüfung.

SNMP-ID:

1.36.1.2

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP**

Name

Name der ICMP-Konfiguration.

SNMP-ID:

1.36.1.2.1

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

Ziel

Dieser Eintrag enthält Ziel der letzten Überprüfung.

SNMP-ID:

1.36.1.2.2

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

Zeitstempel

Genaue Zeitangabe zu dem der Eintrag angelegt wurde.

SNMP-ID:

1.36.1.2.3

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

Pkt-Loss-Percent

Dieser Eintrag zeigt die Anzahl verloren gegangener Datenpakete in Prozent..

SNMP-ID:

1.36.1.2.4

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

RTT-Min

Dieser Eintrag zeigt die minimale Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.2.5

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

RTT-Max

Dieser Eintrag zeigt die maximale Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.2.6

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letzte-Ergebnisse**

RTT-Avg

Dieser Eintrag zeigt die durchschnittliche Paketumlaufzeit der ICMP-Pakete an.

SNMP-ID:

1.36.1.2.7

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letze-Ergebnisse**

Warnung

Dieser Eintrag enthält die Anzahl gemeldeter Warnungen.

SNMP-ID:

1.36.1.2.8

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letze-Ergebnisse**

Kritisch

Dieser Eintrag enthält die Anzahl gemeldeter Fehler.

SNMP-ID:

1.36.1.2.9

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP** > **Letze-Ergebnisse**

Werte-loeschen

Mit diesem Eintrag haben Sie die Möglichkeit, alle Werte zu löschen.

SNMP-ID:

1.36.1.3

Pfad Telnet:

Status > **SLA-Monitor** > **ICMP**

5.5.5 Ergänzungen im Setup-Menü

SLA-Monitor

Dieses Menu enthält die Einstellungen für SLA-Monitor.

SNMP-ID:

2.45

Pfad Telnet:

Setup

ICMP

In diesem Menü konfigurieren Sie das Internet Control Message Protocol (ICMP).

SNMP-ID:

2.45.1

Pfad Telnet:

Setup > **SLA-Monitor**

Name

Enthält den Namen der ICMP-Konfiguration.

SNMP-ID:

2.45.1.1

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

leer

Aktiv

Dieser Eintrag steuert, ob das jeweilige ICMP-Profil verwendet werden soll.

SNMP-ID:

2.45.1.2

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

ja
nein

Default-Wert:

ja

Ziel

Legen Sie eine IPv4-Adresse fest, an die das ICMP Diagnose- oder Fehlermeldungen senden soll.

SNMP-ID:

2.45.1.3

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 40 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

Rtg-Tag

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

SNMP-ID:

2.45.1.4

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

0

Loopback-Addresse

Das Gerät sieht diese Adresse als eigene Adresse an, die auch dann verfügbar ist, wenn z. B. eine physikalische Schnittstelle deaktiviert ist.

SNMP-ID:

2.45.1.5

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 56 Zeichen aus `[0-9]`

Default-Wert:

leer

Intervall

Zeitlicher Abstand in Sekunden, in dem ICMP Diagnose- oder Fehlermeldungen an das definierte Ziel übermittelt.

SNMP-ID:

2.45.1.6

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]`

Default-Wert:

30

Start-Offset

Definieren Sie eine Startverzögerung für die ICMP-Übermittlungen in Millisekunden.

SNMP-ID:

2.45.1.7

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]`

Default-Wert:

0

Anzahl

Legen Sie die Anzahl der gleichzeitig zu übermittelnden ICMP-Pakete fest.

SNMP-ID:

2.45.1.8

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

5

Paket-Verzoegerung

Legt fest, in welchem Abstand die ICMP-Pakete verzögert übermittelt werden. Verzögerung in Millisekunden.

SNMP-ID:

2.45.1.9

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

1000

Paketgroesse

Legt die Paketgröße für ICMP-Meldungen fest. Die Angabe erfolgt in Byte.

SNMP-ID:

2.45.1.10

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

56

Warn-Lvl-RTT-Max

Maximal zulässige Paketumlaufzeit bevor der SLA-Monitor eine Warnung ausgibt.

SNMP-ID:

2.45.1.11

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

100

Crit-Lvl-RTT-Max

Maximal zulässige Paketumlaufzeit bevor der SLA-Monitor einen Fehler meldet.

SNMP-ID:

2.45.1.12

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

200

Warn-Lvl-RTT-Avg

Durchschnittliche Paketumlaufzeit bevor der SLA-Monitor eine Warnung ausgibt.

SNMP-ID:

2.45.1.13

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

80

Crit-Lvl-RTT-Avg

Durchschnittliche Paketumlaufzeit bevor der SLA-Monitor einen Fehler meldet.

SNMP-ID:

2.45.1.14

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

170

Warn-Lvl-Pkt-Loss-Percent

Anzahl verlorener Datenpakete in Prozent vor Ausgabe einer Warnung.

SNMP-ID:

2.45.1.15

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

10

Crit-Lvl-Pkt-Loss-Percent

Anzahl verlorener Datenpakete in Prozent vor Ausgabe eines Fehlers.

SNMP-ID:

2.45.1.16

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

20

IP-Version

Definiert den verwendeten IP-Standard des Internet Control Message Protocols.

SNMP-ID:

2.45.1.17

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

Auto
IPv4
IPv6

Default-Wert:

Auto

Kommentar

Bemerkung zu dieser ICMP-Konfiguration.

SNMP-ID:

2.45.1.19

Pfad Telnet:

Setup > **SLA-Monitor** > **ICMP**

Mögliche Werte:

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

Default-Wert:

leer

Event-Anzahl

Anzahl der Ereignisse, die der SLA Monitor protokollieren soll.

SNMP-ID:

2.45.2

Pfad Telnet:

Setup > **SLA-Monitor**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

100

Start-Verzoegerung

Verzögerungszeit in Millisekunden bis zum Start der Überwachung.

SNMP-ID:

2.45.3

Pfad Telnet:

Setup > **SLA-Monitor**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

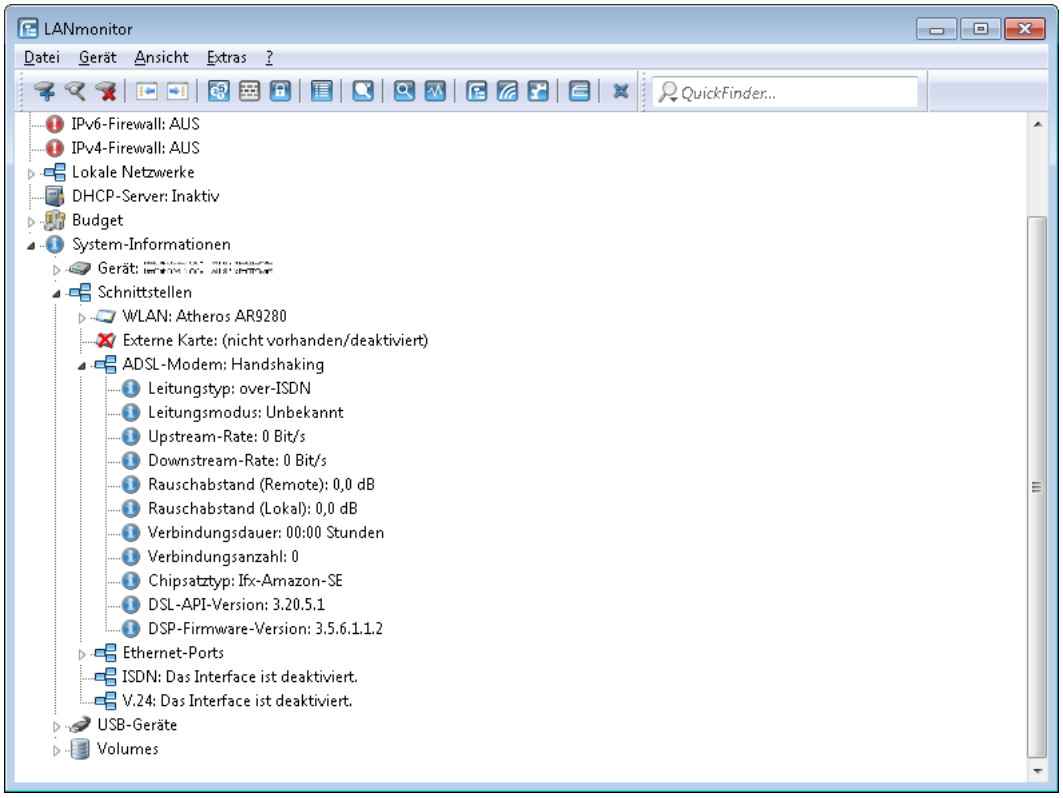
10

5.6 Zusätzliche DSL-Modem-Statuswerte

Ab Version 9.20 stellt LCOS für DSL-Verbindungen zusätzlich die Statuswerte für Verbindungsdauer und Verbindungsanzahl zur Verfügung.

5.6.1 DSL-Modem-Statuswerte mit LANmonitor auslesen

Mit dem LANmonitor lassen sich für jedes registrierte Gerät mit ADSL-/VDSL-Modem im Abschnitt **System-Informationen** > **Schnittstellen** > **ADSL-Modem: <Status>** die Statuswerte des DSL-Modems auslesen.



5.6.2 Ergänzungen im Status-Menü

Verbindungsanzahl

Dieser Eintrag enthält die Anzahl der DSL-Verbindungen seit dem letzten System-Neustart.

SNMP-ID:

1.75.53

Pfad Telnet:

Status > **VDSL**

Verbindungsdauer

Dieser Eintrag enthält die Dauer der DSL-Verbindung seit der letzten Synchronisation.

SNMP-ID:

1.75.54

Pfad Telnet:

Status > **VDSL**

Verbindungsanzahl

Dieser Eintrag enthält die Anzahl der DSL-Verbindungen seit dem letzten System-Neustart.

SNMP-ID:

1.75.25.53

Pfad Telnet:

Status > **VDSL** > **Advanced**

Verbindungsdauer

Dieser Eintrag enthält die Dauer der DSL-Verbindung seit der letzten Synchronisation.

SNMP-ID:

1.75.25.54

Pfad Telnet:

Status > **VDSL** > **Advanced**

5.7 Anzeige der Mobilfunkstandards

Ab LCOS-Version 9.20 nennt LANconfig nicht nur die Bezeichnungen der Mobilfunkstandards, sondern auch die entsprechenden Generationsbezeichnungen:

- GPRS: 2G
- GSM: 2G
- EDGE: 2.5G
- UMTS: 3G
- HSPA: 3.5G
- HSDPA: 3.5G
- HSUPA: 3.5G
- HSPA+: 3.5G
- LTE: 4G

5.7.1 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
3G
Ausschließlicher UMTS-Betrieb
2G
Ausschließlicher GPRS-Betrieb
3G-2G
Kombinierter UMTS-GPRS-Betrieb
4G
Ausschließlicher LTE-Betrieb
4G-3G
Kombinierter LTE-UMTS-Betrieb
4G-2G
Kombinierter LTE-GPRS-Betrieb

Default-Wert:

Auto

5.7.2 Ergänzungen im Status-Menü

Modus

Dieser Eintrag zeigt den Mobilfunkmodus.

SNMP-ID:
1.49.9.3

Pfad Telnet:
Status > **Modem-Mobilfunk** > **Netzliste**

Mögliche Werte:

unbekannt
2G
3G
4G

Modus

Dieser Eintrag enthält den Mobildfunk-Modus.

SNMP-ID:
1.49.12

Pfad Telnet:
Status > **Modem-Mobilfunk**

Mögliche Werte:

unbekannt
UMTS(3G)
GPRS(2G)
GSM(2G)
EDGE(2.5G)
HSDPA(3.5G)
HSUPA(3.5G)
HSPA+(3.5G)
LTE(4G)
HSPA(3.5G)

Default-Wert:

unbekannt

Mode

Dieser Eintrag enthält die Statuswerte für Mode.

SNMP-ID:

1.49.16.5

Pfad Telnet:

Status > **Modem-Mobilfunk** > **Historie**

Mögliche Werte:

unbekannt
UMTS(3G)
GPRS(2G)
GSM(2G)
EDGE(2.5G)
HSDPA(3.5G)
HSUPA(3.5G)
HSPA+(3.5G)
LTE(4G)
HSPA(3.5G)

Default-Wert:

unbekannt

AcT

Dieser Eintrag enthält die Statuswerte für AcT.

SNMP-ID:

1.49.47.5

Pfad Telnet:

Status > **Modem-Mobilfunk** > **Netzliste**

Mögliche Werte:

unbekannt
2G
3G
4G

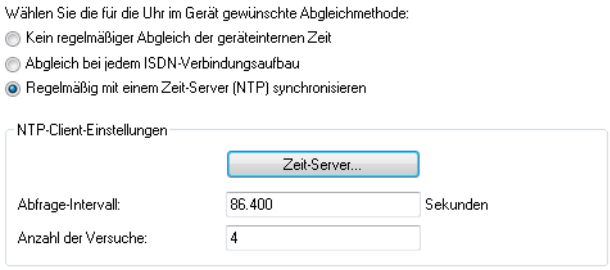
6 IPv6

6.1 IPv6-Unterstützung durch (S)NTP-Client und -Server

LCOS-Version 9.20 unterstützt IPv6 für den (S)NTP-Client und -Server.

6.1.1 Konfiguration des Zeit-Servers unter LANconfig

Damit ein Gerät die aktuelle Zeit im Netzwerk bekannt machen kann, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** den regelmäßigen Abgleich mit einem Zeitserver.



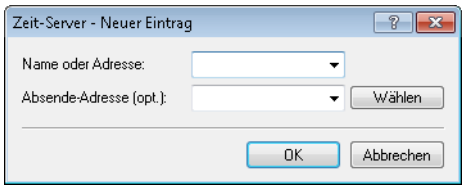
Abfrage-Intervall

Geben Sie hier das Zeitintervall in Sekunden an, nach dem eine Überprüfung und gegebenenfalls Neusynchronisierung der internen Uhr des Gerätes mit einem der angegebenen Zeit-Server (NTP) erfolgen soll.

Anzahl der Versuche

Geben Sie hier an, wie oft das Gerät eine Synchronisation mit dem Zeit-Server versuchen soll. Bei Angabe einer Null versucht das Gerät solange eine Verbindung, bis es eine gültige Synchronisation erreicht hat.

Im Abschnitt **NTP-Einstellungen** konfigurieren Sie anschließend unter **Zeit-Server** die Einstellungen für den Zeitabgleich mit dem entsprechenden Server.



Name oder Adresse

Geben Sie hier einen Zeit-Server (NTP) an, den das Gerät abfragen soll. Der Zeit-Server sollte über eines der vorhandenen Interfaces erreichbar sein.

Die Angabe einer Adresse ist möglich als FQDN, IPv4- oder IPv6-Adresse. Liefert die DNS-Namensauflösung für den Zeit-Server eine IPv6-Adresse zurück, bevorzugt das Gerät diese IPv6-Adresse.

Die Reihenfolge, in der das Gerät mehrere angegebene Zeit-Server abfragt, bestimmen Sie in der Übersicht der Einträge

Absende-Adresse (opt.)

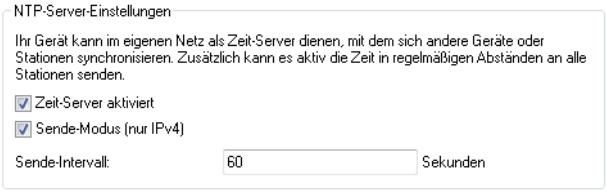
Konfigurieren Sie hier optional eine Absendeadresse, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, geben Sie diese hier als Absendeadresse an.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IPv4- oder IPv6-Adresse

Mit diesen Einstellungen bezieht zunächst nur das Gerät selbst die Zeit von den öffentlichen Zeitservern. Um die aktuelle Zeit auch im LAN den anderen Geräte bekannt zu machen, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** im Abschnitt **NTP-Server-Einstellungen** den Zeit-Server im Gerät.



Zeit-Server aktiviert

Aktivieren Sie diese Option, wenn das Gerät als Zeit-Server im Netz funktionieren soll.

Sende-Modus (nur IPv4)

Soll das Gerät regelmäßig als Zeit-Server an alle Stationen im Netz die aktuelle Zeit senden, aktivieren Sie den „Sende-Modus“.

Der Sende-Modus des Gerätes unterstützt nur IPv4-Adressen.

Sende-Intervall

Geben Sie den zeitlichen Abstand in Sekunden an, in welchem der Zeit-Server des Gerätes die aktuelle Zeit an die erreichbaren Stationen im Netz senden soll.

6.1.2 Ergänzungen im Setup-Menü

BC-Modus

Soll das Gerät regelmäßig als Zeit-Server an alle Stationen im Netz die aktuelle Zeit senden, aktivieren Sie den „Sende-Modus“.

Der Sende-Modus des Gerätes unterstützt nur IPv4-Adressen.

SNMP-ID:

2.26.3

Pfad Telnet:

Setup > **NTP**

Mögliche Werte:

nein

Der Sende-Modus ist deaktiviert.

ja

Der Sende-Modus ist aktiviert.

Default-Wert:

nein

RQ-Address

Geben Sie hier einen Zeit-Server (NTP) an, den das Gerät abfragen soll. Der Zeit-Server sollte über eines der vorhandenen Interfaces erreichbar sein.

Die Angabe einer Adresse ist möglich als FQDN, IPv4- oder IPv6-Adresse. Liefert die DNS-Namensauflösung für den Zeit-Server eine IPv6-Adresse zurück, bevorzugt das Gerät diese IPv6-Adresse.

SNMP-ID:

2.26.11.1

Pfad Telnet:

Setup > **NTP** > **RQ-Adresse**

Mögliche Werte:

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

Default-Wert:

leer

Loopback-Addr.

Konfigurieren Sie hier optional eine Absendeadresse, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, geben Sie diese hier als Absendeadresse an.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.

- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IPv4- oder IPv6-Adresse

SNMP-ID:

2.26.11.2

Pfad Telnet:

Setup > **NTP** > **RQ-Adresse**

Mögliche Werte:

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

Default-Wert:

leer

7 VPN

7.1 IKEv2-Unterstützung

Ab LCOS-Version 9.20 unterstützt LCOS IKEv2.

7.1.1 Funktionen des VPN-Moduls

In diesem Abschnitt sind alle Funktionen und Eigenschaften des LCOS-VPN-Moduls aufgelistet. Experten im Bereich VPN bietet er eine stark komprimierte Zusammenfassung über die Leistungsfähigkeit der Funktion. Das Verständnis der verwendeten Fachtermini setzt allerdings solide Kenntnisse über die technischen Grundlagen von VPN voraus. Für die Inbetriebnahme und den Normalbetrieb von VPN sind diese Informationen jedoch nicht erforderlich.

- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- LANCOM Dynamic VPN: Öffentliche IP-Adressen können statisch oder dynamisch sein (für den Aufbau zu Gegenstellen mit dynamischer IP-Adresse ist eine ISDN-Verbindung erforderlich)
- VPN nach dem IPSec-Standard
- IPSec-Protokolle ESP, AH und IPCOMP im Tunnelmodus
- Hash-Algorithmen:
  - HMAC-MD5-96, Hashlänge 128 Bits
  - HMAC-SHA-1-96, Hashlänge 160 Bits
  - HMAC-SHA-256, Hashlänge 256 Bits
  - HMAC-SHA-384, Hashlänge 384 Bits
  - HMAC-SHA-512, Hashlänge 512 Bits
- Kompression mit „Deflate“ (ZLIB)
- Schlüsselmanagement nach ISAKMP (IKEv1, IKEv2)
- Symmetrische Verschlüsselungsverfahren
  - AES, Schlüssellänge 128, 192 und 256 Bits
  - Triple-DES (3DES), Schlüssellänge 168 Bits
  - Blowfish, Schlüssellänge 128-448 Bits
  - CAST, Schlüssellänge 128 Bits
  - DES, Schlüssellänge 56 Bits
- IKEv1 Main- und Aggressive-Modus
- IKEv1/IKEv2 Config Mode
- IKEv1 mit Preshared Keys und IKEv2
- IKEv1 und IKEv2 mit RSA-Signature und digitalen Zertifikaten (X.509)
- Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit Schlüssellänge 768 Bits, 1024 Bits, 1536 Bits, 2048 Bits, 3072 Bits und 4096 Bits (well known groups 1, 2, 5, 14, 15 und 16)

7.1.2 IKEv2

Der VPN-Aufbau ist mit LANCOM-Geräten sowohl über IKEv1 als auch über IKEv2 möglich.

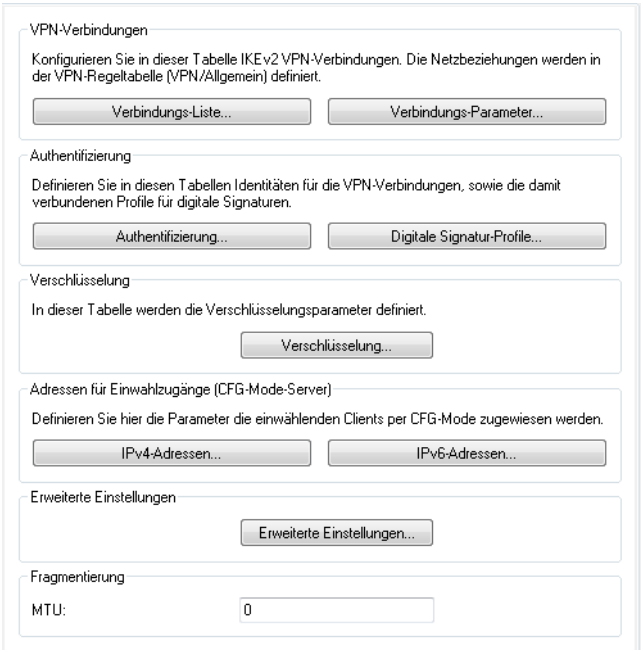
IKEv2 ermöglicht einen schnelleren und sichereren Verbindungsaufbau von VPN-Tunneln. Erstmals ist zudem die VPN-verschlüsselte Vernetzung von IPv6-basierten Standorten auch im Mischbetrieb mit IPv4 möglich.

Die Einrichtung einer VPN-Verbindung über IKEv1 ist bei manueller Konfiguration komplex und fehleranfällig, so dass viele Implementationen von IPSec inkompatibel zueinander konfiguriert sein können und damit eine VPN-Verbindung zwischen den Geräten durch fehlerhafte Konfigurationsvorgänge scheitern kann. Die IKEv2-Konfiguration im LCOS ermöglicht es dem Administrator, zuverlässig eine Übereinstimmung der Konfiguration mit der Gegenstelle einzurichten. Der Administrator hat z. B. die Möglichkeit, mehrere Diffie-Hellman-Gruppen anzuwählen. Damit erhält das Gerät über die überarbeitete Benutzeroberfläche an vielen Konfigurationsparametern empfohlene Default-Werte. Dieser vereinfachte Konfigurationsablauf mit IKEv2 beseitigt folglich Fehlerquellen, was wiederum zu einem geringeren Administrationsaufwand führt. Zusätzlich ist der VPN-Verbindungsaufbau bei IKEv2 performanter, denn IKEv2 nutzt für den Informationsaustausch bei der Aushandlung eines VPN-Tunnels nur 4 Pakete (je VPN-Partner ein REQUEST und ein REPLY), anstatt wie bei IKEv1 zwischen 6 (im „aggressive/quick mode“) und 12 (im „main mode“) Paketen. Der Sicherheitsstandard ist bei IKEv2 genauso hoch wie bei IKEv1.

Bei der Verwendung von IKEv2 werden *RFC 7296*, *RFC 7427* und im IKEv2-Client-Betrieb *RFC 5685* unterstützt.

7.1.3 IKEv2 mit LANconfig konfigurieren

IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec**.



VPN-Verbindungen

In diesem Abschnitt konfigurieren Sie die IKEv2-VPN-Verbindungen und Verbindungsparameter.

Authentifizierung

Definieren Sie in dieser Tabelle die Identitäten für die VPN-Verbindungen.

Digitale Signatur-Profile

Definieren Sie in dieser Tabelle die Authentifizierungs-Methode für die VPN-Verbindungen.

Verschlüsselung

Definieren Sie in dieser Tabelle die Verschlüsselungsparameter.

Adressen für Einwahlzugänge (CFG-Mode-Server)

Definieren Sie in dieser Tabelle die Parameter, die das Gerät den einwählenden Clients per CFG-Mode zuweist.

Erweiterte Einstellungen

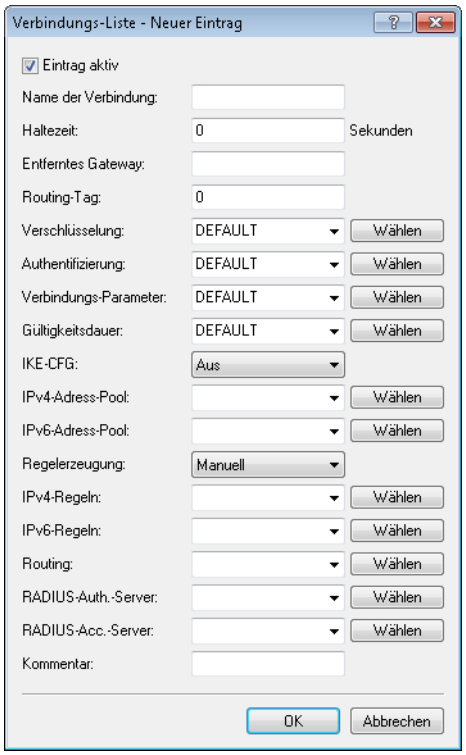
Konfigurieren Sie in diesem Abschnitt die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter und die Präfixe für das IKEv2-Routing.

Um eine IKEv2-Verbindung zu konfigurieren, ist zunächst ein Eintrag in der **Verbindungs-Liste** erforderlich. Um den Konfigurationsaufwand gering zu halten, enthält LCOS Default-Einträge, die die meisten Parameter mit den gängigen Einstellungen für starke Verschlüsselungsalgorithmen, Dead-Peer-Detection oder Gültigkeitszeiträume vorbelegen. Lediglich die Angabe der VPN-Gegenstellen-Adresse, der Authentifizierungs-Parameter (unter **Authentifizierung**) sowie der VPN-Regeln (unter **VPN** > **Allgemein** > **Netzwerk-Regeln**) ist erforderlich.

Der Konsolenbefehl `show vpn` zeigt, ob die so eingerichtete VPN-Verbindung erfolgreich ist.

Verbindungs-Liste

In dieser Tabelle konfigurieren Sie die IKEv2-Verbindungen zu VPN-Partnern.



Eintrag aktiv

Aktiviert oder deaktiviert die Verbindung zu dieser VPN-Gegenstelle.

Name der Verbindung

Enthält den Namen der Verbindung zur Gegenstelle.

Haltezeit

Gibt die Haltezeit in Sekunden an, die das Gerät eine Verbindung ohne Datenfluss aufrecht erhält.

Entferntes Gateway

Enthält die Adresse (IPv4- oder IPv6-Adresse, FQDN) des VPN-Partners.

Routing-Tag

Enthält das Routing-Tag für diese VPN-Verbindung.

Verschlüsselung

Bestimmt die Verschlüsselung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verschlüsselung**.

Authentifizierung

Bestimmt die Authentifizierung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Authentifizierung**.

Verbindungs-Parameter

Bestimmt die allgemeinen Parameter der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verbindungs-Parameter**.

Gültigkeitsdauer

Bestimmt die Lebensdauer der Schlüssel einer VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Erweiterte Einstellungen** > **Gültigkeitsdauer**.

IKE-CFG

Bestimmt den IKEv2-Config-Modus dieser Verbindung für RAS-Einwahlen.

Mögliche Werte sind:

- Aus: IKEv2-Config-Modus deaktiviert
- Server: Der Router verteilt Konfigurationsparameter (z. B. Adressen oder DNS-Server) an VPN-Clients Die zu vergebenden Parameter werden im IPv4- bzw. IPv6-Adresspool konfiguriert.
- Client: Der Router fragt beim Server Konfigurationsparameter (z. B. Adressen oder DNS-Server an).

IPv4-Adress-Pool

IPv4-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

IPv6-Adress-Pool

IPv6-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

Regelerzeugung

Bestimmt, wie VPN-Regeln erstellt werden.

Mögliche Werte:

Automatisch

Als Quellnetz wird das lokale Intranet eingesetzt (privater IP-Adressbereich, zu dem das lokale VPN-Gateway selbst gehört). Als Zielnetze dienen für die automatisch erstellten VPN-Regeln die Netzbereiche aus der IP-Routing-Tabelle, für die als Router ein entferntes VPN-Gateway eingetragen ist.

Werden zwei einfache lokale Netzwerke gekoppelt, ist es der VPN-Automatik möglich, aus dem IP-Adressbereich des eigenen LANs und dem Eintrag des entfernten LAN in der IP-Routing-Tabelle die erforderliche Netzbeziehung ableiten.

Manuell

Die Regelerstellung für die Netzbeziehungen erfolgt wie die manuelle Regel-Definition für IPv4 oder IPv6.

IPv4-Regeln

Gibt an, welche IPv4-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv4-Regeln stehen in der Tabelle **VPN** > **Netzwerk-Regeln**.

IPv6-Regeln

Gibt an, welche IPv6-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv6-Regeln stehen in der Tabelle **VPN** > **Netzwerk-Regeln**.

Routing

Gibt die Routen an, die der Gegenseite dynamisch per IKE-CFG Mode übermittelt werden sollen. Diese Funktion ist nur im IKEv2-CFG Mode für Client und Server möglich.

Die Routen für IPv4- und IPv6-Verbindungen stehen in den Tabellen **Erweiterte Einstellungen** > **IPv4-Routing/IPv6-Routing**.

RADIUS-Auth.-Server

Bestimmt den RADIUS-Server für die Autorisierung des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

RADIUS-Auth.-Server

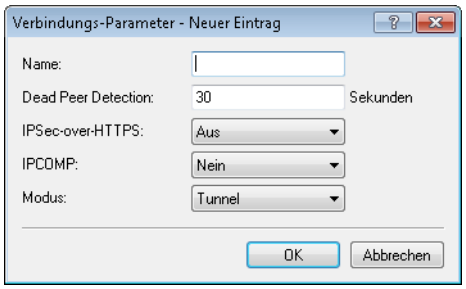
Bestimmt den RADIUS-Server für das Accounting des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

Verbindungs-Parameter

In dieser Tabelle definieren Sie die Parameter von IKEv2-VPN-Verbindungen, die nicht Bestandteil der SA-Verhandlung sind. Es existiert ein Standardeintrag „DEFAULT“ mit gängigen Einstellungen.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Verbindungs-Parameter“ zu.

Dead Peer Detection

Enthält die Zeit in Sekunden, nach der das Gerät die Verbindung beendet, wenn es in der Zwischenzeit den entfernten Peer nicht mehr erreicht.

IPSec-over-HTTPS

Gibt an, ob die Verbindung IKEv2 über HTTPS verwendet.

IPCOMP

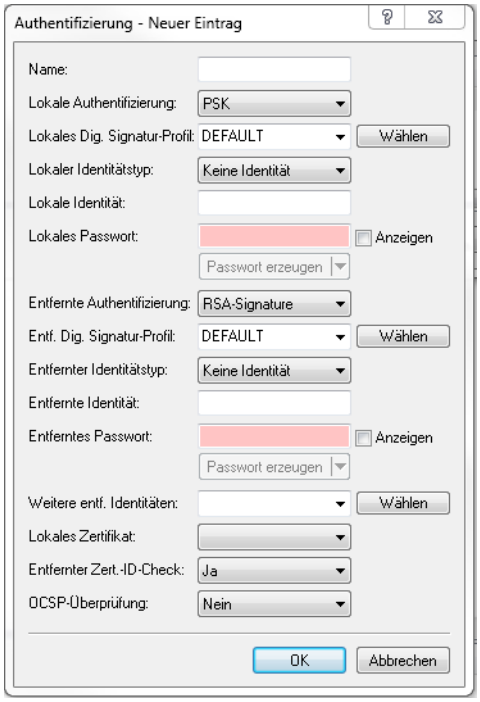
Gibt an, ob die Geräte die IKEv2-Datenpakete komprimiert übertragen.

Modus

Bestimmt den Übertragungsmodus.

Authentifizierung

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung der lokalen und mindestens einer entfernten Identität.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Authentifizierung" zu.

Lokale Authentifizierung

Legt die Authentifizierungsmethode für die lokale Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema
- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Lokales Digitales Signatur-Profil

Profilname des verwendeten lokalen Digital-Signatur-Profils.

Lokaler Identitätstyp

Zeigt den ID-Typ der lokalen Identität an. Entsprechend interpretiert das Gerät die Eingabe unter „Lokale Identität". Mögliche Angaben sind:

- Keine Identität: Es wird keine Identität übertragen.
- IPv4-Adresse: Das Gerät verwendet eine IPv4-Adresse als lokale ID.
- IPv6-Adresse: Das Gerät verwendet eine IPv6-Adresse als lokale ID.

- Domänen-Name (FQDN): Das Gerät verwendet einen Domänen-Namen als lokale ID.
- E-Mail-Adresse (FQUN): Das Gerät verwendet eine E-Mail-Adresse als lokale ID.
- ASN.1-Distinguished-Name: Das Gerät verwendet einen Distinguished Name als lokale ID (z. B. „CN=client01.example.com,O=test,C=DE“
- Key-ID (Gruppenname): Das Gerät verwendet den Gruppennamen als lokale ID. Den Gruppennamen können sie beliebig definieren.

Lokale Identität

Enthält die lokale Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Lokaler Identitätstyp“.

Lokales Passwort

Enthält das Passwort der lokalen Identität. Mit diesem Passwort authentifiziert sich das Gerät bei der Gegenseite. Das lokale und entfernte Passwort kann identisch oder unterschiedlich sein.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema
- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Entferntes Digitales Signatur-Profil

Profilname des entfernten Digital-Signatur-Profils.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter „Entfernte Identität“. Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld „Entfernte Identität“ ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.
- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID (z. B. „CN=client01.example.com,O=test,C=DE“).
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Entfernter Identitätstyp“.

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

Weitere entf. Identitäten

Für redundante VPN-Szenarien ist die Angabe von alternativen entfernten Identitäten möglich.

Konfigurieren Sie hier weitere entfernte Identitäten aus der Tabelle **Erweiterte Einstellungen** > **Identitäten-Liste**.

Lokales Zertifikat

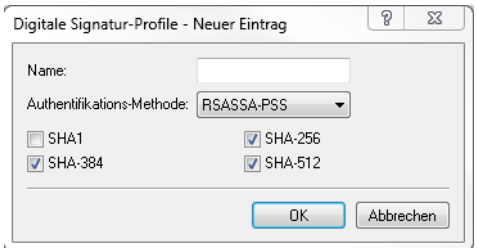
Zeigt das lokale Zertifikat an.

Entfernte Zertifikatsprüfung

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

Digitale Signatur-Profile

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung der lokalen und mindestens einer entfernten Identität.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Authentifizierung" zu.

Authentifizierungs-Methode

Legt die Authentifizierungsmethode für die digitale Signatur fest. Mögliche Werte sind:

- RSASSA-PSS: RSA mit verbessertem probabilistischem Signatur-Schema nach Version 2.1 von PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA nach der älteren Version des Signature-Schemas nach Version 1.5 von PKCS #1 (signature scheme with appendix)

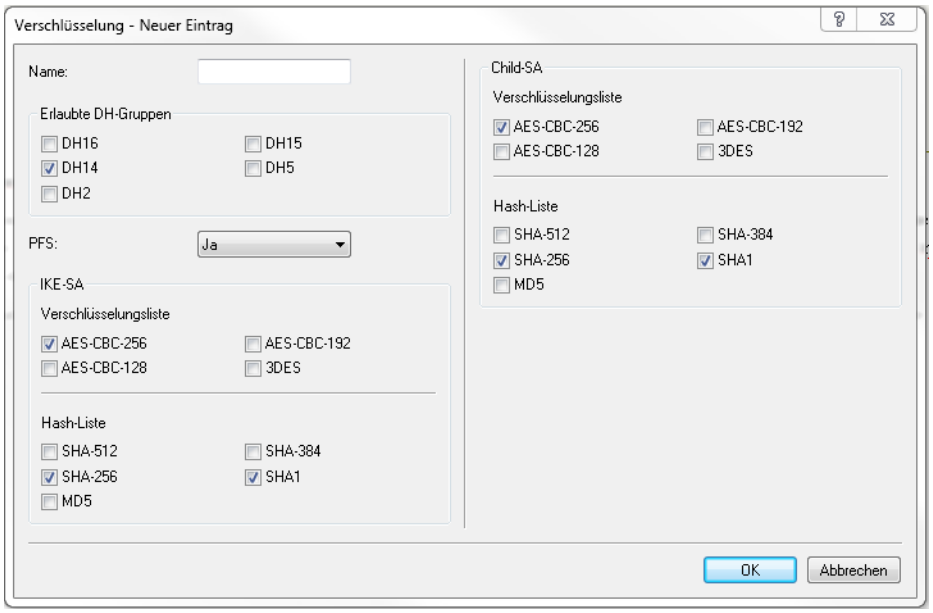
Legen Sie zudem die zu verwendenden Secure Hash Algorithmen (SHA) fest.

Verschlüsselung

In dieser Tabelle konfigurieren Sie die Verschlüsselungsparameter. Es existiert ein Standardeintrag „DEFAULT" mit gängigen Einstellungen.

Eine Mehrfachauswahl der Parameter ist möglich. Diese Parameterlisten propagiert das Gerät im IKE-Protokoll und in CHILD-SAs. Beide VPN-Partner verständigen sich anschließend auf einen Algorithmus der propagierten Listen. Beim Aufbau der ersten IKE-SA einigen sich die VPN-Partner auf die höchste der gegenseitig propagierten DH-Gruppen. Diese DH-Gruppe nutzen die VPN-Partner, wenn sie die IKE-SAs erneuern oder wenn sie CHILD-SAs erzeugen oder erneuern (bei aktiviertem PFS).

Die Verbindung zwischen den VPN-Partnern kommt zustande, wenn es in der Menge der konfigurierten Verschlüsselungsparameter Gemeinsamkeiten gibt. Stimmen die Parameter in keinem Fall überein, findet keine Verbindung statt.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld „Verschlüsselung“ zu.

Erlaubte DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel. Aktuell werden folgende Gruppen unterstützt:

- DH-2 (1024-Bit Modulus)
- DH-5 (1536-Bit Modulus)
- DH-14 (2048-Bit Modulus)
- DH-15 (3072-Bit Modulus)
- DH-16 (4096-Bit Modulus)

PFS

Gibt an, ob Perfect Forward Secrecy (PFS) aktiviert ist.

Verschlüsselungsliste

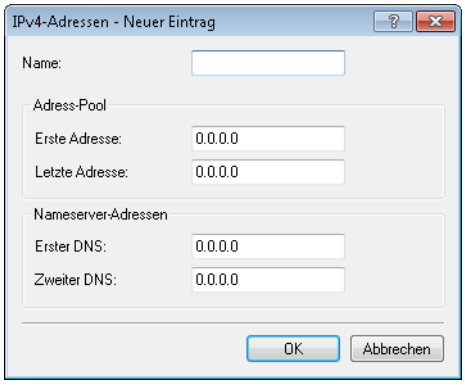
Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind.

Hash-Liste

Gibt an, welche Hash-Algorithmen aktiviert sind.

IPv4-Adressen

In dieser Tabelle konfigurieren Sie die IPv4-Parameter, die das Gerät den einwählenden VPN-Clients per CFG-Mode zuweist.



Name

Enthält den Namen der Schnittstelle für den Einwahlzugang.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Nameserver-Adressen

Erster DNS

Enthält die erste DNS-Adresse.

Zweiter DNS

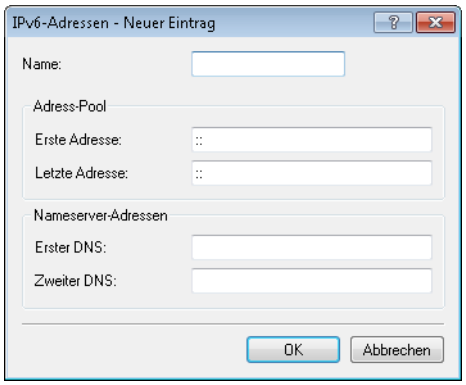
Enthält die zweite DNS-Adresse.

IPv6-Adressen

Wenn das Gerät als „CFG-Mode-Server" arbeitet, vergibt der Server per IKEv2-Configuration-Payload eine Adresse aus einem lokalen Adress-Pool an Clients. Außerdem kann er dem Client bis zu zwei DNS-Server zuweisen.

Serverseitig aktivieren Sie dazu in der VPN-Verbindungsliste den CFG-Mode „Server" und auf der Client-Seite den CFG-Mode „Client".

In dieser Tabelle konfigurieren Sie die IPv6-Parameter, die das Gerät den einwählenden VPN-Clients im CFG-Mode „Server“ zuweist.



Name

Enthält den Namen der Schnittstelle für den Einwahlzugang.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Nameserver-Adressen

Erster DNS

Enthält die erste DNS-Adresse.

Zweiter DNS

Enthält die zweite DNS-Adresse.

Erweiterte Einstellungen

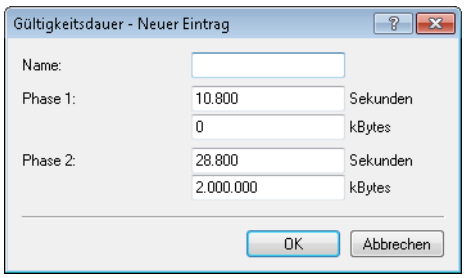
In diesem Dialog konfigurieren Sie die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter, die Präfixe für da IKEv2-Routing sowie die RADIUS-Server für IKEv2.

Gültigkeitsdauer

In dieser Tabelle definieren Sie die IKEv2-Rekeying-Parameter. Es existiert ein Standardeintrag „DEFAULT" mit gängigen Einstellungen.

Je Phase unterscheidet das Gerät nach Zeit oder zu übertragender Datenmenge. Der Parameter, der als erstes seinen festgelegten Grenzwert erreicht, startet die Erneuerung des entsprechenden IKEv2-Schlüssels.

Der Wert „0" bedeutet, dass das Gerät keinen Grenzwert für den entsprechenden Schlüssel festlegt.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Phase 1

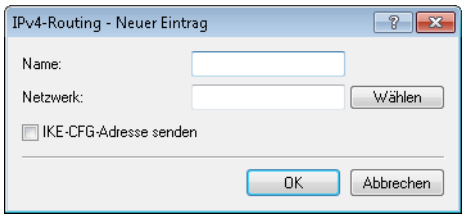
Enthält die Zeit in Sekunden oder die Datenmenge in Kilobyte bis zur Erneuerung des IKE-SA-Schlüssels.

Phase 2

Enthält die Zeit in Sekunden oder die Datenmenge in Kilobyte bis zur Erneuerung des CHILD-SA-Schlüssels.

IPv4-Routing

In dieser Tabelle konfigurieren Sie die IPv4-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IP-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/IP-Maske
- IP-Adresse/Präfixlänge
- IP-Schnittstellen-Name

Die Konfiguration der IP-Subnetze erfolgt unter **IPv4** > **Allgemein** im Abschnitt **Eigene Adressen**.

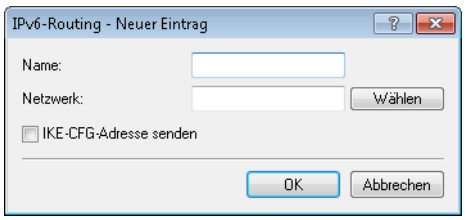
IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

IPv6-Routing

In dieser Tabelle konfigurieren Sie die IPv6-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IPv6-Adresse
- IPv6-Adresse/Präfixlänge
- IPv6-Schnittstellen-Name

Die Konfiguration der IP-Subnetze erfolgt unter **IPv6** > **Allgemein** im Abschnitt **IPv6-Netzwerke**.

IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

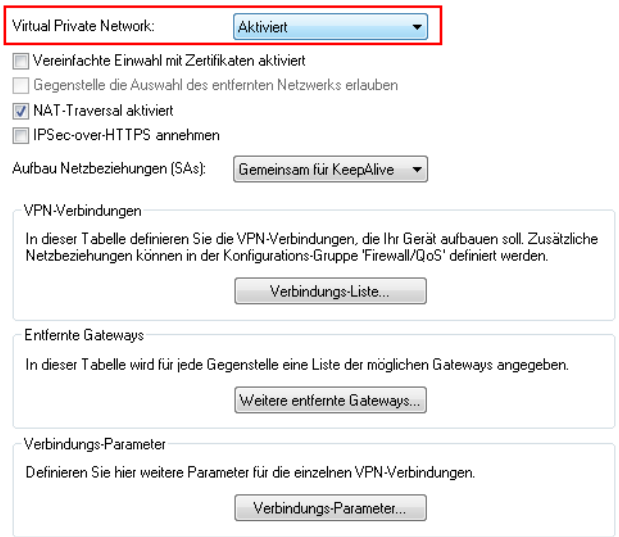
Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

7.1.4 Tutorial: Einrichtung von IKEv2 unter LANconfig

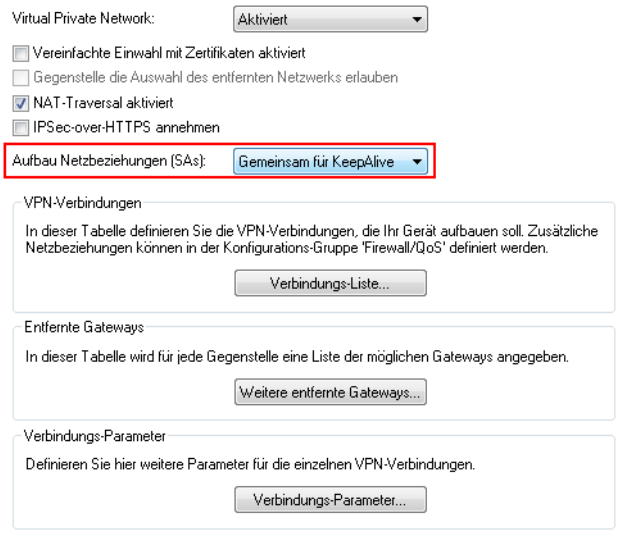
Ausgangsszenario: Zwei LANCOM-Router sind über eine WAN-Verbindung miteinander verbunden und sollen mit Hilfe von IKEv2/IPSec-VPN eine sichere VPN-Verbindung untereinander aufbauen. Bei den Routern handelt es sich um einen LANCOM 1781AW in der Zentrale und einen LANCOM 1781VA-4G in der Filiale.

Eine bestehende WAN-Verbindung zwischen beiden Geräten wird vorausgesetzt.

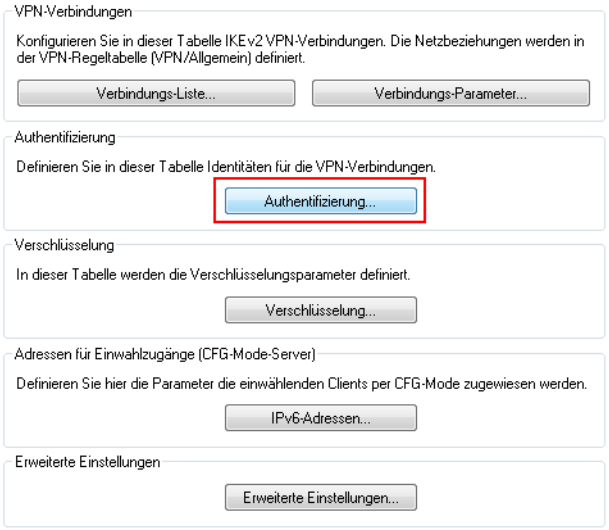
1. **Aktivieren von VPN**: Öffnen Sie den Menüpunkt **VPN** > **Allgemein** in der Konfiguration der beiden Router und wählen Sie unter **Virtual Private Network** die Option **Aktiviert**. Hiermit haben Sie VPN auf dem jeweiligen Gerät aktiviert.



2. **Konfiguration des Aufbaus der Netzbeziehungen (SAs)**: Damit die Netzbeziehungen korrekt und nach dem gleichen Schema aufgebaut werden, wählen Sie bei beiden Routern unter **Aufbau Netzbeziehungen (SAs)** die Option **Gemeinsam für KeepAlive**.

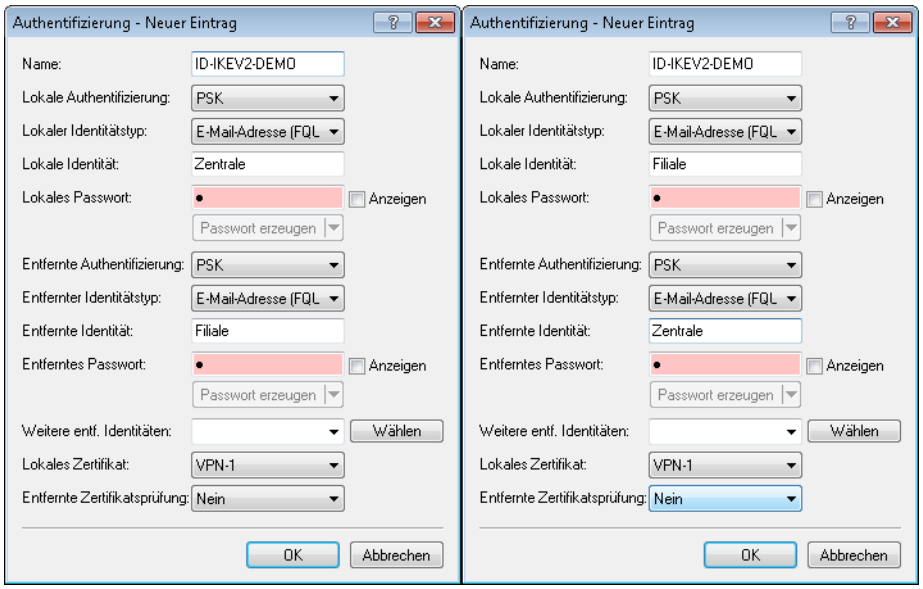


3. **Konfiguration der Authentifizierung**: Definieren Sie für die VPN-Verbindung die Art der Authentifizierung. Öffnen Sie dazu den Menüpunkt **VPN** > **IKEv2/IPSec** und klicken Sie auf die Schaltfläche **Authentifizierung**.



4. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Authentifizierung zu konfigurieren. Tragen Sie in dem Konfigurationsfenster die Informationen zur Authentifizierung für die VPN-Verbindung ein.

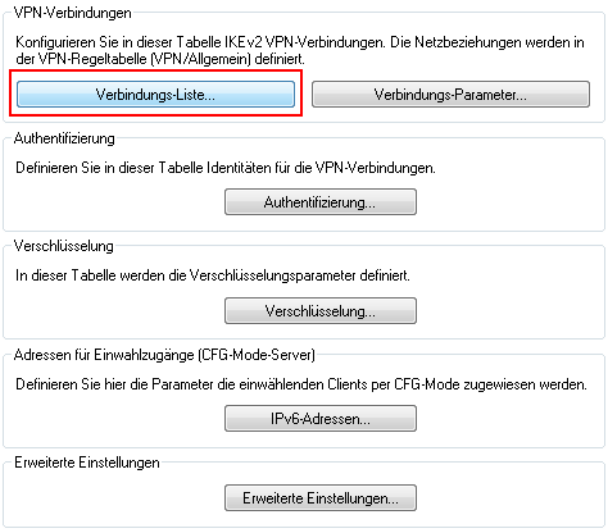
Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

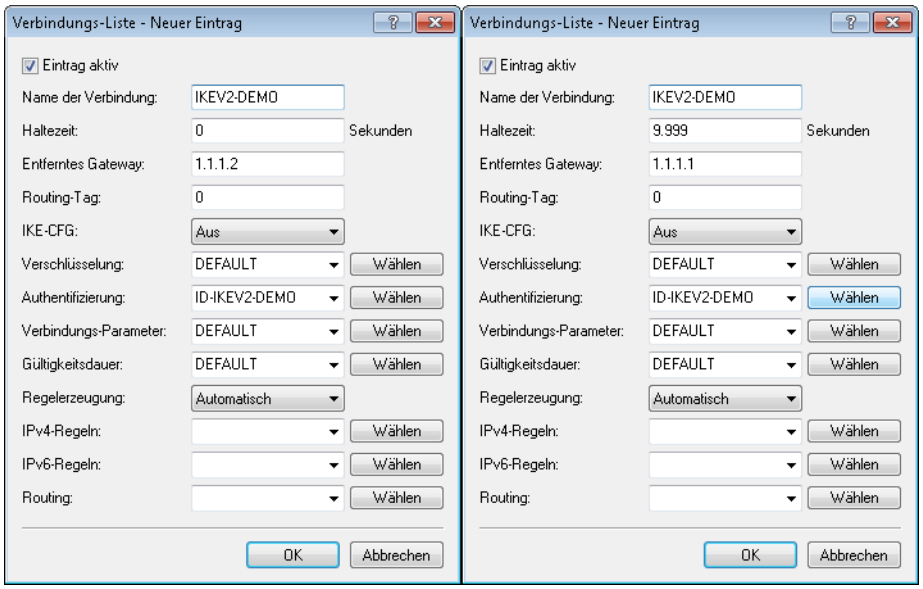
Parameter	Beschreibung
Name	Geben Sie den Namen für die Authentifizierung ein. In diesem Beispiel wurde **ID-IKEV2-DEMO** auf beiden Geräten gewählt. Dieser Eintrag wird später in der VPN-Verbindungs-Liste genutzt.
Lokale Authentifizierung	Wählen Sie den Typ der Authentifizierung an diesem Router aus. In diesem Beispiel wird die Authentifizierung über einen Pre-shared Key (PSK) vorgenommen.
Lokaler Identitätstyp	Wählen Sie den Typ der Identität bei diesem Router aus. In diesem Beispiel wurde der Identitätstyp **E-Mail-Adresse (FQUN)** gewählt.
Lokale Identität	Bestimmen Sie die lokale Identität. In diesem Beispiel wurde für den 1781AW die lokale Identität **Zentrale** und für den 1781VA-4G die lokale Identität **Filiale** gewählt.
Lokales Passwort	Der Pre-shared Key, der verwendet wird, um sich an diesem Router erfolgreich zu authentifizieren.
Entfernte Authentifizierung	Wählen Sie den Authentifizierungstypen des Routers der Gegenseite aus. Bei dem 1781AW entspricht dieser Eintrag dem Eintrag „Lokale Authentifizierung" am 1781VA-4G.
Entfernter Identitätstyp	Wählen Sie den Typ der entfernten Identität (des Routers der Gegenseite) aus. Bei dem 1781AW entspricht dieser Eintrag dem lokalen Identitätstyp des 1781VA-4G.
Entfernte Identität	Geben Sie die Identität der Gegenseite an. Bei dem 1781AW entspricht dieser Eintrag dem Eintrag „Lokale Identität" am 1781VA-4G.
Entferntes Passwort	Der Pre-shared Key, der verwendet wird, um sich an der Gegenseite zu authentifizieren. Bei dem 1781AW entspricht dieser Eintrag dem lokalen Passwort des 1781VA-4G.

5. **Konfiguration der Verbindungs-Liste**: Konfigurieren Sie die Verbindungs-Listen der einzelnen Router. Zur Konfiguration öffnen Sie den Menüpunkt **VPN** > **IKEv2/IPSec** und klicken Sie auf die Schaltfläche **Verbindungs-Liste**.



6. Um eine neue VPN-Verbindung zu erstellen, klicken Sie auf die Schaltfläche **Hinzufügen**.

Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.

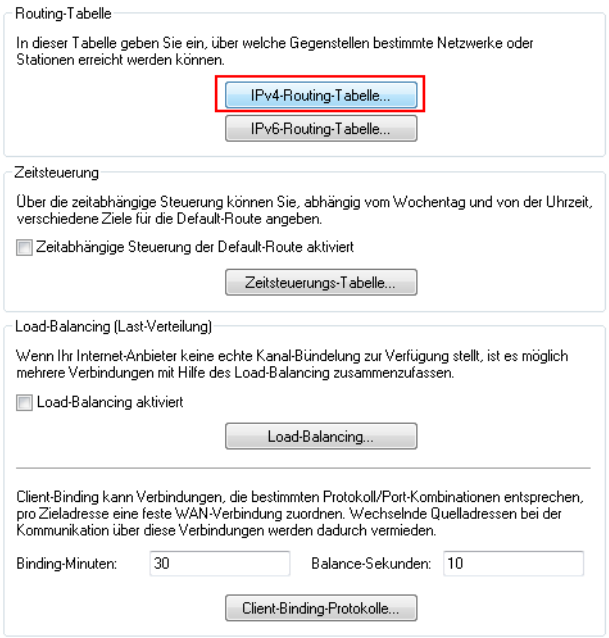


In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

Parameter	Beschreibung
Eintrag aktiv	Setzen Sie den Haken in der Checkbox, um die Verbindung zu aktivieren.
Name der Verbindung	Geben Sie die Bezeichnung für die VPN-Verbindung an. Dieser Eintrag wird später in der Routing-Tabelle genutzt.
Haltezeit	Geben Sie die Haltezeit in Sekunden für die VPN-Verbindung an. In diesem Beispiel wird bei dem 1781AW eine **0** eingetragen. Dies bedeutet, dass dieser Router die VPN-Verbindung nicht

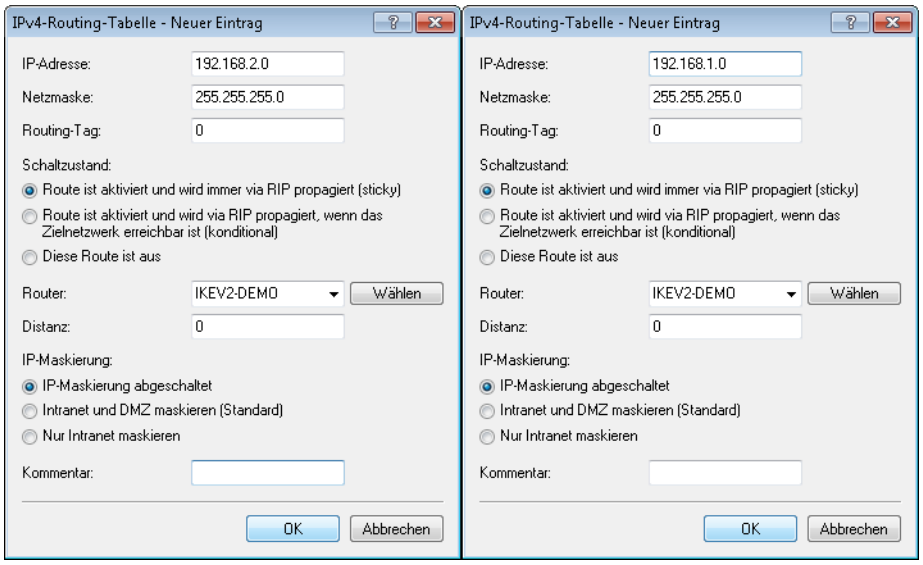
Parameter	Beschreibung
	aktiv aufbaut. Bei dem 1781VA-4G wird der Wert **9999** eingetragen. Dieser Wert besagt, dass der Router die Verbindung nicht aktiv trennt und nach einer Trennung versucht, diese direkt wieder aufzubauen.
Entferntes Gateway	Geben Sie die IP-Adresse an, unter der die Gegenseite erreichbar ist. In diesem Beispiel ist die IP-Adresse der WAN-Schnittstelle des 1781AW `1.1.1.1` und die des 1781VA-4G `1.1.1.2`.
Authentifizierung	Wählen Sie die Authentifizierung aus. Der Eintrag entspricht hierbei dem Namen der Authentifizierung, die Sie in **Schritt 3** festgelegt haben.

7. **Konfiguration der Routing-Tabelle**: Konfigurieren Sie die Routen, damit die Pakete vom Router durch den VPN-Tunnel an die VPN-Gegenstelle geschickt werden können. Hierzu öffnen Sie den Menüpunkt **IP-Router** > **Routing** und klicken auf die Schaltfläche **IPv4-Routing-Tabelle**.



8. Um eine weitere Route zu erzeugen, klicken Sie auf die Schaltfläche **Hinzufügen**. In dem Konfigurationsfenster werden die Informationen zu der zu konfigurierenden Route der einzelnen Router eingetragen.

Im folgenden Screenshot sind die Konfigurationen für beide Geräte zum direkten Vergleich nebeneinander aufgeführt. Hierbei wird nur auf die Konfigurationsparameter eingegangen, die von den Default-Werten abweichen.



In der linken Bildhälfte ist der LANCOM 1781AW abgebildet, rechts sehen Sie die Parameter des LANCOM 1781VA-4G.

Parameter	Beschreibung
IP-Adresse	Tragen Sie das IP-Netzwerk ein, welches durch den VPN-Tunnel erreicht werden soll. In diesem Beispiel soll das IP-Netzwerk `192.168.2.0` vom 1781AW und das IP-Netzwerk `192.168.1.0` vom 1781VA-4G erreicht werden.
Netzmaske	Geben Sie die Netzmaske des oben angegebenen IP-Netzwerkes an.
Schaltzustand	Wählen Sie den Schaltzustand **Route ist aktiviert und wird immer per RIP propagiert** aus. Dies aktiviert den Eintrag, so dass er benutzt werden kann.
Router	Als Router tragen Sie den Namen der VPN-Verbindung ein, den Sie in **Schritt 4** eingetragen haben.
IP-Maskierung	Wählen Sie **IP-Maskierung abgeschaltet** aus, damit der Router das andere Netzwerk nicht hinter seiner IP-Adresse maskiert.

9. Schreiben Sie die Konfiguration in beide Geräte zurück.
10. Überprüfen Sie die VPN-Verbindung einfach über LANmonitor. LANmonitor zeigt Ihnen den Status der VPN-Verbindung an.

7.1.5 Ergänzungen im Setup-Menü

IKEv2

In diesem Verzeichnis konfigurieren Sie die IKEv2-Parameter.

SNMP-ID:

2.19.36

Pfad Telnet:

Setup > **VPN**

Gegenstellen

In dieser Tabelle konfigurieren Sie die IKEv2-Verbindungen zu VPN-Partnern.

Der Kommandozeilen-Befehl `show vpn` zeigt an, ob die Verbindung erfolgreich ist.

SNMP-ID:

2.19.36.1

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Gegenstelle

Enthält den Namen der Verbindung zur Gegenstelle.

Dieser Name erscheint später in der Routing-Tabelle.

SNMP-ID:

2.19.36.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Aktiv

Gibt an, ob die VPN-Gegenstelle aktiv ist.

SNMP-ID:

2.19.36.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

Ja
Die VPN-Gegenstelle ist aktiv.

Nein
Die VPN-Gegenstelle ist nicht aktiv.

Default-Wert:

Ja

SH-Zeit

Gibt die Haltezeit in Sekunden an, die das Gerät eine Verbindung ohne Datenfluss aufrecht erhält.

SNMP-ID:

2.19.36.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

0

0 … 9999

Besondere Werte:

0
Das Gerät baut nicht aktiv eine Verbindung auf, sondern wartet auf ankommende Datenpakete.

9999
Keepalive: Das Gerät baut aktiv eine dauerhafte Verbindung auf.

Entferntes-Gateway

Enthält die Adresse (IPv4- oder IPv6-Adresse, FQDN) des VPN-Partners.

SNMP-ID:

2.19.36.1.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Rtg-Tag

Enthält das Routing-Tag für diese VPN-Verbindung.

SNMP-ID:

2.19.36.1.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

0

Verschluesselung

Bestimmt die Verschlüsselung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Setup** > **VPN** > **IKEv2** > **Verschluesselung**.

SNMP-ID:

2.19.36.1.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Authentifizierung

Bestimmt die Authentifizierung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

SNMP-ID:

2.19.36.1.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

Allgemeines

Bestimmt die allgemeinen Parameter der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Setup** > **VPN** > **IKEv2** > **Allgemeines**.

SNMP-ID:

2.19.36.1.8

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Lebensdauer

Bestimmt die Lebensdauer der Schlüssel einer VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Setup** > **VPN** > **IKEv2** > **Lebensdauer**.

SNMP-ID:

2.19.36.1.9

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IKE-CFG

Bestimmt den IKEv2-Config-Modus dieser Verbindung für RAS-Einwahlen.

SNMP-ID:

2.19.36.1.10

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

Aus
Die RAS-Dienste sind deaktiviert.

Client
Das Gerät arbeitet als RAS-Client und wählt sich bei einem Server ein.

Server
Das Gerät arbeitet als Server. RAS-Clients können sich bei ihm einwählen.

Default-Wert:

Aus

Regelerzeugung

Bestimmt, wie VPN-Regeln erstellt werden.

SNMP-ID:

2.19.36.1.11

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

Auto
Das Gerät erzeugt die VPN-Regeln automatisch.

Manuell
Das Gerät nutzt manuell erzeugte Regeln.

Default-Wert:

Auto

IPv4-Regeln

Gibt an, welche IPv4-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv4-Regeln stehen in der Tabelle **Setup** > **VPN** > **Netzwerkregeln** > **IPv4-Regellisten**.

SNMP-ID:

2.19.36.1.12

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

IPv6-Regeln

Gibt an, welche IPv6-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv6-Regeln stehen in der Tabelle **Setup** > **VPN** > **Netzwerkregeln** > **IPv6-Regellisten**.

SNMP-ID:

2.19.36.1.13

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

Kommentar

Geben Sie einen Kommentar zu diesem Eintrag an.

SNMP-ID:

2.19.36.1.17

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

IPv4-CFG-Pool

Bestimmen Sie mit diesem Eintrag einen IPv4-Adressen-Pool für die IKEv2-Gegenstelle.

SNMP-ID:

2.19.36.1.18

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

IPv6-CFG-Pool

Bestimmen Sie mit diesem Eintrag einen IPv6-Adressen-Pool für die IKEv2-Gegenstelle.

SNMP-ID:

2.19.36.1.19

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Verschluesselung

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Verschlüsselung.

SNMP-ID:

2.19.36.2

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Name

Enthält den Namen für diese Konfiguration.

SNMP-ID:

2.19.36.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

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

Default-Wert:

DEFAULT

DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen.

SNMP-ID:

2.19.36.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

DH16
DH15
DH14
DH5
DH2

Default-Wert:

DH14

PFS

Gibt an, ob Perfect Forward Secrecy (PFS) aktiviert ist.

SNMP-ID:

2.19.36.2.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

Ja
Nein

Default-Wert:

Ja

IKE-SA-Verschluesselungsliste

Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind.

SNMP-ID:

2.19.36.2.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES

Default-Wert:

AES-CBC-256

IKE-SA-Integ-Alg-Liste

Gibt an, welche Hash-Algorithmen aktiviert sind.

SNMP-ID:

2.19.36.2.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default-Wert:

SHA-256

SHA1

Child-SA-Verschluesselungsliste

Gibt an, welche Verschlüsselungsalgorithmen in der Child-SA aktiviert sind.

SNMP-ID:

2.19.36.2.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES

Default-Wert:

AES-CBC-256

Child-SA-Integ-Alg-Liste

Gibt an, welche Hash-Algorithmen in der Child-SA aktiviert sind.

SNMP-ID:

2.19.36.2.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschluesselung**

Mögliche Werte:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default-Wert:

SHA-256

SHA1

Auth

In diesem Menü konfigurieren Sie die Parameter für die IKEv2-Authentifizierung.

SNMP-ID:

2.19.36.3

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Parameter

In dieser Tabelle konfigurieren Sie die lokale und eine entsprechende entfernte Identität für die IKEv2-Authentifizierung.

SNMP-ID:

2.19.36.3.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.19.36.3.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Local-Auth

Legt die Authentifizierungsmethode für die lokale Identität fest.

SNMP-ID:

2.19.36.3.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*.

Default-Wert:

PSK

Local-ID-Typ

Zeigt den ID-Typ der lokalen Identität an. Entsprechend interpretiert das Gerät die Eingabe unter **Local-ID**.

SNMP-ID:

2.19.36.3.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

No-Identity
Die ID ist die lokale Gateway-Adresse.

Ist diese Option ausgewählt, hat der Eintrag unter **Local-ID** keine Auswirkung.

IPv4-Adresse
IPv6-Adresse
Domain-Name
Email-Adresse
Distinguished-Name
Key-ID

Default-Wert:

Email-Adresse

Local-ID

Enthält die lokale Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter **Local-ID-Typ**.

SNMP-ID:

2.19.36.3.1.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Local-Password

Enthält das Passwort der lokalen Identität.

SNMP-ID:

2.19.36.3.1.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Auth

Legt die Authentifizierungsmethode für die entfernte Identität fest.

SNMP-ID:

2.19.36.3.1.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*.

Default-Wert:

PSK

Remote-ID-Typ

Zeigt den ID-Typ der entfernten Identität an. Entsprechend interpretiert das Gerät die Eingabe unter **Remote-ID**.

SNMP-ID:

2.19.36.3.1.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

No-Identity

Das Gerät akzeptiert alle Verbindungen von entfernten IDs.

Ist diese Option ausgewählt, hat der Eintrag unter **Remote-ID** keine Auswirkung.

IPv4-Adresse
IPv6-Adresse
Domain-Name
Email-Adresse
Distinguished-Name
Key-ID

Default-Wert:

Email-Adresse

Remote-ID

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter **Remote-ID-Typ**.

SNMP-ID:

2.19.36.3.1.8

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Password

Enthält das Passwort der entfernten Identität.

SNMP-ID:

2.19.36.3.1.9

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Local-Zertifikat

Enthält das lokale VPN-Zertifikat, das das Gerät bei ausgehenden Verbindungen verwendet.

Die entsprechenden VPN-Zertifikate „VPN1" bis „VPN9" konfigurieren Sie unter **Setup** > **Zertifikate** > **SCEP-Client** > **Zertifikate**.

SNMP-ID:

2.19.36.3.1.11

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Cert-ID-Check

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

SNMP-ID:

2.19.36.3.1.12

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

Ja

Das Gerät prüft auf Existenz der entfernten Identität im Zertifikat.

Nein

Das Gerät prüft nicht auf Existenz der entfernten Identität im Zertifikat.

Default-Wert:

Ja

Local-Dig-Sig-Profile

Enthält den Profilnamen des verwendeten lokalen Digital-Signatur-Profils

SNMP-ID:

2.19.36.3.1.13

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Dig-Sig-Profile

Enthält den Profilnamen des entfernten Digital-Signatur-Profils

SNMP-ID:

2.19.36.3.1.14

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

OCSP-Check

Mit dieser Einstellung aktivieren Sie die Echtzeitüberprüfung eines X.509-Zertifikats via OCSP, welche den Gültigkeitsstatus des Zertifikats der Gegenstelle abfragt. Um die OCSP-Prüfung für einzelne VPN-Verbindungen zu verwenden, müssen Sie zunächst den globalen OCSP-Client für VPN-Verbindungen aktivieren und anschließend Profillisten gültiger Zertifizierungsstellen anlegen, bei denen das Gerät die Echtzeitprüfung durchführt.

SNMP-ID:

2.19.36.3.1.15

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Allgemeines

In dieser Tabelle konfigurieren Sie die allgemeinen IKEv2-Parameter.

SNMP-ID:

2.19.36.4

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.19.36.4.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

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

Default-Wert:

DEFAULT

DPD-Inakt-Timeout

Enthält die Zeit in Sekunden, nach der das Gerät die Verbindung beendet, wenn es in der Zwischenzeit den entfernten Peer nicht mehr erreicht.

SNMP-ID:

2.19.36.4.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

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

Default-Wert:

30

SSL-Encaps.

Gibt an, ob die Verbindung IKEv2 über HTTPS verwendet.

SNMP-ID:

2.19.36.4.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

IPCOMP

Gibt an, ob die Geräte die IKEv2-Datenpakete komprimiert übertragen.

SNMP-ID:

2.19.36.4.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Encaps-Mode

Bestimmt den Übertragungsmodus.

SNMP-ID:

2.19.36.4.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Allgemeines**

Mögliche Werte:

Tunnel

Default-Wert:

Tunnel

Lebensdauer

In dieser Tabelle konfigurieren Sie die Lebensdauer der IKEv2-Schlüssel.

SNMP-ID:

2.19.36.5

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.19.36.5.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Lebensdauer**

Mögliche Werte:

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

Default-Wert:

DEFAULT

IKE-SA-Sec

Enthält die Zeit in Sekunden bis zur Erneuerung des IKE-SA-Schlüssels.

SNMP-ID:

2.19.36.5.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Lebensdauer**

Mögliche Werte:

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

Default-Wert:

108000

Besondere Werte:

0

Keine Erneuerung des Schlüssels.

IKE-SA-KB

Enthält die übertragene Datenmenge in Kilobyte bis zur Erneuerung des IKE-SA-Schlüssels.

SNMP-ID:

2.19.36.5.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Lebensdauer**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Keine Erneuerung des Schlüssels.

Child-SA-Sec

Enthält die Zeit in Sekunden bis zur Erneuerung des CHILD-SA-Schlüssels.

SNMP-ID:

2.19.36.5.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Lebensdauer**

Mögliche Werte:

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

Default-Wert:

28800

Besondere Werte:

0

Keine Erneuerung des Schlüssels.

Child-SA-KB

Enthält die übertragene Datenmenge in Kilobyte bis zur Erneuerung des CHILD-SA-Schlüssels.

SNMP-ID:

2.19.36.5.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Lebensdauer**

Mögliche Werte:

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

Default-Wert:

2000000

Besondere Werte:

0

Keine Erneuerung des Schlüssels.

IKE-CFG

Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der IKE-CFG-Modus „Server" angegeben.

In diesem Menü konfigurieren Sie die Adresspools, die das Gerät im CFG-Modus „Server" den Clients übergibt.

SNMP-ID:

2.19.36.7

Pfad Telnet:

Setup > **VPN** > **IKEv2**

IPv4

In dieser Tabelle konfigurieren Sie die IPv4-Adressen des Adressen-Pools für den IKEv2-CFG-Mode „Server".

SNMP-ID:

2.19.36.7.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Name

Enthält den Namen des IPv4-Adressen-Pools.

SNMP-ID:

2.19.36.7.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Mögliche Werte:

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

Start-Adresspool

Geben Sie hier die erste IPv4-Adresse des Adressbereiches ein, den Sie den Einwahl-Clients zur Verfügung stellen wollen.

SNMP-ID:

2.19.36.7.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

Ende-Adresspool

Geben Sie hier die letzte IPv4-Adresse des Adressbereiches ein, den Sie den Einwahl-Clients zur Verfügung stellen wollen.

SNMP-ID:

2.19.36.7.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

Erster-DNS

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen.

SNMP-ID:

2.19.36.7.1.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Mögliche Werte:

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

Default-Wert:

0.0.0.0

Zweiter-DNS

Geben Sie hier die Adresse eines alternativen Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen, falls die Verbindung zum ersten Nameserver gestört ist.

SNMP-ID:

2.19.36.7.1.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Mögliche Werte:

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

Default-Wert:

leer

IPv6

In dieser Tabelle konfigurieren Sie die IPv6-Adressen des Addressen-Pools für den IKEv2-CFG-Mode „Server".

SNMP-ID:

2.19.36.7.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Name

Enthält den Namen des IPv6-Adressen-Pools.

SNMP-ID:

2.19.36.7.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

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

Start-Adresspool

Geben Sie hier die erste IPv6-Adresse des Adressbereiches ein, den Sie den Einwahl-Clients zur Verfügung stellen wollen.

SNMP-ID:

2.19.36.7.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Ende-Adresspool

Geben Sie hier die letzte IPv6-Adresse des Adressbereiches ein, den Sie den Einwahl-Clients zur Verfügung stellen wollen.

SNMP-ID:

2.19.36.7.2.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Erster-DNS

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen.

SNMP-ID:

2.19.36.7.2.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

Zweiter-DNS

Geben Sie hier die Adresse eines alternativen Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen, falls die Verbindung zum ersten Nameserver gestört ist.

SNMP-ID:

2.19.36.7.2.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Mögliche Werte:

max. 39 Zeichen aus `[A-F][a-f][0-9]:.`

7.2 Unterstützung IKEv2-Fragmentierung

Ab LCOS-Version 9.20 unterstützt LCOS IKEv2-Fragementierung.

7.2.1 IKEv2-Fragmentierung

Die Fragmentierung von Datenpaketen richtet sich nach der Maximum Transmission Unit (MTU). Die MTU bezeichnet die maximale Größe, die ein Paket haben darf, um als Payload über einen Kanal versendet werden zu können. Diese wird zu Beginn einer Übertragung von beiden Kommunikationspartnern ausgehandelt, um die optimale Datenübertragung ohne eine zusätzliche Fragmentierung von Datenpaketen gewährleisten zu können.

In LCOS ist die IKEv2-Fragmentierung automatisch aktiviert. Sie können davon abweichend manuell eine maximale MTU definieren.

Wechseln Sie dazu in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec**.

Geben Sie im Abschnitt **Fragmentierung** im Feld **MTU** die maximale IP-Paketlänge/-größe in Byte an. Je kleiner Sie den Wert wählen, je stärker ist die Fragmentierung der Nutzdaten.

7.2.2 Ergänzungen im Setup-Menü

MTU

Dieser Eintrag enthält die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) für IKEv2.

SNMP-ID:

2.19.36.8

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Mögliche Werte:

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

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Die Vorgabe einer MTU ist deaktiviert. Die beiden IKEv2-Endpunkte handeln die MTU untereinander aus.

7.3 RADIUS-Unterstützung für IKEv2

Ab LCOS-Version 9.20 unterstützt RADIUS das Protokoll IKEv2 für Autorisierung und Accounting.

7.3.1 RADIUS-Unterstützung für IKEv2

LCOS ermöglicht es, die IKEv2-Konfiguration für Autorisierung und Accounting von VPN-Peers durch einen externen RADIUS-Server durchführen zu lassen.

In mittleren bis großen VPN-Szenarien sind die Tabellen für VPN-Konfigurationen in der Regel sehr umfangreich und komplex. Wenn mehrere VPN-Gateways aus Redundanzgründen zum Einsatz kommen, muss sichergestellt werden, dass die Konfiguration auf allen VPN-Gateways identisch ist.

Der Einsatz eines zentralen RADIUS-Servers ermöglicht die fast vollständige Auslagerung der Konfiguration der VPN-Parameter vom VPN-Gateway auf einen oder mehrere RADIUS-Server. Sobald eine VPN-Gegenstelle eine VPN-Verbindung zum Gerät aufbauen will, versucht das Gerät, die ankommende Verbindung per RADIUS zu authentifizieren und weitere notwendige Verbindungsparameter wie z. B. VPN-Netzbeziehungen, CFG-Mode-Adresse oder DNS-Server vom RADIUS-Server abzurufen.

Dabei kann die VPN-Konfiguration entweder vollständig oder nur teilweise vom RADIUS-Server abgerufen mit lokal vorhandenen Parametern kombiniert werden. Dieser Mechanismus funktioniert nur für ankommende Verbindungen.

Durch das optionale RADIUS-Accounting können Informationen über VPN-Verbindungen zentral auf einem RADIUS-Server gesammelt werden. Diese Informationen können z. B. aus Verbindungsdauer des Clients, Aufbauzeitpunkt oder das übertragene Datenvolumen bestehen.

Die Konfiguration der RADIUS-Server erfolgt in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen**.

RADIUS-Autorisierung

Das LANCOM-Gateway überträgt bei der Anmeldung eines VPN-Peers die folgenden RADIUS-Attribute im `Access-Request` an den RADIUS-Server:

ID	Bezeichnung	Bedeutung
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der AUTH-Verhandlung mit dem LANCOM-Gateway überträgt.
2	User-Passwort	Das Dummy-Passwort, wie es in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Passwort** konfiguriert ist.
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „95“ (siehe unten).
6	Servcie-Type	Der Service-Type ist immer „Outbound (5)“ bzw. „Dialout-Framed-User“.
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).

ID	Bezeichnung	Bedeutung
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv4-Verbindung, überträgt das Gateway stattdessen das Attribut „4“ (siehe oben).

Von den in der `Access-Accept`-Antwort des RADIUS-Servers enthaltenen Attributen wertet das LANCOM-Gateway daraufhin die folgenden, teils vendor-spezifischen Attribute aus:

ID	Bezeichnung	Bedeutung
8	Framed-IP-Address	IPv4-Adresse für den Client (im IKE-CFG-Mode „Server“).
22	Framed-Route	IPv4-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen.
39	Tunnel-Password	Setzt bei Verwendung von synchronen PSKs die Passwörter der lokalen und der entfernten Identität auf den selben Wert.
88	Framed-Pool	Name des IPv4-Adressen-Pools, aus dem der Client die IP-Adresse und den DNS-Server bezieht. Die Werte in „Framed-IP-Address“ und „LCS-DNS-Server-IPv4-Address“ haben gegenüber diesem Attribut Vorrang.
99	Framed-IPv6-Route	IPv6-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen.
168	Framed-IPv6-Address	IPv6-Adresse für den Client (im IKE-CFG-Mode „Server“).
169	DNS-Server-IPv6-Address	IPv6-DNS-Server für den Client (im IKE-CFG-Mode „Server“).
172	Stateful-IPv6-Address-Pool	Name des IPv6-Adressen-Pools (im IKE-CFG-Mode „Server“).
Lancom 19	LCS-IKEv2-Local-Password	Lokaler IKEv2-PSK
Lancom 20	LCS-IKEv2-Remote-Password	Entfernter IKEv2-PSK
Lancom 21	LCS-DNS-Server-IPv4-Address	IPv4-DNS-Server für den Client (im IKE-CFG-Mode „Server“)
Lancom 22	LCS-VPN-IPv4-Rule	Beinhaltet die IPv4-Netzwerkregeln (Beispiele: siehe unten)
Lancom 23	LCS-VPN-IPv6-Rule	Beinhaltet die IPv6-Netzwerkregeln (Beispiele: siehe unten)
Lancom 24	LCS-Routing-Tag	Routing-Tag, das für den Client konfiguriert werden soll (IPv4/IPv6).
Lancom 25	LCS-IKEv2-IPv4-Route	Routen in Präfix-Schreibweise (z. B. „192.168.1.0/24“), die das LANCOM-Gateway per `INTERNAL_IP4_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.
Lancom 26	LCS-IKEv2-IPv6-Route	Routen in Präfix-Schreibweise (z. B. „2001:db8::/64“), die das LANCOM-Gateway per `INTERNAL_IP6_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.

Beipiele für Netzwerkregeln

Das Format für eine Netzwerkregel im Radius-Server gestaltet sich in der Form `<lokale Netze> * <entfernte Netze>`.

Die Einträge für `<Lokale Netze>` und `<entfernte Netze>` setzen sich dabei aus komma-separierten Listen zusammen.

Beispiel 1: `10.1.1.0/24,10.2.0.0/16 * 172.32.0.0/12`

Daraus ergeben sich die folgenden Netzwerkregeln:

- `10.2.0.0/255.255.0.0` <-> `172.16.200.0/255.255.255.255`
- `10.1.1.0/255.255.255.0` <-> `172.16.200.0/255.255.255.255`

Beispiel 2: `10.1.1.0/24 * 0.0.0.0/0`

Daraus ergibt sich die folgende Netzwerkregel:

- `10.1.1.0/255.255.255.0` <-> `0.0.0.0/0.0.0.0`

Dabei bedeutet `0.0.0.0/0` „ANY“, d. h. ein beliebiges Netz. `0.0.0.0/32` kann dazu verwendet werden, einen CFG-Mode-Client genau auf seine (noch unbekannte) Config-Mode-Adresse einzuschränken. Diese Adresse kommt z. B. aus einem Adress-Pool auf dem Gerät oder ebenfalls aus dem RADIUS-Server.

Beispiel 3: `2001:db8:1::/48 * 2001:db8:6::/48`

RADIUS-Accounting

Das LANCOM-Gateway zählt die übertragenen Datenpakete und -Oktette und sendet diese Daten regelmäßig als `Accounting-Request`-Nachrichtenan an den Accounting-RADIUS-Server. Der RADIUS-Server beantwortet diese Meldung daraufhin jeweils mit einer `Accounting-Response`-Nachricht.

Die `Accounting-Request`-Nachrichten besitzen die folgenden Status-Typen:

Start

Sobald sich ein VPN-Peer am LANCOM-Gateway anmeldet, startet das Gateway über IKEv2 eine Accounting-Session und sendet eine `Start`-Statusmeldung mit entsprechenden RADIUS-Attributen an den Accounting-RADIUS-Server.

Interim-Update

Während einer laufenden Accounting-Session sendet das Gateway in definierten Zeitabständen `Interim-Update`-Statusmeldungen an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

Stop

Nach dem Ende einer Sitzung sendet das LANCOM-Gateway eine `Stop`-Statusmeldung an den Accounting-RADIUS-Server. Auch diese Meldung sendet es nur an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

In der `Access-Request`-Meldung überträgt das Gateway die folgenden RADIUS-Attribute an den RADIUS-Server:

ID	Bezeichnung	Bedeutung	Status-Typ
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der AUTH-Verhandlung mit dem LANCOM-Gateway überträgt.	■ Start ■ Interim-Update ■ Stop
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „95“ (siehe unten).	■ Start ■ Interim-Update ■ Stop
8	Framed-IP-Address	IPv4-Adresse des VPN-Clients.	■ Start ■ Interim-Update

ID	Bezeichnung	Bedeutung	Status-Typ
			■ Stop
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).	■ Start ■ Interim-Update ■ Stop
32	NAS-Identifier	Der Gerätename des Gateways.	■ Start ■ Interim-Update ■ Stop
40	Acct-Status-Type	Beinhaltet den Status-Typ „Start“ (1).	■ Start
40	Acct-Status-Type	Beinhaltet den Status-Typ „Interim-Update“ (3).	■ Interim-Update
40	Acct-Status-Type	Beinhaltet den Status-Typ „Stop“ (2).	■ Stop
42	Acct-Input-Octets	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	■ Interim-Update ■ Stop
43	Acct-Output-Octets	Enthält die Anzahl der zum VPN-Peer gesendeten Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	■ Interim-Update ■ Stop
44	Acct-Session-Id	Der Name des VPN-Peers und der Zeitstempel zum Session-Start bilden die eindeutige Session-ID.	■ Start ■ Interim-Update ■ Stop
46	Acct-Session-Time	Enthält die verstrichene Zeit in Sekunden seit Beginn der Session.	■ Interim-Update ■ Stop
47	Acct-Input-Packets	Enthält die Anzahl der aktuell aus Richtung VPN-Peer empfangenen Datenpakete.	■ Interim-Update ■ Stop
48	Acct-Output-Packets	Enthält die Anzahl der aktuell zum VPN-Peer gesendeten Datenpakete.	■ Interim-Update ■ Stop
49	Acct-Terminate-Cause	Enthält die Ursache für die Beendigung der Session.	■ Stop
52	Acct-Input-Gigawords	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	■ Interim-Update ■ Stop
53	Acct-Input-Gigawords	Enthält die Anzahl der zum VPN-Peer gesendeten Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	■ Interim-Update ■ Stop
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut „4“ (siehe oben).	■ Start ■ Interim-Update ■ Stop
168	Framed-IPv6-Address	IPv6-Adresse des VPN-Clients.	■ Start ■ Interim-Update ■ Stop

RADIUS-Authentifizierung

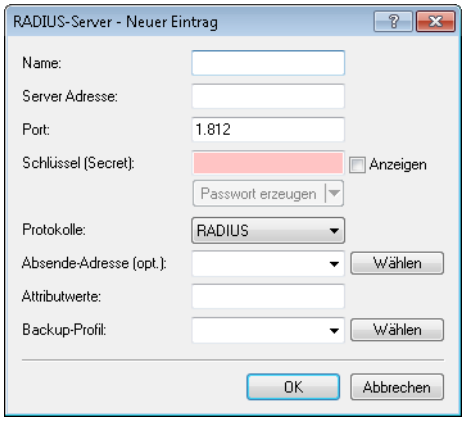
Im Abschnitt **RADIUS-Authentifizierung** konfigurieren Sie die Einstellungen der RADIUS-Server zur Autorisierung von VPN-Clients.

Bestimmen Sie im Feld **Passwort** das Passwort, das der RADIUS-Server im Access-Request-Attribut als Benutzer-Passwort erhält.

Der RADIUS-Server ordnet dieses Passwort normalerweise direkt einem VPN-Peer zu, um diesen für den Netzwerkzugang zu autorisieren. Bei IKEv2 autorisiert jedoch nicht der RADIUS-Server den anfragenden VPN-Peer, sondern das LANCOM-Gateway, nachdem es die entsprechende Autorisierung in der `Access-Accept`-Nachricht des RADIUS-Servers erhalten hat.

Entsprechend geben Sie an dieser Stelle ein Dummy-Passwort ein.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert „1812" ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form
`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Auth.-Server**.

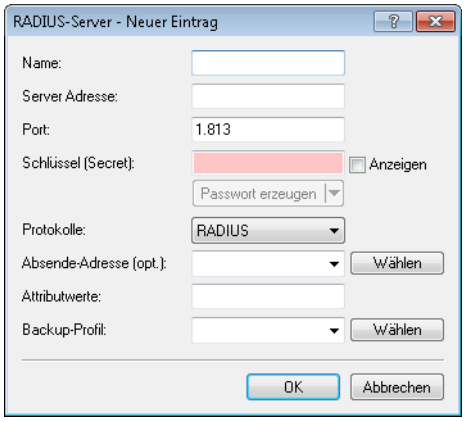
RADIUS-Accounting

Im Abschnitt **RADIUS-Accounting** konfigurieren Sie die Einstellungen der RADIUS-Server zum Accounting von VPN-Clients.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.

Bestimmen Sie im Feld **Update-Zyklus** die Zeit in Sekunden zwischen zwei aufeinanderfolgenden Interim-Update-Nachrichten. Das Gerät fügt zufällig eine Toleranz von ±10% ein, um die Update-Nachrichten paralleler Accounting Sessions zeitlich voneinander abzutrennen.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert „1813“ ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form
`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Acc.-Server**.

7.3.2 Ergänzungen im Setup-Menü

RADIUS-Autorisierung

Hier bestimmen Sie den RADIUS-Server für die Autorisierung.

Wählen Sie einen Eintrag aus der Tabelle unter **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**.

Wenn Sie keinen RADIUS-Server zur Autorisierung angeben, verwendet das Gerät die lokale IKEv2-Konfiguration.

SNMP-ID:

2.19.36.1.15

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

RADIUS-Accounting

Mit diesem Eintrag bestimmen Sie den RADIUS-Server für das Accounting.

Wählen Sie einen Eintrag aus der Tabelle unter **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

Wenn Sie keinen RADIUS-Server angeben, erfolgt kein Accounting für diesen VPN-Peer.

SNMP-ID:

2.19.36.1.16

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

RADIUS

Dieses Menü enthält die RADIUS-Konfiguration für IKEv2.

SNMP-ID:

2.19.36.9

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Autorisierung

Dieses Menu enthält die Konfiguration für die RADIUS-Autorisierung über IKEv2.

SNMP-ID:

2.19.36.9.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS**

Server

Diese Tabelle enthält die Server-Konfiguration für die RADIUS-Autorisierung unter IKEv2.

SNMP-ID:

2.19.36.9.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung**

Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

SNMP-ID:

2.19.36.9.1.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Server-Hostname

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

SNMP-ID:

2.19.36.9.1.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Port

Geben Sie den UDP-Port des RADIUS-Servers an.

SNMP-ID:

2.19.36.9.1.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

1812

Schluessel

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

SNMP-ID:

2.19.36.9.1.1.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Protokoll

Wählen Sie zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

SNMP-ID:

2.19.36.9.1.1.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Loopback-Adresse

Dieser Eintrag enthält die Loopback-Addresse des am RADIUS-Server anfragenden LANCOM-Gateways.

SNMP-ID:

2.19.36.9.1.1.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Attribut-Werte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

SNMP-ID:

2.19.36.9.1.1.8

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Backup

Geben Sie als Backup-Server den Namen eines alternativen RADIUS-Servers aus der Liste der bisher konfigurierten RADIUS-Server an.

SNMP-ID:

2.19.36.9.1.1.9

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Passwort

Bestimmen Sie hier das Passwort, das der RADIUS-Server im Access-Request-Attribut als Benutzer-Passwort erhält.

Der RADIUS-Server ordnet dieses Passwort normalerweise direkt einem VPN-Peer zu, um diesen für den Netzwerkzugang zu autorisieren. Bei IKEv2 autorisiert jedoch nicht der RADIUS-Server den anfragenden VPN-Peer, sondern das LANCOM-Gateway, nachdem es die entsprechende Autorisierung in der `Access-Accept`-Nachricht des RADIUS-Servers erhalten hat.

Entsprechend geben Sie an dieser Stelle ein Dummy-Passwort ein.

SNMP-ID:

2.19.36.9.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung**

Mögliche Werte:

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

Default-Wert:

leer

Accounting

Dieses Menu enthält die Konfiguration für das RADIUS-Accounting über IKEv2.

SNMP-ID:

2.19.36.9.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS**

Server

Diese Tabelle enthält die Server-Konfiguration für das RADIUS-Accounting unter IKEv2.

SNMP-ID:

2.19.36.9.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

SNMP-ID:

2.19.36.9.2.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Server-Hostname

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

SNMP-ID:

2.19.36.9.2.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Port

Geben Sie den UDP-Port des RADIUS-Servers an.

SNMP-ID:

2.19.36.9.2.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

1813

Schluessel

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des LANCOM-Gateways am RADIUS-Server.

Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

SNMP-ID:

2.19.36.9.2.1.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Protokoll

Wählen Sie zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

SNMP-ID:

2.19.36.9.2.1.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Loopback-Addresse

Dieser Eintrag enthält die Loopback-Addresse des am RADIUS-Server anfragenden LANCOM-Gateways.

SNMP-ID:

2.19.36.9.2.1.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Attribut-Werte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

SNMP-ID:

2.19.36.9.2.1.7

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Backup

Geben Sie als Backup-Server den Namen eines alternativen RADIUS-Servers aus der Liste der bisher konfigurierten RADIUS-Server an.

SNMP-ID:

2.19.36.9.2.1.8

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Mögliche Werte:

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

Default-Wert:

leer

Interim-Interval

Bestimmen Sie die Zeit in Sekunden zwischen zwei aufeinanderfolgenden Interim-Update-Nachrichten. Das Gerät fügt zufällig eine Toleranz von ±10% ein, um die Update-Nachrichten paralleler Accounting Sessions zeitlich voneinander abzutrennen.

SNMP-ID:

2.19.36.9.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

Mögliche Werte:

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

0 … 4294967295

Default-Wert:

0

Besondere Werte:

0

Der Versand von Interim-Update-Nachrichten ist deaktiviert.

Routen-fuer-RAS-SAs-erzeugen

Definiert, ob automatisch Routen aus VPN-Regeln für Einwahlclients in der Betriebsart CFG-Mode Server erzeugt werden sollen. Eine Deaktivierung der automatischen Routenerzeugung ist dann sinnvoll, wenn die Routen durch ein Routingprotokoll erzeugt werden sollen.

SNMP-ID:

2.19.36.10

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Mögliche Werte:

nein

Es werden keine Routen für RAS-SAs erzeugt.

ja

Es werden Routen für RAS-SAs erzeugt.

Default-Wert:

ja

Erweiterte-Parameter

Diese Tabelle enthält erweiterte Parameter zu IKEv2-Gegenstellen.

SNMP-ID:

2.19.36.11

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Name

Name der Gegenstelle.

SNMP-ID:

2.19.36.11.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Erweiterte Parameter**

Mögliche Werte:

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

Default-Wert:

leer

PRF-als-Sig-Hash

Definiert, ob die PRF (pseudo-random function) aus der IKEv2-Verhandlung als Signatur-Hash bei RSA-Signature verwendet werden soll. Diese Funktion sollte nur zur Kompatibilität mit Fremdprodukten verwendet werden. Die Einstellung muss auf beiden Seiten der VPN-Gegenstellen gleich konfiguriert werden.

SNMP-ID:

2.19.36.11.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Erweiterte Parameter**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

7.3.3 Ergänzungen im Status-Menü

RADIUS

Dieses Menu enthält Statuswerte für alle aktuellen VPN-Peers, deren Verwaltung über einen RADIUS-Server erfolgt (Autorisierung und Accounting).

SNMP-ID:

1.26.39

Pfad Telnet:

Status > **VPN**

Autorisierung

Dieses Verzeichnis enthält die Statuswerte für alle aktuellen VPN-Peers, die ein RADIUS-Server autorisiert hat.

Ein neuer VPN-Peer erscheint in dieser Tabelle, sobald der erste Access-Request an einen RADIUS-Server erfolgt. Der Eintrag für einen VPN-Peer wird aus der Tabelle entfernt, sobald dessen IKE SA (Phase 1) gelöscht ist.

SNMP-ID:

1.26.39.1

Pfad Telnet:

Status > **VPN** > **RADIUS**

Gegenstelle

Dieser Eintrag zeigt die Bezeichnung der Gegenstelle.

SNMP-ID:

1.26.39.1.1

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Remote-ID

Dieser Eintrag zeigt die Remote-ID des VPN-Peers, wie sie das Gerät an den RADIUS-Server weitergeleitet hat.

SNMP-ID:

1.26.39.1.2

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Lokales-Gateway

Dieser Eintrag enthält die IPv4- oder IPv6-Adresse des LANCOM-Gateways, an das der VPN-Peer seine VPN-Anfrage gesendet hat. Das LANCOM-Gateway überträgt diese Adresse als RADIUS-Attribut „NAS-IP-Address“ oder „NAS-IPv6-Address“ innerhalb des Access-Requests an den RADIUS-Server.

SNMP-ID:

1.26.39.1.3

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Entferntes-Gateway

Dieser Eintrag enthält die IPv4- oder IPv6-Adresse, von der der VPN-Peer seine VPN-Anfrage an das LANCOM-Gateway gesendet hat. Das LANCOM-Gateway überträgt diese Adresse als RADIUS-Attribut „Calling-Station-Id“ innerhalb des Access-Requests an den RADIUS-Server.

SNMP-ID:

1.26.39.1.4

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Zustand

Zeigt den Zustand des VPN-Peers an. Die folgenden Zustände sind möglich:

Running

Die „Access-Request"-Anfrage an den RADIUS-Server ist erfolgt, aber noch nicht beantwortet.

Succeeded

Die „Access-Accept"-Nachricht des RADIUS-Servers ist erfolgt.

Failed

Die „Access-Request"-Anfrage an den RADIUS-Server oder den konfigurierten Backup-RADIUS-Server war nicht erfolgreich.

SNMP-ID:

1.26.39.1.5

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Server-Hostname

Zeigt den Hostnamen des angefragten RADIUS-Servers an, sobald dieser eine Anfrage beantwortet hat. Der Eintrag entspricht der Konfiguration unter **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Autorisierung** > **Server**.

SNMP-ID:

1.26.39.1.6

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv4-Adresse

Zeigt den vom RADIUS-Server im RADIUS-Attribut „Framed-IP-Address" zurückgemeldeten Wert an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.7

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv4-DNS-Server

Zeigt eine komma-separierte Liste von IPv4-DNS-Servern an, die der RADIUS-Server im vendor-spezifischen RADIUS-Attribut „LCS-DNS-Server-IPv4-Address" zurückmeldet. Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.8

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv4-Pool

Zeigt den vom RADIUS-Server zurückgemeldeten Framed-IPv4-Adressenpool an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.9

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv6-Adresse

Zeigt den vom RADIUS-Server im RADIUS-Attribut „Framed-IPv6-Address" zurückgemeldeten Wert an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.10

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv6-DNS-Server

Zeigt eine komma-separierte Liste von IPv6-DNS-Servern an, die der RADIUS-Server im vendor-spezifischen RADIUS-Attribut „LCS-DNS-Server-IPv6-Address" zurückmeldet. Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.11

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

CFG-IPv6-Pool

Zeigt den vom RADIUS-Server zurückgemeldeten Framed-IPv6-Adressenpool an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.12

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Rtg-Tag

Dieser Eintrag enthält das vom RADIUS-Server in der „Access-Accept"-Nachricht zurückgemeldete IPv4- oder IPv6-Routing-Tag (vendor-spezifisches RADIUS-Attribut „LCS-Routing-Tag").

SNMP-ID:

1.26.39.1.13

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Framed-IPv4-Routen

Dieser Eintrag enthält eine komma-separierte Liste von IPv4-Präfixen, die der RADIUS-Server in der „Access-Accept"-Nachricht im RADIUS-Attribut „Framed-Route" zurückgemeldet hat.

Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.14

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Framed-IPv6-Routen

Dieser Eintrag enthält eine komma-separierte Liste von IPv6-Präfixen, die der RADIUS-Server in der „Access-Accept"-Nachricht im RADIUS-Attribut „Framed-IPv6-Route" zurückgemeldet hat.

Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.15

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

IKE-IPv4-Routen

Dieser Eintrag enthält eine komma-separierte Liste von IPv4-Präfixen, die der RADIUS-Server in der „Access-Accept"-Nachricht im vendor-spezifischen RADIUS-Attribut „LCS-IKEv2-IPv4-Route" zurückgemeldet hat.

Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.16

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

IKE-IPv6-Routen

Dieser Eintrag enthält eine komma-separierte Liste von IPv6-Präfixen, die der RADIUS-Server in der „Access-Accept"-Nachricht im vendor-spezifischen RADIUS-Attribut „LCS-IKEv2-IPv6-Route" zurückgemeldet hat.

Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.1.17

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Weitere-Attribute

Dieser Eintrag enthält eine komma- bzw. leerzeichen-separierte Liste von weiteren Attributen, die der RADIUS-Server in der „Access-Accept"-Nachricht übertragen hat.

Befindet sich der VPN-Peer in den Zuständen „Running" oder „Failed", oder hat der RADIUS-Server keinen entsprechenden Wert in der „Access-Accept"-Nachricht zurückgemeldet, bleibt dieser Eintrag leer.

Mögliche Werte sind:

Lokales-Passwort

Inhalt der Attribute „LCS-IKEv2-Local-Password“ oder „Tunnel-Password“.

Entferntes-Passwort

Inhalt der Attribute „LCS-IKEv2-Remote-Password“ oder „Tunnel-Password“.

IPv4-Netzregel

Inhalt des Attributs „LCS-VPN-IPv4-Rule“.

IPv6-Netzregel

Inhalt des Attributs „LCS-VPN-IPv6-Rule“.

SNMP-ID:

1.26.39.1.18

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Autorisierung**

Accounting

Dieses Verzeichnis enthält die Statuswerte für alle aktuellen VPN-Peers, für die ein RADIUS-Server das Accounting übernimmt.

SNMP-ID:

1.26.39.2

Pfad Telnet:

Status > **VPN** > **RADIUS**

Gegenstelle

Dieser Eintrag zeigt die Bezeichnung der Gegenstelle.

SNMP-ID:

1.26.39.2.1

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Session-ID

Der Name des VPN-Peers und der Zeitstempel zum Session-Start bilden die eindeutige Session-ID.

SNMP-ID:

1.26.39.2.2

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Remote-ID

Dieser Eintrag zeigt die Remote-ID des VPN-Peers, wie sie das Gerät an den RADIUS-Server weitergeleitet hat.

SNMP-ID:

1.26.39.2.3

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Lokales-Gateway

Dieser Eintrag enthält die IPv4- oder IPv6-Adresse des LANCOM-Gateways, an das der VPN-Peer seine VPN-Anfrage gesendet hat. Das LANCOM-Gateway überträgt diese Adresse als RADIUS-Attribut „NAS-IP-Address" oder „NAS-IPv6-Address" innerhalb des Access-Requests an den RADIUS-Server.

SNMP-ID:

1.26.39.2.4

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Entferntes-Gateway

Dieser Eintrag enthält die IPv4- oder IPv6-Adresse, von der der VPN-Peer seine VPN-Anfrage an das LANCOM-Gateway gesendet hat. Das LANCOM-Gateway überträgt diese Adresse als RADIUS-Attribut „Calling-Station-Id" innerhalb des Access-Requests an den RADIUS-Server.

SNMP-ID:

1.26.39.2.5

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

CFG-IPv4-Adresse

Zeigt den vom RADIUS-Server im RADIUS-Attribut „Framed-IP-Address" zurückgemeldeten Wert an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.2.6

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

CFG-IPv6-Adresse

Zeigt den vom RADIUS-Server im RADIUS-Attribut „Framed-IPv6-Address“ zurückgemeldeten Wert an. Falls der RADIUS-Server keinen Wert zurückgemeldet hat, bleibt dieser Eintrag leer.

SNMP-ID:

1.26.39.2.7

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Zustand

Zeigt den Zustand des VPN-Peers an. Die folgenden Zustände sind möglich:

Starting

Eine „Accounting-Response“-Nachricht vom RADIUS-Server ist noch nicht erfolgt.

Start-Failed

IKE hat keine gültige „Start“-Nachricht übertragen, oder der VPN-Peer hat keine gültige „Accounting-Response“-Nachricht vom RADIUS-Server erhalten.

Running

Der VPN-Peer hat eine gültige „Accounting-Response“-Nachricht erhalten, und das letzte Interim-Update war erfolgreich.

Update-Failed

Das letzte Interim-Update war nicht erfolgreich.

SNMP-ID:

1.26.39.2.8

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Server-Hostname

Zeigt den Hostnamen des angefragten RADIUS-Servers an, sobald dieser eine Anfrage beantwortet hat. Der Eintrag entspricht der Konfiguration unter **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

SNMP-ID:

1.26.39.2.9

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Sitzungsdauer

Zeigt die verstrichene Zeit in Sekunden seit Beginn der Session an.

SNMP-ID:

1.26.39.2.10

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Eingehende-Oktette

Zeigt die Anzahl der aus Richtung VPN-Peer empfangenen Oktette an. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.

SNMP-ID:

1.26.39.2.11

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Ausgehende-Oktette

Zeigt die Anzahl der zum VPN-Peer gesendeten Oktette an. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.

SNMP-ID:

1.26.39.2.12

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Eingehende-Pakete

Zeigt die Anzahl der aktuell aus Richtung VPN-Peer empfangenen Datenpakete an.

SNMP-ID:

1.26.39.2.13

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

Ausgehende-Pakete

Zeigt die Anzahl der aktuell zum VPN-Peer gesendeten Datenpakete an.

SNMP-ID:

1.26.39.2.14

Pfad Telnet:

Status > **VPN** > **RADIUS** > **Accounting**

7.4 Unterstützung von IKEv2-Routing

LCOS unterstützt ab Version 9.20 beim IKEv2-Config-Exchange die Funktionen

- CFG_Request
- CFG_Reply
- CFG_Set
- CFG_Ack

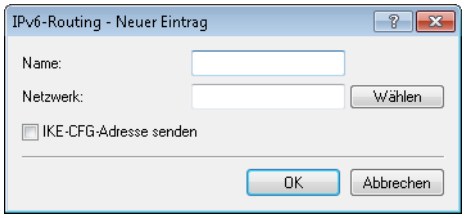
Die Konfiguration der Präfixe für das dynamische Routing über IKEv2 erfolgt in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** im Abschnitt **IKEv2-Routing**.

7.4.1 IPv4-Routing

IKEv2-Routing ermöglicht es, innerhalb eines IKEv2-Tunnels lokale Netze zu propagieren bzw. entfernte Netze zu lernen.

7.4.2 IPv6-Routing

In dieser Tabelle konfigurieren Sie die IPv6-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IPv6-Adresse
- IPv6-Adresse/Präfixlänge

- IPv6-Schnittstellen-Name

Die Konfiguration der IP-Subnetze erfolgt unter **IPv6** > **Allgemein** im Abschnitt **IPv6-Netzwerke**.

IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

7.4.3 Ergänzungen im Setup-Menü

Routing

Gibt die Route der VPN-Verbindung an.

Die Routen für IPv4- und IPv6-Verbindungen stehen im Menü **Setup** > **VPN** > **IKEv2** > **Routing**.

SNMP-ID:

2.19.36.1.14

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

Routing

In diesem Menü konfigurieren Sie die Routing-Tabellen für das IKEv2-Routing.

Die Routing-Tabellen definieren IPv4/IPv6-Routen, die die VPN-Verbindungen verwenden, wenn keine entsprechende Route im IPv4/IPv6-Router vorhanden ist.

SNMP-ID:

2.19.36.6

Pfad Telnet:

Setup > **VPN** > **IKEv2**

IPv4

In dieser Tabelle konfigurieren Sie die IPv4-Tabellen für das IKEv2-Routing.

SNMP-ID:

2.19.36.6.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.19.36.6.1.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Netze

Enthält die kommaseparierte Liste von IPv4-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/IP-Maske
- IP-Adresse/Präfix
- IP-Schnittstellen-Name

SNMP-ID:

2.19.36.6.1.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Mögliche Werte:

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

IKE-CFG-Adr-Senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server). Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

SNMP-ID:

2.19.36.6.1.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Mögliche Werte:

nein

Die IPv4 Adresse wird nicht gesendet

ja

Die IPv4 Adresse wird gesendet.

Default-Wert:

ja

IPv6

In dieser Tabelle konfigurieren Sie die IPv6-Tabellen für das IKEv2-Routing.

SNMP-ID:

2.19.36.6.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing**

Name

Enthält den Namen für diesen Eintrag.

SNMP-ID:

2.19.36.6.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Netze

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/IP-Maske

- IP-Adresse/Präfix
- IP-Schnittstellen-Name

SNMP-ID:

2.19.36.6.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Mögliche Werte:

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

IKE-CFG-Adr-Senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server). Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

SNMP-ID:

2.19.36.6.2.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Mögliche Werte:

nein

Die IPv6 Adresse wird nicht gesendet

ja

Die IPv6 Adresse wird gesendet.

Default-Wert:

ja

7.5 "Match Remote Identity" für IKEv2

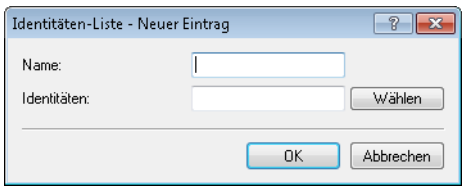
LCOS unterstützt ab Version 9.20 für IKEv2-Verbindungen die Konfiguration mehrerer entfernter Identitäten, um diese einer VPN-Gegenstelle zuordnen zu können.

Die Konfiguration weiterer entfernter Identitäten erfolgt in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** im Abschnitt **Authentifizierung**.

Die zusätzliche Zuordnung einer entfernten Identität für VPN-Verbindung nehmen Sie unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** im Feld **Weitere entf. Identitäten** vor.

7.5.1 Identitäten-Liste

In dieser Tabelle fassen Sie weitere entfernte Identitäten in einer Gruppe zusammen.



Name

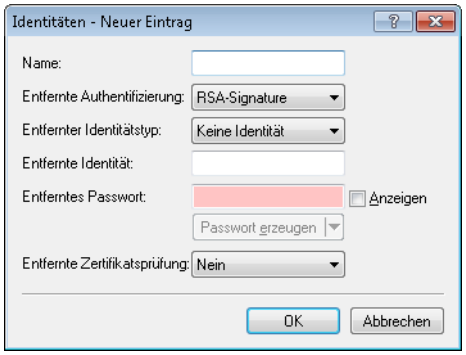
Enthält den eindeutigen Namen dieses Eintrages.

Identität

Listet die weiteren entfernten Identitäten auf, die in dieser Gruppe zusammengefasst sind. Diese Identitäten konfigurieren Sie unter **Identitäten**.

7.5.2 Identitäten

In dieser Tabelle konfigurieren Sie weitere entfernte Identitäten. Diesen Namen wählen Sie bei der Gruppierung von entfernten Identitäten unter **Identitäten-Liste** aus.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter „Entfernte Identität". Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld „Entfernte Identität" ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.
- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID.
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter „Entfernter Identitätstyp".

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

Entfernte Zertifikatsprüfung

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

7.5.3 Ergänzungen im Setup-Menü

Addit.-Remote-ID-List

Enthält zusätzliche entfernte Identitäten, die in der Tabelle **Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List** angegeben sind.

SNMP-ID:

2.19.36.3.1.10

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Mögliche Werte:

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

Default-Wert:

leer

Addit.-Remote-ID-List

In dieser Tabelle konfigurieren Sie Listen von zusätzlichen entfernten Identitäten.

SNMP-ID:

2.19.36.3.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Legt den Namen der ID-Liste fest.

SNMP-ID:

2.19.36.3.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Mögliche Werte:

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

Default-Wert:

leer

Addit.-Remote-IDs

Enthält die entfernten Identitäten, die Sie mit dieser Liste zusammenfassen möchten. Die IDs entnehmen Sie der Tabelle **Addit.-Remote-IDs**.

Geben Sie mehrere IDs durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.36.3.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Mögliche Werte:

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

Default-Wert:

leer

Addit.-Remote-IDs

In dieser Tabelle konfigurieren Sie zusätzliche entfernte Identitäten.

SNMP-ID:

2.19.36.3.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Enthält den Namen dieser entfernten Identität.

SNMP-ID:

2.19.36.3.3.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Auth

Legt die Authentifizierungsmethode für die entfernte Identität fest.

SNMP-ID:

2.19.36.3.3.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

RSA-Signature
Die Authentifizierung erfolgt über eine RSA-Signatur.

PSK
Die Authentifizierung erfolgt über Pre-shared Key (PSK).

Digital-Signature
Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*.

Default-Wert:

PSK

Remote-ID-Typ

Zeigt den ID-Typ der entfernten Identität an. Entsprechend interpretiert das Gerät die Eingabe unter **Remote-ID**.

SNMP-ID:

2.19.36.3.3.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

No-Identity
Das Gerät akzeptiert alle Verbindungen von entfernten IDs.

IPv4-Adresse
IPv6-Adresse
Domain-Name
Email-Adresse
Distinguished-Name
Key-ID

Default-Wert:

Email-Adresse

Remote-ID

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter **Remote-ID-Typ**.

SNMP-ID:

2.19.36.3.3.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Password

Enthält das Passwort der entfernten Identität.

SNMP-ID:

2.19.36.3.3.5

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

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

Default-Wert:

leer

Remote-Cert-ID-Check

Diese Funktion prüft, ob die angegebene entfernte ID auch im Zertifikat enthalten ist, das die Gegenseite zum Aufbauen benutzt.

SNMP-ID:

2.19.36.3.3.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Mögliche Werte:

Ja
Nein

Default-Wert:

Ja

Digital-Signatur-Profile

In dieser Tabelle konfigurieren Sie die Profile der Digitalen Signatur.

SNMP-ID:

2.19.36.3.4

Pfad Telnet:

Setup > **VPN** > **IKEv2**

Name

Name des Profils.

SNMP-ID:

2.19.36.3.4.1

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Digital-Signatur-Profile**

Mögliche Werte:

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

Default-Wert:

DEFAULT

Auth-Methode

Legt die Authentifizierungsmethode für die Digitale Signatur fest.

SNMP-ID:

2.19.36.3.4.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Digital-Signatur-Profile**

Mögliche Werte:

RSASSA-PSS
RSASSA-PKCS1-v1_5

Default-Wert:

RSASSA-PSS

Hash-Algorithmen

Legt die Hash-Algorithmen für die Digitale Signatur fest.

SNMP-ID:

2.19.36.3.4.3

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Digital-Signatur-Profile**

Mögliche Werte:

SHA-512, SHA-384, SHA-256, SHA1

Default-Wert:

SHA-512, SHA-384, SHA-256, SHA1

7.6 Redirect-Mechanismus für IKEv2

Ab LCOS-Version 9.20 unterstützt LCOS bei VPN-Verbindungen über IKEv2 den Redirect-Mechanismus nach RFC 5685. Dieser wird zunächst nur als Client unterstützt. Somit ist es lediglich möglich, dass ein IKEv2-Server einen Client via Redirect auf ein anderes Gateway umleitet.

7.6.1 Ergänzungen im Setup-Menü

7.7 VPN über IPv6-Verbindung mit IKEv1

Ab LCOS-Version 9.20 unterstützen aktuelle VPN-Geräte IKEv1 für VPN-Verbindungen über IPv6.

7.7.1 Ergänzungen im Setup-Menü

7.8 VPN-Netzwerkregeln für IPv4 und IPv6

Ab LCOS-Version 9.20 verfügen aktuelle VPN-Geräte über flexibel konfigurierbare Netzwerkregeln für VPN-Verbindungen über IPv4 und IPv6.

7.8.1 Ergänzungen im Setup-Menü

Netzwerkregeln

In diesem Verzeichnis konfigurieren Sie die VPN-Netzwerkregeln für IPv4- und IPv6-Verbindungen.

SNMP-ID:

2.19.35

Pfad Telnet:

Setup > **VPN**

IPv4-Regeln

In dieser Tabelle konfigurieren Sie die VPN-Netzwerkregeln für IPv4-Verbindungen.

SNMP-ID:

2.19.35.1

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln**

Name

Enthält den Namen für diese Regel.

SNMP-ID:

2.19.35.1.1

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv4-Regeln**

Mögliche Werte:

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

Default-Wert:

leer

Lokale-Netze

Enthält die lokalen Netze, für die diese Regel gelten soll.

Die folgenden Einträge sind gültig:

- Namen der IP-Netzwerke, deren Adressen eingesetzt werden sollen.
- „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.

Geben Sie mehrere Netze durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.1.2

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv4-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Entfernte-Netze

Enthält die entfernten Netze, für die diese Regel gelten soll.

Die folgenden Einträge sind gültig:

- Namen der IP-Netzwerke, deren Adressen eingesetzt werden sollen.
- „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.

Geben Sie mehrere Netze durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.1.3

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv4-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

IPv4-Regelliste

In dieser Tabelle fassen Sie die VPN-Netzwerkregeln für IPv4-Verbindungen in einer Regelliste zusammen.

SNMP-ID:

2.19.35.2

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln**

Name

Enthält den Namen für diese Regelliste.

SNMP-ID:

2.19.35.2.1

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv4-Regeln**

Mögliche Werte:

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

Default-Wert:

leer

Regeln

Enthält die Regeln, die Sie mit dieser Regelliste zusammenfassen möchten.

Geben Sie mehrere Regeln durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.2.2

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv4-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default-Wert:

leer

IPv6-Regeln

In dieser Tabelle konfigurieren Sie die VPN-Netzwerkregeln für IPv6-Verbindungen.

SNMP-ID:

2.19.35.3

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln**

Name

Enthält den Namen für diese Regel.

SNMP-ID:

2.19.35.3.1

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv6-Regeln**

Mögliche Werte:

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

Default-Wert:

leer

Lokale-Netze

Enthält die lokalen Netze, für die diese Regel gelten soll.

Geben Sie mehrere Netze durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.3.2

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv6-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Entfernte-Netze

Enthält die entfernten Netze, für die diese Regel gelten soll.

Geben Sie mehrere Netze durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.3.3

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv6-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

IPv6-Regelliste

In dieser Tabelle fassen Sie die VPN-Netzwerkregeln für IPv6-Verbindungen in einer Regelliste zusammen.

SNMP-ID:

2.19.35.4

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln**

Name

Enthält den Namen für diese Regelliste.

SNMP-ID:

2.19.35.4.1

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv6-Regeln**

Mögliche Werte:

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

Default-Wert:

leer

Regeln

Enthält die Regeln, die Sie mit dieser Regelliste zusammenfassen möchten.

Geben Sie mehrere Regeln durch Leerzeichen getrennt ein.

SNMP-ID:

2.19.35.4.2

Pfad Telnet:

Setup > **VPN** > **Netzwerkregeln** > **IPv6-Regeln**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default-Wert:

leer

8 Virtuelle LANs (VLANs)

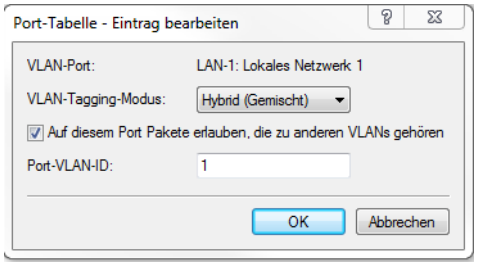
8.1 VLAN-Tagging-Modus "ankommend gemischt" entfernt

Ab LCOS-Version 9.20 entfällt der VLAN-Tagging-Modus "ankommend gemischt" in der VLAN-Porttabelle.

In Bestandskonfigurationen wird dieser Tagging-Modus automatisch in den Modus "Hybrid (gemischt)" konvertiert. Für Neukonfigurationen gilt als Defaultwert ebenfalls der Modus "Hybrid (gemischt)".

8.1.1 Die Porttabelle

In der Porttabelle werden die einzelnen Ports des Gerätes für die Verwendung im VLAN konfiguriert. Die Tabelle hat einen Eintrag für jeden Port des Gerätes mit folgenden Werten:



LANconfig: Schnittstellen / VLAN / Port-Tabelle

WEBconfig: LCOS-Menübaum / Setup / VLAN / Port-Tabelle

- **Port**: Der Name des Ports, nicht editierbar
- **Tagging-Modus**

  Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

  - Access (Niemals): Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werden so behandelt, als hätten sie kein VLAN-Tag. Haben die eingehenden Pakete ein VLAN-Tag, so wird es ignoriert und so behandelt, als ob es zur Payload des Paketes gehört. Eingehende Pakete werden immer dem für diesen Port definierten VLAN zugewiesen.
  - Trunk (Immer): Ausgehende Pakete erhalten auf diesem Port immer ein VLAN-Tag, egal ob sie dem für diesen Port definierten VLAN angehören oder nicht. Eingehende Pakete müssen über ein VLAN-Tag verfügen, anderenfalls werden sie verworfen.
  - Hybrid (Gemischt): Erlaubt einen gemischten Betrieb von Paketen mit und ohne VLAN-Tags auf dem Port. Pakete ohne VLAN-Tag werden dem für diesen Port definierten VLAN zugeordnet. Ausgehende Pakete erhalten ein VLAN-Tag, außer sie gehören dem für diesen Port definierten VLAN an.
  - Default: Hybrid (gemischt)

- **Auf diesem Port Pakete erlauben, die zu anderen VLANs gehören**

  Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port nicht Mitglied dieses VLANs ist.

- **Port-VLAN-ID**

  Diese Port-ID hat zwei Funktionen:

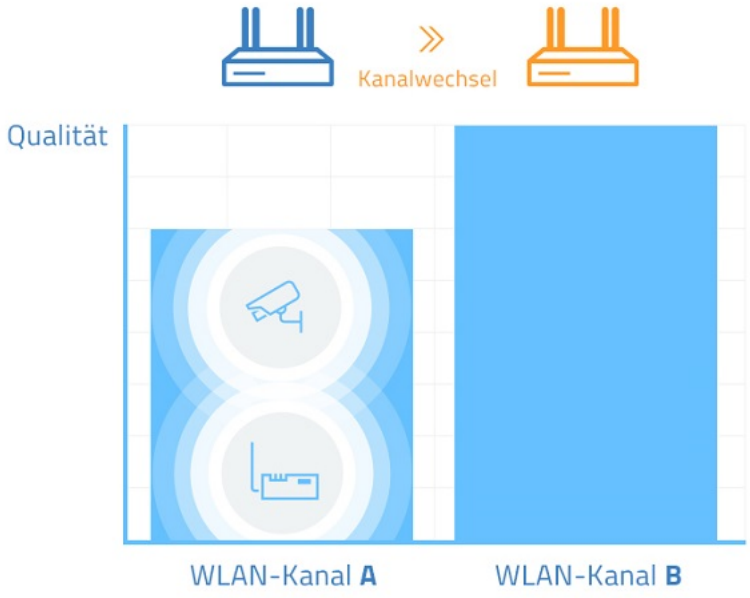
- Ungetaggte Pakete, die auf diesem Port im Modus "Hybrid (gemischt)" empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus "Access (Niemals)".
- Im Modus "Hybrid (gemischt)" entscheidet dieser Wert darüber, ob ausgehende Pakete ein VLAN-Tag erhalten oder nicht: Pakete, die dem für diesen Port definierten VLAN zugeordnet wurden, erhalten **kein** VLAN-Tag, alle anderen erhalten ein VLAN-Tag.

9 WLAN

9.1 Adaptive RF Optimization

Höherer WLAN-Durchsatz dank dynamischer Auswahl des qualitativ besten WLAN-Kanals durch den Access Point bei Kanalstörungen.

Mit der Auswahl des WLAN-Kanals wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Um in der Funkreichweite eines anderen APs ein WLAN störungsfrei betreiben zu können, sollte jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen (Shared Medium). Zu diesem Zweck nutzen LANCOM APs das Feature Adaptive RF Optimization. Dabei scannt der AP permanent das Funkfeld auf Störsignale. Wird ein bestimmter Schwellwert (auf Basis der „Wireless Quality Indicators") im aktuell verwendeten WLAN-Kanal überschritten, wechselt der AP automatisch auf einen qualitativ besseren Kanal. Diese intelligente Funktion ermöglicht es dem AP, sich an ein sich veränderndes Funkfeld dynamisch anzupassen, um somit die Robustheit des WLANs zu maximieren.



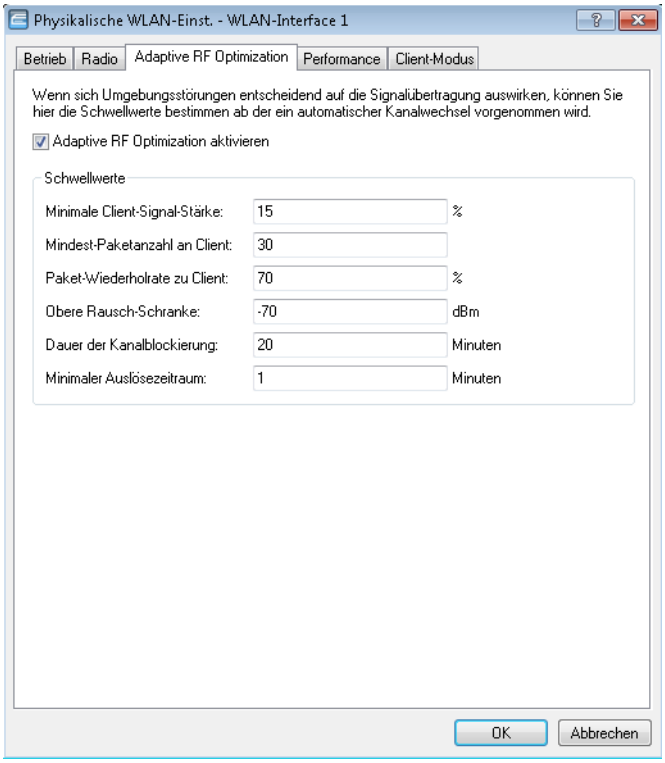
Sie haben in LANconfig die Möglichkeit, die Schwellwerte, die zu einem automatischen Kanalwechsel führen, manuell festzulegen.

Mit der aktuellen LCOS-Version ist die Verwendung der **Adaptive RF Optimization** auf folgenden Geräten möglich: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

9.1.1 Adaptive RF Optimization mit LANconfig konfigurieren

Um die Funktion Adaptive RF Optimization über LANconfig konfigurieren zu können, ist es erforderlich, dass die zu konfigurierenden Geräte das Feature "Wireless Quality Indicators" anbieten. Weitere Informationen zu WQI entnehmen Sie bitte dem Referenzhandbuch.

Um die Adaptive RF Optimization mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt „Interfaces“ auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Adaptive RF Optimization**.



Adaptive RF Optimization aktivieren

Um die Überwachung der WLAN-Umgebung durch die Adaptive RF Optimization zu aktivieren, markieren Sie die Option **Adaptive RF Optimization aktivieren**.

Konfigurieren Sie anschließend die Schwellwerte, die einen automatischen Kanalwechsel auslösen sollen.

Minimale Client-Signal-Stärke

Definieren Sie die minimale Signalstärke, mit der ein Client gesehen werden muss. Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein. Die Angabe erfolgt in % (Defaultwert: 15).

Mindest-Paketanzahl an Client

Geben Sie an, wie viele Pakete mindestens an einen Client gesendet werden müssen (TX). Wird dieser Wert unterschritten, wird der entsprechende Client nicht in der Auswertung berücksichtigt und kann somit auch kein Auslöser für einen Kanalwechsel sein (Defaultwert: 30).

Paket-Wiederholrate zu Client

Hier definieren Sie die Obergrenze der Paket-Wiederholrate zu Clients. Hat ein Client mehr als die hier angegebene Prozentzahl an Paketen erhalten, berücksichtigt das Gerät diesen Client bei der Entscheidung für einen Kanalwechsel. Die Angabe erfolgt in % (Defaultwert: 70).

Obere Rausch-Schranke

Definieren Sie die Obergrenze des zulässigen Kanalrauschens. Die Angabe erfolgt in dBm (Defaultwert: -70).

Dauer der Kanalblockierung

Wird ein Kanal als unbrauchbar erkannt, wird er für diese Zeit markiert / blockiert. Dieser Wert steuert auch die Blockierungszeit des Kanalwechseltriggers, falls alle Kanäle gleichzeitig blockiert sind. Die Angabe erfolgt in Minuten (Defaultwert: 20).

Minimaler Auslösezeitraum

Geben Sie an, für wie lange ein Limit überschritten sein muss, bevor das Gerät eine Aktion auslöst. Erfolgt pro Periode (20 Sekunden) keine Limitüberschreitung, setzt das Gerät die abgelaufene Zeit zurück. Bei einer Limitüberschreitung über den gesamten angegebenen Zeitraum markiert / blockiert das Gerät den Kanal. Die Angabe erfolgt in Minuten (Defaultwert: 1).

Für diesen Wert empfehlen sich kleine einstellige Werte.

9.1.2 Ergänzungen im Setup-Menü

Adaptive-RF-Optimization

Die **Adaptive RF Optimization** beobachtet und bewertet auf Basis der „Wireless Quality Indicators"-Kenngrößen permanent die WLAN-Umgebung und kann so die Qualität des Netzwerkes bestimmen. Nimmt die Qualität des Netzwerkes ab, sucht die Adaptive RF Optimization nach einem neuen Kanal, der für den Betrieb besser geeignet ist.

SNMP-ID:

2.23.20.23

Pfad Telnet:

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

Ifc

Zeigt das Interface an, für das die Einstellungen der Adaptive RF Optimization gelten.

SNMP-ID:

2.23.20.23.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Aktiv

Aktiviert oder deaktiviert die Adaptive RF Optimization für diese Schnittstelle.

SNMP-ID:

2.23.20.23.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Min-Client-Phy-Signal

Definieren Sie hier die minimale Signalstärke der Clients.

SNMP-ID:

2.23.20.23.3

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

15

Min-Client-Tx-Pakete

Geben Sie hier die minimale Anzahl Pakete an, die an Clients gesendet werden soll.

SNMP-ID:

2.23.20.23.4

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

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

Default-Wert:

30

Tx-Client-Retry-Ratio-Limit

Geben Sie in diesem Feld an, wie schnell ein Paket erneut an den Client übermittelt werden soll.

SNMP-ID:

2.23.20.23.5

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

70

Rauschpegel-Limit

Definieren Sie die Obergrenze des Rauschpegels.

SNMP-ID:

2.23.20.23.6

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

-70

Kanal-Markierung-Timeout

Legen Sie fest, wie lange der zur Zeit verwendete Kanal blockiert sein muss.

SNMP-ID:

2.23.20.23.7

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

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

Default-Wert:

20

Trigger-Zeitspanne

Wählen Sie hier den minimalen Auslösezeitraum.

SNMP-ID:

2.23.20.23.8

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Adaptive-RF-Optimization**

Mögliche Werte:

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

Default-Wert:

1

9.2 Managed RF Optimization

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, die APs in Ihrer WLAN-Umgebung eine automatische Kanalwahl durchführen zu lassen.

9.2.1 Managed RF Optimization

Mit der automatischen Kanalwahl stellen die Geräte sicher, dass immer der optimale Kanal für den Betrieb verwendet wird. Managed RF Optimization bietet Ihnen die Möglichkeit, einen AP per Knopfdruck anzuweisen, sich den passenden Kanal zu suchen. Grundlage und Voraussetzung ist dabei das Inter Access Point Protocol (IAPP), das es den APs ermöglicht, sich untereinander auszutauschen.

APs nutzen das IAPP-Protokoll, um sich über die Roaming-Vorgänge der eingebuchten WLAN-Clients zu informieren. Die APs senden dazu regelmäßig bestimmte Multicast-Nachrichten aus (Announces), mit deren Hilfe die Geräte die BSSIDs und IP-Adressen der anderen APs lernen. Bei einem Roaming-Vorgang informiert der WLAN-Client den neuen AP darüber, bei welchem AP er bisher eingebucht war. Der neue AP kann mit den aus den IAPP-Announces gelernten Informationen den bisherigen AP informieren, der den WLAN-Client umgehend aus seiner Tabelle der eingebuchten Clients entfernen kann.

Eine Kanalwahl können Sie manuell anstoßen oder automatisch von den Geräten durchführen lassen.

Dabei führt ein einzelner AP nach dem Befehl zum Durchführen der automatischen Kanalwahl folgende Aktionen durch:

- Das betreffende WLAN wird deaktiviert.
- Der AP bestimmt seine Priorität anhand der IAPP-Tabelle.
- Der AP wartet eine definierte Zeitspanne ab (Priorität * Wartezeit (10 Sekunden)).
- Der AP reaktiviert das betreffende WLAN.
- Der AP führt eine automatische Kanalwahl durch.

Jeder AP im gleichen Netzwerk sucht seinen optimalen Kanal in einer bestimmten Reihenfolge. Somit ist sichergestellt, dass nicht alle Geräte gleichzeitig eine Kanalwahl starten.

Kanalwahl über das Statusmenü aktivieren

Um die Kanalauswahl über das Statusmenü zu aktivieren, wechseln Sie im LCOS-Menübaum in die Ansicht **Status** > **WLAN** > **Auto-Kanal-Auswahl**.

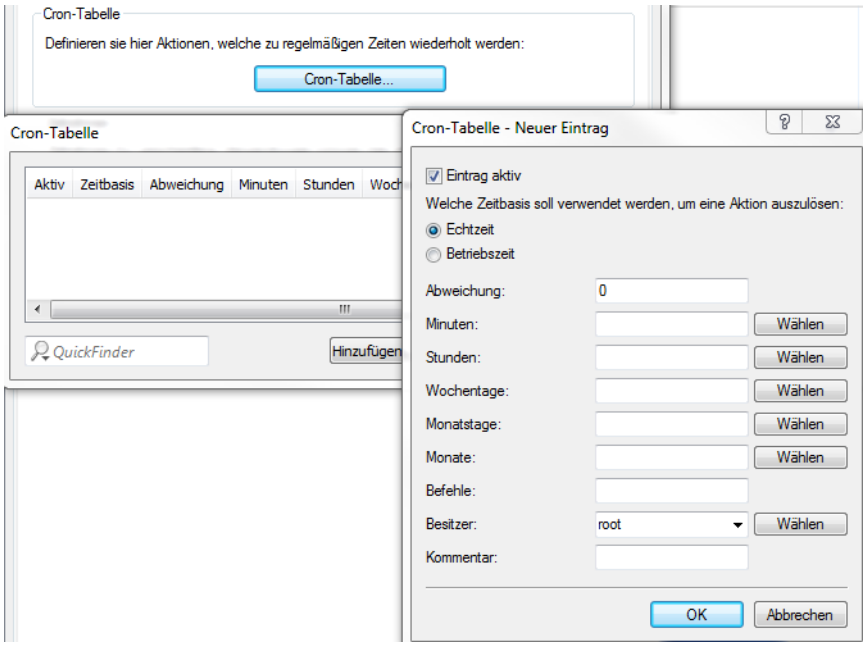
Definieren Sie eine WLAN-Schnittstelle (z. B WLAN-1), welche einen neuen Kanal wählen soll, und klicken Sie anschließend auf die Schaltfläche **Ausführen**.

Beachten Sie bitte, dass die Kanalwahl nur auf dem jeweiligen Gerät ausgeführt wird!

Geben Sie als Parameter "*" an, um alle Schnittstellen einen neuen Kanal suchen zu lassen.

Managed RF Optimization mit LANconfig konfigurieren

Um die automatische Kanalauswahl mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Datum / Zeit** > **Allgemein**. Klicken Sie anschließend im Abschnitt „Cron-Tabelle“ auf die Schaltfläche **Cron-Tabelle** und fügen Sie der Tabelle einen neuen Eintrag hinzu.



Definieren Sie die Eigenschaften des neuen Cron-Jobs.

Eintrag aktiv

Aktivieren oder deaktivieren Sie den aktuellen Eintrag.

Echtzeit

Wählen Sie Echtzeit als Zeitbasis für den Cron-Job.

Die Echtzeit muss gültig sein, andernfalls werden die definierten Befehle nicht ausgeführt.

Betriebszeit

Wählen Sie Betriebszeit als Zeitbasis für den Cron-Job.

Bei der Auswahl der Betriebszeit für die Befehlsausführung werden nur die Stunden- und Minuten-Felder der Cron-Tabelle ausgewertet.

Abweichung

Stellen Sie hier die Basis für einen Zufallswert ein, mit der die Aktion in Bezug auf den angegebenen Zeitpunkt in Minuten verzögert wird.

Bleibt der Wert bei der Default-Einstellung „0“, so werden die Aktionen zur angegebenen Zeit ausgeführt. Es findet keine Abweichung statt.

Minuten

Geben Sie hier alle Minuten an, zu denen der definierte Befehl ausgeführt werden soll.

Stunden

Geben Sie hier alle Stunden an, zu denen der definierte Befehl ausgeführt werden soll.

Wochentage

Geben Sie hier alle Wochentage an, zu denen der definierte Befehl ausgeführt werden soll.

Monatstage

Geben Sie hier alle Tage eines Monates an, zu denen der definierte Befehl ausgeführt werden soll.

Monate

Geben Sie hier alle Monate eines Jahres an, zu denen der definierte Befehl ausgeführt werden soll.

Befehle

Geben Sie hier den Befehl für die Channel-Selection an.

```
do /Status/WLAN/Auto-Channel-Selection [Schnittstellen-Name]
```

Folgende Schnittstellen-Namen sind möglich: "WLAN-1", "WLAN-2" oder "*" für beide Schnittstellen.

Besitzer

Wenn Sie einen Besitzer angeben, so wird die zugehörige Aktion mit dessen Rechten ausgeführt.

Kommentar

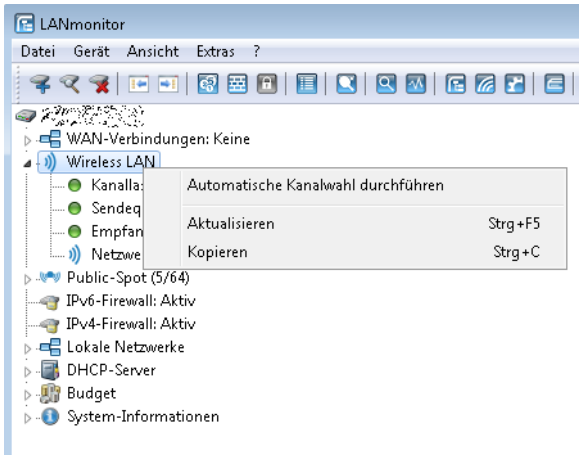
Geben Sie hier einen beschreibenden Kommentar an.

Beachten Sie bitte, dass die Kanalwahl nur auf dem jeweiligen Gerät ausgeführt wird!

Bei mehreren APs innerhalb der WLAN-Umgebung ist die Kanaloptimierung über ein Script auf dem WLC sinnvoll, das auf die einzelnen APs im Netzwerk ausgerollt wird.

Manueller Kanalwechsel über LANmonitor

Sie haben über LANmonitor die Möglichkeit, jeden AP im Netzwerk manuell anzuweisen, einen Kanalwechsel durchzuführen. Wechseln Sie dazu in die Ansicht **Wireless LAN**. Betätigen Sie die rechte Maustaste auf der Schnittstelle, die eine Kanalwahl durchführen soll, und wählen Sie im Untermenü **Automatische Kanalwahl durchführen** aus.



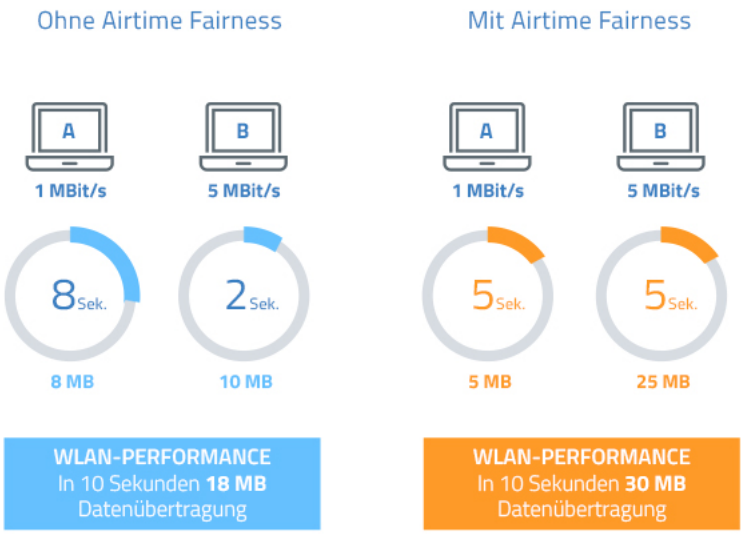
Beachten Sie bitte, dass Sie keine Rückmeldung über den Kanalwechsel erhalten.

9.3 Airtime Fairness

Bessere WLAN-Performance durch effiziente Ausnutzung der zur Verfügung stehenden Bandbreite dank einer fairen Aufteilung der WLAN-Übertragungszeiten unter den aktiven Clients

Insbesondere in WLAN-Szenarien mit einer hohen Dichte an Endgeräten konkurrieren die Clients um die zur Verfügung stehende Bandbreite. Dabei sendet der AP reihum an die aktiven Clients – ohne Berücksichtigung der notwendigen Übertragungszeit. So kommt es, dass langsamere (Legacy) Clients während der Übertragung von Datenpaketen schnellere Clients ausbremsen, obwohl diese in sehr kurzer Zeit ihre Datenübertragung abschließen könnten. Das Feature „Airtime Fairness" stellt sicher, dass die zur Verfügung stehende Bandbreite effizient ausgenutzt wird. Dazu wird die WLAN-Übertragungszeit („Airtime") zwischen den aktiven Clients fair aufgeteilt. Die Folge: Dadurch, dass alle Clients

dieselbe Airtime zur Verfügung haben, können schnellere Clients entsprechend mehr Datendurchsatz in derselben Zeit erreichen.



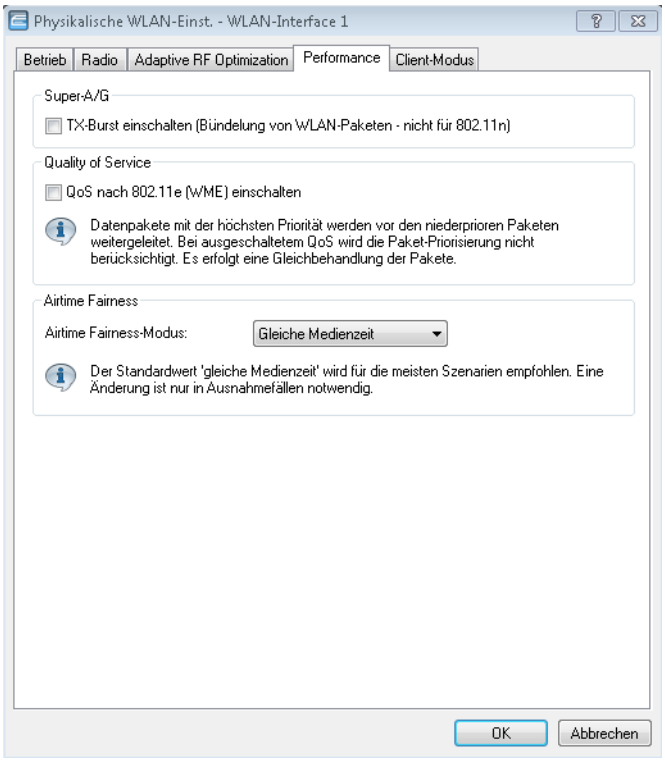
„Airtime" bedeutet WLAN-Übertragungszeit. Airtime Fairness stellt somit allen aktiven Clients eine WLAN-Übertragungszeit in Richtung der Clients entsprechend dem konfigurierten Airtime Fairness-Modus zur Verfügung. Dies verhindert z. B., dass ältere Clients moderne Clients ausbremsen.

Bei Geräten mit WLAN-Modulen, die den Standard IEEE 802.11ac unterstützen, ist die Funktion **Airtime Fairness** automatisch im WLAN-Modul aktiviert.

Folgende LANCOM-Geräte unterstützen **Airtime Fairness**: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

9.3.1 Airtime Fairness mit LANconfig konfigurieren

Wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**. Klicken Sie anschließend im Abschnitt **Interfaces** auf die Schaltfläche **Physikalische WLAN-Einst.**. Wählen Sie bei Geräten mit mehreren WLAN-Schnittstellen die gewünschte WLAN-Schnittstelle aus und wechseln Sie danach auf den Reiter **Performance**.



Wählen Sie unter **Airtime Fairness-Modus** aus den verfügbaren Einstellmöglichkeiten die für Ihre WLAN-Umgebung passende Option aus:

Round-Robin-Verteilung

Das Gerät sendet nacheinander an die aktiven Clients im Netzwerk.

Gleiche Medienzeit

Alle Clients verfügen über die gleiche Airtime. Clients mit einer höheren Datenrate profitieren von dieser Einstellung, da sie in der gleichen Zeit mehr Daten empfangen können.

IEEE 802.11ac-fähige WLAN-Module verwenden bereits hardwareseitig einen Algorithmus, der dieser Einstellung entspricht.

802.11n bevorzugen

Diese Einstellung bevorzugt IEEE 802.11n-Clients gegenüber älteren Clients. Demnach erhalten Clients mit dem Standard 802.11a oder 802.11g im Verhältnis zum 802.11n lediglich 25% Airtime. Clients mit 802.11b-Standard erhalten nur 6,25% Airtime. Daher versendet das Gerät deutlich schneller Daten an Clients mit dem Standard IEEE 802.11n.

Gleiches Medienvolumen

Diese Einstellung bewirkt, dass das Gerät die Airtime so zuweist, dass alle Clients die gleiche Datenmenge aus Richtung des APs erhalten. Allerdings bremsen langsamere Clients die schnelleren Teilnehmer bei dieser Option aus.

Diese Einstellung ist nur sinnvoll, wenn ein gleicher Datendurchsatz bei allen Clients erforderlich ist.

9.3.2 Ergänzungen im Setup-Menü

Airtime-Fairness-Modus

Die Funktion **Airtime Fairness** optimiert die Übertragungsgeschwindigkeit, insbesondere in High-Density-Umgebungen, indem sie die verfügbare Bandbreite des WLANs gleichmäßig auf die Clients verteilt. In der Standardeinstellung ist **Airtime Fairness** aktiviert.

SNMP-ID:

2.23.20.9.6

Pfad Telnet:

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

Mögliche Werte:

Round-Robin

Jeder Client im Netzwerk erhält nacheinander eine Sendegelegenheit (TXOP).

Gleiche-Medienzeit

Alle Clients verfügen über die gleiche Airtime. Clients mit einer höheren Datenrate profitieren von dieser Einstellung, da sie in der gleichen Zeit einen höheren Datendurchsatz erzielen können.

802.11ac-fähige Geräte verwenden bereits hardwareseitig einen Algorithmus, der dieser Einstellung entspricht.

Bevorzuge-802.11n-Medienzeit

Diese Einstellung bevorzugt IEEE 802.11n-Clients gegenüber älteren Clients. Demnach erhalten Clients mit dem Standard 802.11a oder 802.11g im Verhältnis zum 802.11n lediglich 25% Airtime. Clients mit 802.11b-Standard erhalten nur 6,25% Airtime. Daher übertragen Clients mit dem Standard 802.11n ihre Daten wesentlich schneller.

Gleiches-Volumen

Erhalten alle Clients das gleiche Airtime-Kontingent, ist sichergestellt, dass jeder Client in der WLAN-Umgebung den gleichen Datendurchsatz erreicht. Allerdings bremsen langsamere Clients die schnelleren Teilnehmer bei dieser Option aus.

Diese Einstellung ist nur sinnvoll, wenn ein gleicher Datendurchsatz bei allen Clients erforderlich ist.

Default-Wert:

Gleiche-Medienzeit

9.3.3 Ergänzungen im Status-Menü

Powersave-Wiederholungen

Für jedes aufgrund eines einschränkenden Airtime-Fairness-Modus zurückgestellte Datenpaket erhöht sich der Zähler in dieser Spalte.

SNMP-ID:

1.3.54.29

Pfad Telnet:

Status > **WLAN** > **Fehler**

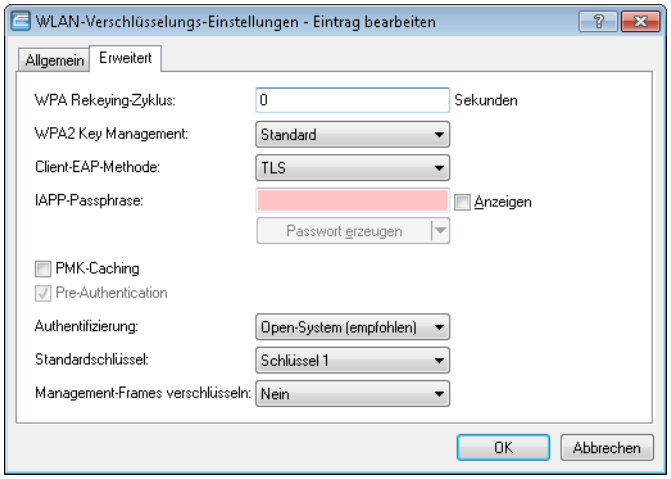
9.4 Verschlüsseltes OKC über IAPP

Ab LCOS-Version 9.20 besteht die Möglichkeit, OKC (Opportunistic Key Caching) auch in Netzwerken zu verwenden, die vom LANCOM Large Scale Rollout & Management (LSR) verwaltet werden.

9.4.1 Verschlüsseltes OKC über IAPP

Durch eine definierte IAPP-Passphrase (PMK-IAPP-Secret) auf einem AP ist es möglich, den PMK (Pairwise Master Key) verschlüsselt zu den anderen APs zu übertragen und dort zu speichern.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **802.11i/WEP** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.



9.4.2 Ergänzungen im Setup-Menü

PMK-IAPP-Secret

Vernetzte APs tauschen Daten angemeldeter WLAN-Clients über das IAPP aus, um ein sicheres Roaming dieser WLAN-Clients in Controller-less WLAN-Netzen zu ermöglichen, die vom LANCOM LSR verwaltet werden.

Der AP nutzt diese Passphrase, um den PMK zu verschlüsseln und die Mobility Domain des jeweiligen WLAN-Clients zu errechnen.

Jeder Wert ungleich 0 startet automatisch den Austausch des Master Secrets zwischen den jeweiligen APs.

SNMP-ID:

2.23.20.3.20

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Besondere Werte:

leer

OKC über IAPP ist deaktiviert.

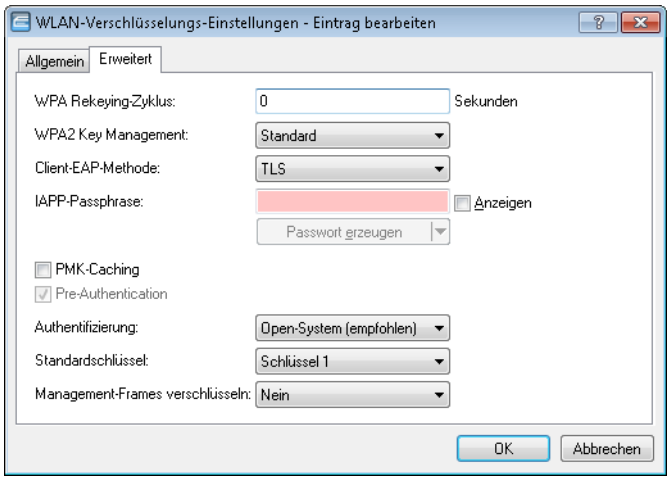
9.5 Fast Roaming

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, Fast Roaming (IEEE 802.11r) auch in Netzwerken zu verwenden, die vom LANCOM Large Scale Rollout & Management (LSR) verwaltet werden.

9.5.1 Fast Roaming über IAPP

Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können APs mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **Verschlüsselung** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.



Beachten Sie bitte, dass es für die Verwendung von IEEE 802.11r erforderlich ist, in den Verschlüsselungs-Einstellungen unter **WPA2 Key Management** die Option „Fast Roaming“ auszuwählen.

9.5.2 Ergänzungen im Setup-Menü

PMK-IAPP-Secret

Vernetzte APs tauschen Daten angemeldeter WLAN-Clients über das IAPP aus, um ein sicheres Roaming dieser WLAN-Clients in Controller-less WLAN-Netzen zu ermöglichen, die vom LANCOM LSR verwaltet werden.

Der AP nutzt diese Passphrase, um den PMK zu verschlüsseln und die Mobility Domain des jeweiligen WLAN-Clients zu errechnen.

Jeder Wert ungleich 0 startet automatisch den Austausch des Master Secrets zwischen den jeweiligen APs.

SNMP-ID:

2.23.20.3.20

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Besondere Werte:

leer

OKC über IAPP ist deaktiviert.

9.6 Wireless Intrusion Detection System (WIDS)

Ein Intrusion Detection System (IDS) erkennt Angriffe auf ein Netzwerk und meldet diese Angriffe an ein übergeordnetes Netzwerk-Management-System. Gerade in Unternehmens-Netzwerken ist der Einsatz eines IDS unerlässlich, um eventuelle Angriffe oder Störungen sofort erkennen und abstellen zu können.

Das Wireless Intrusion Detection System (WIDS) in LCOS-Geräten überprüft die verfügbaren WLANs anhand umfangreicher, definierter Grenzwerte. Damit Sie im Falle eines Angriffes rechtzeitig reagieren können, meldet das WIDS Angriffe über E-Mail, SYSLOG oder SNMP-Traps.

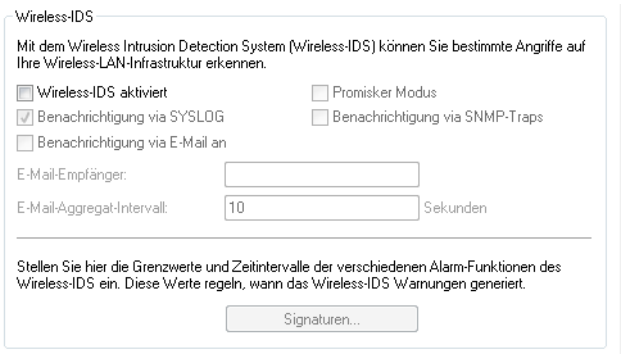
Die Erkennung von Angriffen erfolgt dabei auf Basis von bekannten oder gleichartigen Mustern.

Die WIDS-Konfiguration erfolgt entweder direkt im AP oder über die Zuordnung eines WIDS-Profils zum AP in einem WLC.

Beachten Sie bitte, dass die Erkennung von Angriffsmustern (Heuristik) auch zu Fehlalarmen („False Positive“) führen kann!

9.6.1 WIDS im AP mit LANconfig konfigurieren

Um das Wireless Intrusion Detection System (WIDS) mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Security**.



Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

Promisker Modus

Bei aktiviertem Modus („promiscuous mode") empfängt der AP auch Pakete, die nicht an ihn gerichtet sind, sondern an andere Netzwerkteilnehmer.

Dieser Modus ist erforderlich, um einige der unten genannten Angriffe erkennen zu können. Der promiscuous mode beeinflusst allerdings die Leistung. Daher wird mit der Aktivierung des promiscuous mode automatisch die Frame Aggregation abgeschaltet.

Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO" und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

Das Feld muss eine gültige E-Mail-Adresse enthalten.

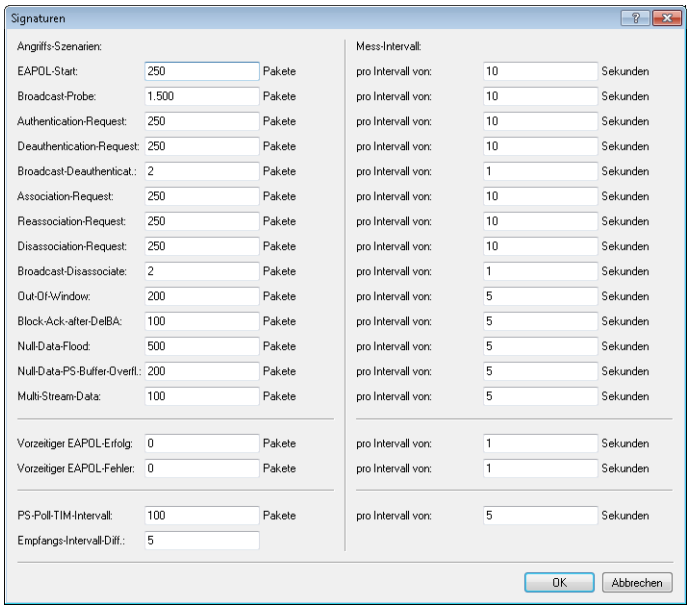
E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

Signaturen

Hier konfigurieren Sie die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.



Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (*)
- Broadcast-Disassociate
- Out-Of-Window
- Block-Ack-after-DelBA
- Null-Data-Flood
- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data
- Vorzeitiger EAPOL-Erfolg (*)
- Vorzeitiger EAPOL-Fehler (*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

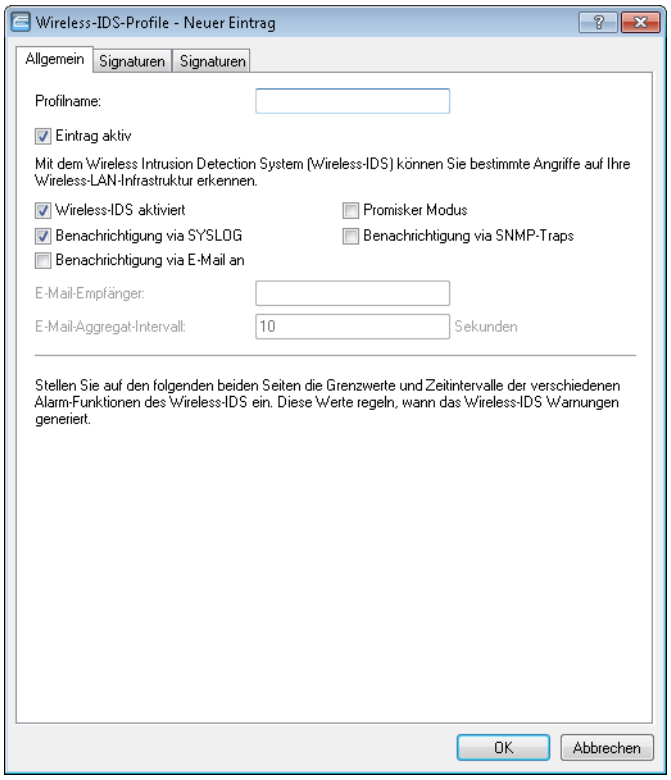
Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

(*) Diese Angriffe werden nur bei aktivem promiscuous mode erkannt!

9.6.2 WIDS-Profile im WLC mit LANconfig konfigurieren

Um ein Profil für das Wireless Intrusion Detection System (WIDS) mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **WLAN-Controller** > **Profile** und klicken Sie auf **Erweiterte Profile**.

Unter **Wireless-IDS-Profile** erstellen oder bearbeiten Sie die WIDS-Profile.



Profilname

Vergeben Sie eine Bezeichnung für das Profil. Diesen Profilnamen geben Sie bei der Zuordnung zu einem WLAN-Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile** an.

Die Angabe eines Profilnamens ist für die Konfiguration der WIDS-Signaturen notwendig.

Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

Promisker Modus

Bei aktiviertem Modus („promiscuous mode") empfängt der AP auch Pakete, die nicht an ihn gerichtet sind, sondern an andere Netzwerkteilnehmer.

Dieser Modus ist erforderlich, um einige der unten genannten Angriffe erkennen zu können. Der promiscuous mode beeinflusst allerdings die Leistung. Daher wird mit der Aktivierung des promiscuous mode automatisch die Frame Aggregation abgeschaltet.

Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO" und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

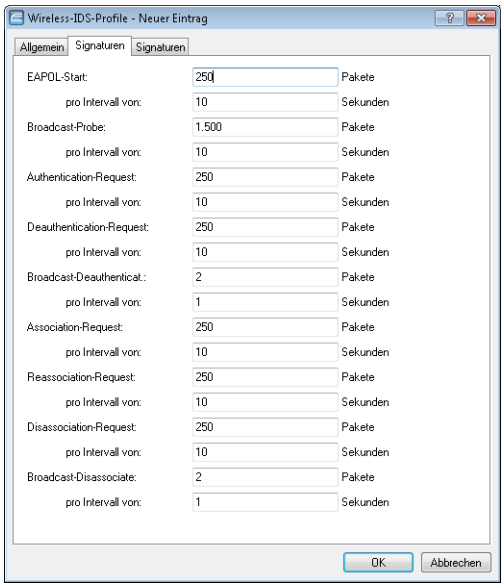
Das Feld muss eine gültige E-Mail-Adresse enthalten.

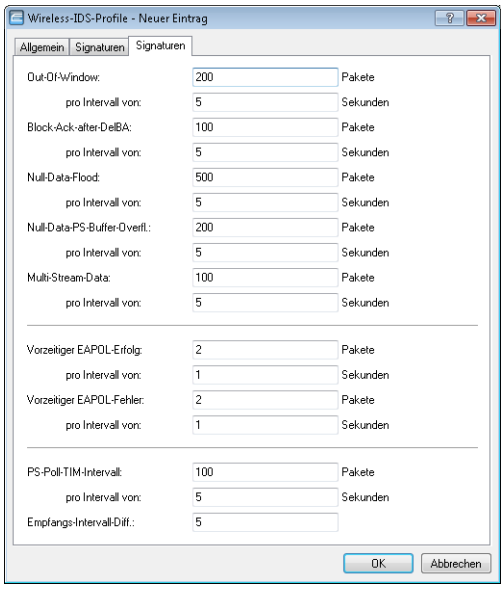
E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

Auf den Reitern „Signaturen" konfigurieren Sie die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.





Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

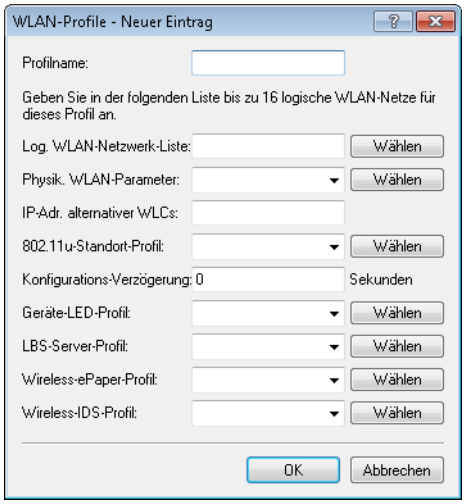
- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (*)
- Broadcast-Disassociate
- Out-Of-Window
- Block-Ack-after-DelBA
- Null-Data-Flood

- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data
- Vorzeitiger EAPOL-Erfolg (*)
- Vorzeitiger EAPOL-Fehler (*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

(*) Diese Angriffe werden nur bei aktivem promiscuous mode erkannt!

Speichern Sie das WIDS-Profil und ordnen Sie es anschließend unter **WLAN-Controller** > **Profile** > **WLAN-Profile** einem WLAN-Profil zu.



9.6.3 Ergänzungen im Setup-Menü

Wireless-IDS

In diesem Verzeichnis konfigurieren Sie das Wireless Intrusion Detection System (WIDS).

SNMP-ID:

2.12.248

Pfad Telnet:

Setup > **WLAN**

IDS-operational

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

SNMP-ID:

2.12.248.9

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

nein
Das WIDS ist deaktiviert.

ja
Das WIDS ist aktiviert.

Default-Wert:

nein

Syslog-Operational

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO“ und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

SNMP-ID:

2.12.248.10

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

nein
Die WIDS-Meldungen erfolgen nicht über SYSLOG.

ja
Die WIDS-Meldungen erfolgen über SYSLOG.

Default-Wert:

ja

SNMPTraps-Operational

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

SNMP-ID:

2.12.248.11

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

nein
Die SNMP-Traps sind deaktiviert.

ja
Die SNMP-Traps sind aktiviert.

Default-Wert:

nein

E-Mail

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

SNMP-ID:

2.12.248.12

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

nein
Die WIDS-Meldungen über E-Mail sind deaktiviert.

ja
Die WIDS-Meldungen erfolgen über E-Mail.

Default-Wert:

nein

E-Mail-Empfaenger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiv ist.

Das Feld muss eine gültige E-Mail-Adresse enthalten.

SNMP-ID:

2.12.248.13

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

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

E-Mail-Zusammenfassungs-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

SNMP-ID:

2.12.248.14

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

Signaturen

In diesem Verzeichnis konfigurieren Sie die Grenzwerte und Zeitintervalle der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.

SNMP-ID:

2.12.248.50

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS**

AssociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Association-Request-Angriffe.

SNMP-ID:

2.12.248.50.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Association-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.1.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Association-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.1.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Mögliche Werte:

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

Default-Wert:

10

ReassociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Reassociation-Request-Angriffe.

SNMP-ID:

2.12.248.50.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Reassociation-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.2.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Reassociation-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.2.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Mögliche Werte:

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

Default-Wert:

10

AuthenticateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Authentication-Request-Angriffe.

SNMP-ID:

2.12.248.50.3

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Authentication-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.3.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Authentication-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.3.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Mögliche Werte:

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

Default-Wert:

10

EAPOLStart

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für EAPOL-Start-Angriffe.

SNMP-ID:

2.12.248.50.4

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der EAPOL-Start-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.4.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die EAPOL-Start-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.4.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Mögliche Werte:

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

Default-Wert:

10

ProbeBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Probe-Angriffe.

SNMP-ID:

2.12.248.50.5

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Probe-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.5.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Mögliche Werte:

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

Default-Wert:

1500

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Probe-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.5.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Mögliche Werte:

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

Default-Wert:

10

DisassociateBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Disassociate-Angriffe.

SNMP-ID:

2.12.248.50.6

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Disassociate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.6.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Mögliche Werte:

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

Default-Wert:

2

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Disassociate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.6.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Mögliche Werte:

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

Default-Wert:

1

DeauthenticateBroadcast

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Broadcast-Deauthenticate-Angriffe.

SNMP-ID:

2.12.248.50.7

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Broadcast-Deauthenticate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.7.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Mögliche Werte:

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

Default-Wert:

2

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Deauthenticate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.7.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Mögliche Werte:

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

Default-Wert:

1

DisassociateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Disassociation-Request-Angriffe.

SNMP-ID:

2.12.248.50.8

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Disassociation-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.8.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Disassociation-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.8.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Mögliche Werte:

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

Default-Wert:

10

BlockAckOutOfWindow

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Out-Of-Window-Angriffe.

SNMP-ID:

2.12.248.50.9

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Out-Of-Window-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.9.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Mögliche Werte:

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

Default-Wert:

200

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Out-Of-Window-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.9.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Mögliche Werte:

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

Default-Wert:

5

BlockAckAfterDelBA

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Block-Ack-after-DelBA-Angriffe.

SNMP-ID:

2.12.248.50.10

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Block-Ack-after-DelBA-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.10.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Mögliche Werte:

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

Default-Wert:

100

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Block-Ack-after-DelBA-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.10.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Mögliche Werte:

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

Default-Wert:

5

NullDataFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Null-Data-Angriffe.

SNMP-ID:

2.12.248.50.11

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Null-Data-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.11.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Mögliche Werte:

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

Default-Wert:

500

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Null-Data-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.11.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Mögliche Werte:

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

Default-Wert:

5

NullDataPSBufferOverflow

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Null-Data-PS-Buffer-Overflow-Angriffe.

SNMP-ID:

2.12.248.50.12

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Null-Data-PS-Buffer-Overflow-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.12.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Mögliche Werte:

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

Default-Wert:

200

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Null-Data-PS-Buffer-Overflow-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.12.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Mögliche Werte:

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

Default-Wert:

5

PSPollTIMInterval

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für PS-Poll-TIM-Intervall-Angriffe.

SNMP-ID:

2.12.248.50.13

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der PS-Poll-TIM-Intervall-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.13.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Mögliche Werte:

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

Default-Wert:

100

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die PS-Poll-TIM-Intervall-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.13.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Mögliche Werte:

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

Default-Wert:

5

Intervall-Diff

SNMP-ID:

2.12.248.50.13.3

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Mögliche Werte:

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

Default-Wert:

5

SMPSMUltiStream

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Multi-Stream-Data-Angriffe.

SNMP-ID:

2.12.248.50.14

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Multi-Stream-Data-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.14.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Mögliche Werte:

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

Default-Wert:

100

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Multi-Stream-Data-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.14.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Mögliche Werte:

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

Default-Wert:

5

DeauthenticateReqFlood

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Deauthentication-Request-Angriffe.

SNMP-ID:

2.12.248.50.15

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Deauthentication-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.15.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Mögliche Werte:

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

Default-Wert:

250

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Deauthentication-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.15.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Mögliche Werte:

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

Default-Wert:

10

PrematureEAPOLSuccess

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Vorzeitiger-EAPOL-Erfolg-Angriffe.

SNMP-ID:

2.12.248.50.16

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Vorzeitiger-EAPOL-Erfolg-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.16.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Mögliche Werte:

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

Default-Wert:

2

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Vorzeitiger-EAPOL-Erfolg-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.16.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Mögliche Werte:

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

Default-Wert:

1

PrematureEAPOLFailure

In diesem Verzeichnis konfigurieren Sie die Grenzwerte für Vorzeitiger-EAPOL-Fehler-Angriffe.

SNMP-ID:

2.12.248.50.17

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Zaehlerlimit

Definieren Sie die Anzahl der Vorzeitiger-EAPOL-Fehler-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.17.1

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Mögliche Werte:

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

Default-Wert:

2

Zaehlerintervall

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Vorzeitiger-EAPOL-Fehler-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.12.248.50.17.2

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Mögliche Werte:

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

Default-Wert:

1

Promiscuous-Mode

Aktiviert oder deaktiviert den Promiscuous-Modus. Dieser Modus verarbeitet auch Pakete, die nicht an das Gerät selbst gesendet wurden. Diese Pakete werden an das LCOS weitergeleitet, um eine Analyse durch das WIDS zu ermöglichen.

Der Promiscuous-Modus erkennt folgende Angriffe:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess
- DeauthenticateReqFlood
- DisassociateReqFlood

Bitte beachten Sie, dass der Promiscuous-Modus die Leistung des Gerätes stark beeinträchtigt. So wird z. B. die Frame-Aggregation automatisch deaktiviert. Nutzen Sie diesen Modus daher nur bei konkretem Verdacht.

SNMP-ID:

2.12.248.51

Pfad Telnet:

Setup > **WLAN** > **Wireless-IDS** > **Signaturen**

Mögliche Werte:

nein

Der Promiscuous-Modus ist deaktiviert.

ja

Der Promiscuous-Modus ist aktiviert.

Default-Wert:

nein

9.6.4 Ergänzungen im Status-Menü

Wireless-IDS

In diesem Verzeichnis finden Sie Statistiken des Wireless Intrusion Detection Systems (WIDS).

SNMP-ID:

1.3.248

Pfad Telnet:

Status > **WLAN**

Event-Table

Die Event-Tabelle zeigt Ihnen Einzelheiten der letzten Angriffe an, z. B. Ereignistyp, ID und Zeitpunkt des Ereignisses. Ein AP speichert bis zu 100 Einträge.

SNMP-ID:

1.3.248.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS**

Event-Type

Dieser Eintrag zeigt an, um welche Angriffsart es sich gehandelt hat.

SNMP-ID:

1.3.248.1.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Event-Table**

ID

Ereignis-Index mit fortlaufender Nummer für Ereigniseinträge.

SNMP-ID:

1.3.248.1.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Event-Table**

Event-Time

Dieser Eintrag zeigt den Zeitpunkt an, zu dem der Angriff erfolgte.

SNMP-ID:

1.3.248.1.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Event-Table**

Event-Rate

Dieser Eintrag zeigt die Anzahl erkannter Angriffe eines Typs während des konfigurierten Zeitraumes an.

SNMP-ID:

1.3.248.1.4

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Event-Table**

Interface

Dieser Eintrag zeigt die Schnittstelle an, über die der Angriff erfolgte.

SNMP-ID:

1.3.248.1.5

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Event-Table**

Signaturen

Dieses Verzeichnis beinhaltet Statistiken über die erkannten Angriffe.

SNMP-ID:

1.3.248.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS**

AssociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Association-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Association-Request-Angriffe an.

SNMP-ID:

1.3.248.2.1.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.1.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.1.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AssociateReqFlood**

ReassociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Reassociation-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Mögliche Werte:

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

Default-Wert:

10

Counter

Zeigt die Anzahl der Reassociation-Request-Angriffe an.

SNMP-ID:

1.3.248.2.2.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.2.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.2.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ReassociateReqFlood**

AuthenticateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Authentication-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Authentication-Request-Angriffe an.

SNMP-ID:

1.3.248.2.3.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.3.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.3.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **AuthenticateReqFlood**

EAPOLStart

Dieses Verzeichnis beinhaltet die Statistik über EAPOL-Start-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.4

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der EAPOL-Start-Angriffe an.

SNMP-ID:

1.3.248.2.4.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.4.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.4.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **EAPOLStart**

ProbeBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Probe-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.5

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Probe-Angriffe an.

SNMP-ID:

1.3.248.2.5.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.5.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.5.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **ProbeBroadcast**

DisassociateBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Disassociate-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.6

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Disassociate-Angriffe an.

SNMP-ID:

1.3.248.2.6.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.6.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.6.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateBroadcast**

DeauthenticateBroadcast

Dieses Verzeichnis beinhaltet die Statistik über Broadcast-Deauthenticate-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.7

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Broadcast-Deauthenticate-Angriffe an.

SNMP-ID:

1.3.248.2.7.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.7.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.7.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateBroadcast**

DisassociateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Disassociation-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.8

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Disassociation-Request-Angriffe an.

SNMP-ID:

1.3.248.2.8.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.8.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.8.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DisassociateReqFlood**

BlockAckOutOfWindow

Dieses Verzeichnis beinhaltet die Statistik über Out-Of-Window-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.9

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Out-Of-Window-Angriffe an.

SNMP-ID:

1.3.248.2.9.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.9.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.9.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckOutOfWindow**

BlockAckAfterDelBA

Dieses Verzeichnis beinhaltet die Statistik über Block-Ack-after-DelBA-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.10

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Block-Ack-after-DelBA-Angriffe an.

SNMP-ID:

1.3.248.2.10.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.10.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.10.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **BlockAckAfterDelBA**

NullDataFlood

Dieses Verzeichnis beinhaltet die Statistik über Null-Data-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.11

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Null-Data-Angriffe an.

SNMP-ID:

1.3.248.2.11.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.11.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.11.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataFlood**

NullDataPSBufferOverflow

Dieses Verzeichnis beinhaltet die Statistik über Null-Data-PS-Buffer-Overflow-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.12

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Null-Data-PS-Buffer-Overflow-Angriffe an.

SNMP-ID:

1.3.248.2.12.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.12.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.12.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **NullDataPSBufferOverflow**

PSPollTIMInterval

Dieses Verzeichnis beinhaltet die Statistik über PS-Poll-TIM-Intervall-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.13

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der PS-Poll-TIM-Intervall-Angriffe an.

SNMP-ID:

1.3.248.2.13.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.13.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.13.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PSPollTIMInterval**

SMPSMUltiStream

Dieses Verzeichnis beinhaltet die Statistik über Multi-Stream-Data-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.20.14

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Multi-Stream-Data-Angriffe an.

SNMP-ID:

1.3.248.2.14.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.14.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.14.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **SMPSMUltiStream**

DeauthenticateReqFlood

Dieses Verzeichnis beinhaltet die Statistik über Deauthentication-Request-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.15

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Deauthentication-Request-Angriffe an.

SNMP-ID:

1.3.248.2.15.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.15.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.15.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **DeauthenticateReqFlood**

PrematureEAPOLSuccess

Dieses Verzeichnis beinhaltet die Statistik über Vorzeitiger-EAPOL-Erfolg-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.16

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Vorzeitiger-EAPOL-Erfolg-Angriffe an.

SNMP-ID:

1.3.248.2.16.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.16.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.16.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLSuccess**

PrematureEAPOLFailure

Dieses Verzeichnis beinhaltet die Statistik über Vorzeitiger-EAPOL-Fehler-Angriffe.

Je nach Anzahl der Schnittstellen im Gerät unterscheidet sich die Anzeige der Parameter.

SNMP-ID:

1.3.248.2.17

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen**

Counter

Zeigt die Anzahl der Vorzeitiger-EAPOL-Fehler-Angriffe an.

SNMP-ID:

1.3.248.2.17.1

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Alarm-State-Ifc-1

Zeigt den Alarm-Zustand der ersten Schnittstelle.

SNMP-ID:

1.3.248.2.17.2

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

Alarm-State-Ifc-2

Zeigt den Alarm-Zustand der zweiten Schnittstelle.

SNMP-ID:

1.3.248.2.17.3

Pfad Telnet:

Status > **WLAN** > **Wireless-IDS** > **Signaturen** > **PrematureEAPOLFailure**

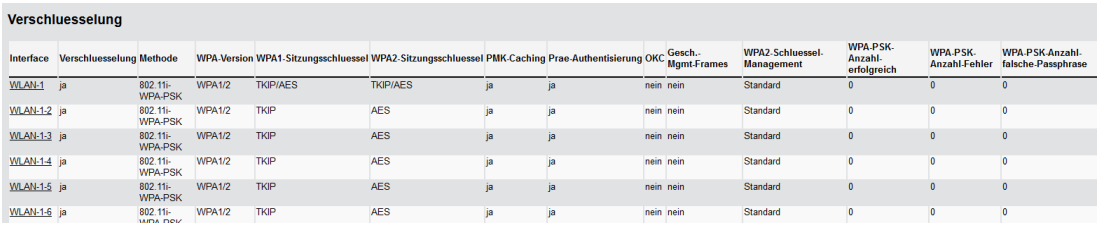
9.7 Status-Zähler für fehlgeschlagene WPA-PSK / IEEE802.1X-Anmeldevorgänge

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, sich die Anzahl fehlgeschlagener Anmeldevorgänge für WPA und IEEE 802.1X anzeigen zu lassen.

9.7.1 Status-Zähler für WPA-PSK-Anmeldevorgänge

Eine Übersicht über die Anzahl fehlgeschlagener WPA-PSK Anmeldevorgänge finden Sie im LCOS-Menübaum unter **Status** > **WLAN** > **Verschlüsselung**.

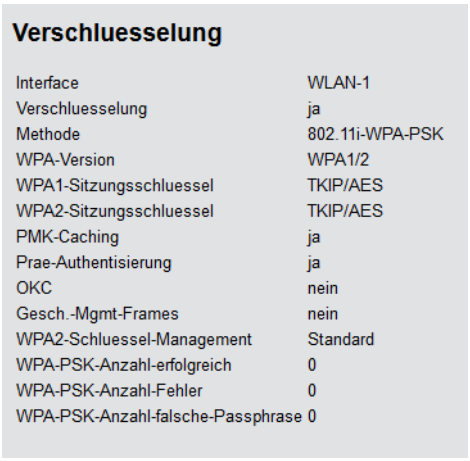
Zusätzlich erhalten Sie eine Übersicht über erfolgreiche Anmeldeversuche sowie die Anzahl zurückgewiesener Anmeldungen aufgrund falscher Passphrasen.



Verschluesselung

Interface	Verschluesselung	Methode	WPA-Version	WPA1-Sitzungsschluessel	WPA2-Sitzungsschluessel	PMK-Caching	Prae-Authentisierung	OKC	Gesch.-Mgmt-Frames	WPA2-Schluessel-Management	WPA-PSK-Anzahl-erfolgreich	WPA-PSK-Anzahl-Fehler	WPA-PSK-Anzahl-falsche-Passphrase
WLAN-1	ja	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-2	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-3	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-4	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-5	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1-6	ja	802.11i-	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0

Wählen Sie in der Tabelle eine Schnittstelle aus (z. B. WLAN-1), um sich Informationen für die gewählte Schnittstelle anzeigen zu lassen.



Verschluesselung

Interface	WLAN-1
Verschluesselung	ja
Methode	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Sitzungsschluessel	TKIP/AES
WPA2-Sitzungsschluessel	TKIP/AES
PMK-Caching	ja
Prae-Authentisierung	ja
OKC	nein
Gesch.-Mgmt-Frames	nein
WPA2-Schluessel-Management	Standard
WPA-PSK-Anzahl-erfolgreich	0
WPA-PSK-Anzahl-Fehler	0
WPA-PSK-Anzahl-falsche-Passphrase	0

9.7.2 Status-Zähler für IEEE 802.1X-Anmeldevorgänge

Eine Übersichtstabelle mit der Anzahl akzeptierter und zurückgewiesener Verbindungsanfragen je logischer Schnittstelle finden Sie im LCOS-Menübaum unter **Status** > **IEEE802.1x** > **Ports**.

Zusätzlich zeigt Ihnen die Übersicht an, wie oft bei einer Schnittstelle das Authorisierungslimit erreicht wurde.

Ports

Port	Anzahl-Accept	Anzahl-Reject	Anzahl-ReauthMax-erreicht
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

9.7.3 Ergänzungen im Status-Menü

Verschluesselung

Diese Tabelle enthält Informationen über die Verschlüsselung je Schnittstelle.

SNMP-ID:

1.3.64

Pfad Telnet:

Status > **WLAN**

WPA-PSK-Anzahl-falsche-Passphrase

Zeigt die Anzahl der aufgrund einer fehlerhaften Passphrase zurückgewiesenen WPA-Anfragen an dieser Schnittstelle an.

SNMP-ID:

1.3.64.20

Pfad Telnet:

Status > **WLAN** > **Verschlüsselung**

WPA-PSK-Anzahl-erfolgreich

Zeigt die Anzahl der erfolgreichen WPA-Anfragen an dieser Schnittstelle an.

SNMP-ID:

1.3.64.21

Pfad Telnet:

Status > **WLAN** > **Verschlüsselung**

WPA-PSK-Anzahl-Fehler

Zeigt die Anzahl der zurückgewiesenen WPA-Anfragen an dieser Schnittstelle an.

SNMP-ID:

1.3.64.22

Pfad Telnet:

Status > **WLAN** > **Verschlüsselung**

Ports

In dieser Tabelle erhalten Sie eine Übersicht der angenommenen oder abgewiesenen Verbindungsanfragen je logischer Schnittstelle.

SNMP-ID:

1.46.3

Pfad Telnet:

Status > **IEEE802.1x**

Port

Zeigt die Bezeichnung der Schnittstelle an.

SNMP-ID:

1.46.3.1

Pfad Telnet:

Status > **IEEE802.1x** > **Ports**

Anzahl-Accept

Zeigt die Anzahl der erfolgreichen WPA-Anfragen an dieser Schnittstelle an.

SNMP-ID:

1.46.3.2

Pfad Telnet:

Status > **IEEE802.1x** > **Ports**

Anzahl-Reject

Zeigt die Anzahl der zurückgewiesenen WPA-Anfragen an dieser Schnittstelle an.

SNMP-ID:

1.46.3.3

Pfad Telnet:

Status > **IEEE802.1x** > **Ports**

Anzahl-ReauthMax-erreicht

SNMP-ID:

1.46.3.4

Pfad Telnet:

Status > **IEEE802.1x** > **Ports**

9.8 Adaptive Transmission Power

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, ausgefallene APs im Netzwerk durch Erhöhung der Sendeleistung weiterer APs automatisch auszugleichen.

9.8.1 Adaptive Transmission Power

Die dynamische Sendeleistungsanpassung ist gerade für professionelle Backup-Szenarien in WLAN-Umgebungen unverzichtbar. Fällt ein AP aus, erhöhen die verbleibenden APs automatisch ihre Sendeleistung, sodass eine vollständige WLAN-Abdeckung zu jeder Zeit sichergestellt ist.

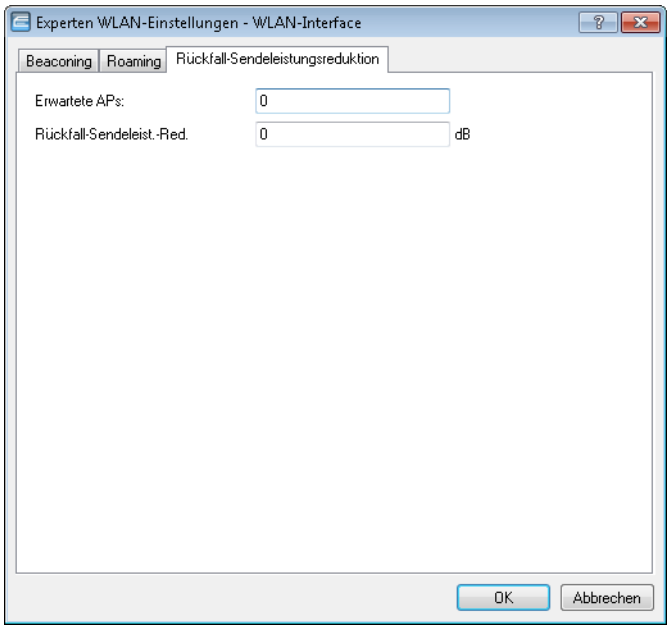
Geben Sie dazu an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden. Solange alle Geräte erreichbar sind, gilt für alle innerhalb dieser Gruppe befindlichen APs eine konfigurierbare Sendeleistungsreduktion (z. B. -6 dB). Dabei überprüfen die APs über das IAPP (Inter Access Point Protocol) ständig die korrekte Anzahl der APs im Netzwerk.

Fällt nun ein AP aus, ergibt die Überprüfung, dass die Anzahl der tatsächlich vorhandenen APs nicht der Anzahl der erwarteten APs entspricht, und die übrigen APs aktivieren die konfigurierte Rückfall-Sendeleistungs-Reduktion (z. B. 0 dB). Sobald der ausgefallene AP wieder erreichbar ist, entspricht bei der Überprüfung die tatsächliche Anzahl der APs der Anzahl der erwarteten Geräte. Die übrigen APs senken die Sendeleistung wieder auf den Standardwert.

Adaptive Transmission Power mit LANconfig konfigurieren

Für die Konfiguration wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **Allgemein**. Im Abschnitt "Erweiterte Einstellungen" klicken Sie auf die Schaltfläche **Experten WLAN-Einstellungen** und wählen ggf. bei APs mit mehreren

WLAN-Schnittstellen die entsprechende Schnittstelle aus. Stellen Sie anschließend auf dem Reiter **Rückfall-Sendeleistungsreduktion** die Anzahl der erwarteten APs und die Rückfall-Sendeleistungs-Reduktion ein.



Erwartete APs

Geben Sie an, wie viele APs sich innerhalb einer Broadcast-Domäne befinden.

Rückfall-Sendeleist.-Red.

Geben Sie hier die Sendeleistungs-Reduktion in dB an, die der AP nutzen soll, falls ein AP aus der konfigurierten Gruppe nicht mehr erreichbar sein sollte.

Die standardmäßige Sendeleistungs-Reduktion konfigurieren Sie unter **Wireless-LAN** > **Allgemein** mit der Schaltfläche **Physikalische WLAN-Einst.** (und ggf. Auswahl der WLAN-Schnittstelle) im Dialog unter **Radio**.

9.8.2 Ergänzungen im Setup-Menü

Redundanz-Einstellungen

In diesem Verzeichnis konfigurieren Sie die dynamische Sendeleistungs-Anpassung beim Ausfall eines APs im Verbund mit mehreren APs.

SNMP-ID:

2.23.20.24

Pfad Telnet:

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

Ifc

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

SNMP-ID:

2.23.20.24.1

Pfad Telnet:

Setup > **Schnittstelle** > **WLAN** > **Redundanz-Einstellungen**

Andere-APs-erwartet

Geben Sie hier die Anzahl der anderen APs an, die sich im AP-Verbund befinden.

Solange alle Geräte erreichbar sind, gilt für alle innerhalb dieser Gruppe befindlichen APs eine konfigurierbare Sendeleistungsreduktion (z. B. -6 dB). Dabei überprüfen die APs über das IAPP (Inter Access Point Protocol) ständig die korrekte Anzahl der APs im Netzwerk.

Fällt nun ein AP aus, ergibt die Überprüfung, dass die Anzahl der tatsächlich vorhandenen APs nicht der Anzahl der erwarteten APs entspricht, und die übrigen APs aktivieren die konfigurierte Rückfall-Sendeleistungs-Reduktion (z. B. 0 dB). Sobald der ausgefallene AP wieder erreichbar ist, entspricht bei der Überprüfung die tatsächliche Anzahl APs der Anzahl der erwarteten Geräte. Die übrigen APs senken die Sendeleistung wieder auf den Standardwert.

SNMP-ID:

2.23.20.24.2

Pfad Telnet:

Setup > **Schnittstelle** > **WLAN** > **Redundanz-Einstellungen**

Mögliche Werte:

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

Backup-Sendeleistungs-Reduktion

Geben Sie hier die Sendeleistungs-Reduktion in dB an, die der AP nutzen soll, falls ein AP aus der konfigurierten Gruppe nicht mehr erreichbar sein sollte.

SNMP-ID:

2.23.20.24.3

Pfad Telnet:

Setup > **Schnittstelle** > **WLAN** > **Redundanz-Einstellungen**

Mögliche Werte:

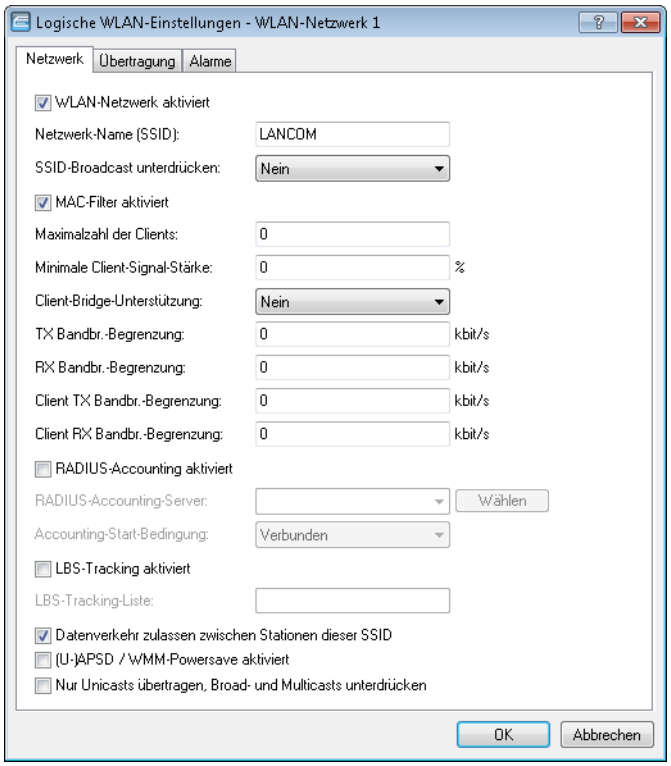
max. 3 Zeichen aus `[0-9]`

9.9 Erweiterte Startbedingungen für WLAN-RADIUS-Accounting

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, die RADIUS-Accounting-Start-Nachricht erst dann zu erzeugen, wenn der Client eine valide IP-Adresse erhalten hat. Somit erhält der RADIUS-Accounting-Server immer eine gültige Framed-IP-Adresse.

Wechseln Sie in LANconfig zu der Ansicht **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen**. Aktivieren Sie anschließend unter dem Reiter „Netzwerk" die Checkbox **RADIUS-Accounting aktiviert**.

Jetzt können Sie die Accounting-Start-Bedingungen über das Dropdown-Menü verändern. Dabei stehen Ihnen folgende Einstellungen zur Verfügung:



Accounting-Start-Bedingung

Im Normalfall sendet der WLAN-Stack eine RADIUS-Accounting-Start-Nachricht, sobald der WLAN-Client verbunden ist. Vielfach hat der WLAN-Client zu diesem Zeitpunkt noch keine IP-Adresse, weil sie u. U. vom DHCP-Server noch nicht zur Verfügung gestellt wurde. Das Attribut `Framed-IP-Address` innerhalb der RADIUS-Accounting-Nachricht kann somit nicht sinnvoll befüllt werden.

Verbunden

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client in den Status „Verbunden" wechselt. Diese Einstellung ist als Standardwert definiert.

Gültige IP-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IP-Adresse erhält (IPv4 oder IPv6).

Gültige IPv4-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv4-Adresse erhält.

Gültige IPv6-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv6-Adresse erhält.

APIPA-Adressen (`169.254.1.0` bis `169.254.254.255` sowie `fe80:`) werden nicht als gültige IP-Adressen anerkannt.

9.9.1 Ergänzungen im Setup-Menü

Accounting-Start-Bedingung

Legen Sie mit diesem Eintrag fest, wann der DHCP-Server einem RADIUS-Accounting-Server den den Beginn des Abrechnungszeitraums meldet.

SNMP-ID:

2.23.20.1.27

Pfad Telnet:

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

Mögliche Werte:

keine

Das Accounting beginnt in dem Moment, in dem der WLAN-Client in den Status „Verbunden" geht.

gueltige-IP-Adresse

Das Accounting beginnt in dem Moment, in dem der WLAN-Client vom DHCP-Server eine gültige IP-Adresse erhalten hat (IPv4 oder IPv6).

gueltige IPv4-Adresse

Das Accounting beginnt in dem Moment, in dem der WLAN-Client vom DHCP-Server eine gültige IPv4-Adresse erhalten hat.

gueltige IPv6-Adresse

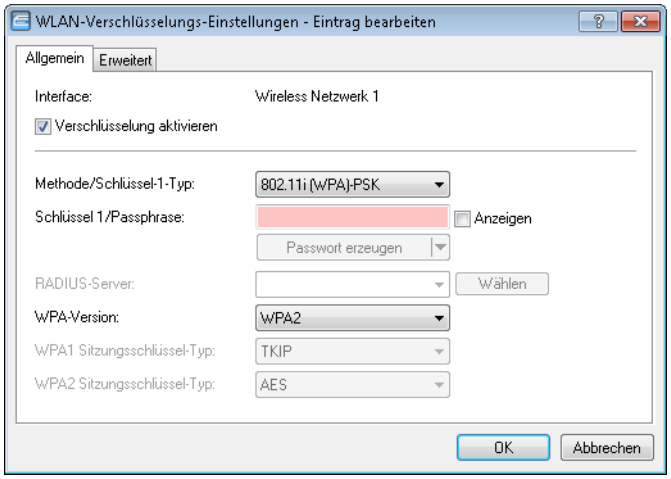
Das Accounting beginnt in dem Moment, in dem der WLAN-Client vom DHCP-Server eine gültige IPv6-Adresse erhalten hat.

Default-Wert:

keine

9.10 Auswahl eines RADIUS-Server-Profils bei Authentifizierung nach 802.1X

Ab LCOS-Version 9.20 steht Ihnen bei Verwendung einer Authentifizierung nach Standard IEEE 802.1X die Angabe eines RADIUS-Server-Profils zur Verfügung.



RADIUS-Server

Wenn Sie unter **Methode/Schlüssel-1-Typ** eine Authentifizierung nach dem Standard IEEE 802.1X auswählen, geben Sie hier das Profil eines RADIUS-Servers an.

9.10.1 Ergänzungen im Setup-Menü

RADIUS-Profile

Wenn Sie eine Authentifizierung nach dem Standard IEEE 802.1X verwenden, geben Sie hier das Profil eines RADIUS-Servers an.

SNMP-ID:

2.23.20.3.21

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

9.11 Konfigurierbare Datenraten pro WLAN-Modul

Ab LCOS-Version 9.20 ist es möglich, die Datenraten pro WLAN-Modul separat zu konfigurieren.

Die folgenden LANCOM-Geräte unterstützen diese Möglichkeit:

- L-151
- L-3xx
- L-4xx
- L-822
- LN-830
- L-13xx
- IAP-xxx
- OAP-xxx
- Alle Geräte der E-Serie

Die aktuell genutzte Datenrate ist im Statusbaum am WLAN-Client und im LANmonitor sichtbar.

9.11.1 Konfigurierbare Datenraten je WLAN-Modul

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client „ankündigt", die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

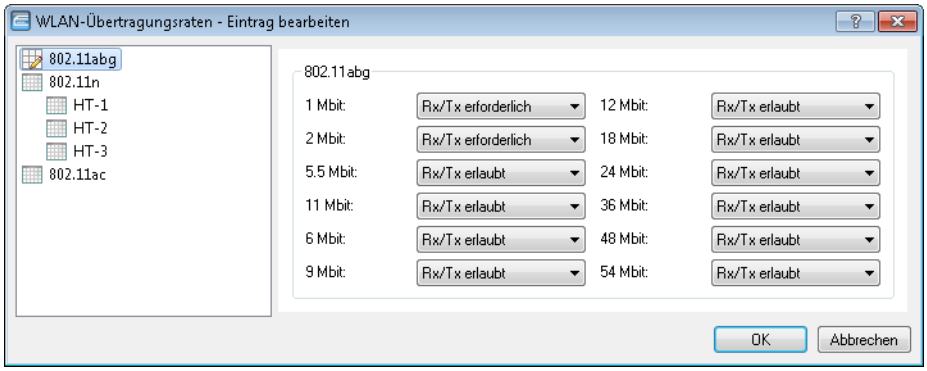
Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr.

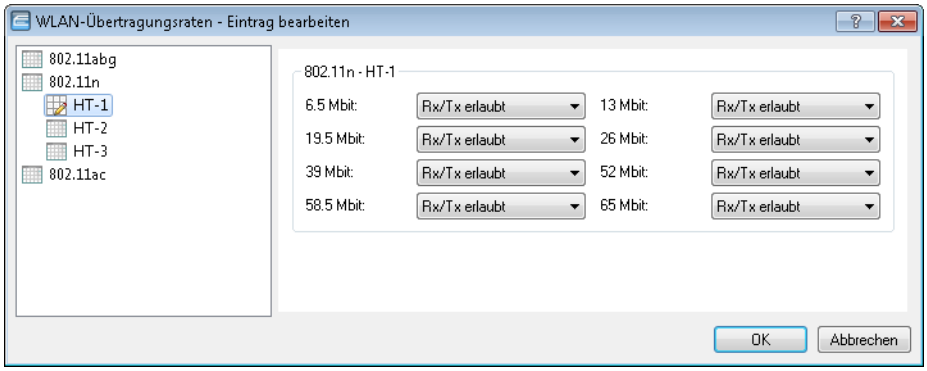
Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

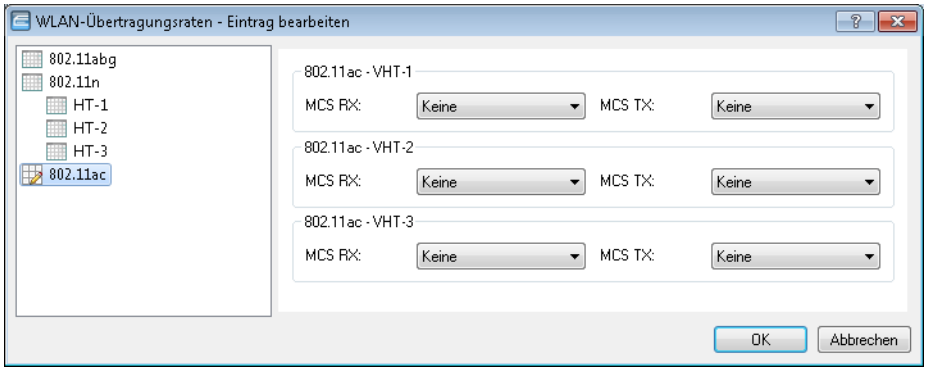
Konfiguration der Datenraten über LANconfig

Um die Datenraten mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** und öffnen Sie im Abschnitt **Erweiterte Einstellungen** den Dialog **WLAN-Übertragungsraten**. LANconfig listet die Einstellungen aller verfügbaren Schnittstellen auf. Um die Einstellung für eine Schnittstelle zu ändern, markieren Sie die entsprechende Schnittstelle und klicken Sie auf **Bearbeiten**.

Wählen Sie links den zu konfigurierenden Standard aus.







Die Konfiguration ist separat möglich für die Standards

- 802.11abg
- 802.11n
  - HT-1
  - HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Je nach Standard sind für jede Übertragungsrate je SSID und P2P-Strecke explizit die folgenden Einstellungen verfügbar:

Rx/Tx erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx erlaubt

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx erlaubt

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Deaktiviert

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

MCS-9/8/7

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

Keine

Bei 802.11ac-Modulen ist die jeweilige Stream-Variante für die entsprechende Datenrichtung deaktiviert.

9.11.2 Ergänzungen im Setup-Menü

Ratenauswahl

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client „ankündigt“, die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr, was unter Umständen Airtime sparen kann.

Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

In diesem Verzeichnis konfigurieren Sie diese Datenraten.

SNMP-ID:

2.23.20.25

Pfad Telnet:

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

1M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.1

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx-erforderlich

2M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.2

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx-erforderlich

Ifc

Dieser Eintrag zeigt die zu konfigurierende Schnittstelle an.

SNMP-ID:

2.23.20.25.3

Pfad Telnet:

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

5,5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.4

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

11M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.6

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

6M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.8

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

9M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.9

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

12M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.10

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

18M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.11

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

24M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.12

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

36M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.13

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

48M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.14

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

54M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.15

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-6.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.28

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-13M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.29

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-19.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.30

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-26M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.31

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.32

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-52M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.33

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-58.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.34

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-1-65M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.35

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-13M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.36

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-26M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.37

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.38

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-52M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.39

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-78M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.40

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-104M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.41

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-117M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.142

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-2-130M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.43

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-19.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.44

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-39M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.45

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-58.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.46

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-78M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.47

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-117M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.48

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-156M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.49

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-175.5M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.50

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt" an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt" an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

HT-3-195M

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

SNMP-ID:

2.23.20.25.51

Pfad Telnet:

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

Mögliche Werte:

nein

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

Rx/Tx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt" und „erforderlich" in Beacons und Probe Responses an und nutzt sie selber auch zur Kommunikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx

Der AP kündigt dem Client die Rate als „unterstützt“ an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx-erforderlich

Der AP kündigt dem Client die Rate als „unterstützt“ und „erforderlich“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx

Der AP kündigt dem Client die Rate als „unterstützt“ an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Default-Wert:

Rx/Tx

VHT-1-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.105

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

VHT-1-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.106

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

VHT-2-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.115

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

VHT-2-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.116

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

VHT-3-Max-Tx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.125

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

VHT-3-Max-Rx-MCS

Hier konfigurieren Sie, wie der AP diese Datenrate für diese Schnittstelle behandeln soll.

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

SNMP-ID:

2.23.20.25.126

Pfad Telnet:

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

Mögliche Werte:

None
MCS7
MCS8
MCS9

Default-Wert:

MCS9

9.12 Max. Länge des AP-Gerätenamens in WLC-Konfig auf 64 Zeichen erhöht

Ab LCOS-Version 9.20 ist es möglich, AP-Gerätenamen in der Access-Points-Tabelle mit bis zu 64 Zeichen anzugeben.

9.12.1 Ergänzungen im Setup-Menü

Name

Name des APs im Managed-Modus.

SNMP-ID:

2.37.1.4.2

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

9.13 LANconfig: Dialog für WLAN-Verschlüsselung modifiziert

In LCOS-Version 9.20 hat sich der Dialog für die Konfiguration der WLAN-Verschlüsselungs-Einstellungen geändert.

Die WLAN-Verschlüsselungs-Einstellungen erreichen Sie nun in LAnconfig unter **Wireless-LAN** > **Verschlüsselung**.

10 WLAN-Management

10.1 WIDS-Integration in WLC

Ab LCOS-Version 9.20 verwalten WLCs WIDS-Profile zur Konfiguration von Wireless Intrusion Detection Einstellungen auf den verwalteten APs.

10.1.1 Wireless Intrusion Detection System mit WLC-Profilen verwalten

Das Wireless Intrusion Detection System (WIDS) in LCOS-Geräten überprüft die verfügbaren WLANs anhand umfangreicher, definierter Grenzwerte. Damit Sie im Falle eines Angriffes rechtzeitig reagieren können, meldet das WIDS Angriffe über E-Mail, SYSLOG oder SNMP-Traps.

Die Erkennung von Angriffen erfolgt dabei auf Basis von bekannten oder gleichartigen Mustern.

Beachten Sie bitte, dass die Erkennung von Angriffsmustern (Heuristik) auch zu Fehlalarmen („False Positive“) führen kann!

Um auch in umfangreichen Netzwerkumgebungen die WIDS-Einstellungen auf allen APs komfortabel über einen WLC zu verwalten, nutzen Sie dort WIDS-Profile, die Sie den APs zuordnen.

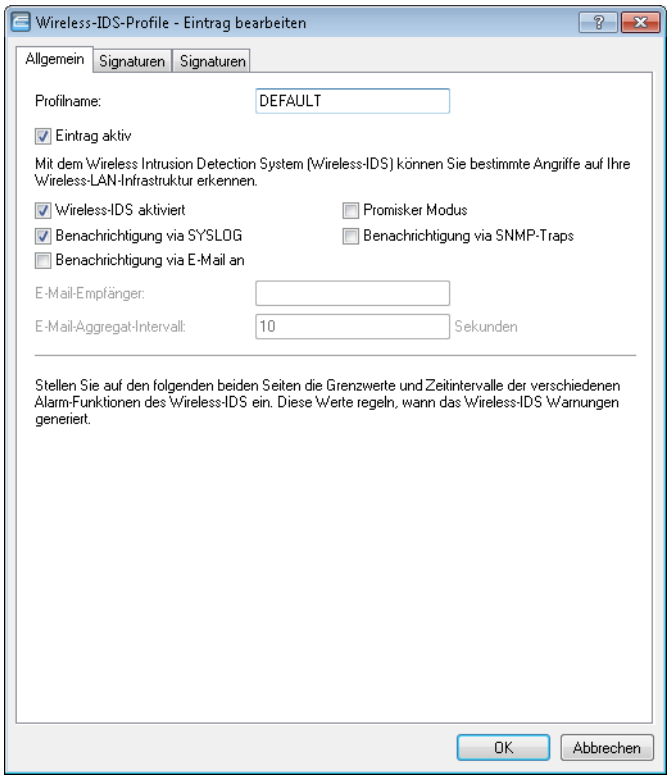
In der Standardeinstellung existiert bereits ein WIDS-Profil mit der Bezeichnung „DEFAULT“, das mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt ist.

WIDS-Profile mit LANconfig verwalten

Wechseln Sie in die Ansicht **WLAN-Controller** > **Profile** und öffnen Sie den Dialog **Erweiterte Profile**.

Öffnen Sie den Dialog **Wireless-IDS-Profile**. Es existiert bereits ein Profil „DEFAULT“, das mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt ist. Um dieses Profil zu bearbeiten, klicken Sie auf **Bearbeiten**. Um ein neues WIDS-Profil anzulegen, klicken Sie auf **Hinzufügen**.

Auf dem Reiter **Allgemein** konfigurieren Sie die allgemeinen Profil-Einstellungen.



Profilname

Vergeben Sie einen eindeutigen Profilnamen.

Eintrag aktiv

Aktivieren oder deaktivieren Sie dieses Profil.

Wireless-IDS aktiviert

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

Promisker Modus

Bei aktiviertem Modus („promiscuous mode“) empfängt der AP auch Pakete, die an andere Netzwerkteilnehmer adressiert sind. Dies betrifft z. B. Datenpakte, die keine Broadcasts sind deren Ziel-MAC-Adresse von der MAC-Adresse des APs abweicht.

Dieser Umstand stellt sicher, dass einige der weiter unten genannten Angriffstypen erkannt werden können. Allerdings beeinträchtigt dieser Modus die Performance des Gerätes. Daher wird die Frame Aggregation bei Aktivierung des Promiscous Modes automatisch deaktiviert.

Benachrichtigung via SYSLOG

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

Die generierte SYSLOG-Meldung besitzt den Severity Level „INFO“ und enthält den Zeitpunkt, die betroffene Schnittstelle sowie den Auslöser (Art des Angriffes und überschrittener Grenzwert).

Benachrichtigung via SNMP-Traps

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

Benachrichtigung via E-Mail an

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

E-Mail-Empfänger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiviert ist.

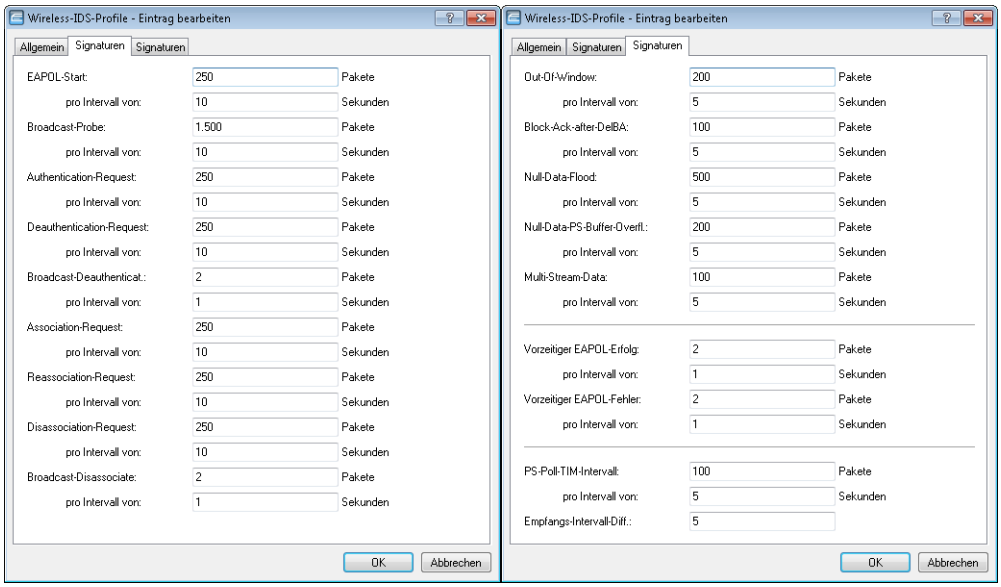
Das Feld muss eine gültige E-Mail-Adresse enthalten.

E-Mail-Aggregat-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

In den beiden Ansichten **Signatur** konfigurieren Sie die Grenzwerte und Zeitintervalle (Datenpakete pro Sekunde) der verschiedenen Alarm-Funktionen des WIDS. Diese Werte regeln, wann das WIDS Warnungen generiert.



Die Angabe von Grenzwerten und Zeitintervallen für die folgenden Angriffs-Szenarien ist möglich:

- EAPOL-Start
- Broadcast-Probe
- Authentication-Request
- Deauthentication-Request (*)
- Broadcast-Deauthenticate
- Association-Request
- Reassociation-Request
- Disassociation-Request (*)
- Broadcast-Disassociate
- Out-Of-Window
- Block-Ack-after-DelBA
- Null-Data-Flood
- Null-Data-PS-Buffer-Overflow
- Multi-Stream-Data

- Vorzeitiger EAPOL-Erfolg (*)
- Vorzeitiger EAPOL-Fehler (*)
- PS-Poll-TIM-Intervall
- Empfangs-Intervall-Differenz

Alle Felder sind bereits mit für das jeweilige Angriffs-Szenario typischen Werten vorbelegt.

(*): Nur bei aktivem Promiscuous Mode.

WIDS-Statistiken mit LANmonitor einsehen

10.1.2 Ergänzungen im Setup-Menü

Name

In diesem Verzeichnis konfigurieren Sie die Wireless-IDS-Profile für die verwalteten APs.

SNMP-ID:

2.37.1.248

Pfad Telnet:

Setup > **WLAN-Management**

Name

Enthält den eindeutigen Namen dieses WIDS-Profils.

SNMP-ID:

2.37.1.248.1

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

Max. 31 Zeichen aus

Aktiv

Legen Sie fest, ob dieses Profil aktiv oder inaktiv ist. Inaktive Profile überträgt der WLC nicht zu einem AP.

SNMP-ID:

2.37.1.248.2

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

ja
nein

Default-Wert:

ja

EAPOLStartCounterLimit

Definieren Sie die Anzahl der EAPOL-Start-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.3

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

EAPOLStartCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die EAPOL-Start-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.4

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

ProbeBroadCounterLimit

Definieren Sie die Anzahl der Broadcast-Probe-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.5

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

1500

ProbeBroadCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Probe-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.6

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

DeauthenticateBroadCounterLimit

Definieren Sie die Anzahl der Broadcast-Deauthenticate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.7

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

2

DeauthenticateBroadCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Broadcast-Deauthenticate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.8

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

1

DeauthenticateCounterLimit

Definieren Sie die Anzahl der Deauthentication-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.9

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

DeauthenticateCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Deauthentication-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.10

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

AssociateReqCounterLimit

Definieren Sie die Anzahl der Association-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.11

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

AssociateReqCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Association-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.12

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

ReAssociateReqCounterLimit

Definieren Sie die Anzahl der Reassociation-Request-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.13

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

ReAssociateReqCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Reassociation-Request-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.14

Pfad Telnet:

Setup > **WLAN-Management** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

AuthenticateCounterLimit

Definieren Sie mit diesem Eintrag das Maximum der Login-Versuche, bei dessen Überschreitung das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.15

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

AuthenticateCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Anzahl der Loginversuche ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.16

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

DisAssociateCounterLimit

Definieren Sie die Anzahl der Disassociate-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.17

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

250

DisAssociateCounterInterval

Definieren Sie das Zeitintervall in Sekunden, innerhalb dessen die Disassociate-Datenpakete ihren gesetzten Grenzwert überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.18

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

IDS-Operational

Aktiviert oder deaktiviert das Wireless Intrusion Detection System (WIDS).

SNMP-ID:

2.37.1.248.19

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

nein

Das WIDS ist deaktiviert.

ja

Das WIDS ist aktiviert.

Default-Wert:

ja

Syslog-Operational

Aktiviert oder deaktiviert die WIDS-Meldungen über SYSLOG.

SNMP-ID:

2.37.1.248.20

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

nein

WIDS-Meldungen erfolgen nicht über SYSLOG.

ja

WIDS-Meldungen erfolgen über SYSLOG.

Default-Wert:

ja

SNMPTraps-Operational

Aktiviert oder deaktiviert die SNMP-Traps für WIDS-Meldungen.

SNMP-ID:

2.37.1.248.21

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

nein

Das Senden und Empfangen von SNMP-Traps ist deaktiviert.

ja

Das Senden und Empfangen von SNMP-Traps ist aktiviert.

Default-Wert:

nein

E-Mail

Aktiviert oder deaktiviert die WIDS-Meldungen über E-Mail.

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

SNMP-ID:

2.37.1.248.22

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

nein

Die WIDS-Meldungen über E-Mail sind deaktiviert.

ja

Die WIDS-Meldungen über E-Mail sind aktiviert.

Default-Wert:

nein

E-Mail-Empfaenger

Geben Sie einen E-Mail-Empfänger an, wenn die Benachrichtigung über E-Mail aktiv ist.

Das Feld muss eine gültige E-Mail-Adresse enthalten.

SNMP-ID:

2.37.1.248.23

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

leer

E-Mail-Zusammenfassungs-Intervall

Legen Sie die Verzögerung in Sekunden vor dem Versenden einer E-Mail fest, in der das WIDS nach dem Eintreffen eines ersten Wireless-IDS-Ereignisses weitere Ereignisse sammelt.

Diese Funktion verhindert, dass eine Flut von Angriffen eine E-Mail-Flut verursacht.

SNMP-ID:

2.37.1.248.24

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

10

BlockAck-Out-Of-Window-Counter

Mit diesem Eintrag definieren Sie die Anzahl der Out-Of-Window-Ereignisse, bei deren Überschreitung WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.26

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

200

BlockAck-Out-Of-Window-Counter-Time

Geben Sie einen Zeitraum in Sekunden an, in dem Out-Of-Window-Ereignisse zu zählen sind.

SNMP-ID:

2.37.1.248.27

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

BlockAck-Frames-Rx-After-D-E-L-B-A-Counter

Mit diesem Eintrag definieren Sie die Anzahl der Frames-Rx-After-D-E-L-B-A-Ereignisse, bei deren Überschreitung WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.28

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

100

BlockAck-Frames-Rx-After-D-E-L-B-A-Counter-Time

Geben Sie einen Zeitraum in Sekunden an, in dem Frames-Rx-After-D-E-L-B-A-Ereignisse zu zählen sind.

SNMP-ID:

2.37.1.248.29

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

Null-Data-DoS-Counter

Definieren Sie die Anzahl der Null-Data-Datenpakete, bei deren Überschreitung je Zeitintervall das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.31

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Null-Data-DoS-Counter-Time

Geben Sie einen Zeitraum in Sekunden an, in dem Null-Data-DoS-Ereignisse zu zählen sind.

SNMP-ID:

2.37.1.248.32

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

Null-Data-P-S-Buffer-Overflow-Counter

Mit diesem Eintrag definieren Sie die Anzahl der für Null-Data-P-S-Buffer-Overflow-Ereignisse, bei deren Überschreitung WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.34

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

200

Null-Data-P-S-Buffer-Overflow-Counter-Time

Geben Sie einen Zeitraum in Sekunden an, in dem Null-Data-P-S-Buffer-Overflow-Ereignisse zu zählen sind.

SNMP-ID:

2.37.1.248.35

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

P-S-Poll-T-I-M-Interval-Diff

Definieren Sie ein Empfangsintervall, dessen gesetzten Grenzwert P-S-Poll-T-I-M-Interval-Datenpakete überschreiten müssen, damit das WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.37

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

P-S-Poll-T-I-M-Interval-Diff-Counter

Mit diesem Eintrag legen Sie den Grenzwert für PS-Poll-TIM-Intervall-Pakete pro Intervall fest.

SNMP-ID:

2.37.1.248.38

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

100

PS-Poll-T-I-M-Interval-Diff-Counter-Time

Definieren Sie mit diesem Eintrag das Zeitintervall in Sekunden, in dem PS-Poll-TIM-Intervall-Pakete gezählt werden..

SNMP-ID:

2.37.1.248.39

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

S-M-P-S-Mul-Stream-Frame-Counter

Mit diesem Eintrag definieren Sie die Anzahl der für S-M-P-S-Mul-Stream-Frame-Ereignisse, bei deren Überschreitung WIDS einen Angriff meldet.

SNMP-ID:

2.37.1.248.41

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

100

S-M-P-S-Mul-Stream-Frame-Counter-Time

Geben Sie einen Zeitraum in Sekunden an, in dem S-M-P-S-Mul-Stream-Frame-Ereignisse zu zählen sind.

SNMP-ID:

2.37.1.248.42

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

5

DisAssociateBroadCounterLimit

Mit diesem Eintrag legen Sie den Grenzwert für Broadcast-Disassociate-Pakete pro Intervall fest, bevor WIDS einen Alarm meldet.

SNMP-ID:

2.37.1.248.45

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

2

DisAssociateBroadCounterInterval

Definieren Sie das Zeitintervall in Sekunden, in dem Broadcast-Disassociate-Pakete gezählt werden.

SNMP-ID:

2.37.1.248.46

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

1

EAPOLSuccessCounterLimit

Enthält den Grenzwert für EAPOL-Erfolgs-Pakete pro Intervall.

SNMP-ID:

2.37.1.248.47

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

2

EAPOLSuccessCounterInterval

Dieser Eintrag enthält das Zeitintervall in Sekunden, in dem EAPOL-Erfolgs-Pakete gezählt werden.

SNMP-ID:

2.37.1.248.48

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

1

EAPOLFailureCounterLimit

Enthält den Grenzwert für EAPOL-Fehler-Pakete pro Intervall.

SNMP-ID:

2.37.1.248.49

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

2

EAPOLFailureCounterInterval

Dieser Eintrag enthält das Zeitintervall in Sekunden, in dem EAPOL-Fehler-Pakete gezählt werden.

SNMP-ID:

2.37.1.248.50

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

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

Default-Wert:

1

Promiscuous-Mode

Mit diesem Eintrag aktivieren oder deaktivieren Sie den Promiscuous-Mode.

SNMP-ID:

2.37.1.248.51

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-IDS**

Mögliche Werte:

nein

Der Promiscuous-Mode ist deaktiviert.

ja

Der Promiscuous-Mode ist aktiviert.

Default-Wert:

nein

10.1.3 Ergänzungen im Status-Menü

Alarme

Dieser Eintrag enthält die Statuswerte der WIDS-Alarme.

Eine Änderung löst eine SNMP-Trap „88" aus. Geht die Verbindung zu einem AP in dieser Liste verloren, löscht LCOS alle Einträge für diesen AP aus dieser Liste.

SNMP-ID:

1.73.248.2

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS**

MAC-Addresse

Dieser Eintrag enthält die MAC-Addresse des APs, der den WIDS-Alarm ausgelöst hat.

SNMP-ID:

1.73.248.2.1

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

Ifc

Dieser Eintrag die Schnittstelle an, an der der WIDS-Alarm ausgelöst wurde.

SNMP-ID:

1.73.248.2.2

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

Signatur

Dieser Eintrag enthält die Signatur des WIDS-Alarms.

SNMP-ID:

1.73.248.2.3

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

Name

Dieser Eintrag enthält den Namen des APs.

SNMP-ID:

1.73.248.2.4

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

Zaehler

Dieser Eintrag enthält die Anzahl der WIDS-Alarme.

SNMP-ID:

1.73.248.2.5

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

Alarm-Status

Dieser Eintrag enthält Status des WIDS-Alarms.

SNMP-ID:

1.73.248.2.6

Pfad Telnet:

Status > **WLAN-Management** > **Wireless-IDS** > **Alarme**

IDS-Operational

Dieser Eintrag zeigt an, ob an dieser Schnittstelle WIDS aktiviert ist.

SNMP-ID:

1.73.9.2.37

Pfad Telnet:

Status > **WLAN-Management** > **AP-Status** > **Active-Radios**

10.2 IAPP bei bestehendem CAPWAP-Tunnel automatisch abschalten

Ab LCOS-Version 9.20 deaktiviert ein WLC auf den verwalteten APs automatisch das IAPP, sobald ein CAPWAP-Verwaltungstunnel zwischen APs und WLC existiert.

10.3 Mehrere AutoWDS-Profile konfigurierbar

Ab LCOS-Version 9.20 verwalten WLCs mehrere AutoWDS-Profile.

10.3.1 Ergänzungen im Setup-Menü

AutoWDS-Profile

Diese Tabelle enthält die Parameter für AutoWDS-Profile, die Sie über das WLAN-Profil den einzelnen APs zuweisen, um den Aufbau vermaschter Netze zu realisieren. AutoWDS-Profile gruppieren die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und der AutoWDS-Basisnetze.

In einfachen Netzwerk-Umgebungen genügt die Verwendung des voreingestellten AutoWDS-Profils „DEFAULT". Beim Einsatz mehrerer unterschiedlicher AutoWDS-Profile gilt es, die folgenden Rahmenbedingungen zu beachten:

- APs unterschiedlicher AutoWDS-Profile lassen sich nicht automatisch oder manuell untereinander verbinden.
- Die maximale Anzahl an AutoWDS-Profilen entspricht der maximal möglichen Anzahl der WLAN-Profile im WLC.
- Sie können den Eintrag für das vorhandene AutoWDS-Profil „DEFAULT" weder löschen noch umbenennen.
- Die Rollout-SSID für zwei unterschiedliche AutoWDS-Profile muss unterschiedlich sein. Ebenso muss die Verlinkung von einem AutoWDS-Profil zu einem WLAN-Profil eindeutig und einmalig sein. Ist dies nicht der Fall, meldet der WLC einen Profilfehler.
- Jedes AutoWDS-Profil verwendet jeweils eine eigene SSID. Dadurch verringert sich die Zahl der für die Profile zur Verfügung stehenden SSIDs. Bei mehrfacher Nutzung einer SSID meldet der WLC einen Profilfehler.
- Es gibt nur ein WLC-TUNNEL-AUTOWDS-Interface im WLC. Die einzelnen Rollout-SSIDs nutzen somit auf dem WLC das gleiche Interface als Endpunkt. Die Kommunikation der WLAN-Clients untereinander während der Integration ist per Default unterbunden.

- Bei aktivierter Express-Integration spielt die Rollout-SSID für unkonfigurierte WLAN-Clients zunächst keine Rolle. Somit kann während einer Express-Integration ein AP über den AP eines anderen AutoWDS-Profils seine Konfiguration vom WLC beziehen, erhält dabei jedoch dann lediglich sein AutoWDS-Profil und die manuell konfigurierten Topologie-Einträge bzw. P2P-Strecken. Es erfolgt keine Generierung einer automatischen P2P-Konfiguration, wenn die AutoWDS-Profile zweier beteiligter APs nicht übereinstimmen. Wurde in diesem Fall lediglich ein AutoWDS-Profil übertragen, fällt der AP nach gewohnter Zeit in den Scan-Modus zurück, besitzt dann allerdings seine zugewiesene AutoWDS-Rollout-SSID und wird sich im nächsten Schritt an entsprechenden AutoWDS-APs (passend zu seinem Profil) integrieren.

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.

Sie können den Eintrag für das vorhandene AutoWDS-Profil „DEFAULT" weder löschen noch umbenennen.

SNMP-ID:

2.37.1.15.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

max. 15 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.

Verschiedene AutoWDS-Profile dürfen sich nicht auf das gleiche WLAN-Profil beziehen.

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 dieses AutoWDS-Profil 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-Rollout

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

Default-Wert:

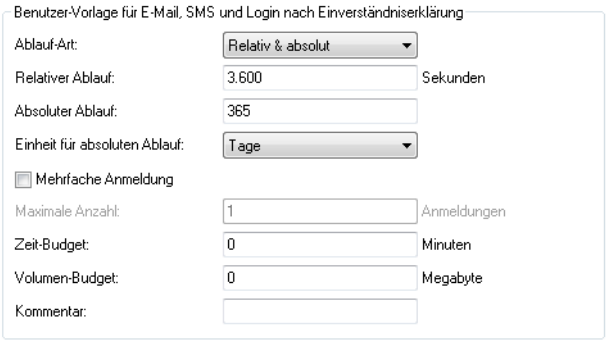
leer

11 Public Spot

11.1 Kürzere Einheiten für absolute Ablaufzeit

Ab LCOS-Version 9.20 ist es möglich, die Gültigkeit von Public Spot Vouchern mit kürzeren Zeiteinheiten (Tage, Stunden, Minuten) zu gestalten. Dies ist gerade in Szenarien mit hoher Kundenfrequenz bei gleichzeitig kurzer Verweildauer von Vorteil.

Um kürzere Ablaufzeiten für Public Spots mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.



Einheit für absoluten Ablauf

Um kürzere Ablaufzeiten zu konfigurieren, wählen Sie im Dropdown-Menü die Einheit für den absoluten Ablauf aus. Passen Sie ggf. den Wert des absoluten Ablaufes an.

11.2 Circuit-ID als Public Spot-URL-Redirect-Variable

Ab LCOS-Version 9.20 haben Sie mit der Redirect-Variable "%d" die Möglichkeit, die Willkommensseite auf angemeldeten Clients je nach Standort zu verändern.

%d

Geben Sie den URL-Parameter "%d" als Circuit-ID an, z. B. `http://ipaddress/?circuit=%d&nas=%i`. Diese Variable ersetzt das Public Spot Modul mit der Circuit-ID, die im DHCP-Request des Clients erkannt wurde.

Dafür ist es erforderlich, dass auf dem AP "DHCP Snooping" so konfiguriert ist, dass der AP die Circuit-ID in der Public Spot-Stationstabelle des WLCs abfragen kann.

Somit ist es möglich, die Public Spot-Willkommensseite auf den angemeldeten Clients je nach Standort zu verändern.

11.3 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, über die Web-API Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anzulegen.

11.3.1 Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Bei der Verwendung von Smart Ticket erhält der Benutzer im RADIUS-Server des lokalen Public Spot-Gateways einen entsprechenden Public Spot-Account.

Sind jedoch mehrere Public Spot-Gateways im Einsatz und soll nur ein Gateway die Benutzerkonten in seinem RADIUS-Server vorhalten, wird der Public Spot-Account bei der Verwendung von Smart Ticket auf dem zentralen RADIUS-Server angelegt. Dazu ist es notwendig, das entfernte Public Spot-Gateway im LCOS-Menübaum unter **Setup** > **Public-Spot-Modul** > **Authentifizierungs-Module** festzulegen.

Sofern kein entferntes Public Spot-Gateway definiert wird, werden Public Spot-Benutzerkonten auf dem lokalen Public Spot-Gateway angelegt.

11.3.2 Ergänzungen im Setup-Menü

Radius-Server

In diesem Menü nehmen Sie die Einstellungen zum Anlegen von Public Spot-Benutzerkonten auf dem RADIUS-Server des entfernten Public-Spot-Gateways vor.

SNMP-ID:

2.24.41.5

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

Anbieter

Über diesen Eintrag definieren Sie das RADIUS-Server-Profil aus der Public Spot-Anbietertabelle, das den RADIUS-Server des entfernten Public Spot-Gateways referenziert.

SNMP-ID:

2.24.41.5.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Radius-Server**

Mögliche Werte:

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

Default-Wert:

leer

Name

Über diesen Eintrag definieren Sie, mit welchem Administratorkonto Benutzerkonten auf dem entfernten Public Spot-Gateway angelegt werden.

SNMP-ID:

2.24.41.5.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Radius-Server**

Mögliche Werte:

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

Default-Wert:

leer

Passwort

Über diesen Eintrag definieren Sie das Passwort des oben angegebenen Administratorkontos.

SNMP-ID:

2.24.41.5.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Radius-Server**

Mögliche Werte:

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

Default-Wert:

leer

11.4 PMS-Template: AGBs akzeptieren

Die Anmeldung an einem Public Spot ist je nach Konfiguration abhängig davon, ob vorher die Nutzungsbedingungen zu bestätigen sind. Bei der Kombination verschiedener Anmeldemöglichkeiten (z. B. über gespeicherte Reservierungsdaten oder SMS-Authentifizierung) ist die Bestätigung der Nutzungsbedingungen bisher nicht klar zuzuordnen.

Ab LCOS-Version 9.20 wurde die Darstellung der Anmeldeseite bei Verwendung einer Kombination von Anmeldeverfahren überarbeitet.

11.5 Felder im Setup-Wizard "Public-Spot-Benutzer verwalten" ausblenden

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, Tabellenspalten im Assistenten "Public-Spot-Benutzer verwalten" dauerhaft auszublenden.

11.5.1 Felder mit WEBconfig ausblenden

Im Setup-Assistenten "Public-Spot-Benutzer verwalten" haben Sie über die Schaltfläche **Spalte zeigen/verstecken** die Möglichkeit, Tabellenspalten ein- oder auszublenden. Diese Änderungen sind jedoch nur temporär. Nach einem Seiten-Refresh oder bei einer neuen Sitzung werden die ausgeblendeten Spalten wieder angezeigt.

Um bestimmte Felder dauerhaft zu verbergen, wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**. Standardmäßig werden alle Felder angezeigt. Blenden Sie bestimmte Felder aus, um z. B. das Zeit-Budget zu verbergen, bleiben diese Spalten sowohl im Assistenten selbst als auch im Dropdown-Menü unter der Schaltfläche **Spalte zeigen/verstecken** nach einem erneuten Aufrufen der Seite verborgen.

Um einen authentisierten Public Spot-Benutzer zu löschen, müssen die Spalten "Rufende-Station-Id-Maske" und "Gerufene-Station-Id-Maske" im Assistenten sichtbar sein. Nicht authentisierte Benutzer hingegen lassen sich auch löschen, wenn beide Spalten ausgeblendet sind.

Beachten Sie bitte, dass ausgeblendete Felder beim Betätigen der Schaltfläche **Drucken** nicht mit ausgegeben werden. Die Ausgabe als CSV-Datei beinhaltet dagegen alle Daten. Sie haben jedoch die Möglichkeit, die Schaltfläche **Als CSV speichern** zu verbergen. Wechseln Sie dazu im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **CSV-Export-verstecken**. Wählen Sie "Ja" und speichern Sie Ihre Eingabe.

Ergänzungen im Setup-Menü

Zeige-Ablauf-Typ

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Ablauf-Typ" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.12

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Ablauf-Typ" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Ablauf-Typ" aus.

Default-Wert:

ja

Zeige-Abs-Ablauf

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "absoluter Ablauf" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.13

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "absoluter Ablauf" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "absoluter Ablauf" aus.

Default-Wert:

ja

Zeige-Rel-Ablauf

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "relativer Ablauf" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.14

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "relativer Ablauf" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "relativer Ablauf" aus.

Default-Wert:

ja

Zeige-Zeit-Budget

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Zeit-Budget" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.15

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Zeit-Budget" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Zeit-Budget" aus.

Default-Wert:

ja

Zeige-Volumen-Budget

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Volumen-Budget-MByte" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.16

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Volumen-Budget-MByte" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Volumen-Budget-MByte" aus.

Default-Wert:

ja

Zeige-Case-Sensitiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Case-Sensitiv" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.17

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Case-Sensitiv" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Case-Sensitiv" aus.

Default-Wert:

ja

Zeige-aktiv

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "aktiv" im Setup-Wizard zu verbergen.

SNMP-ID:
2.24.44.18

Pfad Telnet:
Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "aktiv" angezeigt.
nein
Der Setup-Wizard blendet die Spalte "aktiv" aus.

Default-Wert:

ja

Zeige-Tx-Limit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Tx-Limit" für die maximale Sende-Bandbreite im Setup-Wizard zu verbergen.

SNMP-ID:
2.24.44.19

Pfad Telnet:
Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Tx-Limit" angezeigt.
nein
Der Setup-Wizard blendet die Spalte "Tx-Limit" aus.

Default-Wert:

ja

Zeige-Rx-Limit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Rx-Limit" für die maximale Empfangs-Bandbreite im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.20

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Rx-Limit" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Rx-Limit" aus.

Default-Wert:

ja

Zeige-Rufende-Station

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Rufende-Station-Id-Maske" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.21

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Rufende-Station-Id-Maske" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Rufende-Station-Id-Maske" aus.

Default-Wert:

ja

Zeige-Gerufene-Station

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Gerufene-Station-Id-Maske" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.22

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Gerufene-Station-Id-Maske" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Gerufene-Station-Id-Maske" aus.

Default-Wert:

ja

Zeige-Online-Zeit

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Online-Zeit" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.23

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Online-Zeit" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Online-Zeit" aus.

Default-Wert:

ja

Zeige-Traffic

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Traffic (Rx / Tx Kbyte)" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.24

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Traffic (Rx / Tx Kbyte)" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Traffic (Rx / Tx Kbyte)" aus.

Default-Wert:

ja

Zeige-Status-Spalte

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Status" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.25

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Im Setup-Wizard wird die Spalte "Status" angezeigt.

nein

Der Setup-Wizard blendet die Spalte "Status" aus.

Default-Wert:

ja

Zeige-Mac-Adresse

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "Mac-Adresse" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.26

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "Mac-Adresse" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "Mac-Adresse" aus.

Default-Wert:

ja

Zeige-Ip-Adresse

Dieser Eintrag bietet Ihnen die Möglichkeit, die Spalte "IP-Adresse" im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.27

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja
Im Setup-Wizard wird die Spalte "IP-Adresse" angezeigt.

nein
Der Setup-Wizard blendet die Spalte "IP-Adresse" aus.

Default-Wert:

ja

11.6 Redirect für HTTPS-Verbindungen umschaltbar

Um die Last auf Public Spot-Gateways gering zu halten, ist ab LCOS-Version 9.20 das Umleiten von HTTPS-Verbindungen unangemeldeter Clients wahlweise abschaltbar.

11.6.1 Redirect für HTTPS-Verbindungen

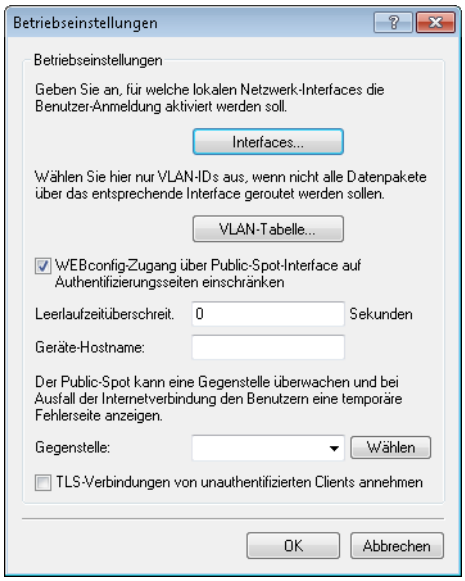
Versucht ein nicht angemeldeter Client über eine Schnittstelle, für die der Public Spot aktiv ist, via HTTPS auf eine Webseite zuzugreifen, wird diese Verbindungsanfrage an das Public Spot-Gateway selber umgeleitet, um dem Nutzer die Anmeldeseite zu präsentieren (ist bei HTTP auch der Fall). In diesem Fall wird dem Benutzer normalerweise eine Zertifikatswarnung seines Browsers präsentiert, da Name oder IP der ursprünglich angesurften Seite nicht dem Namen oder der IP des Public Spot entspricht. Um dies und die Erzeugung von erhöhter Last durch die aufgebauten HTTPS-/TLS-Verbindungen auf dem Public Spot Gateway zu verhindern, können Sie mit dieser Einstellung der Verbindungsaufbau über HTTPS für unangemeldete Clients verhindern.

Ist der Client einmal angemeldet, findet keinerlei Umleitung mehr statt und es können beliebig HTTP- und HTTPS-Verbindungen durch den Client aufgebaut werden.

Heutzutage übliche Clients führen eine "Captive Portal Detection" via HTTP durch. Dabei wird versucht, auf eine bestimmte URL via HTTP zuzugreifen, um das Vorhandensein einer Anmeldeseite (durch Public Spot oder andere Lösungen) zu überprüfen. Dieser Mechanismus wird durch das Ausschalten der HTTPS-Umleitung nicht beeinflusst, da die Erkennung normalerweise über HTTP stattfindet.

Ist es in einem Public Spot-Szenario jedoch nicht vorgesehen, dass unbekannte WLAN-Clients eine Verbindungsanfrage auch über HTTP ausführen sollen, würde dieser wirkungslose HTTPS-Redirect das Public Spot-Gateway unnötig belasten. Entsprechend ist es möglich, diesen HTTPS-Redirect prinzipiell zu deaktivieren. In diesem Fall würde der Benutzer vom Browser eine leere Seite erhalten.

Das Redirect für HTTPS-Verbindungen konfigurieren Sie im LANconfig unter **Public-Spot** > **Server** > **Betriebseinstellungen**.



Um das HTTPS-Redirect einzuschalten, aktivieren Sie die Option **TLS-Verbindungen von unauthentifizierten Clients annehmen**. In der Standardeinstellung ist diese Option deaktiviert.

11.6.2 Ergänzungen im Setup-Menü

TLS-Verbindungen-umleiten

Mit dieser Option bestimmen Sie, ob der Public Spot HTTPS-Verbindungen für unauthentifizierte Clients auf sich selber umleitet. Ist diese Option deaktiviert, können unauthentifizierte Clients keine HTTPS-Verbindungen aufbauen.

SNMP-ID:

2.24.51

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

Nein

Der Public-Spot führt kein HTTPS-Redirect für nicht authentifizierte WLAN-Clients aus.

Ja

Der Public-Spot führt ein HTTPS-Redirect für nicht authentifizierte WLAN-Clients aus.

Default-Wert:

Nein

11.7 Ausgabe des Bandbreitenprofils auf dem Voucher

Ab LCOS-Version 9.20 ist die Ausgabe des nutzerspezifischen Bandbreitenprofils auf dem Voucher möglich. Die Eingabe erfolgt im Voucher-Template in Form dieser neuen Vorlagen-Bezeichner:

BANDWIDTHPROFNAME

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet das Bandbreiten-Profil, mit dem der Benutzer verknüpft ist.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

RXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Empfangsbandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

TXBANDWIDTH

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die maximale Sendebandbreite des Bandbreitenprofils.

Dieser Bezeichner ist ab LCOS-Version 9.18 RU1 verfügbar. Templates mit diesem Bezeichner sind für LCOS-Versionen vor 9.18 RU1 nicht geeignet.

11.8 Template-Vorschau

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, sich eine Vorschau der hochgeladenen Public Spot-Templates anzeigen zu lassen.

11.8.1 Template-Vorschau über WEBconfig

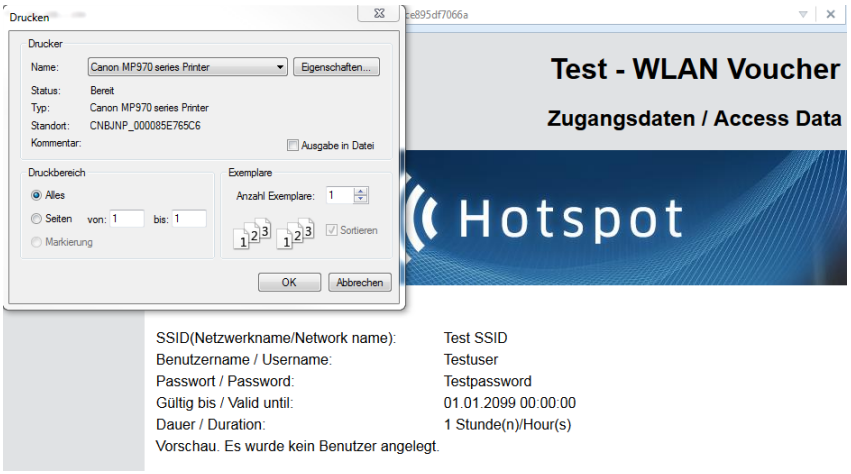
Um Änderungen an den Public Spot-Vorlagen verfolgen zu können, wechseln Sie in WEBconfig zur Ansicht **Extras** > **Public-Spot Template-Vorschau**.

Wählen Sie ein Template zum Anzeigen aus der Liste aus.

Das ausgewählte Template wird im gleichen Browserfenster angezeigt. Über die "Zurück"-Funktion Ihres Browsers gelangen Sie zum WEBconfig zurück.

Einige Templates beinhalten einen Javascript-Code. Dieser Code wird beim Aufrufen des jeweiligen Templates ausgeführt. So enthält das Template "Voucher-Seite" z. B. den Code zum Ausdrucken, sobald die Seite angezeigt wird.

Auf dieser Seite sind Testdaten hinterlegt. Es wird jedoch kein entsprechender Benutzer angelegt. Sie haben also die Möglichkeit, das Template zu testen und auszudrucken.



Sofern kein Template vorliegt oder gefunden werden kann, erscheint eine Fehlermeldung im WEBconfig.

11.9 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

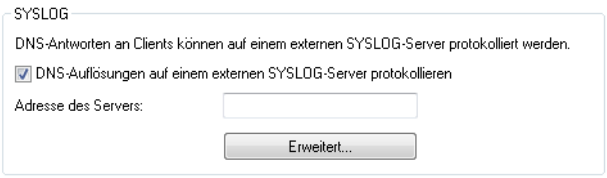
Ab LCOS-Version 9.20 ist im Syslog die Dokumentation von DNS-Anfragen und -Antworten für die von Clients aufgerufenen Domains möglich.

11.9.1 DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Der DNS-Server in LANCOM-Geräten löst DNS-Anfragen von Clients auf. Eine Übersicht darüber, welche Clients welche Namen angefragt und welche Antworten sie erhalten haben, steht im Syslog zur Verfügung.

Das Syslog des Routers/APs selbst kann nicht genutzt werden. Es ist daher erforderlich, einen externen Syslog-Server einzutragen.

Die Konfiguration des DNS-Loggings erfolgt im LANconfig unter **IPv4** > **DNS** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Markieren Sie diese Option, um das DNS-Logging zu aktivieren.

Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter **Meldungen** > **Allgemein** im Abschnitt **SYSLOG**) erfolgt das DNS-Logging.

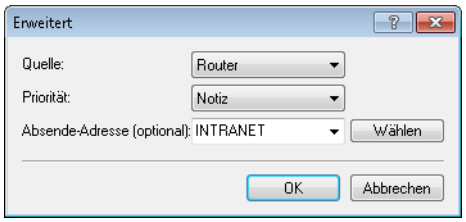
Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

```
PACKET_INFO: DNS for <IP-Address>, TID {Hostname}: Ressource-Record
```

Adresse des Servers

Enthält die IP-Adresse oder den DNS-Namen des zu nutzenden SYSLOG-Servers.

Die Einstellungen hinter der Schaltfläche **Erweitert** beeinflussen die Inhalte der SYSLOG-Meldungen.



Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

Priorität

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

Absende-Adresse (optional)

Enthält die Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

11.9.2 Ergänzungen im Setup-Menü

Syslog

In diesem Verzeichnis konfigurieren Sie die SYSLOG-Protokollierung von DNS-Anfragen.

SNMP-ID:

2.17.20

Pfad Telnet:

Setup > **DNS**

DNS-Aufloesungen-loggen

Diese Option aktiviert oder deaktiviert (Default-Einstellung) den Versand von SYSLOG-Meldungen bei DNS-Anfragen.

Dieser Schalter ist unabhängig vom globalen Schalter im Syslog-Modul unter **Setup** > **SYSLOG** > **Aktiv**. D. h., wenn Sie hier die Option zur Aufzeichnung der DNS-Anfragen aktivieren, sendet der DNS-Server im Gerät auch bei global deaktiviertem SYSLOG-Modul die entsprechenden SYSLOG-Meldungen an einen SYSLOG-Server.

Jede DNS-Auflösung (`ANSWER`-Record oder `ADDITIONAL`-Record) erzeugt jeweils eine SYSLOG-Meldung mit dem Aufbau `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Ressource-Record`.

Dabei haben die Parameter die folgenden Bedeutungen:

- Die `TID` (Transaction-ID) enthält einen 4-stelligen Hexadezimal-Code.
- Der `{Hostname}` ist nur dann Bestandteil der Meldung, wenn der DNS-Server ihn ohne DNS-Anfrage auflösen kann (wie auch im Firewall-Log).
- Die `Ressource-Record` besteht aus drei Teilen: Der Anfrage, dem Typ bzw. der Klasse und der IP-Auflösung (z. B. `www.mydomain.com STD A resolved to 193.99.144.32`)

SNMP-ID:

2.17.20.1

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

nein

Deaktiviert die Aufzeichnung der DNS-Anfragen und -Antworten.

ja

Aktiviert die Aufzeichnung der DNS-Anfragen und -Antworten.

Default-Wert:

nein

Log-Server-Adresse

Die Log-Server-Adresse enthält den zu nutzenden Syslog-Server in Form des entsprechenden DNS-Namens oder einer IP-Adresse.

Die Angabe der IP-Adressen `127.0.0.1` und `::1` ist generell nicht erlaubt, um so die Nutzung eines externen Servers zu erzwingen.

SNMP-ID:

2.17.20.2

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

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

Log-Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

SNMP-ID:

2.17.20.3

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

System
Login
Systemzeit
Konsole-Login
Verbindungen
Accounting
Administration
Router

Default-Wert:

Router

Log-Level

Enthält die Priorität, die in den SYSLOG-Meldungen erscheint.

SNMP-ID:

2.17.20.4

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

Notfall
Alarm
Kritisch
Fehler
Warnung
Hinweis
Info
Debug

Default-Wert:

Hinweis

Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem SYSLOG-Server 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 Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet.

SNMP-ID:

2.17.20.5

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

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

Besondere Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
„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

Facility

Zuordnung der Quellen zu bestimmten Facilities.

SNMP-ID:

2.22.3.2

Pfad Telnet:

Setup > **SYSLOG** > **Facility-Mapper**

Mögliche Werte:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

IP-Adresse

Enthält die IP-Adresse des SYSLOG-Servers. Die Angabe ist möglich als IPv4- bzw. IPv6-Adresse oder als DNS-Name.

SNMP-ID:

2.22.2.7

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

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

11.10 Schutz vor Brute Force-Angriffen

Ab Version 9.20 bietet LCOS Schutz vor Brute Force-Angriffen im Public Spot.

11.10.1 Schutz vor Brute Force-Angriffen

Brute-Force-Angriffe sind die bekanntesten Angriffe auf ein Netzwerk. Diese Art von Angriff besteht darin, eine Menge an möglichen Passwörtern innerhalb kurzer Zeit auszuprobieren, bis das richtige Passwort gefunden wird. Ein möglicher Schutz vor Brute-Force-Angriffen besteht darin, nach einem oder mehreren aufeinander folgenden fehlgeschlagenen Eingabeversuchen die Zeit bis zur nächsten möglichen Eingabe zu verzögern.

Den Schutz vor Brute-Force-Angriffen konfigurieren Sie mit LANconfig unter **Public-Spot** > **Server** im Abschnitt **Brute-Force-Schutz**.

Sperren nach

Bestimmen Sie, nach wie vielen Fehlversuchen die Eingabesperre für weitere Versuche eingreifen soll.

Sperrdauer

Bestimmen Sie, für wie lange die Eingabesperre gelten soll.

Über die Konsole zeigt der Befehl `show pbbruteprotector` den aktuellen Status des Brute-Force-Schutzes:

`show pbbruteprotector`

Zeigt eine Übersicht über alle am Public Spot angemeldeten MAC-Adressen.

`show pbbruteprotector [MAC-Adresse[ MAC-Adresse[ ...]]]`

Die Angabe einer oder mehrerer durch Leerzeichen getrennter MAC-Adressen zeigt den Status der jeweiligen MAC-Adressen an.

Die Angabe von MAC-Adressen erfolgt in den Formaten `11:22:33:44:55:66`, `11-22-33-44-55-66` oder `112233445566`.

11.10.2 Ergänzungen im Setup-Menü

Brute-Force-Schutz

Dieses Menü enthält die Einstellungen für den Brute-Force-Schutz des Public Spot.

SNMP-ID:

2.24.49

Pfad Telnet:

Setup > **Public-Spot-Modul**

Max-Login-Versuche

Bestimmen Sie, nach wievielen Fehlversuchen die Loginsperre für weitere Versuche eingreifen soll.

SNMP-ID:

2.24.49.1

Pfad Telnet:

Setup > **Public-Spot-Module** > **Brute-Force-Schutz**

Mögliche Werte:

max. 3 Zeichen aus `[0-9]`

Default-Wert:

10

Sperrzeit-In-Minuten

Bestimmen Sie, für wie lange die Loginsperre des Brute-Force-Schutzes gelten soll.

SNMP-ID:

2.24.49.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Brute-Force-Schutz**

Mögliche Werte:

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

Default-Wert:

60

Entsperren-Check-In-Sekunden

Bestimmen Sie, in welchem Abstand der AP den Ablauf einer Loginsperre für eine MAC-Adresse prüft.

SNMP-ID:

2.24.49.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Brute-Force-Schutz**

Mögliche Werte:

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

Default-Wert:

60

Entsperren

Mit dieser Aktion entfernen Sie die Loginsperre für eine MAC-Adresse. Geben Sie als Parameter eine oder mehrere durch Leerzeichen getrennte MAC-Adressen ein.

Die Angabe von MAC-Adressen erfolgt in den Formaten `11:22:33:44:55:66`, `11-22-33-44-55-66` oder `112233445566`.

SNMP-ID:

2.24.49.4

Pfad Telnet:

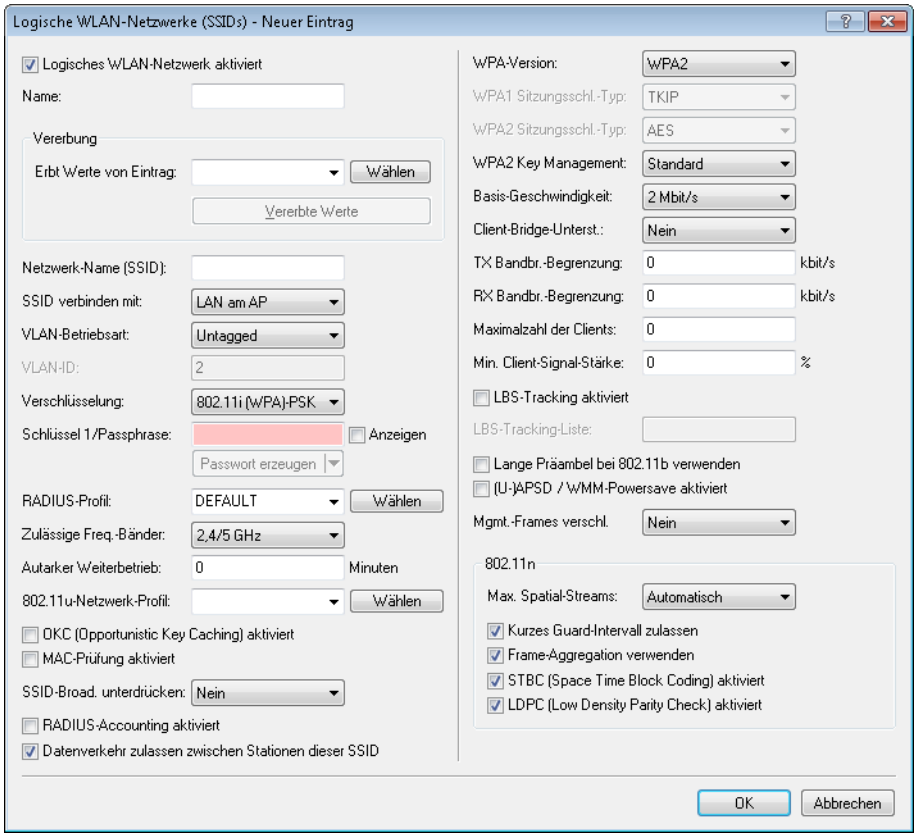
Setup > **Public-Spot-Modul** > **Brute-Force-Schutz**

12 LANCOM Location Based Services (LBS)

12.1 Dynamische und persistente Tracking-Listen von WLAN Clients

Ab LCOS-Version 9.20 konfigurieren Sie die LBS-Tracking-Listen auch über LANconfig.

Im WLC erfolgt die Konfiguration der LBS-Tracking-Liste über **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke**.



LBS-Tracking aktiviert

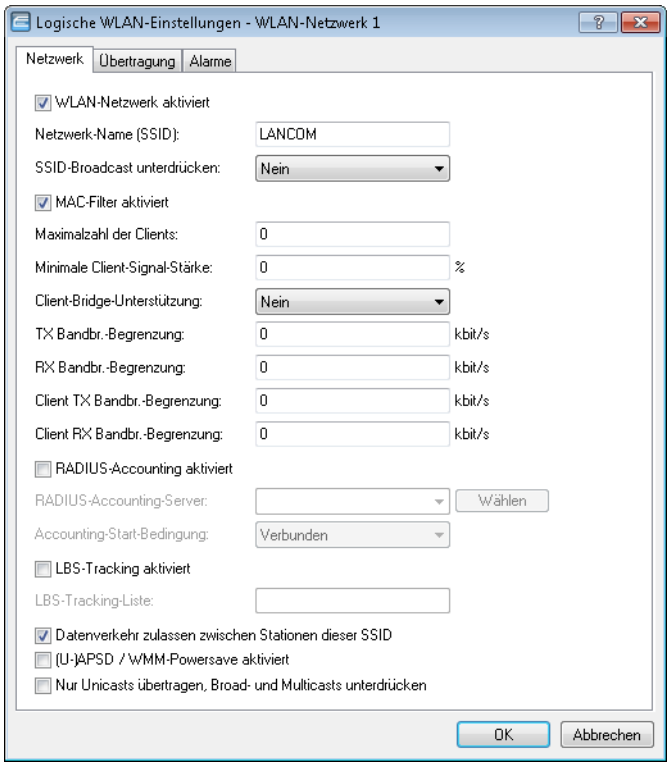
Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Im AP erfolgt die Konfiguration der LBS-Tracking-Liste über **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** auf dem Tab **Netzwerke**.



LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

12.1.1 LBS-Tracking-Listen von Public Spot-Benutzern verwenden

APs und WLCs bieten die Möglichkeit, angemeldete Public Spot-Benutzer in Listen aufzunehmen und an einen LBS-Server (Location Based Service) zu melden.

Diese Funktion konfigurieren Sie für APs und WLCs im LANconfig unter **Public-Spot** > **Benutzer** im Abschnitt **LBS-Tracking**.

LBS-Tracking aktiviert

Bestimmen Sie hier, ob der LBS-Server die am Public Spot angemeldeten Benutzer nachverfolgen darf.

LBS-Tracking-Liste

Name der LBS-Tracking-Liste, die der AP oder WLC an den LBS-Server sendet.

12.1.2 Ergänzungen im Setup-Menü

LBS-Tracking

Bestimmen Sie hier, ob der LBS-Server die am Public Spot angemeldeten Benutzer nachverfolgen darf.

SNMP-ID:

2.24.38

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein
ja

Default-Wert:

nein

LBS-Tracking-Liste

Name der LBS-Tracking-Liste.

SNMP-ID:

2.24.39

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

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

Default-Wert:

leer

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

SNMP-ID:

2.37.1.1.47

Pfad Telnet:

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

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **LBS-Tracking**

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

Default-Wert:

leer

LBS-Tracking

Dieser Eintrag aktiviert oder deaktiviert das LBS-Tracking für diese SSID.

SNMP-ID:

2.23.20.1.25

Pfad Telnet:

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

Mögliche Werte:

nein

LBS-Tracking ist deaktiviert.

ja

LBS-Tracking ist aktiviert.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

SNMP-ID:

2.23.20.1.26

Pfad Telnet:

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

Mögliche Werte:

Name aus **Setup** > **WLAN** > **Netzwerk** > **LBS-Tracking**

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

Default-Wert:

leer

13 Voice over IP - VoIP

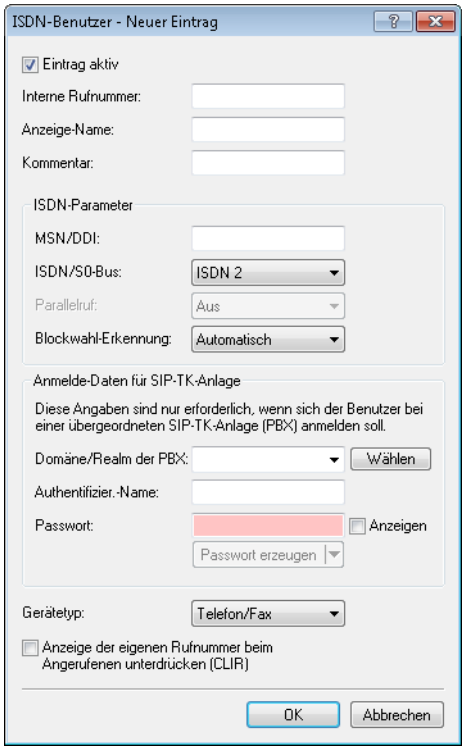
13.1 Parallelruf im ISDN signalisieren

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, einen Ruf parallel auf beiden ISDN-Bussen zu signalisieren.

13.1.1 Parallelruf im ISDN signalisieren

Auf LANCOM-Geräten, die die All-IP Option unterstützen, kann ein Parallelruf aktiviert werden. Wenn Sie diese Funktion verwenden, erfolgt eine Signalisierung auf beiden ISDN-Leitungen (ISDN 1 & ISDN 2). Das Gespräch wird dort geführt, wo zuerst abgehoben wird.

Aktivieren Sie den Parallelruf über **Voice Call Manager** > **Benutzer** > **ISDN-Benutzer**.



Wählen Sie im Abschnitt **ISDN-Parameter** unter **ISDN/S0-Bus** die Option „ISDN 1 & ISDN 2“ und aktivieren Sie anschließend den **Parallelruf** mit der Einstellung „Ein“.

13.1.2 Ergänzungen im Setup-Menü

Parallelruf

Aktivieren oder deaktivieren Sie den Parallelruf.

SNMP-ID:

2.33.3.2.2.13

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **User**

Mögliche Werte:

nein

Parallelruf ist deaktiviert.

ja

Parallelruf ist aktiviert.

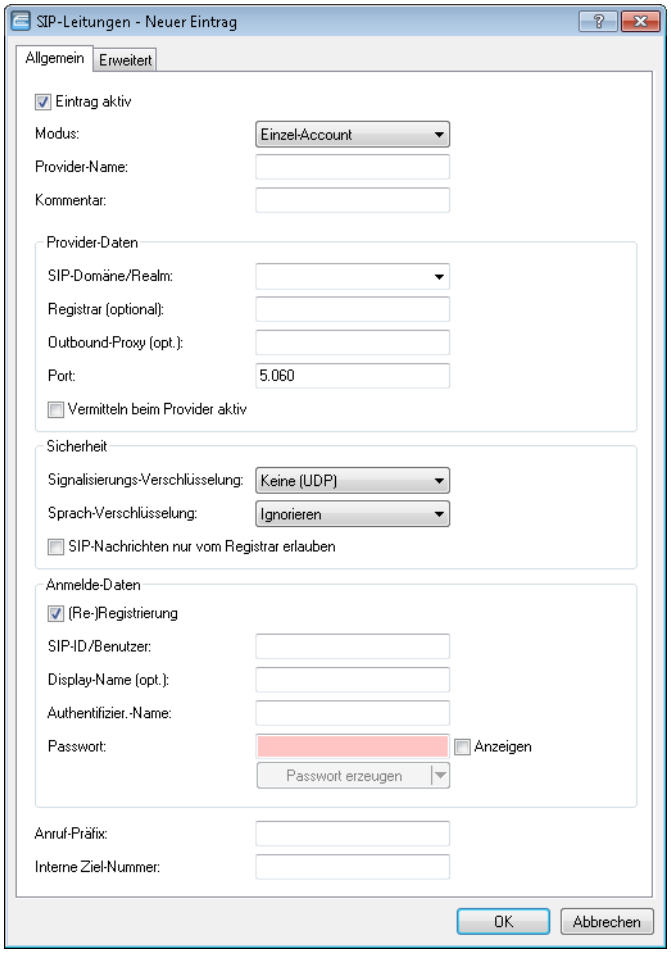
Default-Wert:

nein

13.2 VoSIP-Unterstützung im Voice Call Manager

Ab Version 9.20 unterstützt LCOS Voice over Secure IP (VoSIP). Mit dieser Funktion ist es Ihnen möglich, Signalisierungs- und Sprachdaten zu verschlüsseln. Auf folgenden Geräten können Sie VoSIP einsetzen:

- LANCOM 1783 / 1784
- Alle LANCOM mit All-IP Option



Signalisierungs-Verschlüsselung

Diese Einstellung legt das Protokoll zur Signalisierungs-Verschlüsselung (SIP/SIPS) bei der Kommunikation mit dem Provider fest.

Signalisierungs-Verschlüsselung	
UDP	Alle SIP Pakete werden verbindungslos übertragen. Die meisten Anbieter unterstützen diese Einstellung.
TCP	Alle SIP Pakete werden verbindungsorientiert übertragen. Das Gerät baut eine TCP Verbindung zum Provider auf und erhält diese für die Dauer der Registrierung aufrecht. Spezielle Anbieter, wie z. B. Anbieter von Trunk Anschlüssen, unterstützen oder erzwingen diese Einstellung.
TLS	Gleiche Übertragungsweise wie bei TCP, allerdings werden alle SIP Pakete zusätzlich durch eine Verschlüsselung bis zum Provider geheim gehalten.

Sprach-Verschlüsselung

Diese Einstellung legt fest, ob und wie Sprachdaten (RTP/SRTP) bei der Kommunikation mit dem Provider verschlüsselt werden.

Sprach-Verschlüsselung	
Ablehnen	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist nicht verschlüsselt.
Ignorieren	Eine Verschlüsselung wird bei ausgehenden Gesprächen nicht angeboten. Eingehende Gespräche mit einem Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nicht verschlüsselt.
Bevorzugt	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne einen Verschlüsselungsvorschlag werden akzeptiert. Der Sprachkanal ist nur dann verschlüsselt, wenn auch die Gegenstelle eine Verschlüsselung unterstützt.
Erzwingen	Eine Verschlüsselung wird bei ausgehenden Gesprächen angeboten. Eingehende Gespräche ohne Verschlüsselungsvorschlag werden abgelehnt. Der Sprachkanal ist entweder verschlüsselt oder wird nicht aufgebaut.

Sollen Sprachdaten verschlüsselt übertragen werden, ist es erforderlich, dass auch die Signalisierung über einen verschlüsselten Kanal erfolgt. Beachten Sie aber bitte, dass die Nutzung von SRTP keine Ende-zu-Ende Verschlüsselung garantiert.

13.2.1 Ergänzungen im Setup-Menü

Transport

Legen Sie mit diesem Eintrag fest, mit welchem Protokoll die Datenströme verschlüsselt werden.

SNMP-ID:

2.33.4.1.1.28

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

UDP
TCP
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

UDP

SRTP

Legen Sie mit diesem Eintrag fest, wie SRTP (Secure Real-Time Transport Protocol) behandelt wird.

SNMP-ID:

2.33.4.1.1.29

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

Ablehnen
Ignorieren
Bevorzugt
Erzwungen

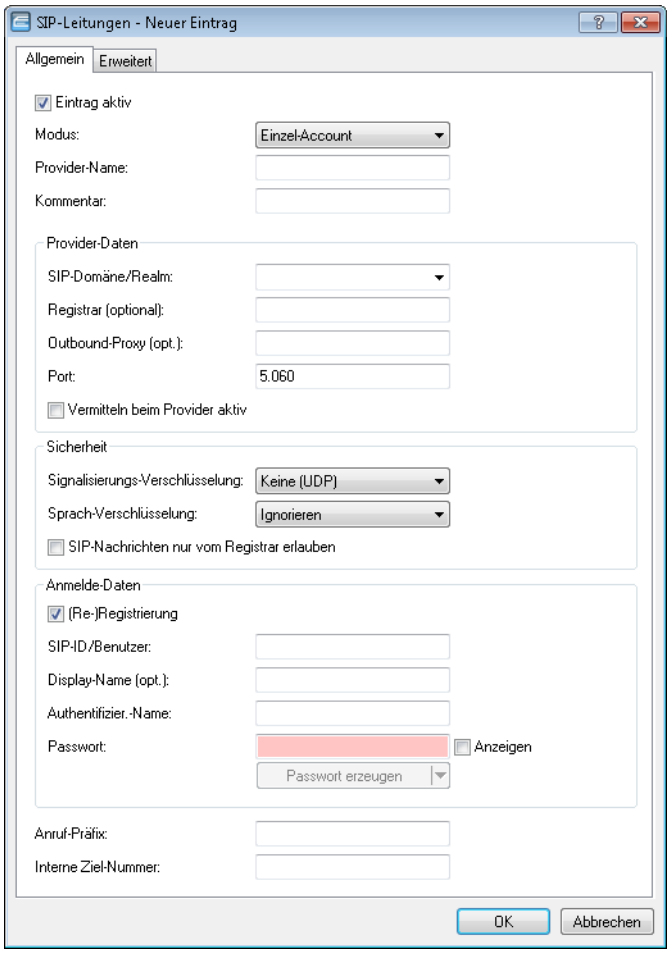
Default-Wert:

Ignorieren

13.3 SIP über TCP im Voice Call Manager

Ab LCOS-Version 9.20 ist es möglich, für SIP-Leitungen das SIP Protokoll auch über TCP zu nutzen. Ob TCP oder UDP verwendet werden soll, legen Sie pro Leitung fest.

Die Konfiguration erfolgt in LANconfig über **VoIP-Call-Manager** > **Leitungen** mit einem Klick auf die Schaltfläche **SIP-Leitungen**. Im Abschnitt "Sicherheit" legen Sie die Signalisierungs-Verschlüsselung fest.



Signalisierungs-Verschlüsselung

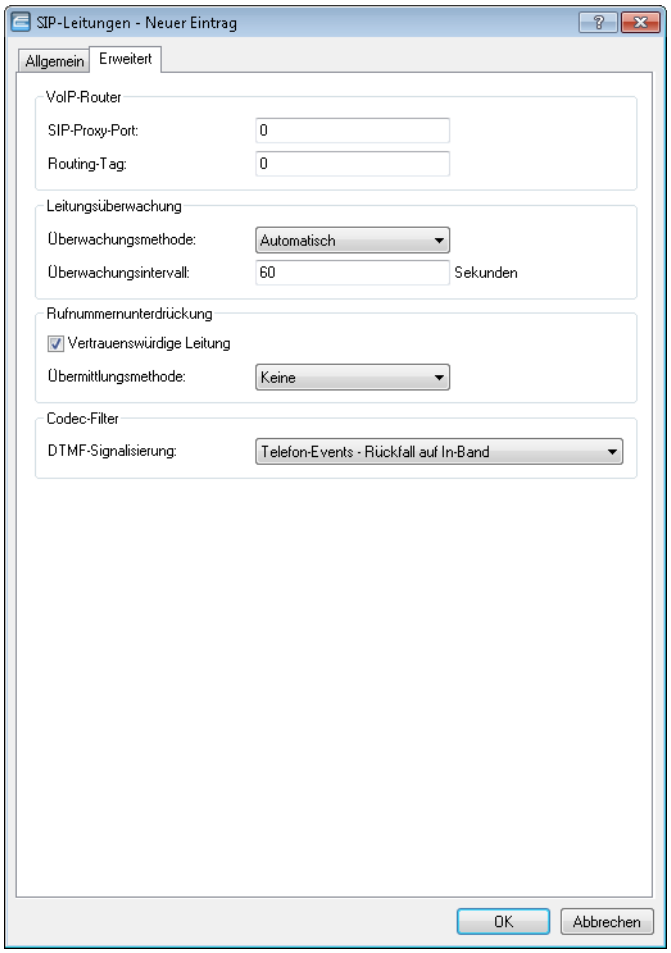
Diese Einstellung legt das Protokoll zur Signalisierungs-Verschlüsselung (SIP/SIPS) bei der Kommunikation mit dem Provider fest.

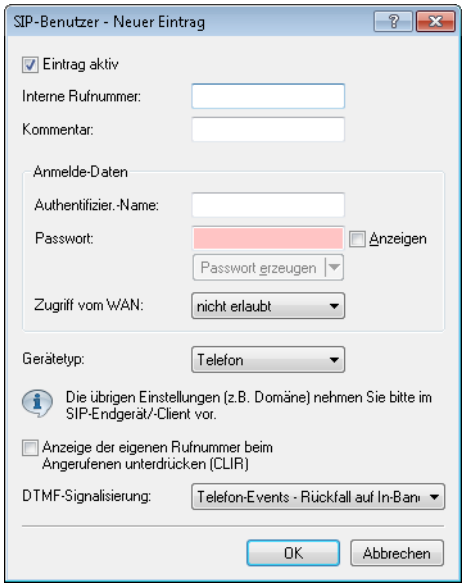
Signalisierungs-Verschlüsselung	
UDP	Alle SIP Pakete werden verbindungslos übertragen. Die meisten Anbieter unterstützen diese Einstellung.
TCP	Alle SIP Pakete werden verbindungsorientiert übertragen. Das Gerät baut eine TCP Verbindung zum Provider auf und erhält diese für die Dauer der Registrierung aufrecht. Spezielle Anbieter, wie z. B. Anbieter von Trunk Anschlüssen, unterstützen oder erzwingen diese Einstellung.
TLS	Gleiche Übertragungsweise wie bei TCP, allerdings werden alle SIP Pakete zusätzlich durch eine Verschlüsselung bis zum Provider geheim gehalten.

13.4 DTMF-Signalisierung bei All-IP-Verbindungen

Ab LCOS-Version 9.20 erfolgt die Übertragung von DTMF-Tönen über All-IP-Verbindungen mit auswählbarer DTMF-Signalisierung.

Die Einstellung der DTMF-Signalisierung ist sowohl über die Konfiguration der SIP-Leitung als auch des SIP-Benutzers möglich.





DTMF-Signalisierung

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

Nur In-Band (im Audio)

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

Nur SIP-Info

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Telefon-Events - Rückfall auf In-Band (Default)

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

Telefon-Events - Rückfall auf SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

13.4.1 Ergänzungen im Setup-Menü

DTMF-Methode

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

SNMP-ID:

2.33.3.1.1.20

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **SIP-User** > **Users**

Mögliche Werte:

Inband

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

SIP-INFO

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

RTP-Event

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

RTP-Event/SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Call-Aufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

Default-Wert:

RTP-Event

DTMF-Methode

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

SNMP-ID:

2.33.4.1.1.27

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

Inband

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

SIP-INFO

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

RTP-Event

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Callaufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

RTP-Event/SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Callaufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

Default-Wert:

RTP-Event

DTMF-Methode

Je nach Anforderung genügt es ggf. nicht, DTMF-Töne „inband" zu übertragen, wenn ein SIP-Empfänger diese Töne nicht erkennt. In diesem Fall ist die Konfiguration einer anderen DTMF-Übertragungsart für All-IP-Verbindungen möglich.

SNMP-ID:

2.33.4.2.1.20

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-PBX** > **PBX**

Mögliche Werte:

Inband

Die Übertragung erfolgt in Form von DTMF-Tönen (G.711) innerhalb des RTP-(Sprach-)Streams.

SIP-INFO

Die Übertragung der DTMF-Töne erfolgt „out-of-band" als SIP-Info-Nachricht mit den Parametern `Signal` und `Duration` (gem. RFC 2976). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

RTP-Event

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Callaufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf Inband-Übertragung nach G.711.

RTP-Event/SIP-Info

Die Übertragung der DTMF-Töne erfolgt als speziell markierte Events innerhalb des RTP-Streams (gem. RFC 4733). Eine parallele Übertragung als G.711-Töne erfolgt nicht.

Falls die Verhandlung beim Callaufbau mit dem Kommunikationspartner im SDP keine `telephone-event`-Signalisierung enthält, erfolgt ein Rückfall auf eine Übertragung als SIP-Info-Nachricht.

Default-Wert:

RTP-Event

13.5 RTP Port-Bereich im Voice Call Manager konfigurierbar

Ab LCOS-Version 9.20 haben Sie die Möglichkeit, den Quell-Port-Bereich der RTP Pakete im Voice Call Manager zu konfigurieren, um den reibungslosen Betrieb hinter einer Firewall sicherzustellen.

13.5.1 Ergänzungen im Setup-Menü

RTP-Port-Start

In diesem Feld legen Sie den ersten verfügbaren RTP Port des RTP Port-Bereiches fest.

SNMP-ID:

2.33.2.21

Pfad Telnet:

Setup > **Voice-Call-Manager** > **General**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Dynamische Auswahl, sofern RTP-Port-Ende auch Wertden "0" gesetzt hat.

RTP-Port-Ende

In diesem Feld legen Sie den letzten verfügbaren RTP Port des RTP Port-Bereiches fest.

SNMP-ID:

2.33.2.22

Pfad Telnet:

Setup > **Voice-Call-Manager** > **General**

Mögliche Werte:

0 … 65535

Default-Wert:

0

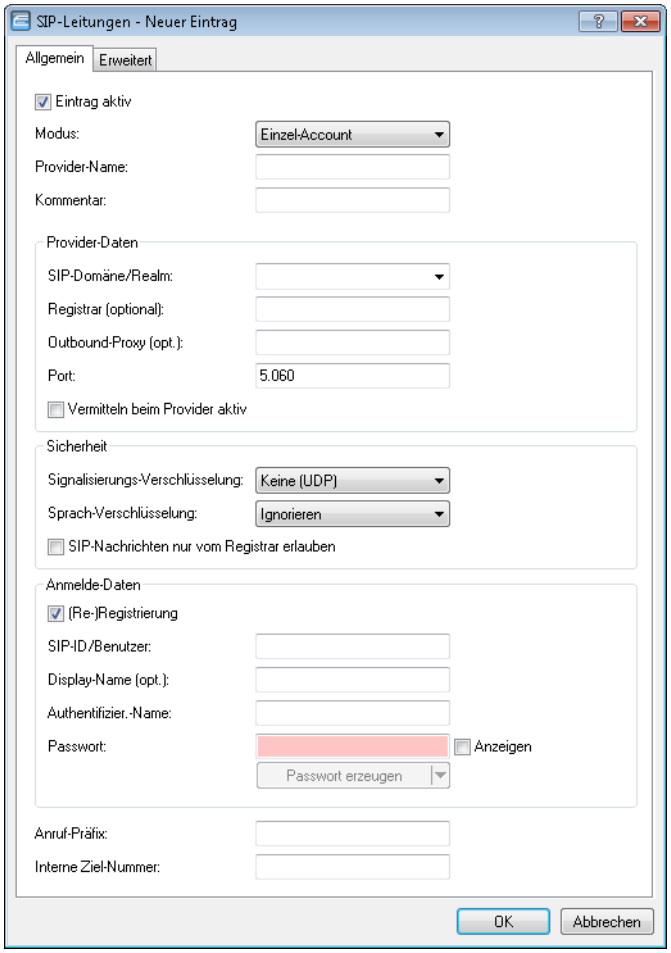
Besondere Werte:

0

Dynamische Auswahl, sofern RTP-Port-Start auch den Wert "0" gesetzt hat.

13.6 SIP-Nachrichten nur vom Registrar erlauben

Ab LCOS-Version 9.20 ist es möglich, die Verarbeitung von SIP-Nachrichten unbekannten VoIP-Servern zu verhindern.



SIP-Nachrichten nur vom Registrar erlauben

Aktivieren Sie diesen Modus, wenn das Gerät eingehende SIP-Nachrichten nur von der registrierten IP-Adresse akzeptieren soll.

Beachten Sie bitte, dass eine hohe Kompatibilität nur bei deaktivierter Funktion sichergestellt ist. Eingehende Rufe werden nicht an den internen Teilnehmer vermittelt, wenn der VoIP-Provider Rufe von Servern / IP-Adressen signalisiert, die nicht dem Registrar entsprechen.

13.6.1 Ergänzungen im Setup-Menü

Strict-Mode

Diese Option aktiviert einen Sicherheitsmechanismus, der verhindert, dass der SIP-User-Agent SIP-Nachrichten von unbekannten VoIP-Servern verarbeitet, die z. B. dazu führen können, dass SIP-Gespräche umgeleitet oder abgebrochen werden.

SNMP-ID:

2.33.4.1.1.30

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Mögliche Werte:

nein

Der Strict-Mode ist deaktiviert.

ja

Der Strict-Mode ist aktiviert.

Default-Wert:

ja

Strict-Mode

Diese Option aktiviert einen Sicherheitsmechanismus, der verhindert, dass der SIP-User-Agent SIP-Nachrichten von unbekannten VoIP-Servern verarbeitet, die z. B. dazu führen können, dass SIP-Gespräche umgeleitet oder abgebrochen werden.

SNMP-ID:

2.33.4.2.1.21

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-PBX** > **PBX**

Mögliche Werte:

nein

Der Strict-Mode ist deaktiviert.

ja

Der Strict-Mode ist aktiviert.

Default-Wert:

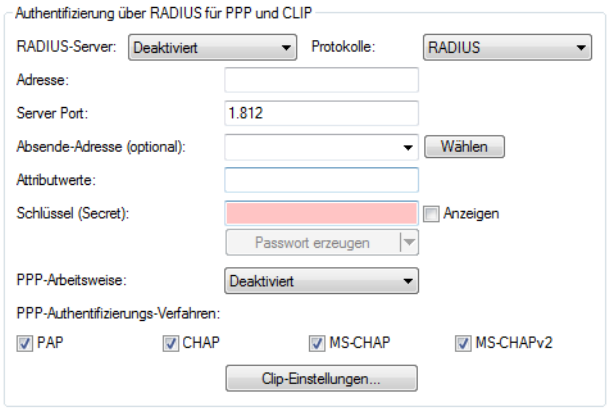
ja

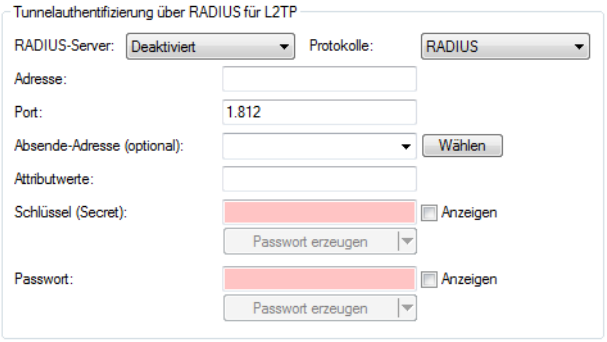
14 RADIUS

14.1 Benutzerdefinierbare Attribute im RADIUS-Client

Ab LCOS-Version 9.20 haben Sie mit LANconfig die Möglichkeit, alle RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server eigenständig zu konfigurieren.

Unter LANconfig konfigurieren Sie die Attribute unter **Kommunikation** > **RADIUS** jeweils in den Abschnitten **Authentifizierung über RADIUS für PPP und Clip** und **Tunnelauthentifizierung über RADIUS für L2TP**.





Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

14.2 Zugriffsinformationen auf dem RADIUS-Server automatisch bereinigen

Ab LCOS-Version 9.20 ist die Funktion "Auto-Loeschen-Accounting-Total" per Default aktiviert.

14.2.1 Ergänzungen im Setup-Menü

Auto-Loeschen-Accounting-Total

Abgeschlossene Accounting-Sessions, deren RADIUS-Account von der Funktion "RADIUS-Nutzertabelle bereinigen" entfernt wurde, werden gelöscht.

SNMP-ID:

2.25.10.18

Pfad Telnet:

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

Mögliche Werte:

nein

Accounting-Informationen werden nicht automatisch gelöscht.

ja

Accounting-Informationen werden automatisch gelöscht.

Default-Wert:

ja

14.3 Vendor Specific RADIUS-Attribut "LCS-Routing-Tag"

Ab LCOS-Version 9.20 unterstützt der RADIUS-Client für PPTP, L2TP und PPPoE das Vendor Specific Radius-Attribut "LCS-Routing-Tag".

15 Weitere Dienste

Ein Gerät 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

15.1 DHCP Snooping: neue Variable für LAN MAC-Adresse

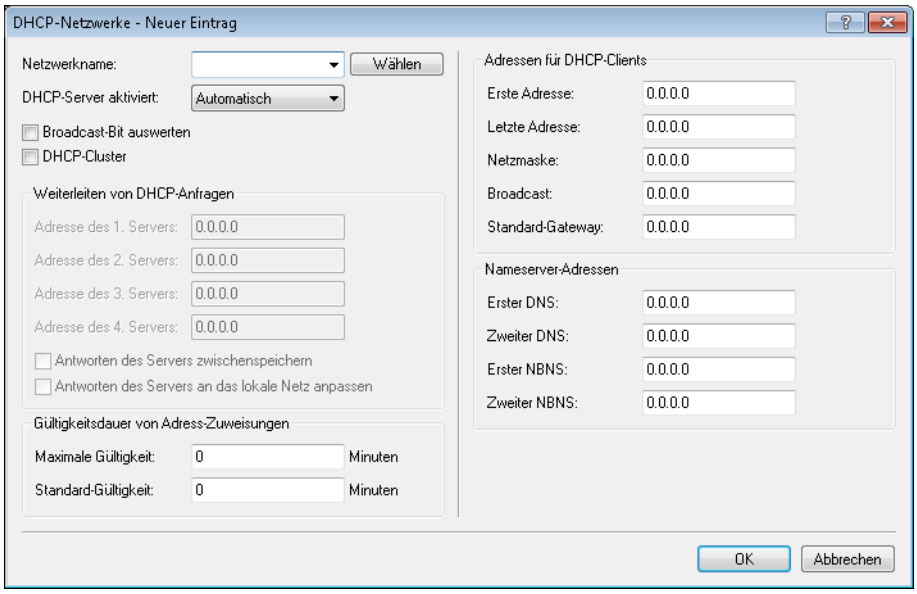
Ab LCOS-Version 9.20 existiert für die LAN MAC-Adresse eine eigene Variable. Diese MAC-Adresse gilt systemweit und wird unter anderem auch in der Sysinfo und in LANconfig angezeigt.

- `%r`: fügt die schnittstellenunabhängige und systemweit gültige MAC-Adresse des Gerätes ein, welches den DHCP-Request erhalten hat.

15.2 DHCP-Leasedauer pro Netzwerk

Ab LCOS-Version 9.20 ist die Angabe einer eigenen Leasedauer pro DHCP-Netzwerk möglich.

Die Konfiguration erfolgt in LANconfig im Konfigurationsmenü unter **IPv4** > **DHCPv4** mit einem Klick auf **DHCP-Netzwerke**.



Gültigkeitsdauer von Adress-Zuweisungen

Neben der global konfigurierten Gültigkeitsdauer unter **IPv4** > **DHCPv4** ist hier die Konfiguration einer Gültigkeitsdauer nur für dieses DHCP-Netzwerk möglich.

Maximale Gültigkeit

Geben Sie hier die maximale Gültigkeitsdauer an, die ein Client anfordern darf.

Standard-Gültigkeit

Wenn ein Client IP-Adressdaten anfordert, ohne eine Gültigkeitsdauer für diese Daten zu fordern, erhält er als Gültigkeitsdauer den hier eingestellten Wert vom DHCP-Client zugewiesen.

15.2.1 Ergänzungen im Setup-Menü

Max.-Gueltigkeit

Neben der global konfigurierten maximalen Gültigkeitsdauer unter **Setup** > **DHCP** ist hier die Konfiguration einer maximalen Gültigkeitsdauer nur für dieses DHCP-Netzwerk möglich.

Geben Sie hier die maximale Gültigkeitsdauer an, die ein Client anfordern darf.

SNMP-ID:

2.10.20.20

Pfad Telnet:

Setup > **DHCP** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Die vom DHCP-Client angefragte Gültigkeitsdauer ist nicht beschränkt.

Def.-Gueltigkeit

Neben der global konfigurierten Standard-Gültigkeitsdauer unter **Setup** > **DHCP** ist hier die Konfiguration einer Standard-Gültigkeitsdauer nur für dieses DHCP-Netzwerk möglich.

Wenn ein Client IP-Adressdaten anfordert, ohne eine Gültigkeitsdauer für diese Daten zu fordern, erhält er als Gültigkeitsdauer den hier eingestellten Wert vom DHCP-Client zugewiesen.

SNMP-ID:

2.10.20.21

Pfad Telnet:

Setup > **DHCP** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Die dem DHCP-Client zugewiesene Gültigkeitsdauer ist nicht beschränkt.

15.3 DHCP-Lease RADIUS-Accounting

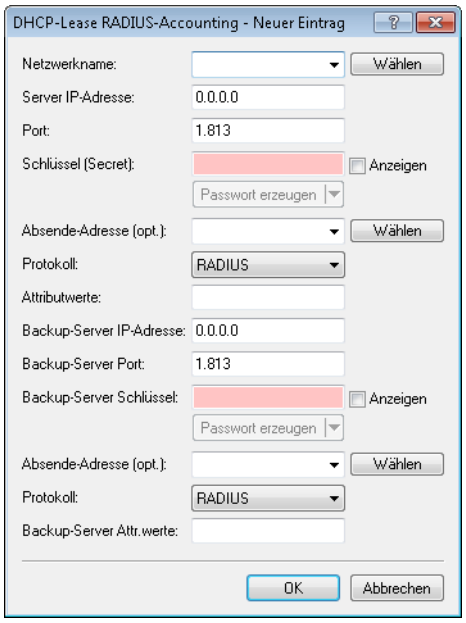
Ab LCOS-Version 9.20 unterstützt LCOS DHCP-RADIUS-Accounting.

15.3.1 DHCP-Lease RADIUS-Accounting

Weist der DHCP-Server einem DHCP-Client eine IP-Adresse zu, sendet er bei aktiviertem RADIUS-Accounting dem entsprechend zugewiesenen Accounting-Server (bzw. dem Backup-RADIUS-Server) ein `RADIUS Accounting Start`. Läuft die Gültigkeit der Adresszuweisung (DHCP-Lease) mangels Verlängerung ab, sendet der DHCP-Server ein `RADIUS Accounting Stop`. Zwischen diesen beiden Ereignissen sendet der DHCP-Server dem RADIUS-Server regelmäßig in einem konfigurierbaren Intervall ein `RADIUS Accounting Interim Update`.

Das RADIUS-Accounting für den DHCP-Server aktivieren oder deaktivieren Sie unter **IPv4** > **DHCPv4** mit einem Klick auf die Option **DHCP-Lease RADIUS-Accounting aktivieren**.

Das Intervall für die RADIUS-Interim-Updates konfigurieren Sie im Eingabefeld **Accounting-Interim-Intervall**. Den RADIUS-Accounting-Server und den entsprechenden Backup-Server konfigurieren Sie mit einem Klick auf **DHCP-Lease RADIUS-Accounting**.



Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das RADIUS-Accounting-Nachrichten gesendet werden sollen.

Server IP-Adresse

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

Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port „1813".

Schlüssel

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

Absende-Adresse (opt.)

Standardmäßig schickt der RADIUS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen alternativen Absende-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den RADIUS-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.

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für die Kommunikation mit dem RADIUS-Accounting-Server verwendet.

Attributwerte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form
`<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Server IP-Adresse

Geben Sie hier die IP-Adresse oder den DNS-Namen des Backup-RADIUS-Servers an.

Backup-Server Port

Geben Sie hier den TCP-Port an, über den der Backup-RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port „1813".

Backup-Server Schlüssel

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

Absende-Adresse (opt.)

Geben Sie hier optional eine alternative Absende-Adresse an, die der DHCP-Server an den Backup-RADIUS-Server überträgt.

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für den Backup-RADIUS-Server verwendet.

Backup-Server Attr.werte

Geben Sie hier die zusätzlichen Attributwerte für die RADIUS-Kommunikation mit dem Backup-Server an.

15.3.2 Ergänzungen im Setup-Menü

RADIUS-Accounting

Weist der DHCP-Server einem DHCP-Client eine IP-Adresse zu, sendet er bei aktiviertem RADIUS-Accounting dem entsprechend zugewiesenen Accounting-Server (bzw. dem Backup-RADIUS-Server) ein `RADIUS Accounting Start`. Läuft die Gültigkeit der Adresszuweisung (DHCP-Lease) mangels Verlängerung ab, sendet der DHCP-Server ein `RADIUS Accounting Stop`. Zwischen diesen beiden Ereignissen sendet der DHCP-Server dem RADIUS-Server regelmäßig in einem konfigurierbaren Intervall ein `RADIUS Accounting Interim Update`.

Dieses Menu enthält die Einstellungen für das DHCP-Lease RADIUS-Accounting.

SNMP-ID:

2.10.23

Pfad Telnet:

Setup > **DHCP**

In-Betrieb

Aktiviert oder deaktiviert das RADIUS-Accounting für den dieses DHCP-Netzwerk.

SNMP-ID:

2.10.23.1

Pfad Telnet:

Setup > **DHCP** > **RADIUS-Accounting**

Mögliche Werte:

nein

RADIUS-Accounting ist für dieses Netzwerk deaktiviert.

ja

RADIUS-Accounting ist für dieses Netzwerk aktiviert.

Default-Wert:

nein

Interim-Intervall

Geben Sie hier das Zeitintervall in Sekunden an, in dem der DHCP-Server ein `RADIUS Interim Update` an den Accounting-Server sendet.

SNMP-ID:

2.10.23.2

Pfad Telnet:

Setup > **DHCP** > **RADIUS-Accounting**

Mögliche Werte:

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

Netzliste

Diese Tabelle enthält die IP-Netze für das RADIUS-Accounting.

SNMP-ID:

2.10.23.20

Pfad Telnet:

Setup > **DHCP** > **RADIUS-Accounting**

Netzwerkname

Enthält den Namen des Netzwerkes.

SNMP-ID:

2.10.23.20.1

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Server-Hostname

Tragen Sie hier den Hostnamen des RADIUS-Accounting-Servers ein.

SNMP-ID:

2.10.23.20.2

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Accnt.-Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port „1813".

SNMP-ID:

2.10.23.20.3

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

1813

Schluessel

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

SNMP-ID:

2.10.23.20.4

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Loopback-Adresse

Standardmäßig schickt der RADIUS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen alternativen Absende-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den RADIUS-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:

2.10.23.20.5

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, das für die Kommunikation mit dem RADIUS-Accounting-Server verwendet wird.

SNMP-ID:

2.10.23.20.6

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Attribut-Werte

LCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

SNMP-ID:

2.10.23.20.7

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Backup-Server-Hostname

Tragen Sie hier den Hostnamen des Backup-Servers ein.

SNMP-ID:

2.10.23.20.12

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Backup-Accnt.-Port

Geben Sie hier den Backup-Port des Backup RADIUS Accounting-Servers an.

SNMP-ID:

2.10.23.20.13

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

0

Backup-Schluessel

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

SNMP-ID:

2.10.23.20.14

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Backup-Loopback-Adresse

Geben Sie eine Loopback-Adresse für den Backup RADIUS Accounting-Server an.

SNMP-ID:

2.10.23.20.15

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

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

Default-Wert:

leer

Backup-Protokoll

Über diesen Eintrag geben Sie das Protokoll für die Kommunikation mit dem Backup-RADIUS-Accounting-Server an.

SNMP-ID:

2.10.23.20.16

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Backup-Attribut-Werte

Geben Sie hier die Attribut-Werte für den Backup RADIUS-Accounting Server an.

SNMP-ID:

2.10.23.20.17

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Netzliste**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

15.4 Unterstützung von SNMPv3

Mit der Version 9.20 unterstützt LCOS auch SNMPv3, so dass jetzt insgesamt die folgenden SNMP-Versionen verfügbar sind:

- SNMPv1
- SNMPv2c
- SNMPv3

15.4.1 Simple Network Management Protocol (SNMP)

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

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

SNMP-Komponenten

Die typische SNMP-Architektur besteht aus drei Komponenten:

SNMP-Manager

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

SNMP-Agent

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

Verwaltetes Gerät

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

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

SNMP-Versionen

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

SNMPv1

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

SNMPv2

In die Version 2 flossen seit 1993 hauptsächlich Verbesserungen im Komfortbereich ein. Mehrere Zwischenschritte und wieder verworfene Konzepte führten letztendlich zur Version SNMPv2c. Diese Version ermöglicht die komfortable Abfrage von großen Datenmengen über einen `GetBulkRequest`-Befehl und die Kommunikation von SNMP-Managern untereinander. Der Austausch des Community-Strings erfolgt allerdings wie bei der Version 1 weiterhin im Klartext.

SNMPv3

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

LCOS unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

SNMPv3-Grundlagen

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

MPD

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

USM

Das USM-Modul verwaltet Sicherheitsfunktionen, die die Authentifizierung der Nutzer sowie die Verschlüsselung und Integrität der Daten sicherstellen. SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen.

VACM

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

SNMPv3-Views

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

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

SNMPv3-Groups

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

Security-Levels

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

NoAuth-NoPriv

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

Auth-NoPriv

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

Auth-Priv

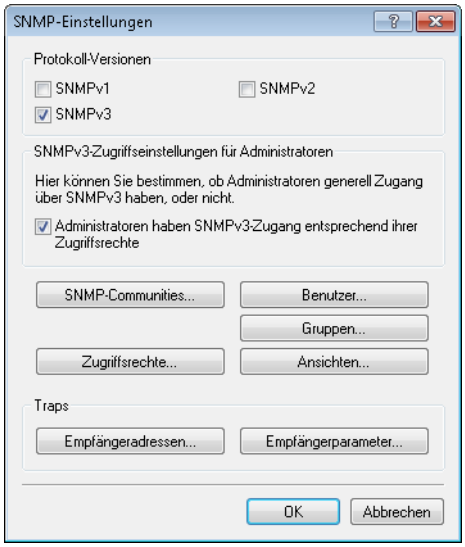
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Kontext

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

SNMP mit LANconfig konfigurieren

In LANconfig konfigurieren Sie SNMP unter **Management** > **Admin** im Abschnitt **SNMP** mit einem Klick auf **SNMP-Einstellungen**.



Protokoll-Versionen

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

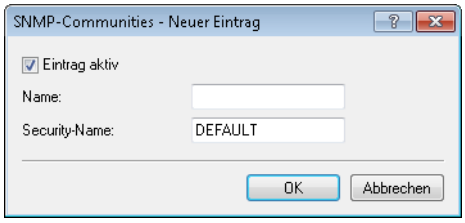
SNMPv3-Zugriffseinstellungen für Administratoren

Sollen registrierte Administratoren auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

SNMP-Communities

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

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



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

Eintrag aktiv

Aktiviert oder deaktiviert diese SNMP-Community.

Name

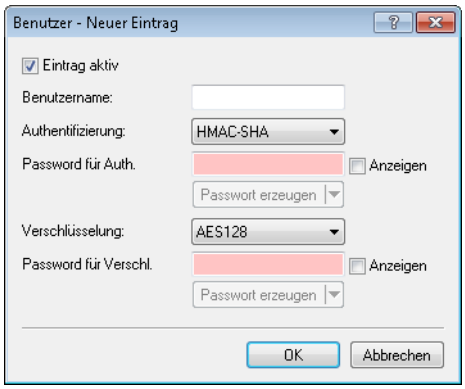
Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

Security-Name

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

Benutzer

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Benutzer.

Benutzername

Vergeben Sie hier einen aussagekräftigen Namen für diesen Benutzer.

Authentifizierung

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

Keine

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

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

HMAC-SHA (Default)

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

Passwort für Auth.

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

Verschlüsselung

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

Keine

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128 (Default)

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits)

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits)

AES256

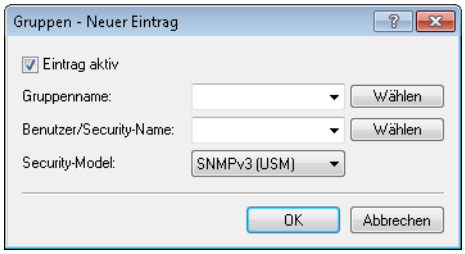
Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Passwort für Verschl.

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

Gruppen

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



Eintrag aktiv

Aktiviert oder deaktiviert diese Gruppe.

Gruppenname

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

Benutzer/Security-Name

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

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

SNMPv1

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

SNMPv2

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

SNMPv3 (USM)

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

NoAuthNoPriv

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

AuthNoPriv

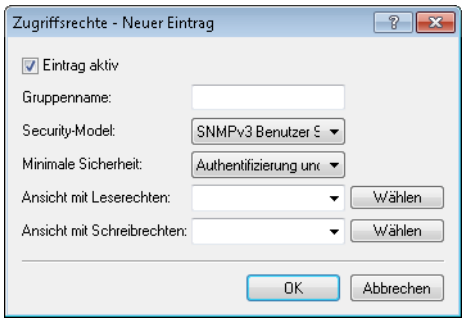
Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv

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

Zugriffsrechte

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Gruppenname

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

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Minimale Sicherheit

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

Ansicht mit Leserechten

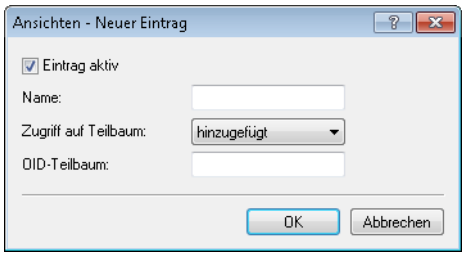
Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.

Ansicht mit Schreibrechten

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

Ansichten

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



Eintrag aktiv

Aktiviert oder deaktiviert diese Ansicht.

Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

Zugriff auf Teilbaum

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

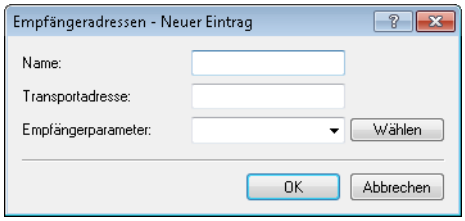
OID-Teilbaum

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

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie im WEBconfig unter **Extras** > **SNMP-Geräte-MIB abrufen** herunterladen können.

Empfängeradressen

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



Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Transportadresse

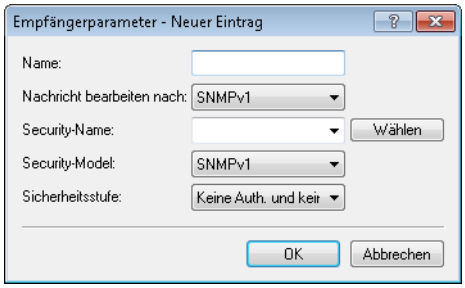
Konfigurieren Sie hier die Adresse des Empfängers.

Empfängerparameter

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

Empfängerparameter

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



Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Nachricht bearbeiten nach

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

Security-Name

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

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Sicherheitsstufe

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

Keine Auth. und keine Verschlüsselung

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

Authentifizierung, aber keine Verschlüsselung

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

Authentifizierung und Verschlüsselung

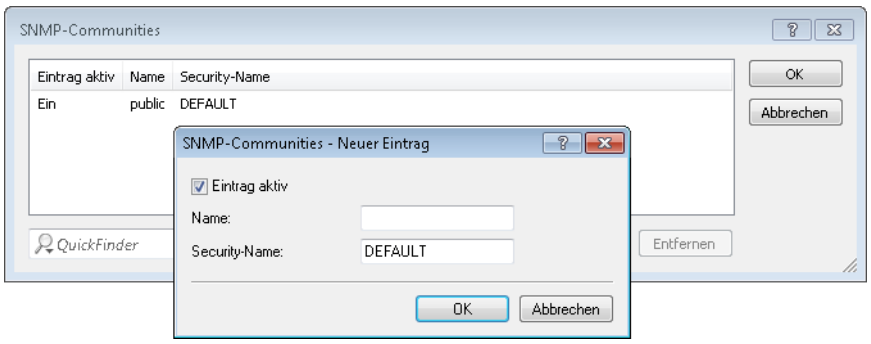
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

15.4.2 Konfigurieren des SNMP-Lesezugriffs

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

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

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



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

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community. Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Der SNMP-Schreibzugriff bleibt ausschließlich Administratoren mit entsprechenden Berechtigungen vorbehalten.

Mehr Informationen zu SNMP finden Sie im Kapitel *Simple Network Management Protocol (SNMP)*

15.4.3 Ergänzungen im Setup-Menü

Communities

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

In dieser Tabelle konfigurieren Sie die SNMP-Communities.

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

SNMP-ID:

2.9.27

Pfad Telnet:

Setup > **SNMP**

Name

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

SNMP-ID:

2.9.27.1

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Security-Name

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

SNMP-ID:

2.9.27.3

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Status

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

SNMP-ID:

2.9.27.8

Pfad Telnet:

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

Mögliche Werte:

aktiv
Die Community ist aktiviert.

inaktiv
Die Community ist deaktiviert.

Default-Wert:

aktiv

Groups

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

SNMP-ID:

2.9.28

Pfad Telnet:

Setup > **SNMP**

Security-Model

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

Entsprechend wählen Sie hier ein Security-Modell aus.

SNMP-ID:

2.9.28.1

Pfad Telnet:

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

Mögliche Werte:

SNMPv1

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

SNMPv2

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

SNMPv3(USM)

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

NoAuthNoPriv

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

AuthNoPriv

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

AuthPriv

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

Default-Wert:

SNMPv3(USM)

Security-Name

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

SNMP-ID:

2.9.28.2

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Group-Name

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

SNMP-ID:

2.9.28.3

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diese Gruppenkonfiguration.

SNMP-ID:

2.9.28.5

Pfad Telnet:

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

Mögliche Werte:

aktiv
inaktiv

Default-Wert:

aktiv

Zugriff

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

SNMP-ID:

2.9.29

Pfad Telnet:

Setup > **SNMP**

Group-Name

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

SNMP-ID:

2.9.29.1

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

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

Default-Wert:

leer

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

SNMP-ID:

2.9.29.3

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

Any
Jedes Modell wird akzeptiert.
SNMPv1
SNMPv1 wird verwendet.
SNMPv2
SNMPv2c wird verwendet.
SNMPv3(USM)
SNMPv3 wird verwendet.

Default-Wert:

Any

Read-View-Name

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

SNMP-ID:

2.9.29.5

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

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

Default-Wert:

leer

Write-View-Name

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

SNMP-ID:

2.9.29.6

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Zugriff**

Mögliche Werte:

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

Default-Wert:

leer

Notify-View-Name

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

SNMP-ID:

2.9.29.7

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

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

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diesen Eintrag.

SNMP-ID:

2.9.29.9

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

aktiv
inaktiv

Default-Wert:

aktiv

Min-Security-Level

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

SNMP-ID:

2.9.29.10

Pfad Telnet:

Setup > **SNMP** > **Zugriff**

Mögliche Werte:

NoAuth-NoPriv

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

Auth-NoPriv

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

Auth-Priv

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

Default-Wert:

Auth-Priv

Views

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

SNMP-ID:

2.9.30

Pfad Telnet:

Setup > **SNMP**

View-Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

SNMP-ID:

2.9.30.1

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

OID-Subtree

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

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie im WEBconfig unter **Extras** > **SNMP-Geräte-MIB abrufen** herunterladen können.

SNMP-ID:

2.9.30.2

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Type

Bestimmen Sie, ob die nachfolgend angegebenen OID-Teilbäume Bestandteil („included") oder kein Bestandteil („excluded") der Ansicht sind.

SNMP-ID:

2.9.30.4

Pfad Telnet:

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

Mögliche Werte:

Included

Diese Einstellung gibt MIB-Werten mit aus.

Excluded

Diese Einstellung blockt die Ausgabe von MIB-Werten.

Default-Wert:

Included

Status

Aktiviert oder deaktiviert diese Ansicht.

SNMP-ID:

2.9.30.6

Pfad Telnet:

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

Mögliche Werte:

aktiv
inaktiv

Default-Wert:

aktiv

SNMPv3-Users

Dieses Menü enthält die Benutzerkonfiguration.

SNMP-ID:

2.9.32

Pfad Telnet:

Setup > **SNMP**

Benutzername

Geben Sie hier den SNMPv3 Benutzernamen an.

SNMP-ID:

2.9.32.2

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Users**

Mögliche Werte:

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

Default-Wert:

leer

Authentifizierungs-Protokoll

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

SNMP-ID:

2.9.32.5

Pfad Telnet:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

None

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

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

HMAC-SHA

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

Default-Wert:

HMAC-SHA

Authentifizierungs-Passwort

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

SNMP-ID:

2.9.32.6

Pfad Telnet:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Privacy-Protokoll

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

SNMP-ID:

2.9.32.8

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Users**

Mögliche Werte:

None

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits).

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits).

AES256

Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Default-Wert:

AES128

Privacy-Passwort

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

SNMP-ID:

2.9.32.9

Pfad Telnet:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Status

Aktiviert oder deaktiviert diesen Benutzer.

SNMP-ID:

2.9.32.13

Pfad Telnet:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

aktiv
inaktiv

Default-Wert:

aktiv

SNMPv3-Notifiers

Dieses Menü enthält die Tabelle mit den SNMPv3-Benachrichtigungen.

SNMP-ID:

2.9.33

Pfad Telnet:

Setup > **SNMP**

Notify-Name

Geben Sie hier einen Namen für diesen Notifier ein.

SNMP-ID:

2.9.33.1

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Notifiers**

Mögliche Werte:

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

Default-Wert:

leer

Notify-Tag

Geben Sie hier das Notifier-Tag an.

SNMP-ID:

2.9.33.2

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Notifiers**

Mögliche Werte:

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

Default-Wert:

leer

Notify-Type

Enthält den Benachrichtigungstypen.

SNMP-ID:

2.9.33.3

Pfad Telnet:

Setup > **SNMP** > **SNMPv3-Notifiers**

Mögliche Werte:

NOTIFICATION-TRAP

Default-Wert:

NOTIFICATION-TRAP

Target-Address

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

SNMP-ID:

2.9.34

Pfad Telnet:

Setup > **SNMP**

Target-Address-Name

Geben Sie hier den Ziel-Adress-Namen an.

SNMP-ID:

2.9.34.1

Pfad Telnet:

Setup > **SNMP** > **Target-Address**

Mögliche Werte:

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

Default-Wert:

leer

Target-Transport-Address

Enthält die IP-Adresse, an die SNMP Traps gesendet werden.

SNMP-ID:

2.9.34.3

Pfad Telnet:

Setup > **SNMP** > **Target-Address**

Mögliche Werte:

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

Default-Wert:

leer

Target-Tag-List

Enthält eine Tag-Liste zum Definieren von Ziel-Adressen für spezielle Aufgaben.

SNMP-ID:

2.9.34.6

Pfad Telnet:

Setup > **SNMP** > **Target-Address**

Mögliche Werte:

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

Default-Wert:

leer

Parameters-Name

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

SNMP-ID:

2.9.34.7

Pfad Telnet:

Setup > **SNMP** > **Target-Address**

Mögliche Werte:

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

Default-Wert:

leer

Target-Params

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

SNMP-ID:

2.9.35

Pfad Telnet:

Setup > **SNMP**

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

SNMP-ID:

2.9.35.1

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Message-Processing-Model

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

SNMP-ID:

2.9.35.2

Pfad Telnet:

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

Mögliche Werte:

SNMPv1
SNMPv2c
SNMPv3

Default-Wert:

SNMPv3

Security-Model

Legen Sie mit diesem Eintrag das Sicherheitsmodell fest.

SNMP-ID:

2.9.35.3

Pfad Telnet:

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

Mögliche Werte:

SNMPv1
SNMPv2
SNMPv3(USM)

Default-Wert:

SNMPv3(USM)

Security-Name

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

SNMP-ID:

2.9.35.4

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Security-Level

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

SNMP-ID:

2.9.35.5

Pfad Telnet:

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

Mögliche Werte:

NoAuth-NoPriv

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

Auth-NoPriv

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

Auth-Priv

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

Default-Wert:

NoAuth-NoPriv

Notification-Server-Enable

Legen Sie mit diesem Eintrag fest, ob die Server-Benachrichtigung aktiviert oder deaktiviert werden soll.

SNMP-ID:

2.9.36

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

nein

Die Server-Benachrichtigung ist deaktiviert.

ja

Die Server-Benachrichtigung ist aktiviert.

Default-Wert:

nein

Admitted-Protocols

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

SNMP-ID:

2.9.37

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

SNMPv1
SNMPv2
SNMPv3

Default-Wert:

SNMPv1

SNMPv2

SNMPv3

SNMPv3-Allow-Admins

Sollen registrierte Administratoren auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

SNMP-ID:

2.9.38

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

nein
ja

Default-Wert:

ja

SNMPv3-Admin-Authentication

Legt die Autorisierungsmethode für Administratoren fest.

Dieser Wert ist nicht änderbar.

SNMP-ID:

2.9.39

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

AUTH-HMAC-SHA

Default-Wert:

AUTH-HMAC-SHA

SNMPv3-Admin-Privacy

Legt die Verschlüsselungseinstellungen für Administratoren fest.

Dieser Wert ist nicht änderbar.

SNMP-ID:

2.9.40

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

AES256

Default-Wert:

AES256

Aktiv

Dieser Eintrag aktiviert oder deaktiviert SNMP-Traps. Deaktivieren Sie die Checkbox, um SNMP-Traps auszuschalten.

SNMP-ID:

2.9.41

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

nein
ja

Default-Wert:

ja

15.5 Protokollierung von DNS-Anfragen über SYSLOG

Ab LCOS-Version 9.20 sendet der DNS-Server im Gerät die DNS-Antworten an den Client auch als SYSLOG-Meldung an einen SYSLOG-Server.

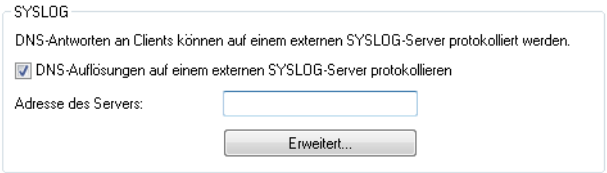
Bei einem Wechsel auf LCOS-Version 9.20 konvertiert LCOS die bestehenden Tabelleneinträge in die neue Form. Bei einem Rückfall auf eine frühere LCOS-Version gehen alle Änderungen verloren, die Sie anschließend in der LCOS-Version 9.20 vorgenommen haben (z. B. die Einträge für IP-Adressen). Solange die Geräte-Konfiguration nach einem Update auf LCOS-Version 9.20 unverändert bleibt, ist auch ein Rückfall auf eine frühere LCOS-Version ohne Verluste möglich.

15.5.1 Protokollierung von DNS-Anfragen über SYSLOG

Um Anfragen von Clients an den DNS-Server zu dokumentieren, besteht die Möglichkeit, dass der DNS-Server im Gerät die Antworten an den Client auch laufend in Form einer SYSLOG-Meldung an einen SYSLOG-Server sendet.

Bitte beachten Sie, dass eine Aufzeichnung der DNS-Anfragen nur gemäß der in ihrem Land gültigen Datenschutzbestimmungen erfolgen darf.

In LANconfig konfigurieren Sie die Dokumentation von DNS-Anfragen unter **IPv4** > **DNS** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Diese Option aktiviert oder deaktiviert (Default-Einstellung) den Versand von SYSLOG-Meldungen bei DNS-Anfragen.

Dieser Schalter ist unabhängig vom globalen Schalter im Syslog-Modul unter **Meldungen** > **Allgemein** > **SYSLOG**. D. h., wenn Sie hier die Option zur Aufzeichnung der DNS-Anfragen aktivieren, sendet der DNS-Server auch bei global deaktiviertem SYSLOG-Modul die entsprechenden SYSLOG-Meldungen an einen SYSLOG-Server.

Jede DNS-Auflösung (`ANSWER`-Record oder `ADDITIONAL`-Record) erzeugt jeweils eine SYSLOG-Meldung mit dem Aufbau `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Ressource-Record`.

Dabei haben die Parameter die folgenden Bedeutungen:

- Die `TID` (Transaction-ID) enthält einen 4-stelligen Hexadezimal-Code.

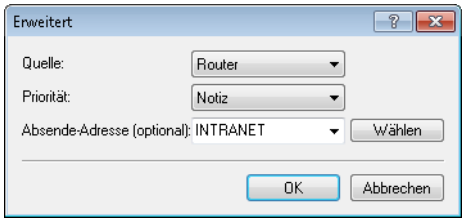
- Der `{Hostname}` ist nur dann Bestandteil der Meldung, wenn der DNS-Server ihn ohne DNS-Anfrage auflösen kann (wie auch im Firewall-Log).
- Die `Ressource-Record` besteht aus drei Teilen: Der Anfrage, dem Typ bzw. der Klasse und der IP-Auflösung (z. B. `www.mydomain.com STD A resolved to 193.99.144.32`)

Adresse des Servers

Geben Sie hier die Adresse des SYSLOG-Servers ein. Die Eingabe als IPv4-/IPv6-Adresse oder als DNS-Name ist möglich.

Die Angabe der IP-Adressen `127.0.0.1` und `::1` ist generell nicht erlaubt, um so die Nutzung eines externen Servers zu erzwingen.

Um die SYSLOG-Meldung zu konfigurieren, klicken Sie auf **Erweitert**.



Quelle

Wählen Sie hier aus, welche Quelle in den SYSLOG-Meldungen eingetragen ist.

Priorität

Wählen Sie hier aus, welche Priorität in den SYSLOG-Meldungen eingetragen ist.

Absende-Adresse (optional)

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem SYSLOG-Server 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 Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet.

Mehr Informationen über SYSLOG und die zur Verfügung stehenden Einstellungen finden Sie im Abschnitt *Das SYSLOG-Modul*.

15.5.2 Ergänzungen im Setup-Menü

Syslog

In diesem Verzeichnis konfigurieren Sie die SYSLOG-Protokollierung von DNS-Anfragen.

SNMP-ID:

2.17.20

Pfad Telnet:

Setup > **DNS**

DNS-Aufloesungen-loggen

Diese Option aktiviert oder deaktiviert (Default-Einstellung) den Versand von SYSLOG-Meldungen bei DNS-Anfragen.

Dieser Schalter ist unabhängig vom globalen Schalter im Syslog-Modul unter **Setup** > **SYSLOG** > **Aktiv**. D. h., wenn Sie hier die Option zur Aufzeichnung der DNS-Anfragen aktivieren, sendet der DNS-Server im Gerät auch bei global deaktiviertem SYSLOG-Modul die entsprechenden SYSLOG-Meldungen an einen SYSLOG-Server.

Jede DNS-Auflösung (`ANSWER`-Record oder `ADDITIONAL`-Record) erzeugt jeweils eine SYSLOG-Meldung mit dem Aufbau `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Ressource-Record`.

Dabei haben die Parameter die folgenden Bedeutungen:

- Die `TID` (Transaction-ID) enthält einen 4-stelligen Hexadezimal-Code.
- Der `{Hostname}` ist nur dann Bestandteil der Meldung, wenn der DNS-Server ihn ohne DNS-Anfrage auflösen kann (wie auch im Firewall-Log).
- Die `Ressource-Record` besteht aus drei Teilen: Der Anfrage, dem Typ bzw. der Klasse und der IP-Auflösung (z. B. `www.mydomain.com STD A resolved to 193.99.144.32`)

SNMP-ID:

2.17.20.1

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

nein

Deaktiviert die Aufzeichnung der DNS-Anfragen und -Antworten.

ja

Aktiviert die Aufzeichnung der DNS-Anfragen und -Antworten.

Default-Wert:

nein

Log-Server-Adresse

Die Log-Server-Adresse enthält den zu nutzenden Syslog-Server in Form des entsprechenden DNS-Namens oder einer IP-Adresse.

Die Angabe der IP-Adressen `127.0.0.1` und `::1` ist generell nicht erlaubt, um so die Nutzung eines externen Servers zu erzwingen.

SNMP-ID:

2.17.20.2

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

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

Log-Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

SNMP-ID:

2.17.20.3

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

System
Login
Systemzeit
Konsole-Login
Verbindungen
Accounting
Administration
Router

Default-Wert:

Router

Log-Level

Enthält die Priorität, die in den SYSLOG-Meldungen erscheint.

SNMP-ID:

2.17.20.4

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

Notfall
Alarm
Kritisch
Fehler
Warnung
Hinweis
Info
Debug

Default-Wert:

Hinweis

Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem SYSLOG-Server 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 Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet.

SNMP-ID:

2.17.20.5

Pfad Telnet:

Setup > **DNS** > **Syslog**

Mögliche Werte:

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

Besondere Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
„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

Quelle

Wählen Sie hier aus, welche Quelle in den SYSLOG-Meldungen eingetragen ist.

SNMP-ID:

2.22.2.3

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

keine
System
Login
Systemzeit
Konsole-Login
Verbindungen
Accounting
Administration
Router

Default-Wert:

keine

Level

Wählen Sie hier aus, welche Priorität in den SYSLOG-Meldungen eingetragen ist. Eine Mehrfachauswahl ist möglich.

SNMP-ID:

2.22.2.4

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

keine
Alarm
Fehler
Warnung
Info
Debug

Default-Wert:

keine

IP-Adresse

Enthält die IP-Adresse des SYSLOG-Servers. Die Angabe ist möglich als IPv4- bzw. IPv6-Adresse oder als DNS-Name.

SNMP-ID:

2.22.2.7

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

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

Facility

Zuordnung der Quellen zu bestimmten Facilities.

SNMP-ID:

2.22.3.2

Pfad Telnet:

Setup > **SYSLOG** > **Facility-Mapper**

Mögliche Werte:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7