connecting your business

Menüreferenz

LCOS 9.10

LANCOM
Systems

Inhalt

1 Einleitung

1.1 Über diese Dokumentation

Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

Installation Guide

In dieser Kurzanleitung finden Sie Antworten auf die folgende Fragen:

- Welche Software muss zur Konfiguration installiert werden?
- Wie wird das Gerät angeschlossen?
- Wie kann das Gerät über LANconfig, WEBconfig oder die serielle Schnittstelle erreicht werden?
- Wie startet man die Setup-Assistenten (z. B. zur Einrichtung des Internetzugangs)?
- Wie wird ein Gerätereset durchgeführt?
- Wo gibt es weitere Informationen und Hilfe?

Benutzerhandbuch oder Hardware-Schnellübersicht

Das Benutzerhandbuch oder die Hardware-Schnellübersicht enthalten alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Handbuch TK-Anlagenfunktionen (nur bei Modellen mit VoIP-Unterstützung)

Im Handbuch TK-Anlagenfunktionen finden Sie eine ausführliche Schritt-für-Schritt-Anleitung, um einen VoIP Router als Telefonanlage für einen Einzelstandort in Betrieb zu nehmen. Ferner werden dort die wichtigsten Bedienhinweise für Teilnehmer und den Anschluss von Endgeräten beschrieben.

Referenzhandbuch

Das Referenzhandbuch geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Die Beschreibungen im Referenzhandbuch orientieren sich überwiegend an der Konfiguration mit LANconfig. Für jeden LANconfig-Dialog wird außerdem der zugehörige Pfad angegeben, unter dem die entsprechenden Parameter bei der Konfiguration mit WEBconfig zu finden sind, z. B.:

LANconfig: Wireless LAN / 802.11i/WEP / WPA- / Einzel-WEP-Einstellungen

WEBconfig: LCOS-Menübaum / Setup / Schnittstellen / WLAN / Verschluesselung

Die Pfade für die Konfiguration über die Konsole/Telnet lassen sich daraus ableiten und werden daher nicht explizit aufgeführt. Der Telnetpfad zu den Verschlüsselungseinstellungen lautet z. B.:

```
cd Setup/Schnittstellen/WLAN/Verschluesselung
```

Menü-Referenz

Die vorliegende Menü-Referenz beschreibt alle Parameter von LCOS, dem Betriebssystem der Geräte. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte mit WEBconfig bzw. über die Konsole (Telnet). Die Parameter werden in der Menü-Referenz in der Reihenfolge der Pfade aufgeführt, wie sie bei der Konfiguration mit WEBconfig erreicht werden können. Zu jedem Parameter werden neben der Beschreibung auch die möglichen Eingabewerte und die Standardbelegung wiedergegeben.

Alle Dokumente, die Ihrem Produkt nicht in gedruckter Form beiliegen, finden Sie als PDF-Datei unter www.lancom.de/download oder auf dem Datenträger, der Ihrem Produkt beiliegt.

LCOS, das Betriebssystem der LANCOM-Geräte

Alle Router, Gateways, Controller und Access Points von LANCOM setzen dasselbe Betriebssystem ein: LCOS. Das von LANCOM selbst entwickelte Betriebssystem ist von außen nicht angreifbar und bietet so eine hohe Sicherheit.

Darüber hinaus steht die konsistente Verwendung von LCOS für eine komfortable und durchgängige Bedienung über alle Produkte. Das umfangreiche Featureset ist für alle Produkte (bei entsprechender Unterstützung durch die Hardware) gleich verfügbar und wird durch kostenlose, regelmäßige Software-Updates ständig weiterentwickelt.

Gültigkeit

Die vorliegende Menü-Referenz gilt für alle Geräte mit einem Firmwarestand Version 8.82 oder neuer.

Die in dieser Menü-Referenz beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt.

An der Erstellung dieser Dokumentation…

…haben Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres Produktes anzubieten. Sollten Sie einen Fehler finden, oder Kritik oder Anregungen zu dieser Dokumentation äußern wollen, kontaktieren Sie uns einfach.

E-Mail: info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf häufig gestellte Fragen (FAQs). Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit. Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefonnummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM Systems-Homepage.

1.2 Die Konfiguration mit Telnet

Telnet-Sitzung starten

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

- `C:\>telnet 10.0.0.1`

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf.

Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Linux und Unix unterstützen auch Telnet-Sitzungen über SSL-verschlüsselte Verbindungen. Je nach Distribution ist es dazu ggf. erforderlich, die Standard-Telnet-Anwendung durch eine SSL-fähige Version zu ersetzen. Die verschlüsselte Telnet-Verbindung wird dann mit dem folgenden Befehl gestartet:

- `C:\>telnet -z ssl 10.0.0.1 telnets`

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. Die Geräte werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

WEBconfig: /Setup/Config-Module/Language

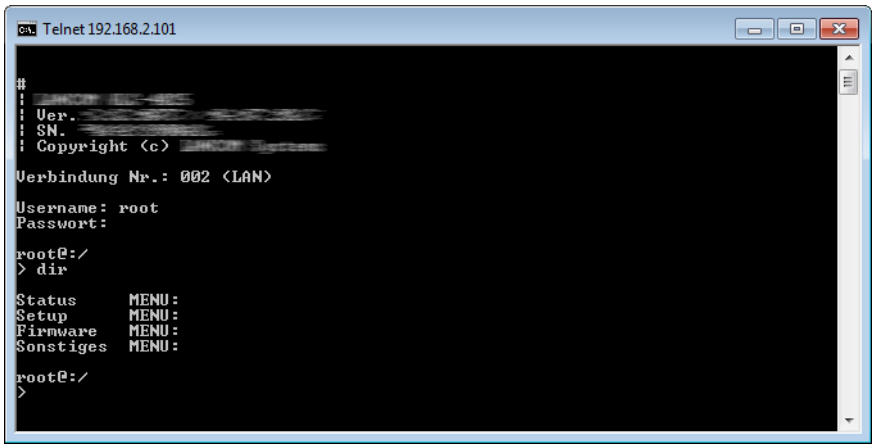
Telnet-Sitzung beenden

Um die Telnet-Sitzung zu beenden, geben Sie an der Eingabeaufforderung den Befehl `exit` ein:

- `C:\>exit`

Die Struktur im Kommandozeilen-Interface

Das Kommandozeilen-Interface ist stets wie folgt strukturiert:



- **Status**

  Enthält die Zustände und Statistiken aller internen Module des Gerätes

- **Setup**

  Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes

- **Firmware**

  Beinhaltet das Firmware-Management

- **Sonstiges**

  Enthält Aktionen für Verbindungsauf- und abbau, Reset, Reboot und Upload

1.3 Befehle für die Kommandozeile

Das Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden. Die verfügbaren LCOS-Menübefehle können durch Aufrufen des HELP-Kommandos jederzeit auf der Kommandozeile angezeigt werden.

Zum Ausführen einiger Befehle sind Supervisor-Rechte erforderlich.

Befehl	Beschreibung
beginscript	Versetzt eine Konsolensitzung in den Script-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im Gerät übertragen, sondern zunächst in den Script-Speicher des Gerätes.
cd [PFAD]	Wechselt das aktuelle Verzeichnis.

Befehl	Beschreibung
	Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc.
default [-r] [PFAD]	Setzt einzelne Parameter, Tabellen oder ganze Menübäume in die Grundkonfiguration zurück. Zeigt PATH auf einen Zweig des Menübaums, muss zwingend die option -r (recursive) angegeben werden.
del [PFAD]*	Löscht eine komplette Tabelle in dem mit Path angegebenen Zweig des Menübaums.
deletebootlog	Löscht den Inhalt des persistenten Bootlog-Speichers.
dir [PFAD] list [PFAD] ls [PFAD] ll [PFAD]	Zeigt den Inhalt des aktuellen Verzeichnisses an. Der angehängte Parameter „-a“ gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte.
do [PFAD] [<Parameter>]	Führt die Aktion [PATH] im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden.
echo <ARG>...	Argument auf Konsole ausgeben
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
flash Yes/No	Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (flash yes) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (flash no), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird.
getenv <NAME>	Umgebungsvariable ausgeben (kein Zeilenvorschub)
history	Zeigt eine Liste der letzen ausgeführten Befehle. Mit dem Befehl !# können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit !3 wird z.B. der dritte Befehl der Liste ausgeführt.
killscript	Löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt.
loadconfig	Konfiguration per TFTP-Client in das Gerät laden
loadfirmware	Firmware per TFTP-Client in das Gerät laden
loadscript	Script per TFTP-Client in das Gerät laden
passwd	Ändern des Passworts
passwd -n neues [altes]	Passwort ändern (Keine Eingabeaufforderung)
ping [IP-Adresse oder Name] ping -6 [IPv6-Adresse]%[Scope]	Sendet einen ICMP echo request an die angegebene IP-Adresse. Weitere Informationen zu dem Befehl und den Besonderheiten beim Anpingen von IPv6-Adressen finden Sie im Kapitel *Übersicht der Parameter im ping-Befehl* auf Seite 23.
printenv	Komplette Umgebung ausgeben
readconfig	Anzeige der kompletten Konfiguration in der Geräte-Syntax
readmib	Anzeige der SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PFAD]	Erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des Geräts im aktuellen Zustand benötigt werden.
release [-x] <Interface 1>...<Interface n>	Der DHCPv6-Client gibt seine IPv6-Adresse und/oder sein Präfix an den DHCPv6-Server zurück. Anschließend fragt er erneut den DHCPv6-Server nach einer Adresse oder einem Präfix. Je nach Provider vergibt der Server dem Client eine neue oder die vorherige Adresse. Ob der Client eine andere Adresse oder ein anderes Präfix erhält, bestimmt alleine der Server. Der Optionsschalter -x unterdrückt eine Bestätigungsmeldung.

Befehl	Beschreibung
	Der Platzhalter * wendet das Kommando auf alle Interfaces und Präfix-Delegationen an.
repeat <INTERVAL> <Kommando>	IPv6-Adressfreigabe: Wiederholt das Kommando alle INTERVAL Sekunden, bis der Vorgang durch neue Eingaben beendet wird.
sleep [-u] Wert[suffix]	Verzögert die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne oder terminiert sie auf einen bestimmten Zeitpunkt. Als Suffix sind `s`, `m`, oder `h` für Sekunden, Minuten, oder Stunden erlaubt, ohne Suffix arbeitet der Befehl in Millisekunden. Mit dem Optionsschalter `-u` nimmt das sleep-Kommando Zeitpunkte im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch) entgegen. Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist.
stop	Beendet den PING-Befehl
set [PFAD] <Wert(e)>	Setzt einen Konfigurationsparameter auf einen bestimmten Wert. Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte ein Wert angegeben werden. Dabei übernimmt das Zeichen * als Eingabewert einen vorhandenen Tabelleneintrag unverändert.
set [PFAD] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
setenv <NAME> <WERT>	Umgebungsvariable setzen
show <Optionen>	Anzeige spezieller interner Daten. Für die Anzeige IPv6-spezifischer Daten lesen Sie auch das Kapitel *Übersicht der IPv6-spezifischen show-Befehle* auf Seite 27. `show ?` zeigt alle verfügbaren Informationen an, z. B. letzte Boot-Vorgänge (bootlog), Firewall Filterregeln (filter), VPN-Regeln (VPN) und Speicherauslastung (mem und heap)
smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)	Nur auf Geräten mit 3G/4G WWAN-Modul verfügbar: Versendet eine Kurznachricht an die angegebene Ziel-Rufnummer. ■ `-s <SMSC-Number>`: Alternative SMSC-Rufnummer (optional). Wenn Sie diesen Befehlsbestandteil weglassen, verwendet das Gerät die in der USIM-Karte hinterlegte oder die unter SNMP-ID 2.83.1 konfigurierte Rufnummer. ■ `-d <Destination>`: Ziel-Rufnummer ■ `-t <Text>`: Inhalt der Kurznachricht mit <=160 Zeichen. Eine Übersicht der verfügbaren Zeichen finden Sie im Abschnitt *Zeichensatz für den SMS-Versand* auf Seite 33. Sonderzeichen sind nur in UTF8-kodierter Form möglich.
sysinfo	Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.)
testmail	Schickt eine E-Mail. Parameter siehe 'testmail ?'
time	Zeit setzen (TT.MM.JJJJ hh:mm:ss)
trace [...]	Konfiguration der Diagnose-Ausgaben. Weitere Informationen zu dem Befehl finden Sie im Kapitel *Übersicht der Parameter im trace-Befehl* auf Seite 25.
unsetenv <NAME>	Umgebungsvariable löschen
who	Aktive Sitzungen auflisten
writeconfig	Laden einer neuen Konfigurationsfile in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten
writeflash	Laden einer neuen Firmware-Datei (nur via TFTP)
!!	Letztes Kommando wiederholen
!<num>	Kommando <num> wiederholen

Befehl	Beschreibung
!<prefix>	Letztes mit <prefix> beginnendes Kommando wiederholen
#<blank>	Kommentar

- PFAD:
  - Pfadname für ein Menü oder einen Parameter, getrennt durch / oder \
  - .. bedeutet eine Ebene höher
  - . bedeutet aktuelle Ebene
- WERT:
  - möglicher Eingabewert
  - "" ist ein leerer Eingabewert
- NAME:
  - Sequenz von _ 0..9 A..Z
  - erstes Zeichen darf keine Ziffer sein
  - keine Unterscheidung Groß/Kleinschreibung

Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden - solange sie eindeutig sind. Zum Beispiel kann der Befehl "`sysinfo`" zu "`sys`" verkürzt werden, oder aber "`cd Management`" zu "`c ma`". Die Eingabe "`cd /s`" dagegen ist ungültig, da dieser Eingabe sowohl "`cd /Setup`" als auch "`cd /Status`" entspräche. Verzeichnisse können über die entsprechende SNMP-ID angesprochen werden. Der Befehl "`cd /2/8/10/2`" bewirkt z. B. das gleiche wie "`cd /Setup/IP-Router/Firewall/Regel-Tabelle`".

Mehrere Werte in einer Tabellezeile können mit **einem** Befehl verändert werden, z.B. in der Regeltabelle der Firewall:

- `set WINS UDP` setzt das Protokoll der Regel WINS auf UDP
- `set WINS UDP ANYHOST` setzt das Protokoll der Regel WINS auf UDP und die Destination auf ANYHOST
- `set WINS * ANYHOST` setzt ebenfalls die Destination der Regel WINS auf ANYHOST, durch das Sternchen wird das Protokoll unverändert übernommen

Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an. Die Destination hat in der Regeltabelle der Firewall z. B. die Nummer 4:

- `set WINS {4} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST
- `set WINS {destination} ANYHOST` setzt auch die Destination der Regel WINS auf ANYHOST
- `set WINS {dest} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST, weil die Angabe von "dest" hier ausreichend für eine eindeutige Spaltenbezeichnung ist.

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

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

Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von `?` auf der Kommandozeile.

Übersicht der Parameter im ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Telnet- oder Terminal-Verbindung sendet ein "ICMP Echo-Request"-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem "ICMP Echo-Reply". Ist der Zielrechner

nicht erreichbar, antwortet das letzte Gerät vor dem Host mit "Network unreachable" (Netzwerk nicht erreichbar) oder "Host unreachable" (Gegenstelle nicht erreichbar).

Die Syntax des Ping-Kommandos lautet wie folgt:

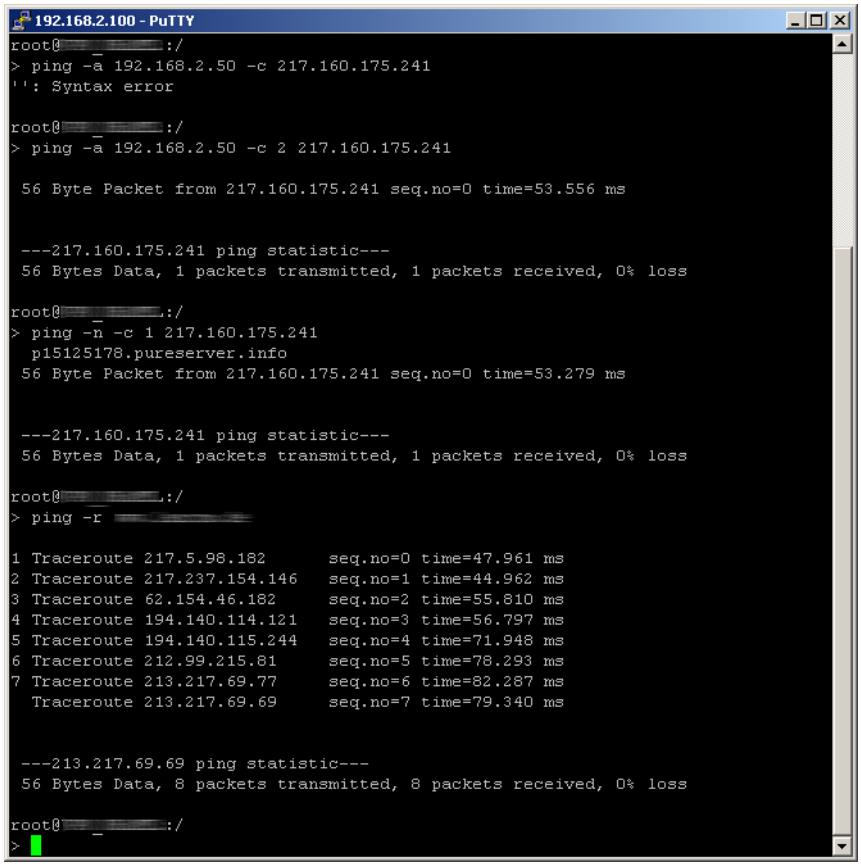
```
ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] Destination
```

Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Tabelle 1: Übersicht aller optionalen Parameter im ping-Befehl

Parameter	Bedeutung
`-a a.b.c.d`	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Gerätes)
`-a INT`	Setzt die Intranet-Adresse des Gerätes als Absenderadresse
`-a DMZ`	Setzt die DMZ-Adresse des Gerätes als Absenderadresse
`-a LBx`	Setzt eine der 16 Loopback-Adressen im Gerät als Absenderadresse. Gültige Werte für x sind die Hexadezimalen Werte 0-f
`-6 <IPv6-Address>%<Scope>`	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus. Der Parameter-Bereich ist bei IPv6 von zentraler Bedeutung: Da ein IPv6-Gerät sich mit mehreren Schnittstellen (logisch oder physikalisch) pro Schnittstelle eine Link-Lokale-Adresse (fe80::/10) teilt, müssen Sie beim Ping auf eine Link-Lokale-Adresse immer den Bereich (Scope) angeben. Nur so kann das Ping-Kommando die Schnittstelle bestimmen, über die es das Paket senden soll. Den Namen der Schnittstelle trennen Sie durch ein Prozentzeichen (%) von der IPv6-Adresse. **Beispiele:** ▪ `ping -6 fe80::1%INTRANET` Ping auf die Link-Lokale-Adresse "fe80::1", die über die Schnittstelle bzw. das Netz "INTRANET" zu erreichen ist. ▪ `ping -6 2001:db8::1` Ping auf die globale IPv6-Adresse "2001:db8::1".
`-6 <Loopback-Interface>`	Setzt ein IPv6-Loopback-Interface als Absenderadresse.
`-f`	flood ping: Sendet große Anzahl von Ping-Signalen in kurzer Zeit. Kann z. B. zum Testen der Netzwerkbandbreite genutzt werden. ACHTUNG: flood ping kann leicht als DoS Angriff fehlinterpretiert werden.
`-n`	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück
`-o`	Schickt nach einer Antwort sofort eine weitere Anfrage
`-q`	Ping-Kommando liefert keine Ausgaben auf der Konsole
`-r`	Wechselt in Traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt
`-s n`	Setze Größe der Pakete auf n Byte (max. 65500)
`-i n`	Zeit zwischen den einzelnen Paketen in Sekunden
`-c n`	Sende n Ping-Signale
`Destination`	Adresse oder Hostnamen des Zielcomputers

Parameter	Bedeutung
`stop /<RETURN>`	Die Eingabe von “stop” oder das Drücken der RETURN-Taste beenden das Ping-Kommando



Übersicht der Parameter im trace-Befehl

Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Kommandozeile angezeigt werden.

Tabelle 2: Übersicht aller durchführbaren Traces

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
`Status`	Status-Meldungen der Verbindungen
`Fehler`	Fehler-Meldungen der Verbindungen
`IPX-Router`	IPX-Routing **wohl** > **an** > **des** tests **nicht**.
`PPP`	Verhandlung des PPP-Protokolls
`SAP`	IPX Service Advertising Protocol
`IPX-Watchdog`	IPX-Watchdog-Spoofing
`SPX-Watchdog`	SPX-Watchdog-Spoofing
`LCR`	Least-Cost-Router
`Script`	Script-Verhandlung

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
IPX-RIP	IPX Routing Information Protocol
Firewall	Zeigt die Aktionen der Firewall
RIP	IP Routing Information Protocol
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
IP-Masquerading	Vorgänge im Masquerading-Modul
DHCP	Dynamic Host Configuration Protocol
NetBIOS	NetBIOS-Verwaltung
DNS	Domain Name Service Protocol
Paket-Dump	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
D-Kanal-Dump	Trace des D-Kanals des angeschlossenen ISDN-Busses
ATM-Cell	ATM-Paketebene
ATM-Error	ATM-Fehler
ADSL	ADSL-Verbindungsstatus
SMTP-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
Mail-Client	E-Mail-Verarbeitung des integrierten Mail-Clients
SNTP	Simple Network Time Protokoll
NTP	Timeserver Trace
Connact	Meldungen aus dem Aktivitätsprotokoll
Cron	Aktivitäten der Zeitautomatik (Cron-Tabelle)
RADIUS	RADIUS-Trace
Serial	Informationen über den Zustand der seriellen Schnittstelle
USB	Informationen über den Zustand der USB-Schnittstelle
Load-Balancer	Informationen zum Load Balancing
VRRP	Informationen über das Virtual Router Redundancy Protocol
Ethernet	Informationen über die Ethernet-Schnittstellen
VLAN	Informationen über virtuelle Netzwerke
IGMP	Informationen über das Internet Group Management Protocol
WLAN	Informationen über die Aktivitäten in den Funknetzwerken
WLAN-ACL	Status-Meldungen über MAC-Filterregeln. Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.
IAPP	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
DFS	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
Bridge	Informationen über die WLAN-Bridge

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
EAP	Trace zum EAP, dem bei WPA/802.11i und 802.1x verwendeten Protokoll zur Schlüsselaushandlung
Spgtree	Informationen zum Spanning Tree Protokoll
LANAUTH	LAN-Authentifizierung (z. B. Public Spot)
SIP-Packet	SIP-Informationen, die zwischen einem VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
VPN-Status	IPSec und IKE Verhandlungen
VPN-Packet	IPSec und IKE Pakete
GRE	Meldungen zu GRE-Tunneln
XML-Interface-PbSpot	Meldungen des Public-Spot-XML-Interfaces
hnat	Informationen zum Hardware-NAT
IPv6-Config	Informationen über die IPv6-Konfiguration
IPv6-Firewall	Ereignisse der IPv6-Firewall
IPv6-Interfaces	Informationen der IPv6-Schnittstellen
IPv6-LAN-Packet	Datenpakete über die IPv6-LAN-Verbindung
IPv6-Router	Informationen über das IPv6-Routing
IPv6-WAN-Packet	Datenpakete über die IPv6-WAN-Verbindung

Übersicht der IPv6-spezifischen show-Befehle

Über die Kommandozeile besteht die Möglichkeit, diverse IPv6-Funktionen abzufragen. Folgende Kommando-Funktionen stehen Ihnen zur Verfügung:

- *IPv6-Adressen*: `show ipv6-adresses`
- *IPv6-Präfixe*: `show ipv6-prefixes`
- *IPv6-Interfaces*: `show ipv6-interfaces`
- *IPv6-Neighbour Cache*: `show ipv6-neighbour-cache`
- *IPv6-DHCP-Server*: `show dhcp6-server`
- *IPv6-DHCP-Client*: `show dhcpv6-client`
- *IPv6-Route*: `show ipv6-route`

Darüber hinaus lässt sich die IPv6-Kommunikation über das `trace`-Kommando mitverfolgen.

IPv6-Adressen

Der Befehl `show ipv6-adresses` zeigt eine aktuelle Liste der genutzten IPv6-Adressen. Diese ist nach Interfaces sortiert. Hierbei ist zu beachten, dass ein Interface mehrere IPv6-Adressen haben kann. Eine dieser Adressen ist immer die Link lokale Adresse, welche mit `fe80:` beginnt.

Die Ausgabe ist folgendermaßen formatiert:

```
<Interface> :
<IPv6-Adresse>, <Status>, <Attribut>, (<Typ>)
```

Tabelle 3: Bestandteile der Kommandozeilenausgabe `show ipv6-adresses`

Ausgabe	Erläuterung
Interface	Der Name des Interfaces

Ausgabe	Erläuterung
IPv6-Adresse	Die IPv6-Adresse
Status	Das Statusfeld kann folgende Werte beinhalten: ■ TENTATIVE Die Duplicate Address Detection (DAD) prüft die Adresse momentan. Sie steht daher einer Verwendung für Unicast noch nicht zu Verfügung. ■ PREFERRED Die Adresse ist gültig ■ DEPRICATED Die Adresse ist noch gültig, befindet sich aber im Status der Abkündigung. Eine Adresse mit dem Status PREFERRED wird für die Kommunikation bevorzugt. ■ INVALID Die Adresse ist ungültig und kann nicht zur Kommunikation genutzt werden. Eine Adresse erhält diesen Status, nachdem die Lifetime ausgelaufen ist.
Attribut	Zeigt ein Attribut der IPv6-Adresse an. Mögliche Attribute sind: ■ None keine besonderen Eigenschaften ■ (ANYCAST) es handelt sich um eine Anycast-Adresse ■ (AUTO CONFIG) es handelt sich um eine über die Autokonfiguration bezogene Adresse ■ (NO DAD PERFORMED) es wird keine DAD durchgeführt
Type	Der Typ der IP-Adresse

IPv6-Präfixe

Der Befehl `show ipv6-prefixes` zeigt alle bekannten Präfixe an. Die Sortierung erfolgt nach folgenden Kriterien:

- **Delegated prefixes:** Alle Präfixe, die der Router delegiert bekommen hat.
- **Advertised prefixes:** Alle Präfixe, die der Router in seinen Router-Advertisements ankündigt.
- **Deprecated prefixes:** Alle Präfixe, die derzeit abgekündigt werden. Diese sind noch funktional, werden allerdings nach einem bestimmten Zeitrahmen gelöscht.

IPv6-Interfaces

Der Befehl `show ipv6-interfaces` zeigt eine Liste der IPv6 Interfaces und deren jeweiligen Status.

Die Ausgabe ist folgendermaßen formatiert:

<Interface> : <Status>, <Forwarding>, <Firewall>

Tabelle 4: Bestandteile der Kommandozeilenausgabe `show ipv6-interfaces`

Ausgabe	Erläuterung
Interface	Der Name des Interfaces
Status	Der Status des Interfaces. Mögliche Einträge sind: ■ oper Status is up

Ausgabe	Erläuterung
	■ oper Status is down
Forwarding	Der Forwarding Status des Interfaces. Mögliche Einträge sind: ■ forwarding is enabled ■ forwarding is disabled
Firewall	Der Status der Firewall. Mögliche Einträge sind: ■ firewall is enabled ■ firewall is disabled

IPv6-Neighbour Cache

Der Befehl `show ipv6-neighbour-cache` zeigt den aktuellen Neighbour Cache an.

Die Ausgabe ist folgendermaßen formatiert:

```
<IPv6-Adresse> iface <Interface> lladdr <MAC-Adresse> (<Switchport>) <Gerätetyp> <Status>
 src <Quelle>
```

Tabelle 5: Bestandteile der Kommandozeilenausgabe `show ipv6-neighbour-cache`

Ausgabe	Erläuterung
IPv6-Adresse	Die IPv6-Adresse des benachbarten Gerätes
Interface	Das Interface, über das der Nachbar erreichbar ist
MAC-Adresse	Die MAC-Adresse des Nachbarn
Switchport	Der Switchport, auf dem der Nachbar festgestellt wurde
Gerätetyp	Gerätetyp des Nachbarn (Host oder Router)
Status	Der Status der Verbindung zum benachbarten Gerät. Mögliche Einträge sind: ■ INCOMPLETE Die Auflösung der Adresse ist noch im Gange und die Link Layer Adresse des Nachbarn wurde noch nicht bestimmt. ■ REACHABLE Der Nachbar ist in den letzten zehn Sekunden erreichbar gewesen. ■ STALE Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber eine Aktualisierung wird erst durchgeführt, wenn versucht wird ihn zu erreichen. ■ DELAY Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber es wurden vor kurzem Daten an ihn gesendet und auf Verifikation durch andere Protokolle gewartet. ■ PROBE Der Nachbar ist nicht länger als REACHABLE qualifiziert. Es werden Neighbour Solicitation Probes an ihn gesendet um die Erreichbarkeit zu bestätigen.
Quelle	Die IPv6-Adresse, über die der Nachbar entdeckt wurde.

IPv6-DHCP-Server

Der Befehl `show dhcpv6-server` zeigt den aktuellen Status des DHCP-Servers. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Server aktiv ist, welche DNS-Server und Präfixe er hat sowie welche Präferenz er für die Clients besitzt.

IPv6-DHCP-Client

Der Befehl `show dhcpv6-client` zeigt den aktuellen Status des DHCP-Clients. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Client aktiv ist sowie darüber, welche DNS-Server und Präfixe er hat.

IPv6-Route

Der Befehl `show ipv6-route` zeigt die vollständige Routing-Tabelle für IPv6 an. Die Anzeigen kennzeichet die im Router fest eingetragenen Routen durch den Anhang [static] und die dynamisch gelernten Routen durch den Anhang [connected]. Die Loopback-Adresse ist durch [loopback] gekennzeichnet. Weitere automatisch generierte Adressen sind mit [local] markiert.

Funktionen zum Editieren der Befehle

Mit den folgenden Befehlen können die Befehle auf der Kommandozeile bearbeitet werden. Die "ESC key sequences" zeigen zum Vergleich die Tastenkombinationen, die auf typischen VT100/ANSI-Terminals verwendet werden:

Funktion	Esc key sequences	Beschreibung
Pfeil nach oben	ESC [A	Springt in der Liste der letzten ausgeführten Befehle eine Position nach oben, in Richtung älterer Befehle.
Pfeil nach unten	ESC [B	Springt in der Liste der letzten ausgeführten Befehle eine Position nach unten, in Richtung neuerer Befehle.
Pfeil nach rechts	Ctrl-F ESC [C	Bewegt die Einfügemarke eine Position nach rechts.
Pfeil nach links	Ctrl-B ESC [D	Bewegt die Einfügemarke eine Position nach links.
Home oder Pos1	Ctrl-A ESC [A ESC [1~ (	Bewegt die Einfügemarke an das erste Zeichen der Zeile.
Ende	Ctrl-E ESC [F ESC OF ESC [4~	Bewegt die Einfügemarke an das letzte Zeichen der Zeile.
Einfg	ESC [ESC [2~	Schaltet um zwischen Einfügemodus und Überschreibemodus.
Entf	Ctrl-D ESC <BS> ESC [3~	Löscht das Zeichen an der aktuellen Position der Einfügemarke oder beendet die Telnet-Sitzung, wenn die Zeile leer ist.
erase	<BS><DEL>	Löscht das nächste Zeichen links neben der Einfügemarke.
erase-bol	Ctrl-U	Löscht alle Zeichen links neben der Einfügemarke.
erase-eol	Ctrl-K	Löscht alle Zeichen rechts neben der Einfügemarke.
Tabulator		Komplettiert die Eingabe von der aktuellen Position der Einfügemarke zu einem Befehl oder Pfad der LCOS-Menüstruktur: **1.** Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. **2.** Wenn es mehrere Möglichkeiten gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Mit einem erneuten Druck auf die Tab-Taste wird eine Liste mit allen Möglichkeiten angezeigt, mit denen die Eingabe vervollständigt werden kann. Geben Sie dann z. B. einen weiteren Buchstaben ein, um ein eindeutiges Vervollständigen der Eingabe zu ermöglichen. **3.** Wenn es keine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Es werden keine weiteren Aktionen ausgeführt.

Funktionstasten für die Kommandozeile

WEBconfig: Setup / Config / Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

- Taste

  Bezeichnung der Funktionstaste.

  Mögliche Werte:

  - Auswahl aus den Funktionstasten F1 bis F12.

  Default:

  - F1

- Abbildung

  Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

  Mögliche Werte:

  - Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

  Default:

  - Leer

  Besondere Werte:

  - Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.
  - ^A steht für Strg-A (ASCII 1)
  - ^Z steht für Strg-Z (ASCII 26)
  - ^[steht für Escape (ASCII 27)
  - ^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst.

Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von Caret-Zeichen + A macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein. Aus Caret-Zeichen + Leerzeichen + A wird dann die Sequenz ^A.

Tab-Kommando beim Scripting

Das `tab`-Kommando aktiviert beim Scripten die gewünschten Spalten einer Tabelle für das nachfolgende `set`-Kommando.

Bei der Konfiguration über ein Kommandozeilen-Tool ergänzen Sie das set-Kommando in der Regel durch die Werte, die Sie den entsprechenden Spalten des Tabelleneintrags zuweisen möchten.

Die Werte für die Performance-Einstellungen eines WLAN-Interfaces setzen Sie z. B. wie folgt:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?

Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 chars from: 1234567890

> set WLAN-1 Yes *
```

In diesem Beispiel umfasst die Tabelle Performance drei Spalten:

- Ifc, also die gewünschte Schnittstelle

- Aktivieren oder Deaktivieren von QoS
- gewünschter Wert für das TX-Bursting

Mit dem Kommando `set WLAN-1 Yes *` aktivieren Sie für das Interface WLAN-1 die QoS-Funktion, den Wert für Tx-Bursting lassen Sie durch die Angabe des * unverändert.

Diese Schreibweise des `set`-Kommandos eignet sich gut für Tabellen mit wenigen Spalten. Tabellen mit sehr vielen Spalten hingegen stellen eine große Herausforderung dar. Die Tabelle unter **Setup** > **Interfaces** > **WLAN** > **Transmission** umfasst z. B. 22 Einträge:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?

Possible Entries for columns in Transmission:
[1][Ifc]              : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17), WLAN-1-4 (18), WLAN-1-5
 (19), WLAN-1-6 (20), WLAN-1-7 (21), WLAN-1-8 (22)
[2][Packet-Size]        : 5 chars from: 1234567890
[3][Min-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M
 (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[9][Max-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M
 (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[4][Basic-Rate]        : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9), 12M (10), 18M
 (11), 24M (12), 36M (13), 48M (14), 54M (15)
[19][EAPOL-Rate]       : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M
(9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15), HT-1-6.5M (28), HT-1-13M
 (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35), HT-2-13M (36),
 HT-2-26M (37), HT-2-39M (38), HT-2-52M (39), HT-2-78M (40), HT-2-104M (41), HT-2-117M
(42), HT-2-130M (43)
[12][Hard-Retries]      : 3 chars from: 1234567890
[11][Soft-Retries]      : 3 chars from: 1234567890
[7][11b-Preamble]       : Auto (0), Long (1)
[16][Min-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4),
 MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15 (8)
[17][Max-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3), MCS-3/11 (4),
 MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15 (8)
[23][Use-STBC]          : No (0), Yes (1)
[24][Use-LDPC]          : No (0), Yes (1)
[13][Short-Guard-Interval]  : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]   : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
[20][Max-Aggr.-Packet-Count]    : 2 chars from: 1234567890
[6][RTS-Threshold]      : 5 chars from: 1234567890
[10][Min-Frag-Len]      : 5 chars from: 1234567890
[21][ProbeRsp-Retries]  : 3 chars from: 1234567890
```

Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 * * * * * * * * * * * * No
```

Die Sternchen für die Werte nach der Spalte für das Short-Guard-Interval sind in diesem Beispiel nicht erforderlich, die Spalten werden automatisch beim Setzen der neuen Werte ignoriert.

Alternativ zu dieser eher unübersichtlichen und fehleranfälligen Schreibweise definieren Sie im ersten Schritt mit dem `tab`-Kommando, welche Spalten der nachfolgende `set`-Befehl verändert:

```
> tab Ifc Short-Guard-Interval
> set WLAN-1-3 No
```

Der `tab`-Befehl erlaubt dabei auch, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> tab Ifc Short-Guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```

Je nach Hardware-Modell enthalten die Tabellen nur einen Teil der Spalten. Der `tab`-Befehl ignoriert Spalten, die in der Tabelle des jeweiligen Geräts fehlen. So haben Sie die Möglichkeit, gemeinsame Scripte für unterschiedliche Hardware-Modelle zu entwickeln. Die `tab`-Anweisungen in den Scripten referenzieren dabei alle maximal erforderlichen Spalten. Je nach Modell führt das Script die `set`-Anweisungen allerdings nur für die tatsächlich vorhandenen Spalten aus.

Den `tab`-Befehl können Sie auch verkürzt über geschweifte Klammern darstellen. Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 {short-guard} No
```

Die geschweiften Klammern ermöglichen ebenfalls, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

Zeichensatz für den SMS-Versand

Der Umfang der in einer SMS verfügbaren Zeichen (max. 160 Zeichen zu je 7 Bit = 1.120 Bit) ergibt sich aus dem GSM-Basiszeichensatz (ingesamt 128 Zeichen) sowie ausgewählten Zeichen aus dem erweiterten GSM-Zeichensatz. Mit dem erweiterten Zeichensatz lassen sich zusätzliche Zeichen darstellen; diese belegen jedoch den doppelten Speicherplatz und reduzieren die maximale Zeichenanzahl entsprechend. Zeichen, die nicht im SMS-Modul implementiert sind, ignoriert das Gerät beim Versand.

Folgende Zeichen sind im **GSM-Basiszeichensatz** definiert:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" bezeichnet in der Übersicht das Leerzeichen. "LF", "CR" und "ESC" bezeichnen die Steuerzeichen für den Zeilenvorschub, den Wagenrücklauf und den Escape auf den erweiterten GSM-Zeichensatz.

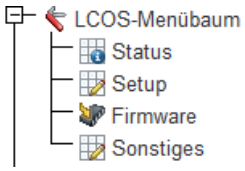
Folgende Zeichen sind aus dem **erweiterten GSM-Zeichensatz** implementiert:

{|}[]~^\€

1.4 Die Konfiguration mit WEBconfig

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im Gerät ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. In einem Netzwerk mit DHCP-Server erreichen Sie das Gerät im Webbrowser unter seiner IP-Adresse.

Der Menübereich "LCOS-Menübaum" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch unter Telnet verwendet wird. Mit einem Klick auf das Fragezeichen können Sie für jeden Konfigurationsparameter eine Hilfe aufrufen.



2 Setup

In diesem Menü finden Sie die Einstellungen des Gerätes.

Pfad Telnet: /Setup

2.1 Name

In diesem Feld können Sie einen beliebigen Namen für Ihr Gerät eintragen.

Pfad Telnet:

Setup

Mögliche Werte:

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

Default-Wert:

leer

2.2 WAN

Dieses Menü enthält die Konfiguration des Wide-Area-Network (WAN).

Pfad Telnet:

Setup

2.2.2 Einwahl-Gegenstellen

Konfigurieren Sie hier die ISDN-Gegenstellen, zu denen Ihr Gerät Verbindungen aufbauen und Daten übertragen soll.

Werden in zwei Gegenstellenlisten (z. B. DSL-Breitband-Gegenstellen und Einwahl-Gegenstellen) Einträge mit identischen Namen für die Gegenstelle vorgenommen, verwendet das Gerät beim Verbindungsaufbau zu der entsprechenden Gegenstelle automatisch das “schnellere” Interface. Das andere Interface wird in diesem Fall als Backup verwendet. Werden in der Liste der DSL-Breitband-Gegenstellen weder Access Concentrator noch Service angegeben, stellt das Gerät eine Verbindung zum ersten AC her, der sich auf die Anfrage über die Vermittlungsstelle meldet. Für ein ggf. vorhandenes DSLoL-Interface gelten die gleichen Einträge wie für ein DSL-Interface. Die Einträge dazu werden in der Liste der DSL-Breitband-Gegenstellen vorgenommen.

Pfad Telnet:

Setup > **WAN**

2.2.2.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.2.2 Rufnummer

Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der RoundRobin-Liste eingetragen werden.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

max. 31 Zeichen aus `0123456789S*#-EF:`

Default-Wert:

leer

2.2.2.3 B1-HZ

Die Verbindung wird abgebaut, wenn sie für die eingestellte Dauer nicht benutzt wurde.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

0 … 9999

Default-Wert:

0

2.2.2.4 B2-HZ

Haltezeit für Bündelungen: Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

0 … 9999

Default-Wert:

0

2.2.2.5 Layername

Wählen Sie einen Eintrag aus der Layer-Liste aus, der für diese Gegenstelle verwendet werden soll.

In der Layer-Liste befinden sich bereits einige Einträge mit häufig benötigten Standardeinstellungen, die Sie hier verwenden können. Den Eintrag PPPHDLC z. B. sollten Sie verwenden, um zu einem Internetprovider eine PPP-Verbindung aufzubauen.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der definierten Layer

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

Default-Wert:

leer

2.2.2.6 Rueckruf

Wenn Sie den Rückruf einschalten, dann wird ein Ruf von dieser Gegenstelle nicht direkt angenommen, sondern die Gegenstelle zurückgerufen.

Dies ist z. B. nützlich, um bei der Gegenseite die Telefongebühren zu minimieren.

Wählen Sie mit Überprüfung des Namens, wenn Sie sicherstellen wollen, dass sich die Gegenstelle authentifizieren muss, bevor der Rückruf erfolgt.

Wenn Sie das schnelle Verfahren wählen, dann kann der Rückruf innerhalb weniger Sekunden erfolgen. Die Gegenstelle muss dieses Verfahren unterstützen und Sie müssen auf der Gegenseite die Option 'Rückruf erwarten' einschalten. Außerdem muss die Gegenstelle in der Nummernliste eingetragen sein.

Die Einstellung 'Name' bietet die höchste Sicherheit, wenn ein Eintrag sowohl in der Nummernliste als auch in der PPP-Liste konfiguriert ist. Die Einstellung 'LANCOM' ermöglicht die schnellste Rückrufmethode zwischen zwei LANCOM-Geräten.

Bei Windows-Gegenstellen muss die Einstellung 'Name' gewählt werden.

Pfad Telnet:

Setup > **WAN** > **Einwahl-Gegenstellen**

Mögliche Werte:

nein

Es wird nicht zurückgerufen.

Auto

Wenn die Gegenstelle in der Nummernliste gefunden wird, so wird diese zurückgerufen. Hierzu wird der Ruf zunächst abgelehnt und, sobald der Kanal wieder frei ist, zurückgerufen (Dauer ca. 8 Sekunden). Wird die Gegenstelle nicht in der Nummernliste gefunden, so wird sie zunächst als DEFAULT-Gegenstelle angenommen, und der Rückruf wird während der Protokollverhandlung ausgehandelt. Dabei fällt eine Gebühr von einer Einheit an.

Name

Bevor ein Rückruf erfolgt, wird immer eine Protokollverhandlung durchgeführt, auch wenn die Gegenstelle in der Nummernliste gefunden wurde (z. B. für Rechner mit Windows, die sich auf dem Gerät einwählen). Dabei fallen geringe Gebühren an.

fast

Wenn die Gegenstelle in der Nummernliste gefunden wird, wird der schnelle Rückruf durchgeführt, d. h., das Gerät sendet ein spezielles Signal zur Gegenstelle und ruft sofort zurück, wenn der Kanal wieder frei ist. Nach ca. 2 Sekunden steht die Verbindung. Nimmt die Gegenstelle den Ruf nicht unmittelbar nach dem Signal zurück, so erfolgt zwei Sekunden später ein Rückfall auf das normale Rückrufverfahren (Dauer wieder ca. 8 Sekunden). Dieses Verfahren steht nur an DSS1-Anschlüssen zur Verfügung.

Looser

Benutzen Sie die Option 'Looser', wenn von der Gegenstelle ein Rückruf erwartet wird. Diese Einstellung erfüllt zwei Aufgaben gleichzeitig. Zum einen sorgt sie dafür, dass ein eigener Verbindungsaufbau zurückgenommen wird, wenn ein Ruf von der gerade angerufenen Gegenstelle hereinkommt, zum anderen wird mit dieser Einstellung die Funktion aktiviert, auf das schnelle Rückruf-Verfahren reagieren zu können. D. h., um den schnellen Rückruf nutzen zu können, muss sich der Anrufer im 'Looser'-Modus befinden, während beim Angerufenen der Rückruf auf 'LANCOM' eingestellt sein muss.

Default-Wert:

nein

2.2.3 RoundRobin

Wenn eine Gegenstelle unter mehreren Rufnummern erreichbar ist, können Sie zusätzliche Rufnummern in dieser Liste eingeben.

Pfad Telnet:

Setup > **WAN**

2.2.3.1 Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

Pfad Telnet:

Setup > **WAN** > **RoundRobin**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

max. 18 Zeichen aus `#[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.2.3.2 Round-Robin

Geben Sie hier die weiteren Rufnummern für diese Gegenstelle ein. Trennen Sie die einzelnen Rufnummern durch Bindestriche.

Pfad Telnet:

Setup > **WAN** > **RoundRobin**

Mögliche Werte:

max. 53 Zeichen aus `0123456789S*#-EF:`

Default-Wert:

leer

2.2.3.3 Anf

Geben Sie an, ob der nächste Verbindungsaufbau mit der zuletzt erfolgreich erreichten Nummer oder immer mit der ersten Nummer durchgeführt werden soll.

Pfad Telnet:

Setup > **WAN** > **RoundRobin**

Mögliche Werte:

letzter
erster

Default-Wert:

letzter

2.2.4 Layer

Stellen Sie hier einzelne Protokolle zu 'Layern' zusammen, die beim Übertragen von Daten zu anderen Routern benutzt werden sollen.

Pfad Telnet:

Setup > **WAN**

2.2.4.1 Layername

Unter diesem Namen wird der Layer in den Gegenstellenlisten ausgewählt.

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

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

Default-Wert:

leer

2.2.4.2 Encaps.

Für die Datenpakete können Sie zusätzliche Kapselungen einstellen.

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

TRANS
Transparent: Keine zusätzliche Kapselung.

ETHER
Ethernet: Kapselung als Ethernet-Frames.

LLC-MUX
Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.

VC-MUX
Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.

Default-Wert:

ETHER

2.2.4.3 Lay-3

Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

PPP
Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d. h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.

APPP
AsyncPPP: Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.

SCPPP
PPP mit eigenem Script. Das Script wird in der Script-Liste angegeben.

SCAPPP
AsyncPPP mit eigenem Script. Das Script wird in der Script-Liste angegeben.

SCTRANS
Transparent mit eigenem Script. Das Script wird in der Script-Liste angegeben.

DHCP
Zuordnung der Netzwerkparameter über DHCP.

TRANS
Transparent: Es wird kein zusätzlicher Header eingefügt.

Default-Wert:

PPP

2.2.4.4 Lay-2

In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert.

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

PPPoE
PPP over Ethernet: Kapselung der PPP-Protokollinformationen in Ethernet-Frames.

TRANS
Transparent: Es wird kein zusätzlicher Header eingefügt.

X.75LABP
Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).

Default-Wert:

X.75LABP

2.2.4.5 L2-Opt.

Hier können Sie die Kompression der übertragenen Daten und die Bündelung von Kanälen aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird. Weitere Informationen finden Sie im Abschnitt 'ISDN-Kanalbündelung mit MLPPP'.

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

keine

compr.

Kompression

bundle

Kanalbündelung

bnd+cmpr

Kanalbündelung + Kompression

Default-Wert:

keine

2.2.4.6 Lay-1

In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) für die WAN-Layer konfiguriert.

Die Umfang der möglichen Werte ist abhängig vom verwendeten Hardware-Modell.

Pfad Telnet:

Setup > **WAN** > **Layer**

Mögliche Werte:

AAL-5

ATM-Anpassungsschicht

ETH

Transparentes Ethernet nach IEEE 802.3

HDLC56K

Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus)

HDLC64K

Sicherung und Synchronisation der Datenübertragung nach HDLC (im 7- oder 8-bit-Modus)

V110_9K6

Übertragung nach V.110 mit maximal 9.600 bit/Sekunde, z. B. für Einwahl per HSCSD-Mobiltelefon

V110_19K2

Übertragung nach V.110 mit maximal 19.200 bit/Sekunde

V110_38K4

Übertragung nach V.110 mit maximal 38.400 bit/Sekunde

SERIAL

Für Verbindungen über ein Analog-Modem oder Mobilfunkmodem mit AT-Schnittstelle. Das Modem kann an das Gerät angeschlossen sein an der seriellen Schnittstelle (Outband) oder mit USB-nach-Seriell-Wandler an einer USB-Schnittstelle. Einige Modelle verfügen über einen CardBus-Slot zur Aufnahme einer entsprechenden Karte. Einige Modelle verfügen über ein integriertes, internes Modem.

MODEM

Für Verbindungen über die interne Modememulation beim Einsatz als V.90 Hostmodem über ISDN. Die Verwendung des internen Modems erfordert ggf. eine zusätzliche Software-Option für das Gerät.

VDSL

VDSL2-Datenübertragung nach ITU G.993.2

Default-Wert:

HDLC64K

2.2.5 PPP

Damit Ihr Gerät PPP- bzw. PPTP-Verbindungen aufbauen kann, müssen Sie in dieser Liste für jede Gegenstelle die entsprechenden Parameter wie Name und Passwort eintragen.

Pfad Telnet:

Setup > **WAN**

2.2.5.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

Mögliche Werte:

Besondere Werte:

DEFAULT

Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim Gerät an. Anhand des Namens kann das Gerät aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über Rufnummer (ISDN-Einwahl), IP-Adresse (PPTP-Einwahl) oder MAC-Adresse (PPPoE-Einwahl) identifiziert werden, die zulässigen Protokolle können also im ersten Schritt nicht ermittelt werden. In diesen Fällen wird die Authentifizierung zunächst mit den Protokollen vorgenommen, die für die Gegenstelle mit dem Namen DEFAULT aktiviert sind. Wenn die Gegenstelle mit diesen Einstellungen erfolgreich authentifiziert wurde, können auch die für die Gegenstelle zulässigen Protokolle ermittelt werden.

Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

2.2.5.2 Authent.request

Verfahren zur Sicherung der PPP-Verbindung, die das Gerät von der Gegenstelle erwartet.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

MS-CHAPv2
MS-CHAP
CHAP
PAP

2.2.5.3 Passwort

Passwort, das von Ihrem Gerät an die Gegenstelle übertragen wird (falls gefordert). Ein '*' in der Liste zeigt an, dass ein Eintrag vorhanden ist.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

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

Default-Wert:

leer

2.2.5.4 Zeit

Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe auch LCP). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z. B. 2 für 20 Sekunden). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein. Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

0 … 99

Default-Wert:

0

2.2.5.5 Wdh.

Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen. Gleichzeitig die

Anzahl der 'Configure Requests', die das Gerät maximal aussendet, bevor es von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

0 … 99

Default-Wert:

5

2.2.5.6 Username

Name, mit dem sich Ihr Gerät bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Name Ihres Gerätes verwendet.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

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

Default-Wert:

leer

2.2.5.7 Conf

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

0 … 255

Default-Wert:

10

2.2.5.8 Fail

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

0 … 255

Default-Wert:

5

2.2.5.9 Term

Mit diesem Parameter wird die Arbeitsweise des PPPs beeinflusst. Der Parameter ist in der RFC 1661 definiert und wird hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in diesem RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise. Im Allgemeinen sind die Default-Einstellungen ausreichend. Dieser Parameter kann nur über LANconfig, SNMP oder TFTP verändert werden.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

0 … 255

Default-Wert:

2

2.2.5.10 Rechte

Gibt die Protokolle an, die zu dieser Gegenstelle geroutet werden können.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

IP
IP+NBT
IPX
IP+IPX
IP+NBT+IPX

Default-Wert:

IP

2.2.5.11 Authent-response

Verfahren zur Sicherung der PPP-Verbindung, die das Gerät bei der Einwahl in eine Gegenstelle anbietet.

Das Gerät verwendet nur die hier aktivierten Protokolle, eine andere Verhandlung mit der Gegenstelle ist nicht möglich.

Pfad Telnet:

Setup > **WAN** > **PPP**

Mögliche Werte:

MS-CHAPv2
MS-CHAP
CHAP
PAP

Default-Wert:

MS-CHAPv2

MS-CHAP

CHAP

PAP

2.2.6 Ankommende Rufnummern

Anhand der Rufnummern in dieser Liste kann Ihr Gerät erkennen, von welcher Gegenstelle ein ankommender Ruf stammt.

Pfad Telnet:

Setup > **WAN**

2.2.6.1 Rufnummer

Tragen Sie hier die Rufnummer ein, die übermittelt wird, wenn Sie von einer bestimmten Gegenstelle angerufen werden. Normalerweise ist das die Nummer der Gegenstelle zusammen mit der zugehörigen Ortsvorwahl samt führender Null, z. B. 0221445566. Bei Gegenstellen im Ausland müssen Sie noch die entsprechende Ländervorwahl mit zwei führenden Nullen voranstellen, z. B. 0049221445566.

Pfad Telnet:

Setup > **WAN** > **Ankommende Rufnummern**

Mögliche Werte:

max. 31 Zeichen aus `0123456789S*#-EF:`

Default-Wert:

leer

2.2.6.2 Gegenstelle

Tragen Sie den Namen der betreffenden Gegenstelle ein. Wenn das Gerät eine Gegenstelle anhand ihrer Rufnummer identifiziert hat, dann wird in der Liste der Gegenstellen ein Eintrag mit dem diesem Namen gesucht und die zugehörigen Einstellungen für die Verbindung verwendet.

Pfad Telnet:

Setup > **WAN** > **Ankommende Rufnummern**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.8 Scripte

Wenn beim Verbinden mit einer Gegenstelle die Abarbeitung eines Login-Scripts notwendig ist, dann tragen Sie es hier ein.

Pfad Telnet:

Setup > **WAN**

2.2.8.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Diese Gegenstelle sollte bereits in der Liste der Gegenstellen vorhanden sein. Sie können auch direkt einen Eintrag aus der Liste der Gegenstellen auswählen.

Pfad Telnet:

Setup > **WAN** > **Skripte**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

max. 18 Zeichen aus `#[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.2.8.2 Script

Geben Sie hier das Login-Script für diese Gegenstelle ein. Damit dieses Script verwendet wird, müssen Sie in der Liste der Gegenstellen für diese Gegenstelle einen Layer mit passenden Protokollen einstellen.

Pfad Telnet:

Setup > **WAN** > **Scripte**

Mögliche Werte:

max. 58 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.2.9 Schutz

Hier stellen Sie ein, unter welchen Umständen das Gerät ankommende Rufe annimmt.

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

kein

Das Gerät nimmt alle Anrufe entgegen.

Nummer

Das Gerät nimmt einen Ruf nur entgegen, wenn der Anrufer in der Nummernliste steht und seine Rufnummer übermittelt wird.

geprueft

Das Gerät nimmt einen Ruf nur entgegen, wenn der Anrufer in der Nummernliste steht, seine Rufnummer übermittelt wird und die übermittelte Rufnummer von der Vermittlungsstelle geprüft wurde.

Default-Wert:

kein

2.2.10 RR-Versuche

Geben sie hier die Anzahl der Rückrufversuche bei Verbindungen mit automatischem Rückruf an.

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

0 … 9

Default-Wert:

3

2.2.11 Router-Interface

Hier können Sie für jedes vom Gerät verwendete WAN-Interface weitere Einstellungen (wie z. B. die Rufnummer) eingeben.

Pfad Telnet:

Setup > **WAN**

2.2.11.1 Ifc

WAN-Interface, auf das sich die Einstellungen aus diesem Eintrag beziehen.

Pfad Telnet:

Setup > **WAN** > **Router-Interface**

2.2.11.2 MSN/EAZ

Geben Sie hier die Rufnummern für dieses Interface an, auf denen das Gerät eingehende Rufe annehmen soll. In der Regel sind diese Nummern die Rufnummern des ISDN-Anschlusses ohne Vorwahl (MSN) beziehungsweise hinter einer Telefonanlage die interne Rufnummer (interne MSN). Sie können mehr als eine Nummer eingeben, indem Sie die einzelnen Nummern durch ein Semikolon voneinander trennen. Dabei wird die erste Rufnummer für ausgehende Rufe verwendet.

Wenn Sie hier eine beliebige Nummer außerhalb Ihres MSN-Nummernpools angeben, nimmt das Gerät gar keine Rufe mehr an.

Wenn Sie hier keine Nummer angeben, nimmt das Gerät jeden Ruf an.

Pfad Telnet:

Setup > **WAN** > **Router-Interface**

Mögliche Werte:

max. 30 Zeichen aus `#0123456789`

Default-Wert:

leer

2.2.11.3 CLIP

Aktivieren Sie diese Option, wenn eine vom Gerät angerufene Gegenstelle Ihre Rufnummer nicht sehen soll.

Diese Funktion muss von Ihrem Netzbetreiber unterstützt werden.

Pfad Telnet:

Setup > **WAN** > **Router-Interface**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.2.11.8 YV.

Y-Verbindung: Legen Sie fest, was geschehen soll, wenn während einer laufenden Verbindung mit Kanalbündelung der Wunsch nach einer zweiten Verbindung zu einer anderen Gegenstelle angemeldet wird.

Bitte beachten Sie, dass bei Verwendung der Kanalbündelung die Kosten für zwei Verbindungen anfallen. Dabei sind keine weiteren Verbindungen über die LANCAPI möglich! Setzen Sie die Kanalbündelung also nur dann ein, wenn die doppelte Übertragungsleistung auch tatsächlich ausgenutzt werden kann.

Pfad Telnet:

Setup > **WAN** > **Router-Interface**

Mögliche Werte:

ja
Das Gerät unterbricht die Bündelverbindung, um die zweite Verbindung zur anderen Gegenstelle aufzubauen. Wenn der zweite Kanal wieder frei wird, holt sich die Bündelverbindung diesen Kanal automatisch wieder zurück (bei statischer Bündelung immer, bei dynamischer nur bei Bedarf).

nein
Das Gerät hält die bestehende Bündelverbindung, die zweite Verbindung muss warten.

Default-Wert:

ja

2.2.11.9 Rufannahme

Geben Sie hier an, ob das Gerät Anrufe auf diesem ISDN-Interface entgegengenommen soll oder nicht.

Haben Sie eine Nummer zur Geräte-Konfiguration angegeben (Management / Admin), so werden Anrufe mit dieser Nummer ungeachtet der hiesigen Auswahl angenommen.

Pfad Telnet:

Setup > **WAN** > **Router-Interface**

Mögliche Werte:

alle
keinen

Default-Wert:

alle

2.2.13 Manuelle Wahl

Dieses Menü enthält die Einstellungen für das manuelle Wählen.

Pfad Telnet:

Setup > **WAN**

2.2.13.1 Aufbau

Baut eine Verbindung zur Gegenstelle auf, die als Parameter angegeben wird.

Pfad Telnet:

Setup > **WAN** > **Manuelle Wahl**

Mögliche Argumente:

<Gegenstelle>

Name einer im Gerät definierten Gegenstelle.

2.2.13.2 Abbau

Trennt die Verbindung zur Gegenstelle, die als Parameter angegeben wird.

Pfad Telnet:

Setup > **WAN** > **Manuelle Wahl**

Mögliche Argumente:

<Gegenstelle>

Name einer im Gerät definierten Gegenstelle.

2.2.18 Backup-St.-Sekunden

Wartezeit bei Ausfall einer Gegenstelle, nach der die Backup-Verbindung aufgebaut wird.

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

0 … 9999 Sekunden

Default-Wert:

30

2.2.19 DSL-Breitband-Gegenstellen

Konfigurieren Sie hier die DSL-Breitband-Gegenstellen, zu denen Ihr Gerät Verbindungen aufbauen und Daten übertragen soll.

Pfad Telnet:

Setup > **WAN**

2.2.19.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.19.2 SH-Zeit

Haltezeit: Geben Sie an, nach wievielen Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

0 … 9999 Sekunden

Besondere Werte:

9999

Sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

Default-Wert:

0

2.2.19.3 AC-Name

Über die Parameter 'Access Concentrator' und 'Service' wird der zu verwendende Internet-Anbieter eindeutig identifiziert. Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.19.4 Servicename

Über die Parameter 'Access Concentrator' und 'Service' wird der zu verwendende Internet-Anbieter eindeutig identifiziert. Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.19.5 Layername

Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.19.9 AC-Name

Über die Parameter 'Access Concentrator' und 'Service' wird der zu verwendende Internet-Anbieter eindeutig identifiziert. Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.19.10 Servicename

Über die Parameter 'Access Concentrator' und 'Service' wird der zu verwendende Internet-Anbieter eindeutig identifiziert. Diese Parameter werden Ihnen von Ihrem Internet-Anbieter mitgeteilt.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.19.11 ATM-VPI

Geben Sie hier den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier) für Ihre ADSL-Verbindung ein. Diese Werte werden Ihnen von Ihrem ADSL-Netzbetreiber mitgeteilt. Übliche Werte für VPI/VCI sind zum Beispiel: 0/35, 0/38, 1/32, 8/35, 8/48.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstelle**

Mögliche Werte:

0 … 999

Default-Wert:

0

2.2.19.12 ATM-VCI

Geben Sie hier den VPI (Virtual Path Identifier) und den VCI (Virtual Channel Identifier) für Ihre ADSL-Verbindung ein. Diese Werte werden Ihnen von Ihrem ADSL-Netzbetreiber mitgeteilt. Übliche Werte für VPI/VCI sind zum Beispiel: 0/35, 0/38, 1/32, 8/35, 8/48.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstelle**

Mögliche Werte:

0 … 99999

Default-Wert:

0

2.2.19.13 ben.-def.-MAC

Tragen Sie hier die zu verwendende eigene MAC-Adresse ein, wenn eine benutzerdefinierte Adresse erforderlich ist.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

max. 12 Zeichen aus `[0-9][a-f]`

Default-Wert:

000000000000

2.2.19.14 DSL-Ifc(s)

Geben Sie hier die Port-Nummer des DSL-Ports an. Es können auch mehrere angegeben werden. Separieren Sie die Liste entweder mit Kommata (1,2,3,4) oder teilen Sie diese in Bereiche (1-4) auf. Aktivieren Sie die Kanal-Bündelung im verwendeten Layer, um DSL-Anschlüsse zu bündeln .

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

max. 8 Zeichen aus `-,01234`

Default-Wert:

0

2.2.19.15 MAC-Typ

Wählen Sie hier aus, welche MAC-Adresse verwendet werden soll.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

global

Wird 'global' gewählt, so wird die Geräte-MAC-Adresse für alle Verbindungen verwendet.

lokal

Wird 'lokal' gewählt, so werden anhand der Geräte-MAC-Adresse weitere virtuelle Adressen für jede WAN-Verbindung gebildet.

ben.-def.

Muss für die Gegenstelle eine bestimmte MAC-Adresse (benutzerdefiniert) definiert sein, so kann diese hier angegeben werden.

Default-Wert:

lokal

2.2.19.16 VLAN-ID

Tragen Sie hier die spezifische ID des VLANs ein, um es auf der DSL-Verbindung eindeutig zu identifizieren.

Pfad Telnet:

Setup > **WAN** > **DSL-Breitband-Gegenstellen**

Mögliche Werte:

0 … 9999

Default-Wert:

0

2.2.20 IP-Liste

Wenn bestimmte Gegenstellen die für eine Verbindung benötigten IP-Parameter nicht automatisch übermitteln, dann tragen Sie diese Werte hier ein.

Nutzen Sie diese Tabelle z. B., um die Extranet-Adresse eines VPN-Tunnels zu konfigurieren.

Pfad Telnet:

Setup > **WAN**

2.2.20.1 Gegenstelle

Geben Sie hier den Namen einer Gegenstelle an.

Bei der Konfiguration eines VPN-Tunnels entspricht dieser Eintrag z. B. der entsprechenden Gegenstelle unter **Setup** > **VPN** > **VPN-Gegenstellen**.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.20.2 IP-Adresse

Wenn Ihr Internet-Anbieter Ihnen eine feste, im Internet gültige IP-Adresse zugewiesen hat, dann tragen Sie diese hier ein. Andernfalls lassen Sie dieses Feld leer. Wenn Sie in Ihrem lokalen Netz einen privaten Adress-Bereich verwenden und dem Gerät eine Adresse aus diesem Bereich zuweisen wollen, dann tragen Sie diese Adresse nicht hier, sondern unter Intranet IP-Adresse ein.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.3 IP-Netzmaske

Geben Sie hier die zur obigen Adresse gehörige Netzmaske ein.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.4 Gateway

Geben Sie hier die Adresse des Standard-Gateways ein.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.5 DNS-Default

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Gerät beim Einloggen automatisch einen Nameserver zuweist, dann können Sie dieses Feld leer lassen.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.6 DNS-Backup

Geben Sie hier einen Nameserver an, der bei Ausfall des ersten DNS verwendet werden soll.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.7 NBNS-Default

Geben Sie hier die Adresse eines Netbios-Nameservers ein, an den NBNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Gerät beim Einloggen automatisch einen Netbios-Nameserver zuweist, dann können Sie dieses Feld leer lassen.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.8 NBNS-Backup

IP-Adresse des NetBIOS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen. Default: 0.0.0.0. Die IP-Adresse des Geräts in diesem Netzwerk wird als NBNS-Server übermittelt, wenn der NetBIOS-Proxy für dieses Netzwerk aktiviert ist. Ist der NetBIOS-Proxy für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als NBNS-Server übermittelt.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.20.9 Masq.-IP-Addr.

Bei fast allen Internet-Providern ist es üblich, dass die Gegenstelle Ihrem Gerät bei der Einwahl eine dynamische IP-Adresse zuteilt. Hat Ihnen Ihr Internet-Provider feste IP-Adressen zugeteilt oder wollen Sie für Ihr VPN-Netzwerk eine Maskierung betreiben, so können Sie diese hier der jeweiligen Verbindung zuweisen. Ist die Maskierungs-IP-Adresse nicht gesetzt, dann wird zur Maskierung die beim Verbindungsaufbau zugewiesene Adresse verwendet.

Das Setzen einer Maskierungsadresse ist für eine VPN-Verbindung erforderlich, wenn ein privates Netz hinter der eigenen Adresse im VPN-Netz maskiert werden soll.

Diese Einstellung ist z. B. auch dann erforderlich, wenn während der PPP-Verhandlung eine private Adresse (172.16.x.x) zugewiesen wird. Damit wäre eine normale Maskierung nicht möglich, da solche Adressen im Internet gefiltert werden.

Pfad Telnet:

Setup > **WAN** > **IP-Liste**

Mögliche Werte:

gültige IPv4-Adresse, max. 15 Zeichen aus `[0-9].`

Default-Wert:

0.0.0.0

2.2.21 PPTP-Gegenstellen

In dieser Tabelle können Sie PPTP-Gegenstellen anzeigen und hinzufügen.

Pfad Telnet:

Setup > **WAN**

2.2.21.1 Gegenstelle

Die Bezeichnung aus der Liste der DSL-Breitband-Gegenstellen.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.21.3 Port

IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

0 … 99999

Default-Wert:

0

2.2.21.4 SH-Zeit

Geben Sie an, nach wie vielen Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

0 … 3600 Sekunden

Default-Wert:

0

Besondere Werte:

9999

Sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

2.2.21.5 Rtg-Tag

Routing-Tag für diesen Eintrag.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.2.21.6 IP-Adresse

Geben Sie hier die IP-Adresse der PPTP-Gegenstelle ein.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.2.21.7 Verschlüsselung

Geben Sie hier die Schlüssellänge an.

Pfad Telnet:

Setup > **WAN** > **PPTP-Gegenstellen**

Mögliche Werte:

Aus
40-Bits
56-Bits
128-Bits

Default-Wert:

Aus

2.2.22 RADIUS

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

Pfad Telnet:

Setup > **WAN**

2.2.22.1 Aktiv

Schaltet die RADIUS-Authentifizierung ein oder aus.

Pfad Telnet:

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

Mögliche Werte:

nein
ja
Exclusiv

Default-Wert:

nein

2.2.22.3 Auth.-Port

Der TCP/UDP-Port, über den der externe RADIUS-Server erreicht werden kann.

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295

Default-Wert:

1812

2.2.22.4 Schlüssel

Geben Sie hier die den Schlüssel (Shared-Secret) Ihres RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Pfad Telnet:

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

Mögliche Werte:

Default-Wert:

0

2.2.22.5 PPP-Operation

Bei der Einwahl von PPP-Gegenstellen können die internen Benutzer-Authentifizierungsdaten aus der PPP-Liste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

Wenn Sie die PPP-Arbeitsweise auf 'Exklusiv' schalten, werden die internen Benutzer-Authentifizierungsdaten ignoriert, ansonsten haben diese Vorrang.

Pfad Telnet:

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

Mögliche Werte:

Ja

Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von PPP-Gegenstellen. Ein in der PPP-Liste vorhandener, passender Eintrag hat allerdings Vorrang.

Nein

Es wird kein externer RADIUS-Server für die Authentifizierung von PPP-Gegenstellen verwendet.

Exklusiv

Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

Default-Wert:

Nein

2.2.22.6 CLIP-Operation

Bei der Einwahl von Gegenstellen kann die interne Rufnummernliste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass der Name des Eintrags der Rufnummer der einwählenden Gegenstelle entspricht.

Pfad Telnet:

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

Mögliche Werte:

Ja

Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von Einwahlgegenstellen. Ein in der Rufnummernliste vorhandener, passender Eintrag hat allerdings Vorrang.

Nein

Es wird kein externer RADIUS-Server für die Authentifizierung von Einwahlgegenstellen verwendet.

Exklusiv

Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von Einwahlgegenstellen. Die Rufnummernliste wird nicht berücksichtigt.

Default-Wert:

Nein

2.2.22.7 CLIP-Passwort

Kennwort für die Anmeldung von Einwahlgegenstellen an einem externen RADIUS-Server.

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass alle Einträge für Rufnummern das hier konfigurierte Kennwort verwenden.

Pfad Telnet:

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

Mögliche Werte:

max. 31 Zeichen aus

Default-Wert:

leer

2.2.22.8 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

Pfad Telnet:

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

Mögliche Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll oder beliebige gültige IP-Adresse

Besondere Werte:

INT

für die Adresse des ersten Intranets

DMZ
für die Adresse der ersten DMZ

LB0 bis LBF
für die 16 Loopback-Adressen

2.2.22.9 Protokoll

Für die Authentifizierung bei einem externen Server kann als Übertragungsprotokoll RADIUS über UDP oder RADSEC über TCP mit TLS verwendet werden.

Pfad Telnet:

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

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

2.2.22.10 Auth.-Protokolle

Verfahren zur Sicherung der PPP-Verbindung, die der externe RADIUS-Server erlaubt. Wenn die Gegenstelle ein Internetprovider ist, den Ihr Gerät anrufen soll, sollten Sie hier kein Verfahren selektieren.

Wenn alle Verfahren selektiert sind, wird jeweils das nächste Verfahren zur Authentifizierung herangezogen, falls das vorherige fehlgeschlagen ist. Wenn keines der Verfahren selektiert ist, wird von der Gegenstelle keine Authentifizierung gefordert.

Pfad Telnet:

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

Mögliche Werte:

MS-CHAPv2
MS-CHAP
CHAP
PAP

Default-Wert:

MS-CHAPv2

MS-CHAP

CHAP

PAP

2.2.22.11 Server-Hostname

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.22.12 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.22.20 L2TP-Aktiv

Hier kann eingestellt werden, ob eine Authentifizierung des Tunnel-Endpunktes über RADIUS erfolgen soll.

Pfad Telnet:

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

Mögliche Werte:

nein

Es findet keine RADIUS-Authentifizierung statt.

ja

Eine RADIUS-Authentifizierung findet statt, wenn in der Tabelle 'L2TP-Endpunkte' das Feld 'Auth-Peer' auf 'ja' steht, aber kein Passwort hinterlegt wurde.

Exclusiv

Es findet immer eine RADIUS-Authentifizierung statt, wenn in der Tabelle 'L2TP-Endpunkte' das Feld 'Auth-Peer' auf 'ja' steht, unabhängig davon, ob ein Passwort angegeben wurde.

Default-Wert:

nein

2.2.22.21 L2TP-Server-Hostname

IP-Adresse des RADIUS-Servers.

Der interne RADIUS-Server des Geräts unterstützt nicht die Tunnel-Authentifizierung. Hierzu wird ein externer RADIUS-Server benötigt.

Pfad Telnet:

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

Mögliche Werte:

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

2.2.22.22 L2TP-Auth.-Port

Der UDP-Port des RADIUS-Servers.

Pfad Telnet:

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

Mögliche Werte:

0 … 65535

2.2.22.23 L2TP-Loopback-Adresse

Die Absender-Adresse, die bei RADIUS-Anfragen genutzt wird.

Pfad Telnet:

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

Mögliche Werte:

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

2.2.22.24 L2TP-Protokoll

Das zu nutzende Protokoll.

Pfad Telnet:

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

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

2.2.22.25 L2TP-Schluessel

Das Shared Secret zwischen Gerät und RADIUS-Server.

Pfad Telnet:

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

Mögliche Werte:

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

2.2.22.26 L2TP-Password

Das Passwort, welches zusammen mit dem Host im RADIUS-Server hinterlegt ist. Nach der Authentifizierung wird vom RADIUS-Server das zu nutzende Passwort für den Tunnel übermittelt.

Pfad Telnet:

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

Mögliche Werte:

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

2.2.22.27 L2TP-Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute für den Tunnel-Endpunkt des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.23 Polling-Tabelle

In dieser Tabelle können Sie für nicht-PPP-basierte Gegenstellen bis zu 4 IP-Adressen angeben, deren Erreichbarkeit zur Überwachung der Verbindung überprüft wird.

Pfad Telnet:

Setup > **WAN**

2.2.23.1 Gegenstelle

Name der Gegenstelle, die über diesen Eintrag geprüft werden soll.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.23.2 IP-Adresse-1

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

gültige IP-Adresse

Default-Wert:

0.0.0.0

2.2.23.3 Zeit

Geben Sie hier das Ping-Intervall ein.

Wenn Sie sowohl hier als auch bei den Wiederholungen '0' eingeben, werden Standardwerte benutzt.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

0

2.2.23.4 Wdh.

Bleibt die Antwort auf einen Ping aus, wird die Gegenstelle in kürzeren Intervallen geprüft. Im Sekundentakt versucht das Gerät dann erneut, die Gegenstelle zu erreichen. Die Anzahl der Wiederholungen gibt an, wie oft dieser Versuch wiederholt wird.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

0 … 255

Default-Wert:

0

Besondere Werte:

0

Verwendet den Standardwert von 5 Wiederholungen.

2.2.23.5 IP-Adresse-2

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

gültige IP-Adresse

Default-Wert:

0.0.0.0

2.2.23.6 IP-Adresse-3

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

gültige IP-Adresse

Default-Wert:

0.0.0.0

2.2.23.7 IP-Adresse-4

IP-Adressen, an die zur Prüfung der Gegenstelle ICMP-Requests gesendet werden.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

gültige IP-Adresse

Default-Wert:

0.0.0.0

2.2.23.8 Loopback-Addr.

Absenderadresse, die in den Ping eingetragen wird und auf der auch die Ping-Antwort erwartet wird.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll oder beliebige gültige IP-Adresse

Besondere Werte:

INT

für die Adresse des ersten Intranets

DMZ

für die Adresse der ersten DMZ

LB0 bis LBF

für die 16 Loopback-Adressen

2.2.23.9 Typ

Über diese Einstellung schalten Sie das Verhalten des Pollings.

Pfad Telnet:

Setup > **WAN** > **Polling-Tabelle**

Mögliche Werte:

erzwungen

Das Gerät pollt im vorgegebenen Intervall. Dieses Verhalten entspricht dem Standardverhalten von LCOS-Versionen <8.00, welche über den Parameter noch nicht verfügten.

auto

Das Gerät pollt nur dann aktiv, wenn keine Daten empfangen wurden. Empfangene ICMP-Pakete gelten nicht als Daten und werden auch weiterhin ignoriert.

Default-Wert:

erzwungen

2.2.24 Backup-Gegenstellen

In dieser Tabelle wird für jede Gegenstelle eine Liste der möglichen Backup-Verbindungen angegeben.

Pfad Telnet:

Setup > **WAN**

2.2.24.1 Gegenstelle

Wählen Sie hier den Namen einer Gegenstelle aus der Gegenstellen-Liste.

Pfad Telnet:

Setup > **WAN** > **Backup-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der Backup-Gegenstellen

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

Default-Wert:

leer

2.2.24.2 Alternative-Gegenstellen

Geben Sie hier eine oder mehrere Gegenstellen für Backup-Verbindungen an.

Pfad Telnet:

Setup > **WAN** > **Backup-Gegenstellen**

Mögliche Werte:

Auswahl aus der Liste der Backup-Gegenstellen

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

Default-Wert:

leer

2.2.24.3 Anf

Geben Sie an, ob der nächste Verbindungsaufbau mit der zuletzt erfolgreich erreichten Nummer oder immer mit der ersten Nummer durchgeführt werden soll.

Pfad Telnet:

Setup > **WAN** > **Backup-Gegenstellen**

Mögliche Werte:

erster
letzter

Default-Wert:

letzter

2.2.25 Aktions-Tabelle

In der Aktions-Tabelle können Sie Aktionen definieren, die ausgeführt werden, wenn sich am Zustand einer WAN-Verbindung etwas ändert.

Pfad Telnet:

Setup > **WAN**

2.2.25.1 Index

Der Index gibt die Position des Eintrags in der Tabelle an und muss daher eindeutig sein. Die Einträge der Aktions-Tabelle werden der Reihe nach ausgeführt, sobald der entsprechende Zustandswechsel der WAN-Verbindung eintritt. Mit dem Eintrag im Feld 'Pruefen-auf' kann das Überspringen von Zeilen je nach Auswertung der Aktion ausgelöst werden. Der Index legt die Position der Einträge in der Tabelle fest (in aufsteigender Reihenfolge) und beeinflusst somit maßgeblich das Verhalten der Aktionen, wenn die Option 'Pruefen-auf' verwendet wird. Über den Index kann außerdem ein Eintrag aus der Aktions-Tabelle über einen Cron-Job angesprochen werden, z. B. um einen Eintrag zu bestimmten Zeiten zu aktivieren oder zu deaktivieren.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

2.2.25.2 Hostname

Name der Aktion. Dieser Name kann mit dem Platzhalter %h (Hostname) in den Feldern 'Aktion' und 'Pruefen-auf' referenziert werden.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

max. 64 Zeichen

Default-Wert:

leer

2.2.25.3 Gegenstelle

Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.25.4 Sperrzeit

Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

0

2.2.25.5 Bedingung

Die Aktion wird ausgeführt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

Aufbau

Die Aktion wird ausgeführt, wenn die Verbindung erfolgreich aufgebaut wurde.

Abbau

Die Aktion wird ausgeführt, wenn die Verbindung durch das Gerät selbst beendet wurde (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).

Ende

Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde (unabhängig vom Grund für den Abbau).

Fehler

Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.

Aufbaufehler

Die Aktion wird ausgeführt, wenn ein Verbindungsaufbau gestartet wurde, die Verbindung aber nicht erfolgreich aufgebaut werden konnte.

Default-Wert:

Aufbau

2.2.25.6 Aktion

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung ausgeführt werden soll. In jedem Eintrag darf nur eine Aktionen ausgeführt werden. Das Ergebnis der Aktionen kann im Feld 'Pruefen-auf' ausgewertet werden.

Prefixe:

- exec: – Mit diesem Prefix leiten Sie alle Befehle ein, wie sie an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion 'exec:do /o/m/d' alle bestehenden Verbindungen beenden.
- dnscheck: – Mit diesem Prefix leiten Sie eine DNS-Namensauflösung ein. Sie können z. B. mit der Aktion 'dnscheck:myserver.dyndns.org' die IP-Adresse des angegebenen Servers ermitteln.
- http: – Mit diesem Prefix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen: http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a (Die Bedeutung der Platzhalter %h und %a wird im folgenden Absatz beschrieben.)
- https: – Wie 'http:', nur über eine verschlüsselte Verbindung.
- gnudip: – Mit diesem Prefix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen: gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
- repeat: – Mit diesem Prefix und der Angabe einer Zeit in Sekunden werden alle Aktionen mit der Bedingung “Aufbau” wiederholt ausgeführt, sobald die Verbindung aufgebaut ist. Mit der Aktion 'repeat:300' werden z. B. alle Aufbau-Aktionen alle fünf Minuten wiederholt.
- mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, wenn eine Verbindung beendet wurde: mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.

Mögliche Variablen zur Erweiterung der Aktionen:

- %a – WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %H – Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %h – wie %h, nur Hostname in Kleinbuchstaben
- %c – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %n – Gerätename

- %s – Seriennummer des Gerätes
- %m – MAC-Adresse des Gerätes (wie im Sysinfo)
- %t – Uhrzeit und Datum, im Format YYYY-MM-DD hh:mm:ss
- %e – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

max. 250 Zeichen

Default-Wert:

leer

2.2.25.7 Pruefen-Auf

Das Ergebnis der Aktion kann hier ausgewertet werden, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen.

Prefixe/Suffixe:

- contains= – Dieses Prefix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
- isequal= – Dieses Prefix prüft, ob das Ergebnis der Aktion der definierten Zeichenkette genau entspricht.
- ?skipiftrue= – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis WAHR liefert.
- ?skipiffalse= – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis FALSCH liefert.

Mögliche Variablen zur Erweiterung der Aktionen:

- %a – WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %H – Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %h – wie %h, nur Hostname in Kleinbuchstaben
- %c – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- %n – Gerätename
- %s – Seriennummer des Gerätes
- %m – MAC-Adresse des Gerätes (wie im Sysinfo)
- %t – Uhrzeit und Datum, im Format YYYY-MM-DD hh:mm:ss
- %e – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

max. 50 Zeichen

Default-Wert:

leer

2.2.25.8 Aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.2.25.9 Besitzer

Besitzer der Aktion. Mit den Rechten dieses Besitzers werden die exec-Aktionen ausgeführt. Verfügt der Besitzer nicht über die notwendigen Rechte (z. B. Administratoren mit Leserechten), so kann die Aktion nicht ausgeführt werden.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

Auswahl aus den im Gerät definierten Administratoren

max. 16 Zeichen

Default-Wert:

root

2.2.25.10 Routing-Tag

Um Aktionen in der Aktionstabelle einer bestimmten WAN-Verbindung zuzuordnen, benötigen Sie das entsprechende Routing-Tag. Das Gerät führt die Aktion über die mit diesem Routing-Tag gekennzeichnete Verbindung aus.

Pfad Telnet:

Setup > **WAN** > **Aktions-Tabelle**

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.2.26 MTU-Liste

In dieser Tabelle können Sie für bestimmte Gegenstellen eine andere MTU (Maximum Transfer Unit) als die üblicherweise automatisch ausgehandelte definieren.

Pfad Telnet:

Setup > **WAN**

2.2.26.1 Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein. Dieser Name muss mit einem Eintrag in der Liste der Gegenstellen übereinstimmen. Sie können auch direkt einen Namen aus der Liste der Gegenstellen auswählen.

Pfad Telnet:

Setup > **WAN** > **MTU-Liste**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

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

Default-Wert:

leer

2.2.26.2 MTU

Hier können Sie zusätzlich zu den automatischen Bestimmungen der verbindungsspezifischen MTU eine manuell konfigurierbare maximale MTU pro Verbindung definieren. Geben Sie die maximale IP-Paketlänge/-größe in Byte an. Je kleiner der Wert ist, je größer ist die Fragmentierung der Nutzdaten.

Pfad Telnet:

Setup > **WAN** > **MTU-Liste**

Mögliche Werte:

0 … 9999 Byte

Default-Wert:

0

2.2.30 Zusaetzliche-PPTP-Gateways

Definieren Sie hier bis zu 32 zusätzliche Gateways um die Verfügbarkeit von PPTP-Gegenstellen sicherzustellen. Jede der PPTP-Gegenstellen hat die Möglichkeit bis zu 33 Gateways zu benutzen. Die zusätzlichen Gateways definieren Sie in einer zusätzlichen Liste.

Pfad Telnet:

Setup > **WAN**

2.2.30.1 Gegenstelle

Wählen Sie hier aus, für welche PPTP-Gegenstelle dieser Eintrag gelten soll.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

Auswahl aus der Liste der definierten PPTP-Gegenstellen

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

Default-Wert:

leer

2.2.30.2 Anfangen-mit

Wählen Sie hier aus, in welcher Reihenfolge die Einträge versucht werden sollen.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

zuletzt-verwendetem
Wählt den Eintrag, zu dem zuletzt erfolgreich eine Verbindung hergestellt werden konnte.

erstem
Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.

zufaelligem
Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

Default-Wert:

zuletzt-verwendetem

2.2.30.3 Gateway-1

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.4 Rtg-Tag-1

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.5 Gateway-2

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.6 Rtg-Tag-2

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.7 Gateway-3

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.8 Rtg-Tag-3

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.9 Gateway-4

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.10 Rtg-Tag-4

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.11 Gateway-5

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.12 Rtg-Tag-5

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.13 Gateway-6

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.14 Rtg-Tag-6

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.15 Gateway-7

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.16 Rtg-Tag-7

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.17 Gateway-8

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.18 Rtg-Tag-8

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.19 Gateway-9

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.20 Rtg-Tag-9

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.21 Gateway-10

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.22 Rtg-Tag-10

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.23 Gateway-11

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.24 Rtg-Tag-11

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.25 Gateway-12

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.26 Rtg-Tag-12

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.27 Gateway-13

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.28 Rtg-Tag-13

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.29 Gateway-14

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.30 Rtg-Tag-14

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.31 Gateway-15

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.32 Rtg-Tag-15

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.33 Gateway-16

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.34 Rtg-Tag-16

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.35 Gateway-17

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.36 Rtg-Tag-17

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.37 Gateway-18

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.38 Rtg-Tag-18

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.39 Gateway-19

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.40 Rtg-Tag-19

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.41 Gateway-20

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.42 Rtg-Tag-20

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.43 Gateway-21

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.44 Rtg-Tag-21

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.45 Gateway-22

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.46 Rtg-Tag-22

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.47 Gateway-23

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.48 Rtg-Tag-23

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.49 Gateway-24

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.50 Rtg-Tag-24

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.51 Gateway-25

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.52 Rtg-Tag-25

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.53 Gateway-26

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.54 Rtg-Tag-26

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.55 Gateway-27

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.56 Rtg-Tag-27

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.57 Gateway-28

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.58 Rtg-Tag-28

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.59 Gateway-29

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.60 Rtg-Tag-29

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.61 Gateway-30

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.62 Rtg-Tag-30

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.63 Gateway-31

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.64 Rtg-Tag-31

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.30.65 Gateway-32

Tragen Sie hier die IP-Adresse des zusätzlichen Gateways ein, das für diese PPTP-Gegenstelle verwendet werden kann.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

gültige IP-Adresse, max. 63 Zeichen

Default-Wert:

leer

2.2.30.66 Rtg-Tag-32

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Pfad Telnet:

Setup > **WAN** > **Zusaetzliche-PPTP-Gateways**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Besondere Werte:

0

Für den zugehörigen Gateway wird das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

2.2.31 PPTP-Quell-Pruefung

Über diesen Eintrag legen Sie fest, worauf das PPTP (Point-to-Point Tunneling-Protokoll) eingehende Verbindungen prüft.

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

Adresse

Das PPTP prüft ausschließlich die Adresse. Dies entspricht dem Standardverhalten älterer LCOS-Versionen ohne diesen Parameter.

Tag+Adresse

Das PPTP prüft neben der Adresse zusätzlich auch das Routing-Tag des Interfaces, über das die Verbindung aufgebaut werden soll.

Default-Wert:

Adresse

2.2.35 L2TP-Endpunkte

In dieser Tabelle werden die grundsätzlichen Einstellungen zur Konfiguration eines L2TP-Tunnels vorgenommen.

Sollen RAS-Verbindungen ohne Konfiguration in einem Gerät über RADIUS authentifiziert werden, muss in dieser Tabelle ein Default-Eintrag mit folgenden Werten angelegt werden:

Identifier: DEFAULT

Poll: 20

Auth-Peer: ja

Verschleiern: nein

Alle anderen Werte müssen leer bleiben. Wird 'Auth-Peer' im DEFAULT-Eintrag auf 'nein' gesetzt, werden alle Hosts ungeprüft angenommen und nur die PPP-Sessions authentifiziert.

Pfad Telnet:

Setup > **WAN**

2.2.35.1 Identifier

Die Bezeichnung des Tunnel-Endpunkts. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge 'Identifier' und 'Hostname' überkreuz übereinstimmen.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

2.2.35.2 IP-Adresse

Die IP-Adresse des Tunnel-Endpunkts. Anstelle einer IP-Adresse (IPv4 oder IPv6) kann auch ein FQDN angegeben werden.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

2.2.35.3 Rtg-Tag

Hier muss das Tag angegeben werden, welches der Route zum Tunnel-Endpunkt zugewiesen ist.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

2.2.35.4 Port

Der zu nutzende UDP-Port.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

Default-Wert:

1701

2.2.35.5 Poll

Das Polling-Intervall in Sekunden.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

0 … 65535

Default-Wert:

20

2.2.35.6 Hostname

Der Benutzername für die Authentifizierung. Wenn zwischen zwei Geräten ein authentifizierter L2TP-Tunnel aufgebaut werden soll, müssen die Einträge 'Identifier' und 'Hostname' überkreuz übereinstimmen.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

2.2.35.7 Passwort

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

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

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

2.2.35.8 Auth-Peer

Angabe, ob die Gegenstelle authentifiziert werden soll.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.2.35.9 Verschleiern

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

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.2.35.10 Absende-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

Gültiger Eintrag aus der Liste möglicher Adressen.
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
leer

Default-Wert:

2.2.36 L2TP-Zusaetzliche-Gateways

In dieser Tabelle können bis zu 32 redundante Gateways je L2TP-Tunnel angegeben werden.

Pfad Telnet:

Setup > **WAN**

2.2.36.1 Identifier

Die Bezeichnung des Tunnel-Endpunkts, welche auch in der Tabelle L2TP-Endpunkte verwendet wurde.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.2 Anfangen-mit

Mit dieser Einstellung wird festgelegt, welcher redundante Gateway zuerst verwendet wird.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

zuletzt-verwendetem

Es wird der zuletzt erfolgreich verwendete Gateway gewählt.

erstem

Es wird immer mit dem ersten Gateways begonnen.

zufaelligem

Bei jedem Versuch wird ein zufälliger Gateway ausgewählt.

Default-Wert:

zuletzt-verwendetem

2.2.36.3 Gateway-1

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.4 Rtg-Tag-1

Das Routing-Tag der Route, über welche Gateway-1 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.5 Gateway-2

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.6 Rtg-Tag-2

Das Routing-Tag der Route, über welche Gateway-2 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.7 Gateway-3

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.8 Rtg-Tag-3

Das Routing-Tag der Route, über welche Gateway-3 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.9 Gateway-4

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.10 Rtg-Tag-4

Das Routing-Tag der Route, über welche Gateway-4 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.11 Gateway-5

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.12 Rtg-Tag-5

Das Routing-Tag der Route, über welche Gateway-5 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.13 Gateway-6

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.14 Rtg-Tag-6

Das Routing-Tag der Route, über welche Gateway-6 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.15 Gateway-7

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.16 Rtg-Tag-7

Das Routing-Tag der Route, über welche Gateway-7 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.17 Gateway-8

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.18 Rtg-Tag-8

Das Routing-Tag der Route, über welche Gateway-8 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.19 Gateway-9

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.20 Rtg-Tag-9

Das Routing-Tag der Route, über welche Gateway-9 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.21 Gateway-10

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.22 Rtg-Tag-10

Das Routing-Tag der Route, über welche Gateway-10 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.23 Gateway-11

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.24 Rtg-Tag-11

Das Routing-Tag der Route, über welche Gateway-11 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.25 Gateway-12

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.26 Rtg-Tag-12

Das Routing-Tag der Route, über welche Gateway-12 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.27 Gateway-13

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.28 Rtg-Tag-13

Das Routing-Tag der Route, über welche Gateway-13 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.29 Gateway-14

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.30 Rtg-Tag-14

Das Routing-Tag der Route, über welche Gateway-14 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.31 Gateway-15

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.32 Rtg-Tag-15

Das Routing-Tag der Route, über welche Gateway-15 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.33 Gateway-16

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.34 Rtg-Tag-16

Das Routing-Tag der Route, über welche Gateway-16 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.35 Gateway-17

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.36 Rtg-Tag-17

Das Routing-Tag der Route, über welche Gateway-17 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.37 Gateway-18

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.38 Rtg-Tag-18

Das Routing-Tag der Route, über welche Gateway-18 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.39 Gateway-19

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.40 Rtg-Tag-19

Das Routing-Tag der Route, über welche Gateway-19 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.41 Gateway-20

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.42 Rtg-Tag-20

Das Routing-Tag der Route, über welche Gateway-20 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.43 Gateway-21

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.44 Rtg-Tag-21

Das Routing-Tag der Route, über welche Gateway-21 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.45 Gateway-22

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.46 Rtg-Tag-22

Das Routing-Tag der Route, über welche Gateway-22 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.47 Gateway-23

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.48 Rtg-Tag-23

Das Routing-Tag der Route, über welche Gateway-23 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.49 Gateway-24

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.50 Rtg-Tag-24

Das Routing-Tag der Route, über welche Gateway-24 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.51 Gateway-25

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.52 Rtg-Tag-25

Das Routing-Tag der Route, über welche Gateway-25 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.53 Gateway-26

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.54 Rtg-Tag-26

Das Routing-Tag der Route, über welche Gateway-26 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.55 Gateway-27

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.56 Rtg-Tag-27

Das Routing-Tag der Route, über welche Gateway-27 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.57 Gateway-28

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.58 Rtg-Tag-28

Das Routing-Tag der Route, über welche Gateway-28 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.59 Gateway-29

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.60 Rtg-Tag-29

Das Routing-Tag der Route, über welche Gateway-29 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.61 Gateway-30

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.62 Rtg-Tag-30

Das Routing-Tag der Route, über welche Gateway-30 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.63 Gateway-31

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.64 Rtg-Tag-31

Das Routing-Tag der Route, über welche Gateway-31 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.36.65 Gateway-32

Die erste alternative IP-Adresse (IPv4 oder IPv6) oder FQDN des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

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

2.2.36.66 Rtg-Tag-32

Das Routing-Tag der Route, über welche Gateway-32 erreicht werden kann.

Pfad Telnet:

Setup > **WAN** > **L2TP-Zusaetzliche-Gateways**

Mögliche Werte:

0 … 65535

2.2.37 L2TP-Gegenstellen

In dieser Tabelle werden die Tunnel-Endpunkte mit den L2TP-Gegenstellen verknüpft, die in der Routing-Tabelle verwendet werden. Ein Eintrag in dieser Tabelle wird für abgehende Verbindungen benötigt, wenn einer eingehenden Session ein Idle-Timeout ungleich 0 zugeordnet oder die Nutzung eines bestimmten Tunnels erzwungen werden soll.

Pfad Telnet:

Setup > **WAN**

2.2.37.1 Gegenstelle

Name der L2TP-Gegenstelle.

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

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

2.2.37.2 L2TP-Endpunkt

Name des Tunnel-Endpunkts.

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

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

2.2.37.3 SH-Zeit

Idle-Timeout in Sekunden.

Pfad Telnet:

Setup > **WAN** > **L2TP-Gegenstellen**

Mögliche Werte:

0 … 9999

2.2.38 L2TP-Quell-Pruefung

In der Voreinstellung wird die Absenderadresse eines eingehenden Tunnels geprüft. Ist sie Teil der konfigurierten Gateways für den Tunnel oder wurden keine Gateways konfiguriert, so wird der Tunnel zugelassen. Zusätzlich kann auch das Routing-Tag geprüft werden, über das entsprechende Pakete eingehen. Hierbei ist zu beachten, dass nur auf Routing-Tags ungleich 0 geprüft wird.

Pfad Telnet:

Setup > **WAN**

Mögliche Werte:

Adresse
Tag+Adresse

Default-Wert:

Adresse

2.2.40 DS-Lite-Tunnel

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

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

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

Pfad Telnet:

Setup > **WAN**

2.2.40.1 Name

Geben Sie hier eine Bezeichnung für den Tunnel ein.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.40.2 Gateway-Adresse

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.40.3 Rtg-Tag

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.2.45 X.25-Bridge

Dieser Menüpunkt enhält die Einstellungen für die TCP-X.25-Bridge.

Pfad Telnet:

Setup > **WAN**

2.2.45.2 Abgehende-Rufe

Diese Tabelle einhält die Einstellungen für die eingehenden TCP-Verbindungen (der LAN-Gegenstelle) und abgehenden X.25-Verbindungen (zur X.25-Gegenstelle).

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

2.2.45.2.1 Name

Geben Sie einen Namen für den Tabelleneintrag bzw. die zu konfigurierende X.25-Verbindung an.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

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

Default-Wert:

DEFAULT

2.2.45.2.2 Prio

Geben Sie die Priorität der gewählten X.25-Verbindung an. Je kleiner der Wert, desto höher die Priorität..

LCOS sortiert die angezeigten Tabelleneinträge gemäß der gesetzten Prioritäten in absteigender Reihenfolge.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.2.45.2.3 Terminal-IP

Geben Sie die IPv4-Adresse der Gegenstelle in Ihrem LAN an, welche Datenpakete über die gewählte X.25-Verbindung senden darf.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 39 Zeichen aus `[0-9][A-F][a-f]:.`

Besondere Werte:

0.0.0.0

Die TCP-X.25-Bridge ist für sämtliche Gegenstellen in Ihrem LAN benutzbar und auch für Gegenstellen aus dem WAN offen.

Default-Wert:

0.0.0.0

2.2.45.2.4 Terminal-Port

Geben Sie den Port der Gegenstelle in Ihrem LAN an, über den die Gegenstelle die Datenpakete senden darf.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Die TCP-X.25-Bridge erlaubt Verbindungen über einen beliebigen Port.

Default-Wert:

0

2.2.45.2.5 Loopback-Adresse

Geben Sie die IPv4-Adresse an, in deren ARF-Kontext Ihr Gerät vom Terminal kommende Verbindungen annimmt. Die Loopback-Adresse ersetzt hierbei die beiden Angaben IP-Adresse/Routing-Tag. Das Gerät wählt das Routing-Tag und seine lokale Adresse anhand der Loopback-Adresse. Ist die Loopback-Adresse leer, nimmt das Gerät Verbindungen auf jeder Adresse (auch dem WAN!) an.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

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

Default-Wert:

leer

2.2.45.2.6 Lokaler-Port

Geben Sie den TCP-Port an, über den Ihr Gerät eine Verbindung zur X.25-Gegenstelle aufbaut.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

1 … 65535

Default-Wert:

1998

2.2.45.2.7 ISDN-Remote

Geben Sie die ISDN-Rufnummer der X.25-Gegenstelle ein.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 21 Zeichen `[0-9]`

Default-Wert:

0

2.2.45.2.8 ISDN-Lokal

Geben Sie die ISDN-Rufnummer an, die Ihr Gerät als abgehende Nummer einsetzt.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 21 Zeichen `[0-9]`

Default-Wert:

leer

2.2.45.2.9 X.25-Remote

Geben Sie die X.25-Adresse der X.25-Gegenstelle an.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 14 Zeichen `[0-9]`

Default-Wert:

leer

2.2.45.2.10 X.25-Lokal

Geben Sie die X.25-Adresse Ihres Gerätes an.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 14 Zeichen `[0-9]`

Default-Wert:

leer

2.2.45.2.11 Protokoll-ID

Geben Sie die X.25-Protokollnummer ein. Ihr Gerät setzt diese ID als Bytes 0 bis 3 in die X.25-*Userdata* ein.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 8 Zeichen `[0-9][a-f]`

Default-Wert:

00000000

2.2.45.2.12 Userdata

Hinterlegen Sie in den X.25-Paketdaten weitere Zusatzinformationen, die Ihr Gerät an die X.25-Gegenstelle übermittelt.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

max. 8 Zeichen `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`#`

Default-Wert:

leer

2.2.45.2.13 Payload-Groesse

Geben Sie die Größe des X.25-Payloads an. Zulässige Werte sind reine Zweierpotenzen von 16 bis 1024.

Der X.25-Standard erlaubt die Festlegung unterschiedlicher Größen für gesendete und empfangene Pakete. Die Konfiguration bezieht sich auf beide Richtungen.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge** > **Abgehende-Rufe**

Mögliche Werte:

16 … 1024 Byte

Default-Wert:

128

2.2.45.4 Disconnect-Verzoegerung

Über diesen Parameter definieren Sie die Zeit, die das Gerät nach Abbau einer X.25-Verbindung wartet, bevor es die ISDN-Verbindung abbaut. Innerhalb dieser Zeit sind weitere X.25-Verbindungen ohne den kompletten Neuaufbau der ISDN-Verbindung herstellbar.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

Mögliche Werte:

0 … 99 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit. Das Gerät baut ISDN-Verbindungen zusammen mit der X.25-Verbindung ab.

Default-Wert:

5

2.2.45.5 Daten-Trace

Über diesen Parameter aktivieren bzw. deaktivieren Sie den Trace der Datenpakete, welche die X.25-Bridge passieren. Die Ausgabe des Traces erfolgt auf der Konsole, auf der Sie den Trace aktiviert haben.

Pfad Telnet:

Setup > **WAN** > **X.25-Bridge**

Mögliche Werte:

Aus

Das Gerät gibt keine Trace-Daten aus.

Ein

Das Gerät gibt Trace-Daten mit der Richtung der Übertragung und der Anzahl der Datenbytes aus. Beispiel für einen Daten-Trace:

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.
```

Erweitert

Identisch mit **Ein**; das Gerät gibt die Daten jedoch zusätzlich als Dump aus. Beispiel für einen Daten-Trace mit zusätzlichem Dump (verkürzt):

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.

Adr:= 04394380
Len:= 00000100
00000000:  C2 79 .. 46 60  50 8C .. E3 B7 | .6y..GF` P.......
00000010:  2D AE .. 24 5D  E9 B6 .. 40 59 | -.0..U$] ..l..g@Y
00000030:  A5 36 .. 3C 6B  01 21 .. 9D 14 | .6.M..<k .!H..u..
00000040:  94 38 .. 89 AA  54 22 .. 81 F7 | .8..2m.. T".=....
00000050:  E0 7C .. F3 28  B6 E8 .. 74 2F | .|.....( ..a]b.t/
[...]
```

Default-Wert:

Aus

2.2.50 EoGRE-Tunnel

Die aktuelle LCOS-Version stellt mehrere "Ethernet over GRE"-Tunnel (EoGRE) zur Verfügung, um Ethernet-Pakete per GRE zu übertragen. Konfigurieren Sie hier die jeweiligen EoGRE-Tunnel.

Pfad Telnet:

Setup > **WAN**

2.2.50.1 Schnittstelle

Name des gewählten EoGRE-Tunnels.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

2.2.50.2 Aktiv

Aktiviert oder deaktiviert den EoGRE-Tunnel. Deaktivierte EoGRE-Tunnel senden oder empfangen keinen Daten.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.50.3 IP-Adresse

Adresse des EoGRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

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

Default-Wert:

leer

2.2.50.4 Routing-Tag

Routing-Tag für die Verbindung zum EoGRE-Tunnel-Endpunkt.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.2.50.5 Schluessel-vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses EoGRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.50.6 Schluessel

Der Schlüssel, der die Datenflusskontrolle in diesem EoGRE-Tunnel sicherstellt.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

2.2.50.7 Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.50.8 Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem EoGRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.51 GRE-Tunnel

Das GRE-Protokoll tunnelt beliebige Layer-3-Datenpakete (u. a. IP, IPsec, ICMP etc.) über eine Point-to-Point-Netzwerkverbindung, indem es diese Daten mit einem IP-Daten-Gerüst umgibt. Konfigurieren Sie hier die jeweiligen GRE-Tunnel.

Pfad Telnet:

Setup > **WAN**

2.2.51.1 Gegenstelle

Name der Gegenstelle dieses GRE-Tunnels. Verwenden Sie diesen Namen z. B. in der Routing-Tabelle, um Daten durch diesen GRE-Tunnel zu versenden.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

2.2.51.3 IP-Adresse

Adresse des GRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

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

Default-Wert:

leer

2.2.51.4 Routing-Tag

Routing-Tag für die Verbindung zum GRE-Tunnel-Endpunkt.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.2.51.5 Schluessel-vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses GRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.51.6 Schluessel

Der Schlüssel, der die Datenflusskontrolle in diesem GRE-Tunnel sicherstellt.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

2.2.51.7 Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.51.8 Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem GRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.2.51.9 Absende-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das gerät die zugehörige IP-Adresse.

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Gültiger Eintrag aus der Liste möglicher Adressen.
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
leer

Default-Wert:

2.3 Gebuehren

Dieses Menü enthält die Einstellungen für die Gebühren-Verwaltung.

SNMP-ID: 2.3

Pfad Telnet: /Setup

2.3.1 Budget-Einheiten

Geben Sie hier ein, wie viele Gebühreneinheiten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut der Router keine weiteren Verbindungen mehr auf.

SNMP-ID: 2.3.1

Pfad Telnet: /Setup/Gebuehren

Mögliche Werte:

- max. 10 Zeichen

Default: 830

2.3.2 Tage-pro-Periode

Geben Sie einen Zeitraum in Tagen an, der als Basis für die Kontrolle der Gebühren- und Zeit-Limits dienen soll.

SNMP-ID: 2.3.2

Pfad Telnet: /Setup/Gebuehren

Mögliche Werte:

- max. 10 Zeichen

Default: 1

2.3.3 Rest-Budget

Anzeige der Gebühreneinheiten, die im angegebenen Zeitraum noch für Router-Verbindungen zur Verfügung stehen.

SNMP-ID: 2.3.3

Pfad Telnet: /Setup/Gebuehren

2.3.4 Router-Einheiten

Anzeige der Minuten, die im aktuellen Zeitraum schon für Router-Verbindungen verbraucht wurden.

SNMP-ID: 2.3.4

Pfad Telnet: /Setup/Gebuehren

2.3.5 Tabelle-Budget

Diese Tabelle zeigt Ihnen eine Übersicht der konfigurierten Budgets nach Budget-Einheiten sortiert für ihre Schnittstellen an.

SNMP-ID: 2.3.5

Pfad Telnet: /Setup/Gebuehren

2.3.5.1 Ifc.

Schnittstelle, auf die sich der Eintrag bezieht.

SNMP-ID: 2.3.5.1

Pfad Telnet: /Setup/Gebuehren/Tabelle-Budget

2.3.5.2 Budget-Einheiten

Anzeige der Budget-Einheiten, die für diese Schnittstelle schon verbraucht wurden.

SNMP-ID: 2.3.5.2

Pfad Telnet: /Setup/Gebuehren/Tabelle-Budget

2.3.5.3 Rest-Budget

Anzeige der Budget-Einheiten die für diese Schnittstelle noch zur Verfügung stehen.

SNMP-ID: 2.3.5.3

Pfad Telnet: /Setup/Gebuehren/Tabelle-Budget

2.3.5.4 Einheiten

Anzeige der Budget-Einheiten, die bisher auf dieser Schnittstelle verbraucht wurden.

SNMP-ID: 2.3.5.4

Pfad Telnet: /Setup/Gebuehren/Tabelle-Budget

2.3.6 Gesamt-Einheiten

Anzeige der gesamten Einheiten, die auf allen Schnittstellen bisher verbraucht wurden.

SNMP-ID: 2.3.6

Pfad Telnet: /Setup/Gebuehren

Default: 10

2.3.7 Zeit-Tabelle

Diese Tabelle zeigt Ihnen eine Übersicht der konfigurierten Budgets nach Budget-Minuten sortiert für ihre Schnittstellen an.

SNMP-ID: 2.3.7

Pfad Telnet: /Setup/Gebuehren

2.3.7.1 Ifc.

Schnittstelle, auf die sich der Eintrag bezieht.

SNMP-ID: 2.3.7.1

Pfad Telnet: /Setup/Gebuehren/Zeit-Tabelle

2.3.7.2 Budget-Minuten

Anzeige der Budget-Minuten, die für diese Schnittstelle schon verbraucht wurden.

SNMP-ID: 2.3.7.2

Pfad Telnet: /Setup/Gebuehren/Zeit-Tabelle

2.3.7.3 Rest-Minuten

Anzeige der Budget-Minuten, die für diese Schnittstelle noch zur Verfügung stehen.

SNMP-ID: 2.3.7.3

Pfad Telnet: /Setup/Gebuehren/Zeit-Tabelle

2.3.7.4 Minuten-aktiv

Anzeige der Budget-Minuten, in der auf dieser Schnittstelle Datenverbindungen aktiv waren.

SNMP-ID: 2.3.7.4

Pfad Telnet: /Setup/Gebuehren/Zeit-Tabelle

2.3.7.5 Minuten-passiv

Anzeige der Budget-Minuten, in der diese Schnittstelle passiv verbunden war.

SNMP-ID: 2.3.7.5

Pfad Telnet: /Setup/Gebuehren/Zeit-Tabelle

2.3.8 DSL-Breitband-Minuten-Budget

Geben Sie hier ein, wie viele Online-Minuten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut das Gerät keine weiteren Verbindungen mehr auf.

SNMP-ID: 2.3.8

Pfad Telnet: /Setup/Gebuehren

Mögliche Werte:

- max. 10 Zeichen

Default: 600

2.3.9 Rest-DSL-Breitband-Minuten-Aktiv

Anzeige der Minuten, die im angegebenen Zeitraum noch für DSL-Breitband-Verbindungen zur Verfügung stehen.

SNMP-ID: 2.3.9

Pfad Telnet: /Setup/Gebuehren

2.3.10 Router-DSL-Breitband-Budget

Anzeige der Minuten, die im aktuellen Zeitraum schon für DSL-Breitband-Verbindungen verbraucht wurden.

SNMP-ID: 2.3.10

Pfad Telnet: /Setup/Gebuehren

2.3.11 Reserve-DSL-Breitband-Budget

Geben Sie hier ein, wie viele Online-Minuten zusätzlich im oben angegebenen Zeitraum verbraucht werden dürfen, wenn die Reserve aktiviert wird.

SNMP-ID: 2.3.11

Pfad Telnet: /Setup/Gebuehren

Mögliche Werte:

- max. 10 Zeichen

Default: 300

2.3.12 Budgets-Zuruecksetzen

Sie können manuell Einheiten-, Zeit- und Volumen-Budgets zurücksetzen.

Geben Sie als Parameter den Namen der WAN-Verbindung an. Mit '*' als Parameter setzen Sie alle Volumen-Budgets zurück. Wenn Sie keinen Parameter angeben, setzen Sie nur die Einheiten- bzw. Zeit-Zähler zurück.

Indem Sie das aktuelle Budget zurücksetzen, heben Sie auch eine bestehende Gebührensperre auf.

Pfad Telnet:

Setup > **Gebuehren**

2.3.13 Einwahl-Minuten-Budget

Geben Sie hier ein, wie viele Online-Minuten maximal im oben angegebenen Zeitraum verbraucht werden dürfen. Sobald dieses Limit erreicht wird, baut das Gerät keine weiteren Verbindungen mehr auf.

SNMP-ID: 2.3.13

Pfad Telnet: /Setup/Gebuehren

Mögliche Werte:

- max. 10 Zeichen

Default: 210

2.3.14 Rest-Einwahl-Minuten

Anzeige der Minuten, die im angegebenen Zeitraum noch für Einwahl-Verbindungen zur Verfügung stehen.

SNMP-ID: 2.3.14

Pfad Telnet: /Setup/Gebuehren

2.3.15 Router-ISDN-Seriell-Minuten-Aktiv

Anzeige der Minuten, die im aktuellen Zeitraum schon für Einwahl-Verbindungen verbraucht wurden.

SNMP-ID: 2.3.15

Pfad Telnet: /Setup/Gebuehren

2.3.16 Aktivieren-Reserve

Einige Provider bieten die Möglichkeit, bei Erreichen des Daten- oder Zeitvolumen-Limits ein zusätzliches Budget freizuschalten. Mit dieser Aktion können Sie das Budget um ein entsprechendes Daten- bzw. Zeit-Volumen erhöhen.

Geben Sie als zusätzliche Parameter den Namen der WAN-Verbindung sowie die Höhe des Budgets in MB an. Wenn Sie kein Budget angeben, schalten Sie das für diese WAN-Verbindung angegebene Budget erneut frei.

Mit der Aktivierung eines zusätzlichen Budgets heben Sie auch eine bestehende Gebührensperre wieder auf.

Pfad Telnet:

Setup > **Gebuehren**

2.3.17 Volumen-Budgets

Mobilfunk- oder Festnetzanbieter können je nach Vertrag auch bei Flatrates ab einem bestimmten Datenvolumen eine Drosselung der Übertragungsrate aktivieren. In diesem Verzeichnis können Sie für jede Gegenstelle ein Datenvolumen festlegen und eine Aktion definieren, die das Gerät bei Überschreiten dieses Limits ausführen soll.

Pfad Telnet:

Setup > **Gebuehren**

2.3.17.1 Gegenstelle

Name der Gegenstelle, für die dieses Datenvolumen gelten soll.

Pfad Telnet:

Setup > **Gebuehren** > **Volumen-Budgets**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 16 Zeichen

Default:

Leer

2.3.17.2 Limit-MB

Datenvolumen in Megabyte, das für die angegebene Gegenstelle gültig sein soll.

Pfad Telnet:

Setup > **Gebuehren** > **Volumen-Budgets**

Mögliche Werte:

0 - 4.294.967.295 MByte

Max. 10 Zeichen

Besondere Werte:

0: Keine Überwachung des Datenvolumens

Default:

0

2.3.17.3 Aktion

Aktion, die das Gerät bei Überschreiten des Budgets ausführen soll. Mögliche Aktionen sind:

- **syslog**: Das Gerät erzeugt eine Syslog-Nachricht (mit dem Flag "Critical"), die Sie im Syslog-Speicher des Gerätes, über LANmonitor oder einen speziellen Syslog-Client auswerten können.
- **mail**: Das Gerät verschickt eine Benachrichtigung an die Email-Adresse, die Sie unter **Setup** > **Gebuehren** > **Gebuehren-Email** angegeben haben.
- **trennen**: Das Gerät trennt die Verbindung zur Gegenstelle.

> Die Aktion **Verbindung trennen** aktiviert die Gebührensperre. Das Gerät kann bis zum Ablauf des Monats keine Verbindung mehr zu dieser Gegenstelle aufbauen, wenn Sie nicht zuvor das Volumen-Budget für diese Gegenstelle erhöhen.

Sie können auch festlegen, dass das Gerät mehrere Aktionen ausführen soll. Ist die Aktion **trennen** darunter, führt das Gerät diese Aktion als letzte aus.

Pfad Telnet:

Setup > **Gebühren** > **Volumen-Budgets**

Mögliche Werte:

syslog

mail

trennen

Default:

leer

2.3.18 Freie-Netze

Wenn die Datenübertragung bestimmter Netze das Volumen-Budget zu einer Gegenstelle nicht belastet, können Sie diese Netze aus der Erfassung herausnehmen.

Pfad Telnet:

Setup > **Gebuehren**

2.3.18.1 Gegenstelle

Name der Gegenstelle, für die die Ausnahme gelten soll.

Sie können pro Gegenstelle auch mehrere Einträge vornehmen, indem Sie den Gegenstellennamen um das #-Zeichen und eine Ziffer erweitern (z. B. "INTERNET", "INTERNET#1", "INTERNET#2", ...). Das ist dann sinnvoll, wenn Sie explizit eine Ausnahme definieren möchten, die nur temporär aktiv ist. Sobald diese Ausnahme nicht mehr gültig ist, löschen Sie nur den Eintrag mit der entsprechend nummerierten Gegenstelle.

Pfad Telnet:

Setup > **Gebuehren** > **Freie-Netze**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 20 Zeichen

Default:

Leer

2.3.18.2 Freie-Netze

Über diesen Parameter definieren Sie einzelne IPv4- und IPv6-Adressen sowie ganze Netze (in Prefix-Schreibweise, z. B. "192.168.1.0/24"), die von der Budget-Erfassung befreit sind.

Pfad Telnet:

Setup > **Gebuehren** > **Freie-Netze**

Mögliche Werte:

Gültige IPv4- und IPv6-Adresse(n), max. 100 Zeichen. Mehrere Werte trennen Sie durch eine kommaseparierte Liste.

Default:

Leer

2.3.19 Budget-Kontrolle

In diesem Verzeichnis legen Sie fest, wann das Gerät die monatliche Aufzeichnung von vorne beginnt.

Pfad Telnet:

Setup > **Gebuehren**

2.3.19.1 Gegenstelle

Name der Gegenstelle, für die der festgelegte Zeitpunkt gelten soll.

Für den Gegenstellennamen können Sie auch Wildcards verwenden. Die Wildcard "*" gilt in diesem Fall für alle Gegenstellen.

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

Auswahl aus der Liste der definierten Gegenstellen

Max. 16 Zeichen

Default:

Leer

2.3.19.2 Tag

Tag des Monats, an dem das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

1 - 31

Default:

1

2.3.19.3 Stunde

Stunde, zu der das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

0 - 23

Default:

0

2.3.19.4 Minute

Minute, zu der das Gerät das Budget zur Kontrolle des Datenvolumens wieder zurücksetzt.

Pfad Telnet:

Setup > **Gebuehren** > **Budget-Kontrolle**

Mögliche Werte:

0 - 59

Default:

0

2.3.20 Gebuehren-Email

Wenn das Gerät bei Überschreiten des Datenvolumens eine Email versenden soll, geben Sie die Email-Adresse hier an.

Pfad Telnet:

Setup > **Gebuehren**

Mögliche Werte:

gültige Email-Adresse mit bis zu 255 Zeichen

Default:

Leer

2.4 LAN

Hier finden Sie die Einstellungen zum LAN.

SNMP-ID: 2.4

Pfad Telnet: /Setup/LAN

2.4.2 MAC-Adresse

Dies ist die Hardware-Adresse des Netzwerk-Adapters in Ihrem Gerät.

SNMP-ID: 2.4.2

Pfad Telnet: /Setup/LAN/MAC-Adresse

2.4.3 Heap-Reserve

Die Heap-Reserve gibt an, wie viele Blöcke des LAN-Heaps für die Kommunikation mit dem Gerät über HTTP(S)/Telnet(S)/SSH reserviert sind. Sie dient dazu, das Gerät auch im Hochlastfall (oder wenn Queueblöcke verlorengehen) noch erreichen zu können. Wenn die Anzahl der Blöcke im Heap unter den angegebenen Wert fällt, dann werden empfangene Pakete sofort verworfen (außer bei TCP-Paketen, die direkt an das Gerät gerichtet sind).

SNMP-ID: 2.4.3

Pfad Telnet: /Setup/LAN/Heap-Reserve

Mögliche Werte:

- maximal 3 numerische Zeichen im Bereich von 0 bis 999

Default: 10

2.4.8 Trace-MAC

Mit diesem Wert beschränken Sie den Ethernet-Trace auf Pakete, welche die angegebene MAC-Adresse als Ziel- oder Quelladresse haben.

SNMP-ID: 2.4.8

Pfad Telnet: /Setup/LAN/Trace-MAC

Mögliche Werte:

- 12 hexadezimale Zeichen

Default: 000000000000

Besondere Werte: Bei einer Einstellung von 000000000000 gibt der Ethernet-Trace alle Pakete uneingeschränkt aus.

2.4.9 Trace-Level

Für den LAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden.

SNMP-ID: 2.4.9

Pfad Telnet: /Setup/LAN/Trace-Level

Mögliche Werte:

- Numerische Zeichen von 0 bis 255

Default: 255

Besondere Werte:

- 0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde
- 1: zusätzlich die physikalischen Parameter der Pakete (Datenrate, Signalstärke, ...)
- 2: zusätzlich der MAC-Header
- 3: zusätzlich der Layer3-Header (z. B. IP/IPX)
- 4: zusätzlich der Layer4-Header (TCP, UDP, ...)
- 5: zusätzlich der TCP/UDP-Payload
- 255: die Ausgabe ist nicht beschränkt

2.4.10 IEEE802.1x

Dieses Menü enthält die Einstellungen für den eingebauten 802.1x-Supplicant. Das Gerät benötigt diese Einstellungen z. B. dann, wenn es an einem Ethernet-Switch mit aktivierter 802.1x-Authentifizierung angeschlossen ist.

SNMP-ID: 2.4.10

Pfad Telnet: /Setup/LAN/IEEE802.1x

2.4.10.1 Supplicant-Ifc-Setup

Diese Tabelle steuert die Funktion des eingebauten 802.1x-Supplicant für die verfügbaren LAN-Interfaces.

SNMP-ID: 2.4.10.1

Pfad Telnet: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup

2.4.10.1.1 Ifc

Wählen Sie hier aus, für welches LAN-Interface die 802.1x-Supplicant-Einstellungen gelten.

SNMP-ID: 2.4.10.1.1

Pfad Telnet: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Ifc

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren LAN-Interfaces, z. B. LAN-1 oder LAN-2.

Default: LAN-1

2.4.10.1.2 Methode

Wählen Sie hier die Methode aus, mit der sich der 802.1x-Supplicant authentisieren soll.

SNMP-ID: 2.4.10.1.2

Pfad Telnet: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Methode

Mögliche Werte:

- Keine
- MD5
- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2
- PEAP/GTC

Default: Keine

Besondere Werte: Der Wert "Keine" deaktiviert den 802.1x Supplicant auf dem jeweiligen Interface.

2.4.10.1.3 Zugangsdaten

Je nach verwendeter EAP/802.1x-Methode tragen Sie hier die zur Anmeldung erforderlichen Zugangsdaten ein. Für TLS ist hier nichts einzutragen. Die Authentisierung erfolgt dann mit dem im Dateisystem hinterlegen EAP/TLS-Zertifikat). Für alle anderen Methoden tragen Sie hier Benutzernamen und Paßwort in der Schreibweise 'user:password' ein.

SNMP-ID: 2.4.10.1.3

Pfad Telnet: /Setup/LAN/IEEE802.1x/Supplicant-Ifc-Setup/Zugangsdaten

Mögliche Zeichen:

- Max. 64 Alphanumerische Zeichen

Default: Leer

2.4.10.2 Authenticator-Ifc-Setup

Über dieses Menü nehmen Sie die Einstellung für die RADIUS-Authentifizierung von Clients vor, die sich über die LAN-Schnittstellen mit dem Gerät verbinden.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x**

2.4.10.2.1 Ifc

Name der LAN-Schnittstelle.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

2.4.10.2.2 In-Betrieb

Über diesen Parameter legen Sie fest, ob die RADIUS-Authentifizierung von Clients auf der gewählten LAN-Schnittstelle erforderlich ist.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.4.10.2.3 Modus

Bestimmen Sie hier, ob sich ein oder mehrere Clients an dieser Schnittstelle über IEEE 802.1X anmelden dürfen.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

Mögliche Werte:

Einzelner-Host
Nur ein Client kann sich an dieser Schnittstelle anmelden.

Mehrfacher-Host
Mehrere Clients können sich an dieser Schnittstelle anmelden. Es genügt, wenn ein Client sich erfolgreich an der Schnittstelle anmeldet. Automatisch authentifiziert das Gerät damit alle anderen Clients an dieser Schnittstelle. Wenn die Verbindung zum angemeldeten Gerät jedoch beendet ist, können auch alle anderen Clients die Verbindung nicht mehr verwenden.

Mehrfache-Auth.
Mehrere Clients können sich an dieser Schnittstelle anmelden, wobei jeder Client sich jeweils authentifizieren muss.

Default-Wert:

Einzelner-Host

2.4.10.2.4 RADIUS-Server

Über diesen Parameter geben Sie den RADIUS-Server an, über den das Gerät die Authentifizierung von LAN-Clients abwickelt.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

Mögliche Werte:

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

gültige(r) IPv4/v6-Adresse oder FQDN, max. 16 Zeichen aus
`#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

2.4.10.2.5 MAC-Auth.-Umgehung

Falls sich ein Gerät an dieser Schnittstelle authentifizieren soll, das kein IEEE 802.1X unterstützt, aktivieren Sie hier die Option, die MAC-Adresse des Gerätes als Benutzername und Kennwort zu verwenden.

Die MAC-Adresse ist leicht zu fälschen und bietet keinen Schutz vor böswilligen Angriffen.

Pfad Telnet:

Setup > **LAN** > **IEEE802.1x** > **Authenticator-Ifc-Setup**

Mögliche Werte:

nein

Die Authentifizierung über die MAC-Adresse ist nicht möglich.

ja

Die Authentifizierung über die MAC-Adresse ist möglich.

Default-Wert:

nein

2.4.11 Linkup-Melde-Verzoegerung-ms

Mit dieser Einstellung bestimmen Sie die Zeit (in Millisekunden), nach der das LAN-Modul dem Gerät meldet, dass ein Link 'up' ist bzw. erfolgreich hergestellt wurde und die Datenübertragung beginnen kann.

Pfad Telnet:

Setup > **LAN** > **Linkup-Melde-Verzoegerung-ms**

Mögliche Werte:

0 bis 4294967295

Default:

50

2.4.12 HNAT

Mit diese Einstellung aktivieren bzw. deaktivieren Sie die Verwendung des Hardware-NAT auf der QVER-Plattform. Bei aktiviertem HNAT übernimmt die Hardware unter bestimmten Bedingungen das Routing von Daten für WAN-Verbindungen, was einerseits den Durchsatz steigert und andererseits die CPU-Auslastung Ihres Gerätes reduziert.

HNAT ist nur auf Geräten der 1781-Serie mit einem Ethernet-Switch AR8327N sowie dem WLC4006+ verfügbar.

Pfad Telnet:

Setup > **LAN**

Mögliche Werte:

nein

ja

Default:

nein

2.4.13.11.1 Schnittstellen-Buendelung

In dieser Tabelle nehmen Sie die Einstellungen für die Bündelung von physikalischen und logischen Schnittstellen vor.

Die Schnittstellen-Bündelung ermöglicht Ihnen die Übertragung von Datenpaketen auf zwei miteinander gepaarten Schnittstellen. Hierzu dupliziert das Gerät ausgehende Datenpakete und überträgt sie auf jeder der beiden Schnittstellen parallel. Beim Empfang akzeptiert das Gerät zuerst eingehende Datenpakete; Duplikate hingegen erkennt und verwirft das Gerät.

Durch Einsetzen einer Schnittstellen-Bündelung lassen sich die Paketfehlerrate und die Latenzzeiten bei der Datenübertragung reduzieren, dies geht allerdings zu Lasten der maximalen Bandbreite auf der betreffenden Schnittstelle.

Pfad Telnet:

Setup > **LAN**

2.4.13.1 Schnittstellen

In dieser Tabelle nehmen Sie die allgemeinen Einstellungen für die Schnittstellen-Bündelung vor.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung**

2.4.13.1.1 Schnittstelle

Dieser Parameter zeigt die logische Bündel-Schnittstelle, unter der Sie die gewählten logischen und physikalischen Geräte-Schnittstellen bündeln.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

BUNDLE-1
BUNDLE-2

2.4.13.1.2 In-Betrieb

Über diesen Parameter aktivieren oder deaktivieren Sie die Schnittstellen-Bündelung.

Wenn Sie die Bündelung aktivieren, fasst das Gerät die gewählten Geräte-Schnittstellen unter einer gemeinsamen logischen Bündel-Schnittstelle zusammen. Im deaktivierten Zustand bleiben die in der dazugehörigen Tabelle ausgewählten Schnittstellen A und B als eigenständige Schnittstellen nutzbar.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.4.13.1.3 Protokoll

Über diesen Parameter legen Sie das für die Schnittstellen-Bündelung verwendete Protokoll fest.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

PRP
Legt das Parallel Redundancy Protocol (PRP) fest.

2.4.13.1.4 MAC-Adresse

Über diesen Parameter stellen Sie optional eine alternative MAC-Adresse ein, welche die ausgewählte Bündel-Schnittstelle verwendet.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

max. 12 Zeichen aus `[a-f][0-9]`

Besondere Werte:

leer
Wenn Sie dieses Feld leer lassen, verwendet das Gerät die systemweite MAC-Adresse.

Default-Wert:

abhängig von der MAC-Adresse Ihres Gerätes

2.4.13.1.5 Schnittstelle-A

Über diesen Parameter wählen Sie die 1. physikalische oder logische Schnittstelle aus, die das Gerät bündelt.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Auswahl aus den verfügbaren Schnittstellen

Default-Wert:

WLAN-1

2.4.13.1.6 Schnittstelle-B

Über diesen Parameter wählen Sie die 2. physikalische oder logische Schnittstelle aus, die das Gerät bündelt.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **Schnittstellen**

Mögliche Werte:

Auswahl aus den verfügbaren Schnittstellen

Default-Wert:

WLAN-2

2.4.13.11 Schnittstellen

In diesem Menü nehmen Sie die Einstellungen speziell für PRP als Bündelungsprotokoll vor.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

2.4.13.11.1 Schnittstellen

Diese Tabelle enthält die Schnittstellen mit allen PRP-relevanten Einstellungen.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

2.4.13.11.1.1 Schnittstelle

Das Parallele-Redundanz-Protokoll (PRP) ermöglicht redundante Übertragungen auf zwei (gebündelten) Schnittstellen. Dazu wählen Sie zwei Schnittstellen aus, die das Gerät intern zu einer Schnittstelle zusammenfasst. Das Gerät dupliziert ausgehende Pakete, sodass das Gerät alle Pakete auf jeder der beiden Schnittstellen überträgt. Empfangsseitig erkennt das Gerät die Duplikate verwirft sie. Dies führt zu einer geringeren Paketfehlerrate und zu geringeren Latenzen auf der gebündelten Schnittstelle im Vergleich zu einer Übertragung auf einer einzelnen Schnittstelle.

Hier geben Sie den Namen für diese Schnittstellen ein.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

max. 18 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.4.13.11.1.2 Duplikate-annehmen

Schaltet das Weiterleiten von Paket-Duplikaten ein oder aus.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

Besondere Werte:

ja
nein

2.4.13.11.1.3 Transparenter-Modus

Schaltet die Transparente Betriebsart ein oder aus. Wenn die Transparente Betriebsart aktiv ist, leitet der Empfänger von PRP-Paketen die Pakete mit Redundancy Control Trailer weiter.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.4.13.11.1.4 Lebens-Pruefungs-Intervall

Bestimmt, wie oft das Gerät Steuer-Pakete sendet.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

100 … 60000 Millisekunden

Default-Wert:

2000

2.4.13.11.1.5 Knoten-Vergessens-Zeit

Gibt die Zeit an, bis das Gerät einen Knoten aus seiner Knoten- oder Proxy-Knoten-Tabelle löscht.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

1000 … 3600000 Millisekunden

Default-Wert:

60000

2.4.13.11.1.6 Eintrag-Vergessens-Zeit

Legt fest, ab wann das Gerät einen Eintrag aus dem Duplikat-Erkennungs-Puffer löscht.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

10 … 60000 Millisekunden

Default-Wert:

400

2.4.13.11.1.7 Knoten-Reboot-Intervall

Legt die Zeit fest, die ein PRP-Gerät passiv auf einem Link horcht, bis das Gerät Pakete über den Link sendet.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

0 … 60000 Millisekunden

Default-Wert:

500

2.4.11.1.8 Dup-Eliminations-Puffer-Groesse

Begrenzt die Anzahl der Einträge im Duplicate-Erkennungs-Speicher.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

16 … 65536 Einträge/Knoten

Default-Wert:

8192

2.4.13.11.1.9 Sende-Ueberwachungs-Pakete

Legt die Einstellungen zum Versenden von Supervision-Paketen fest.

Pfad Telnet:

LAN > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

0
keine

1
nur-eigene-MAC

2
alle-Knoten

Default-Wert:

2

2.4.13.11.1.10 Knoten-Name

Der Knoten-Name ist die Bezeichnung für den Knoten. Sie haben die Möglichkeit, einen beliebigen Namen festzulegen.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

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

2.4.13.11.1.11 Werte-Sup.-Frames-aus

Schaltet die Überwachung von Steuer-Paketen ein oder aus.

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Buendelung** > **PRP** > **Schnittstellen**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.7 TCP-IP

Dieses Menü enthält die TCP/IP Einstellungen.

SNMP-ID: 2.7

Pfad Telnet: /Setup

2.7.1 Aktiv

Aktiviert oder deaktiviert das TCP-IP-Modul.

SNMP-ID: 2.7.1

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.7.6 Zugangs-Liste

In der Zugangs-Liste werden alle Stationen eingetragen, die Zugang zur Konfiguration des Geräts haben sollen. Wenn die Tabelle keinen Eintrag enthält, können alle Stationen auf das Gerät zugreifen.

SNMP-ID: 2.7.6

Pfad Telnet: /Setup/TCP-IP

2.7.6.1 IP-Adresse

IP-Adresse der Station, die Zugriff auf die Konfiguration des Geräts haben soll.

SNMP-ID: 2.7.6.1

Pfad Telnet: /Setup/TCP-IP/Zugangs-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.7.6.2 IP-Netzmaske

IP-Netzmaske der Station, die Zugriff auf die Konfiguration des Geräts haben soll.

SNMP-ID: 2.7.6.2

Pfad Telnet: /Setup/TCP-IP/Zugangs-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.7.6.3 Rtg-Tag

Routing-Tag zur Auswahl einer bestimmten Route.

SNMP-ID: 2.7.6.3

Pfad Telnet: /Setup/TCP-IP/Zugangs-Liste

Mögliche Werte: max. 5 Zeichen

2.7.6.4 Kommentar

Über diesen Parameter hinterlegen Sie zu dem Eintrag einen Kommentar.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.7.7 DNS-Default

Geben Sie hier die Adresse eines Nameservers ein, an den DNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Gerät beim Einloggen automatisch einen Nameserver zuweist, dann können Sie dieses Feld leer lassen.

SNMP-ID: 2.7.7

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.7.8 DNS-Backup

Geben Sie hier einen Nameserver an, der bei Ausfall des ersten DNS verwendet werden soll.

SNMP-ID: 2.7.8

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.7.9 NBNS-Default

Geben Sie hier die Adresse eines Netbios-Nameservers ein, an den NBNS-Anfragen weitergeleitet werden sollen. Wenn Sie einen Internetprovider oder eine andere Gegenstelle haben, die dem Gerät beim Einloggen automatisch einen Netbios-Nameserver zuweist, dann können Sie dieses Feld leer lassen.

SNMP-ID: 2.7.9

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.7.10 NBNS-Backup

Geben Sie hier einen Netbios-Nameserver an, der bei Ausfall des ersten NBNS verwendet werden soll.

SNMP-ID: 2.7.10

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.7.11 ARP-Aging-Minuten

Hier können Sie eine Zeit in Minuten angeben, nach der die ARP-Tabelle automatisch aktualisiert wird, d.h. alle seit der letzten Aktualisierung nicht mehr angesprochenen Adressen entfernt werden.

SNMP-ID: 2.7.11

Pfad Telnet: /Setup/TCP-IP

Mögliche Werte:

- 1 bis 60 Minuten

Default: 15 Minuten

2.7.12 TCP-Aging-Minuten

Geben Sie eine Zeit in Minuten an, nach der die TCP-Tabelle automatisch aktualisiert wird, d.h. alle seit der letzten Aktualisierung nicht mehr angesprochenen Adressen entfernt werden.

Pfad Telnet:

Setup > **TCP-IP**

Mögliche Werte:

max. 2 Zeichen aus `[0-6]`

1 … 60

Default-Wert:

15

2.7.13 TCP-Max.-Verb.

Beschränken Sie mit diesem Eintrag die maximale Anzahl an TCP-Verbindungen.

Pfad Telnet:

Setup > **TCP-IP**

Mögliche Werte:

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

0 … 255

Besondere Werte:

0

Dieser Wert deaktiviert die Beschränkung der TCP-Verbindungen.

Default-Wert:

0

2.7.16 ARP-Tabelle

Das Address Resolution Protocol (ARP) ermittelt zu einer IP-Adresse die MAC-Adresse und speichert diese Information in der ARP-Tabelle.

SNMP-ID: 2.7.16

Pfad Telnet: /Setup/TCP-IP

2.7.16.1 IP-Adresse

IP-Adresse, zu der eine MAC-Adresse ermittelt wurde.

SNMP-ID: 2.7.16.1

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

2.7.16.2 MAC-Adresse

MAC-Adresse, zu der IP-Adresse aus diesem Eintrag ermittelt wurde.

SNMP-ID: 2.7.16.2

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

2.7.16.3 Letzter-Zugriff

Zeitpunkt des letzten Netzwerkzugriffs dieser Station.

SNMP-ID: 2.7.16.3

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

2.7.16.5 Ethernet-Port

Physikalische Schnittstelle, über welche die Station mit dem Gerät verbunden ist.

SNMP-ID: 2.7.16.5

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

2.7.16.6 Gegenstelle

Gegenstelle, über welche die Station erreicht werden kann.

SNMP-ID: 2.7.16.6

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen.

2.7.16.7 VLAN-ID

VLAN-ID des Netzwerks, in dem sich die Station befindet

SNMP-ID: 2.7.16.7

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle

2.7.16.8 Anschluss

Logische Schnittstelle, mit der das gerät verbunden ist.

SNMP-ID: 2.7.16.8

Pfad Telnet: /Setup/TCP-IP/ARP-Tabelle/Anschluss

Mögliche Werte:

- Ein Parameter aus der Liste der logischen Schnittstellen.

2.7.17 Loopback-Liste

In dieser Tabelle können Sie alternative Adressen konfigurieren.

SNMP-ID: 2.7.17

Pfad Telnet: /Setup/TCP-IP

2.7.17.1 Loopback-Addr.

Hier können Sie optional bis zu 16 Lopback-Adressen konfigurieren. Das Gerät sieht jede dieser Adressen als eigene Adresse an und verhält sich, als hätte es das Paket auf dem LAN empfangen. Dies gilt insbesondere auf maskierten Verbindungen. Antworten auf Pakete an eine Loopback-Adresse werden nicht maskiert.

SNMP-ID: 2.7.17.1

Pfad Telnet: /Setup/TCP-IP/Loopback-Liste

Mögliche 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

Default: 0.0.0.0

2.7.17.2 Name

Hier können Sie einen Namen eingeben mit max. 16 Zeichen

SNMP-ID: 2.7.17.2

Pfad Telnet: /Setup/TCP-IP/Loopback-Liste

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.7.17.3 Rtg-tag

Geben Sie hier das Routing-Tag an, mit dem die Routen zu allen entfernten Gateways ermittelt werden, welche kein eigenes Routing-Tag konfiguriert haben (d.h. das Routing-Tag ist 0).

SNMP-ID: 2.7.17.3

Pfad Telnet: /Setup/TCP-IP/Loopback-Liste

Mögliche Werte:

- 0 bis max 65.535

Default: 0

2.7.20 Nichtlok.-ARP-Replies

Wenn diese Option aktiviert ist, dann beantwortet das Gerät auch ARP-Requests für seine Adresse, wenn die Absenderadresse nicht im eigenen lokalen Netz steht.

SNMP-ID: 2.7.20

Pfad Telnet: /Setup/TCP-IP

2.7.21 Alive-Test

Dieses Menü enthält die Einstellungen des Alive-Tests. Der Alive-Test sendet in konfigurierbaren Abständen einen Ping an eine bestimmte Ziel-Adresse. Wenn die Zieladresse nicht erreichbar ist, führt das Gerät nach definierten Kriterien einen Neustart oder eine andere Aktion durch.

Neben der Definition der Ziel-Adresse und der auszuführenden Aktion besteht die Konfiguration des Alive-Test vor allem aus der Gestaltung der Wiederholungsserien für den Ping und dem Grenzwert für das Auslösen der definierten Aktion. Die dazu erforderlichen Parameter haben folgende Default-Werte:

- Fehler-Limit: 10
- Test-Intervall: 10
- Wiederhol-Intervall: 1
- Wiederhol-Zahl: 1

Mit diesen Einstellungen sendet das Gerät alle 10 Sekunden (Test-Intervall) einen Ping. Wird dieser Ping nicht erfolgreich beantwortet, wiederholt das Gerät den Ping nach 1 Sekunde (Wiederhol-Intervall) genau 1 Mal (Wiederhol-Zahl). Bleibt auch die Antwort auf diesen Ping aus, betrachtet das Gerät die Serie als fehlgeschlagen. Wenn 10 Serien in Folge (Fehler-Limit) fehlschlagen, löst das Gerät die definierte Aktion aus, in diesem Fall also nach 10 x 10 Sekunden = 100 Sekunden.

SNMP-ID: 2.7.21

Pfad Telnet: /Setup/TCP-IP

2.7.21.1 Ziel-Adresse

Die Ziel-Adresse, an welche das Gerät einen Ping sendet.

SNMP-ID: 2.7.21.1

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- Gültige IP-Adresse.

2.7.21.2 Test-Intervall

Das zeitliche Intervall in Sekunden, in welchem das Gerät einen Ping an die Ziel-Adresse sendet. Wenn der Ping nicht beantwortet wird, sendet das Gerät optional in definierten Abständen eine gewünschte Anzahl von Wiederholungen. Mit dieser Konfiguration bildet das Gerät "Serien" von Ping-Versuchen. Nur wenn alle diese Pings nicht beantwortet werden, wird die komplette Serie als nicht erfolgreich gewertet.

Das Produkt aus Fehler-Limit und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

SNMP-ID: 2.7.21.2

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- 0 bis 4294967295 Sekunden

Wählen Sie das Test-Intervall größer als das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Default: 10

2.7.21.3 Wiederhol-Zahl

Dieser Wert gibt an, wie oft das Gerät einen nicht beantworteten Ping an die Ziel-Adresse wiederholt.

SNMP-ID: 2.7.21.3

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- 0 bis 4294967295

Wählen Sie die Wiederhol-Zahl so, dass das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Default: 1

Besondere Werte: Bei einer Wiederhol-Zahl von 0 sendet das Gerät keine erneuten Versuche.

2.7.21.4 Wiederhol-Intervall

Dieser Wert gibt an, in welchem zeitlichen Intervall das Gerät einen nicht beantworteter Ping an die Ziel-Adresse wiederholt.

SNMP-ID: 2.7.21.4

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- 0 bis 4294967295

Wählen Sie das Wiederhol-Intervall so, dass das Produkt aus Wiederhol-Intervall und Wiederhol-Zahl kleiner als das gewählte Test-Intervall ist, damit die gewünschten Wiederholungen innerhalb des Test-Intervalls ausgeführt werden können.

Default: 1

Besondere Werte: Bei einem Wiederhol-Intervall von 0 sendet das Gerät keine erneuten Versuche.

2.7.21.5 Fehler-Limit

Dieser Parameter definiert die Anzahl der aufeinander folgenden fehlerhaften Test-Serien, bevor das Gerät neu startet bzw. bevor die konfigurierte Aktion ausgeführt wird.

Das Produkt aus Fehler-Limit und Test-Intervall definiert die gesamte Dauer, die bis zum Neustart bzw. zur Ausführung der Aktion vergeht.

SNMP-ID: 2.7.21.5

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- 0 bis 4294967295

Default: 10

2.7.21.6 Boot-Typ

Diese Aktion führt das Gerät aus, wenn der Ping an die Ziel-Gegenstelle nicht erfolgreich war.

SNMP-ID: 2.7.21.6

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- Kaltstart: Das Gerät führt einen Kaltstart durch.
- Warmstart: Das Gerät führt einen Warmstart durch.
- Aktion: Das Gerät führt eine konfigurierbare Aktion aus. Konfigurieren Sie die gewünschte Aktion unter `/Setup/TCP-IP/Alive-Test` (siehe auch *Aktion*).

Default: Warmstart

2.7.21.7 Aktion

Tragen Sie hier die Aktion ein, die das Gerät ausführt, wenn die Ziel-Adresse nicht erreichbar ist. Sie können alle Aktionen eintragen, die auch in der Cron-Tabelle gültig sind, d.h. neben CLI-Kommandos können Sie auch HTTP-Zugriffe ausführen oder Mails verschicken.

Die hier eingestellte Aktion wird nur ausgeführt, wenn der Boot-Typ auf den Wert **Aktion** eingestellt ist. Den Boot-Typ konfigurieren Sie unter `/Setup/TCP-IP/Alive-Test/Boot-Typ` (siehe auch *Boot-Typ*).

SNMP-ID: 2.7.21.7

Pfad Telnet: /Setup/TCP-IP/Alive-Test

Mögliche Werte:

- 251 Zeichen

Default: leer

2.7.22 ICMP-bei-ARP-Timeout

Wenn das Gerät ein Paket empfängt, das es aufs LAN senden soll, dann löst es den Empfänger mittels eines ARP-requests auf. Wenn dieser nicht beantwortet wird, dann schicht das Gerät ein "ICMP host unreachable" an den Absender des Pakets zurück.

SNMP-ID: 2.7.22

Pfad Telnet: /Setup/TCP-IP

2.7.30 Netzliste

In dieser Tabelle können Sie die IP-Netzwerke definieren. Diese werden von anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) über den Netzwerknamen referenziert.

SNMP-ID: 2.7.30

Pfad Telnet: /Setup/TCP-IP

2.7.30.1 Netzwerkname

Tragen Sie hier einen eindeutigen Namen ein mit max. 16 Zeichen, über den das Netzwerk von anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) referenziert werden kann.

SNMP-ID: 2.7.30.1

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.7.30.2 IP-Adresse

Wenn Sie in Ihrem lokalen Netz einen privaten Adress-Bereich verwenden, dann tragen Sie hier eine freie Adresse aus diesem Bereich ein. Bei Verwendung von IP-Masquerading sind diese Adressen für entfernte Netze nicht sichtbar, sondern werden durch die für die jeweiligen Gegenstelle gültige Internet IP-Adresse ersetzt.

SNMP-ID: 2.7.30.2

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.7.30.3 IP-Netzmaske

Wenn Sie unter Intranet IP-Adresse eine Adresse aus einem privaten Adress-Bereich eingegeben haben, dann geben Sie hier die zugehörige Netzmaske ein.

SNMP-ID: 2.7.30.3

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 255.255.255.0

2.7.30.4 VLAN-ID

An einer physikalischen Schnittstelle können auch mehrere voneinander getrennte VLANs (die "davor" von einem Switch separiert wurden) gebunden werden. Dazu muss dem Router in jedem dieser VLANs eine eigene Adresse bzw. ein eigenes Netz gegeben werden. Hierzu kann jedem Netzwerk neben den Schnittstellen auch ein VLAN zugewiesen werden, für das es gelten soll. Wenn nun auf einer Schnittstelle ein Paket mit dieser VLAN-ID empfangen wird, so wird dieses Paket dem jeweiligen Netzwerk zugeordnet, d.h. das Netzwerk kann nur von Paketen erreicht werden, die dem selben VLAN entstammen. Pakete die dem Netzwerk selbst entstammen, werden beim Versand mit dieser VLAN-ID markiert. Eine "0" steht für ein ungetaggtes netz (kein VLAN). Achtung: Es ist sehr gefährlich diese ID zu verändern. Man kann sich hier sehr leicht vom Zugriff auf das Gerät aussperren, wenn man keinen Zugang zum zugewiesenen VLAN hat. Beachten Sie außerdem, dass sich diese Einstellung auf den gesamten von diesem Netzwerk verwalteten Verkehr auswirkt. Dies schließt alle Pakete ein, welche durch dieses Netzwerk geleitet werden.

SNMP-ID: 2.7.30.4

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- max 4.094

Default: 0

2.7.30.5 Interface

Wählen Sie hier die Schnittstelle aus, die dem Netzwerk zugeordnet sein soll.

Die in der Liste angegebenen Werte für 'x' variieren je Modell.

Pfad Telnet:

Setup > **TCP-IP** > **Netzliste**

Mögliche Werte:

LAN-1
LAN-x
WLAN-x-x
P2P-x-x
BRG-x

Default-Wert:

LAN-1

2.7.30.6 Quellpruefung

Der Schalter beeinflusst die Adressprüfung der Firewall. "Flexibel" ewartet keine Rückroute, d.h. jede Quelladresse wird akzeptiert, wenn das Gerät selbst angesprochen wurde. Das Gerät kann dadurch wie bisher direkt erreicht werden. "Streng" erwartet dagegen eine explizite Rückroute, damit kein IDS-Alarm ausgelöst wird.

SNMP-ID: 2.7.30.6

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- flexibel
- streng

Default: flexibel

2.7.30.7 Typ

Wählen Sie hier den Typ des Netzwerkes aus (Intranet oder DMZ) oder deaktivieren Sie es.

SNMP-ID: 2.7.30.7

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- Deaktiviert
- Intranet
- DMZ

Default: Intranet

2.7.30.8 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die auf diesem Netzwerk empfangen werden, werden intern mit diesem Tag markiert. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel. Zudem hat dieses Tag Einfluss auf die über IP propagierten Routen und auf die vom NetBIOS-Proxy sichtbaren Hosts und Gruppen.

SNMP-ID: 2.7.30.8

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- max. 65.535

Default: 0

2.7.30.9 Kommentar

Hier können Sie einen Kommentar eintragen.

SNMP-ID: 2.7.30.9

Pfad Telnet: /Setup/TCP-IP/Netzliste

Mögliche Werte:

- max. 64 Zeichen

Default: leer

2.8 IP-Router

Dieses Menü enthält die Einstellungen des IP-Routers.

SNMP-ID: 2.8

Pfad Telnet: /Setup

2.8.1 Aktiv

Schaltet den IP-Router ein oder aus.

SNMP-ID: 2.8.1

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.2 IP-Routing-Tabelle

In dieser Tabelle geben Sie ein, über welche Gegenstellen bestimmte Netzwerke oder Stationen erreicht werden können.

SNMP-ID: 2.8.2

Pfad Telnet: /Setup/IP-Router

2.8.2.1 IP-Adresse

Geben Sie hier die Zieladresse für diese Route ein. Dies kann eine einzelne Station sein, die Sie in Ihr Netz einbinden möchten oder ein ganzes Netzwerk, welches Sie mit Ihrem eigenen koppeln wollen.

SNMP-ID: 2.8.2.1

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.2.2 IP-Netzmaske

Geben Sie hier die zu der eingetragenen IP-Adresse gehörige Netzmaske ein. Wenn Sie nur eine einzelne Station adressieren wollen, geben Sie als Netzmaske 255.255.255.255 ein.

SNMP-ID: 2.8.2.2

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.2.3 Peer-oder-IP

Wählen Sie hier den Router, an den die Pakete für diese Route weitergeleitet werden sollen.

Wählen Sie dazu den Namen einer Gegenstelle aus der Liste der Gegenstellen aus.

Wenn diese Route zu einer anderen Station im lokalen Netz führen soll, geben Sie einfach die IP-Adresse dieser Station ein.

SNMP-ID: 2.8.2.3

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

2.8.2.4 Distanz

Geben Sie hier die Anzahl der Hops zu diesem Router an. Normalerweise brauchen Sie diesen Wert nicht zu setzen, er wird automatisch vom Router kontrolliert.

SNMP-ID: 2.8.2.4

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- 0 bis 16

Default: 0

2.8.2.5 Maskierung

Mit der IP-Maskierung können Sie ein logisches Netzwerk hinter einer einzelnen Adresse (der des Routers) verbergen. Wenn Sie beispielsweise einen Internet-Zugang haben, können Sie so Ihr komplettes Netzwerk an das Internet anbinden.

Bei fast allen Internet-Providern ist es üblich, dass die Gegenstelle Ihrem Gerät bei der Einwahl eine dynamische IP-Adresse zuteilt. Sollte Ihnen Ihr Internet-Provider feste IP-Adressen zugeteilt haben, so können Sie diese in der IP-Parameter-Liste der jeweiligen Verbindung zuweisen.

Wenn Sie die IP-Maskierung für alle LAN-Interfaces aktivieren wollen, wählen Sie „Ein" aus. Wenn Sie feste IP-Adressen für die Rechner in der demilitarisierten Zone (DMZ) zuweisen und dennoch die IP-Maskierung für die Rechner an den übrigen LAN-Interfaces (Intranet) aktivieren wollen, so wählen Sie „Intranet" aus.

Wenn Sie mit diesem Eintrag eine VPN-Verbindung maskieren wollen, wählen Sie „Ein" aus.

Pfad Telnet:

Setup > **IP-Router** > **IP-Routing-Tabelle**

Mögliche Werte:

nein

IP-Maskierung abgeschaltet

Ein

Intranet und DMZ maskieren

Intranet

Nur Intranet maskieren

Default-Wert:

nein

2.8.2.6 Aktiv

Bestimmen Sie hier den Schaltzustand. Die Route kann aktiviert werden und entweder immer via RIP propagiert oder nur dann via RIP propagiert werden, wenn das Zielnetzwerk erreichbar ist.

SNMP-ID: 2.8.2.6

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- Die Route ist aktiviert und wird immer via RIP propagiert (sticky).
- Die Route ist aktiviert und wird via RIP propagiert, wenn das Zielnetzwerk erreichbar ist (konditional).
- Die Route ist aus.

Default: Die Route ist aktiviert und wird immer via RIP propagiert (sticky)

2.8.2.7 Kommentar

Dieses Feld steht für einen Kommentar zur Verfügung.

SNMP-ID: 2.8.2.7

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- max. 64 Zeichen

2.8.2.8 Rtg-Tag

Wenn Sie ein Routing-Tag für diese Route angeben, so wird die Route nur für solche Pakete verwendet, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden.

SNMP-ID: 2.8.2.8

Pfad Telnet: /Setup/IP-Router/IP-Routing-Tabelle

Mögliche Werte:

- max. 65535

Default: 0

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechenden, dekorierenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

2.8.5 Proxy-ARP

Hier können Sie den Proxy-ARP-Mechanismus aktivieren bzw. deaktivieren. Mit Proxy-ARP können Sie entfernte Rechner in Ihr lokales Netz einbinden, so als ständen Sie direkt in Ihrem lokalen Netz.

SNMP-ID: 2.8.5

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.6 ICMP-Redirect-Senden

Hier können Sie wählen, ob ICMP-Redirects gesendet werden sollen.

SNMP-ID: 2.8.6

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- aktiv
- inaktiv

Default: Aktiv

2.8.7 Routing-Methode

Dieses Menü enthält die Konfiguration der Routing-Methode für ihren IP-Router.

SNMP-ID: 2.8.7

Pfad Telnet: /Setup/IP-Router

2.8.7.1 Routing-Methode

Auswertung der ToS- oder DiffServ-Felder.

SNMP-ID: 2.8.7.1

Pfad Telnet: /Setup/IP-Router

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

2.8.7.2 ICMP-Routing-Methode

Geben Sie an, ob der Router ICMP-Pakete gesichert übertragen soll.

SNMP-ID: 2.8.7.2

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- Normal
- gesichert

Default: Normal

2.8.7.3 SYN/ACK-Speedup

Geben Sie an, ob TCP SYN- und ACK-Pakete bevorzugt weitergeleitet werden sollen.

SNMP-ID: 2.8.7.3

Pfad Telnet: /Setup/IP-Router/Routing-Methode

Mögliche Werte:

- aktiv
- inaktiv

Default: Aktiv

2.8.7.4 L2-L3-Tagging

Geben Sie an, was mit den DiffServ-Tags aus Layer-2 passieren soll.

SNMP-ID: 2.8.7.4

Pfad Telnet: /Setup/IP-Router/Routing-Methode

Mögliche Werte:

- Ignorieren
- nach Layer-3 kopieren
- automatisch kopieren

Default: ignorieren

2.8.7.5 L3-L2-Tagging

Geben Sie an, ob die DiffServ-Tags aus Layer-3 nach Layer-2 kopiert werden sollen .

SNMP-ID: 2.8.7.5

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.7.6 Interne-Dienste-routen

Wählen Sie hier aus, ob die internen Dienste über den Router geleitet werden sollen.

SNMP-ID: 2.8.7.6

Pfad Telnet: /Setup/IP-Router/Routing-Methode

Mögliche Werte:

- Ja: Die Pakete für die internen Dienste werden über den Router geleitet.
- Nein: Die Pakete werden direkt an den Absender zurückgeschickt.

Default: Nein

Behandeln Sie die internen Services VPN und PPTP speziell, denn das Routing aller Pakete ohne Ausnahme führt zu einem Performance-Verlust. Das Gerät leitet nur die ersten Pakete weiter, die von diesen Services während der Verbindungsherstellung zum Router geschickt werden, wenn Sie diese Option aktivieren. Weitere Pakete werden an den nächsten Port weitergeleitet.

2.8.8 RIP

Dieses Menü enthält die Konfiguration des RIP für ihren IP-Router.

SNMP-ID: 2.8.8

Pfad Telnet: /Setup/IP-Router

2.8.8.2 R1-Maske

Diese Einstellung ist nur nötig, wenn Sie als RIP-Unterstützung RIP-1 ausgewählt haben. Sie beeinflusst die Bildung von Netzwerkmasken für über RIP gelernte Routen.

SNMP-ID: 2.8.8.2

Pfad Telnet: /Setup/IP-Router/RIP

Mögliche Werte:

- Klasse
- Adresse
- Klasse + Adresse

Default: Klasse

2.8.8.4 WAN-Tabelle

Konfigurieren Sie hier für jede Gegenstelle getrennt die WAN-seitige RIP-Unterstützung

SNMP-ID: 2.8.8.4

Pfad Telnet: /Setup/IP-Router/RIP

2.8.8.4.1 Gegenstelle

Name der Gegenstelle, von der WAN-RIP-Pakete gelernt werden sollen.

SNMP-ID: 2.8.8.4.1

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

Default: Leer

Besondere Werte: Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen per WAN-RIP ihre Netze bekannt geben, während für alle anderen User und Filialen eine statische Netzvergabe existiert, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "RIP_" bekommen. In der WAN-RIP-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "RIP_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

2.8.8.4.2 RIP-Typ

Der RIP-Typ gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden.

SNMP-ID: 2.8.8.4.2

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Aus
- RIP-1
- RIP-1 kompatibel

- RIP 2

Default: Aus

2.8.8.4.3 RIP-lernen

In der Spalte RIP-Accept wird angegeben, ob RIP aus dem WAN akzeptiert wird. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

SNMP-ID: 2.8.8.4.3

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.8.8.4.4 Maskierung

In der Spalte Masquerade wird angegeben ob und wie auf der Strecke maskiert wird. Durch diesen Eintrag ist es möglich, das WAN-RIP auch mit einer leeren Routing-Tabelle zu starten.

SNMP-ID: 2.8.8.4.4

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Auto: Der Maskierungstyp wird aus der Routing-Tabelle entnommen. Existiert für die Gegenstelle kein Routing-Eintrag, so wird nicht maskiert.
- An: Alle Verbindungen werden maskiert.
- Intranet: Verbindungen aus dem Intranet werden maskiert, Verbindungen aus der DMZ gehen transparent hindurch.

Default: Ein

2.8.8.4.5 Dft-Rtg-Tag

In der Spalte Dft-Rtg-Tag steht das für die WAN-Verbindung geltende „Default-Routing-Tag". Alle ungetaggten Routen werden beim Versenden im WAN mit diesem Tag getaggt.

SNMP-ID: 2.8.8.4.5

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.8.8.4.6 Rtg-Tag-Liste

In der Spalte Rtg-Tag-List steht eine kommaseparierte Liste der Tags, die auf dem Interface akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Tags akzeptiert. Steht mindestens ein Tag in der Liste, dann werden nur die Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags propagiert.

Alle vom WAN gelernten Routen werden intern als ungetaggte Routen behandelt und auf das LAN mit dem Default-Tag (0) propagiert. Auf das WAN hingegen werden sie mit dem Tag propagiert, mit dem sie auch gelernt wurden.

SNMP-ID: 2.8.8.4.6

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Komma-separierte Liste mit max. 33 Zeichen

Default: leer

2.8.8.4.7 Poisoned-Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

SNMP-ID: 2.8.8.4.7

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.8.8.4.8 RFC2091

Anders als im LAN sind auf WAN-Strecken regelmäßige Updates alle 30 Sekunden ggf. unerwünscht, weil die Bandbreite beschränkt ist. Daher können nach RFC 2091 alle Routen im WAN nur noch einmal beim Verbindungsaufbau übertragen werden, danach nur noch Updates (triggered Updates).

Da in diesem Fall die Updates explizit angefragt werden, können keine Broadcasts oder Multicasts für die Zustellung der RIP-Nachrichten verwendet werden. Stattdessen muss im Filialgerät die IP-Adresse des nächsten erreichbaren Routers in der Zentrale statisch konfiguriert werden. Der Zentralrouter kann sich aufgrund der Anfragen merken, von welchen Filialroutern er Update-Requests empfangen hat, um etwaige Routenänderungen über passende Messages direkt an das Filialgerät zu senden.

SNMP-ID: 2.8.8.4.8

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Ein
- Aus

Default: Aus

In einem Zentral-Gateway kann die Einstellung "RFC 2091" immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

2.8.8.4.9 Gateway

IP-Adresse des nächsten erreichbaren Routers im Zusammenhang mit RFC 2091.

SNMP-ID: 2.8.8.4.9

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

Besondere Werte: Bei Eingabe von 0.0.0.0 wird die Gateway-Adresse aus der PPP-Verhandlung bestimmt.

In einem Router in der Zentrale kann die RFC 2091 ausgeschaltet werden und die Gateway-Adresse auf 0.0.0.0 bleiben, da sich die Zentrale immer an die Anfragen der Filialen hält.

Das Gerät fällt automatisch auf Standard-RIP zurück, wenn das angegebene Gateway RFC 2091 nicht unterstützt.

In einem Zentral-Gateway kann die Einstellung "RFC 2091" immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

2.8.8.4.10 Rx-Filter

Geben Sie hier den Filter an, der beim Empfang von RIP-Paketen verwendet werden soll.

SNMP-ID: 2.8.8.4.10

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

Default: Leer

2.8.8.4.11 Tx-Filter

Geben Sie hier den Filter an, der beim Versand von RIP-Paketen verwendet werden soll.

SNMP-ID: 2.8.8.4.11

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

Default: Leer

2.8.8.4.12 RIP-senden

Stellen Sie ein, ob RIP auf dem WAN Routen propagiert. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

SNMP-ID: 2.8.8.4.12

Pfad Telnet: /Setup/IP-Router/RIP/WAN-Tabelle/RIP-senden

Mögliche Werte:

- Nein
- Ja

Default: Nein/Aus

2.8.8.4.13 Loopback-Adresse

Geben Sie hier eine Loopback-Adresse an. Mögliche Werte sind:

- Name eines ARF-Netzwerkes
- konfigurierte Loopback-Adresse
- IPv4-Adresse

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **WAN-Tabelle**

Mögliche Werte:

Geben Sie eine gültige IPv4-Adresse ein.

Default-Wert:

leer

2.8.8.5 LAN-Tabelle

In dieser Tabelle können Sie RIP Einstellungen vornehmen und auswählen für welches Netzwerk diese gelten sollen.

SNMP-ID: 2.8.8.5

Pfad Telnet: /Setup/IP-Router/RIP

2.8.8.5.1 Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

SNMP-ID: 2.8.8.5.1

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- Intranet
- DMZ

Default: leer

2.8.8.5.2 RIP-Typ

Wählen Sie aus, ob der Router IP-RIP unterstützen soll. Mit IP-RIP können automatisch Routing-Informationen zwischen einzelnen Stationen ausgetauscht werden.

SNMP-ID: 2.8.8.5.2

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- Aus
- RIP-1
- RIP-1 kompatibel
- RIP-2

Default: Aus

2.8.8.5.3 RIP-lernen

Wählen Sie hier, ob Routen von diesem Netzwerk gelernt werden sollen oder nicht.

SNMP-ID: 2.8.8.5.3

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.8.5.4 Propagieren

Wählen Sie hier, ob das zugehörige Netzwerk auf anderen Netzwerken propagiert wird.

SNMP-ID: 2.8.8.5.4

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.8.5.5 Dft-Rtg-Tag

Tragen Sie hier einen Wert für das Standard-Routing-Tag ein, der für die gewählte Schnittstelle gilt. Routen die das Tag der Schnittstelle gesetzt haben, werden auf dieser Schnittstelle mit dem Standard-Routing-Tag propagiert. Von der Schnittstelle gelernte Routen, die das hier konfigurierte Standard-Routing-Tag gesetzt haben, werden mit dem Schnittstellen-Tag in die RIP-Tabelle aufgenommen. Desweiteren werden unmarkierte Routen (also Routen mit dem Tag 0) auf dieser Schnittstelle nicht propagiert, es sei denn, die Schnittstelle besitzt selbst das Tag 0.

SNMP-ID: 2.8.8.5.5

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- 0 bis 65535

Default: 0

2.8.8.5.6 Rtg-Tag-Liste

Hier steht eine Komma-separierte Liste der Routing-Tags, die auf dieser Schnittstelle akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Routen ungeachtet ihrer Routing-Tags akzeptiert. Steht mindestens ein Tag in dieser Liste, dann werden nur Routen mit den Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von markierten Routen nur Routen mit erlaubten (d.h. hier aufgezählte) Tags weitergeleitet. Die Routing-Tag-Liste entspricht insoweit der WAN-RIP-Liste, mit dem Unterschied, dass etwaige Umsetzungen über das Standard-Routing-Tag berücksichtigt werden. D.h. wenn z. B. das Schnittstellen-Tag 1 und das Standard-Routing-Tag 0 ist, muss das Tag 0 in der Routing-Tag-Liste erscheinen, da es beim Empfang intern in das Tag 1 umgewandelt wird. Beim Senden wird entspechend das interne Tag 1 in das externe Tag 0 umgewandelt. Diese Maßnahme ist nötig, damit ein virtualisierter Router mit weiteren Routern im LAN, die keine getaggten Routen unterstützen, zusammenarbeiten kann.

SNMP-ID: 2.8.8.5.6

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- max. 33 Zeichen

Default: leer

2.8.8.5.7 Poisoned-Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

SNMP-ID: 2.8.8.5.7

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.8.5.10 Rx-Filter

Geben Sie hier den beim Empfang (RX) von RIP-Paketen anzuwendende Filter an.

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle/Rx-Filter

Mögliche Werte:

- Max. 16 Alphanumerische Zeichen

Default: Leer

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

2.8.8.5.11 Tx-Filter

Geben Sie hier den beim Senden (TX) von RIP-Paketen anzuwendende Filter an.

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle/Tx-Filter

Mögliche Werte:

- Max. 16 Alphanumerische Zeichen

Default: Leer

Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

2.8.8.5.12 RIP-senden

Wählen Sie hier, ob Routen auf diesem Netzwerk propagiert werden sollen. Dazu muss gleichzeitig der RIP-Typ gesetzt sein

Pfad Telnet: /Setup/IP-Router/RIP/LAN-Tabelle/RIP-senden

Mögliche Werte:

- Nein
- Ja

Default: Nein

2.8.8.6 Einstellungen

Das Routing Information Protocol (RIP) versendet regelmäßige Update-Nachrichten an die benachbarten Router mit Informationen über die erreichbaren Netzwerke und die zugehörigen Metriken (Hops). RIP verwendet verschiedene Timer, um den Austausch der Routing-Informationen zeitlich zu steuern.

SNMP-ID: 2.8.8.6

Pfad Telnet: /Setup/IP-Router/RIP

2.8.8.6.1 Update

Zeit zwischen zwei regelmäßigen Updates. Zu diesem Wert wird immer noch ein Zufallswert von +/- 5 Sekunden addiert.

SNMP-ID: 2.8.8.6.1

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 10 bis 99 Sekunden

Default: 30 Sekunden

2.8.8.6.2 Holddown

Das Holddown-Intervall gibt an, nach wie vielen Update-Intervallen eine von einem Router A gelernte Route durch eine schlechtere eines anderen Routers B ersetzt werden darf, wenn Router A diese Route nicht mehr propagiert.

Bis zum Ablauf der Holddown-Intervalls nimmt das Gerät eine Route nur an, wenn sie von dem gleichen Router propagiert wurden, von dem sie ursprünglich gelernt wurde. Von anderen Routern nimmt das Gerät innerhalb dieser Zeit eine Route nur dann an, wenn sie besser als die bisher bekannt Route ist.

SNMP-ID: 2.8.8.6.2

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 0 bis 99 in Vielfachen des Update-Intervalls

Default: 4

2.8.8.6.3 Invalidate

Das Invalidate-Intervall gibt an nach wie vielen Update-Intervallen eine Route als nicht erreichbar (invalid) markiert wird, wenn der Router, von dem sie ursprünglich gelernt wurde, diese nicht mehr propagiert.

Lernt das Gerät in dieser Zeit eine gleich gute oder bessere Route von einem anderen Router, so wird diese übernommen.

SNMP-ID: 2.8.8.6.3

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 0 bis 99 in Vielfachen des Update-Intervalls

Default: 6

2.8.8.6.4 Flush

Erhält ein Router während des Flush-Intervalls keine Update-Information über eine Route, wird diese Route endgültig aus der dynamischen Routingtabelle gelöscht.

SNMP-ID: 2.8.8.6.4

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 0 bis 99 in Vielfachen des Update-Intervalls

Default: 10

2.8.8.6.5 Upd-Delay

Bei einem Triggered Update werden Änderungen in den Metriken sofort an die benachbarten Router gemeldet, nicht erst beim nächsten regelmäßigen Update. Damit es bei Fehlkonfigurationen im Netzwerk nicht zu massenhaften Update-Nachrichten kommt, wird eine so genannte Update-Verzögerung (Update-Delay) definiert.

Die Update-Verzögerung startet, sobald die Routing-Tabelle bzw. Teile davon propagiert wurden. Solange dieses Verzögerung läuft, werden neue Routing-Informationen zwar angenommen und in die Tabelle eingetragen, aber nicht sofort weitergeleitet. Der Router meldet die aktuellen Einträge erst nach Ablauf der Verzögerung aktiv weiter.

Der hier konfigurierte Wert gibt die Obergrenze der Verzögerung an – die tatsächliche Verzögerung wird immer zufällig ermittelt und liegt zwischen einer Sekunde und dem hier angegebenen Wert.

SNMP-ID: 2.8.8.6.5

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 1 bis 99 Sekunden

Default: 5

2.8.8.6.6 Max-Hopcount

In manchen Szenarien ist es erwünscht, einen größeren maximalen Hopcount als den von RIP vorgesehenen Wert von 16 zu verwenden. Mit dem Parameter Max-Hopcount kann der Wert angepasst werden.

SNMP-ID: 2.8.8.6.6

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 16 bis 99

Default: 16

2.8.8.6.7 Routes-pro-Frame

Anzahl der Routen, die in einem Paket gemeinsam propagiert werden dürfen.

SNMP-ID: 2.8.8.6.7

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen

Mögliche Werte:

- 1 bis 90

Default: 25

2.8.8.6.8 Inter-Packet-Delay

Falls die Anzahl der Geräte im Netzwerk so hoch ist, dass sie nicht mehr in ein einzelnes RIP-Paket passen, teilt der sendende Router sie in mehrere RIP-Pakete auf. Damit auch leistungsschwächere Router im Netzwerk die aufeinanderfolgenden RIP-Pakete verarbeiten können, konfigurieren Sie hier eine Verzögerung in Millisekunden zwischen den einzelnen RIP-Paketen.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Einstellungen**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 255 Millisekunden

Default-Wert:

0

2.8.8.7 Filter

Über RIP gelernte Routen können durch die Einstellungen bei LAN- und WAN-RIP nach dem Routing-Tag gefiltert werden. Um die Routen zusätzlich über die Angabe von Netzadressen zu filtern (z. B. „Lerne nur Routen, die im Netz

192.168.0.0/255.255.0.0 liegen"), werden in einer zentralen Tabelle zunächst die Filter definiert, die dann von Einträgen in der LAN- und WAN-RIP-Tabelle genutzt werden können.

Die in der Filtertabelle definierten Filter können in der LAN-RIP- und WAN-RIP-Tabelle in den Spalten RX- und TX-Filter referenziert werden. Dabei werden mit RX die Filter angesprochen, die das Lernen der Routen von diesen Netzwerken erlauben oder sperren – mit TX werden die Netzwerke definiert, zu denen das Propagieren der Routen erlaubt oder gesperrt werden soll.

SNMP-ID: 2.8.8.7

Pfad Telnet: /Setup/IP-Router/RIP

2.8.8.7.1 Name

Name des Filtereintrags.

SNMP-ID: 2.8.8.7.1

Pfad Telnet: /Setup/IP-Router/RIP/Filter

Mögliche Werte:

- 18 Zeichen

Mit dem Rautezeichen # können mehrere Einträge zu einem einzigen Filter verbunden werden. Die Einträge LAN#1 und LAN#2 bilden zusammen also einen Filter „LAN", der in der RIP-Tabelle aufgerufen werden kann.

2.8.8.7.2 Filter

Kommaseparierte Liste von Netzwerken, die akzeptiert (+) oder abgelehnt (-) werden sollen.

SNMP-ID: 2.8.8.7.2

Pfad Telnet: /Setup/IP-Router/RIP/Filter

Mögliche Werte:

- 64 Zeichen aus ‚+-/0123456789.

Die Angabe des Pluszeichens für akzeptierte Netzwerke ist optional.

Die Filterung über Routing-Tags bleibt davon unberührt, d. h., wenn eine Route schon aufgrund ihres Tags nicht gelernt bzw. propagiert werden darf, dann kann das nicht über die Filtertabellen erzwungen werden.

2.8.8.8 Beste-Routen

In größeren Netzen kann ein Zielnetz auch über mehrere Gateways erreichbar sein. Wenn alle diese Gateways ihre Routen über RIP propagieren, dann lernt das Gerät mehrere Routen zum gleichen Ziel. Die bevorzugten Routen werden in der Tabelle "Beste Routen" abgelegt. Die Einträge der Tabelle beinhalten folgende Einträge:

- IP-Adresse
- IP-Netzmaske
- Rtg-Tag
- Gateway
- Distanz
- Zeit
- Gegenstelle
- Port
- VLAN-ID
- Netzwerkname

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen/Beste-Routen

2.8.8.8.1 IP-Adresse

Die IP-Adresse des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.2 IP-Netzmaske

Die IP-Adresse des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.3 Zeit

Die Zeit, die zum Erreichen des Netzwerks über diese Route notwendig ist.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.4 Distanz

Die Distanz zum Netzwerk, zu dem diese Route gehört (also die Anzahl der dazwischenliegenden Hops).

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.5 Gateway

Das Gateway, über welches das Netzwerk erreichbar ist, zu dem diese Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.6 Rtg-Tag

Die Routing-Tag des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.8 Gegenstelle

Die Gegenstelle, die über diese Route erreicht werden kann.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.10 VLAN-ID

Die VLAN-ID des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.11 Netzwerkname

Der Name des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.8.12 Port

Das (logische) LAN-Interface, über das die Route gelernt wurde.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Beste-Routen**

2.8.8.9 Alle-Routen

In größeren Netzen kann ein Zielnetz auch über mehrere Gateways erreichbar sein. Wenn alle diese Gateways ihre Routen über RIP propagieren, dann lernt das Gerät mehrere Routen zum gleichen Ziel. Diese Routen werden in der Tabelle "Alle Routen" abgelegt. Die Einträge der Tabelle beinhalten folgende Einträge:

- IP-Adresse
- IP-Netzmaske
- Rtg-Tag
- Gateway
- Distanz
- Zeit
- Gegenstelle
- Port
- VLAN-ID
- Netzwerkname

Pfad Telnet: /Setup/IP-Router/RIP/Einstellungen/Alle-Routen

2.8.8.9.1 IP-Adresse

Die IP-Adresse des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.2 IP-Netzmaske

Die IP-Adresse des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.3 Zeit

Die Zeit, die zum Erreichen des Netzwerks über diese Route notwendig ist.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.4 Distanz

Die Distanz zum Netzwerk, zu dem diese Route gehört (also die Anzahl der dazwischenliegenden Hops).

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.5 Gateway

Das Gateway, über welches das Netzwerk erreichbar ist, zu dem diese Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.6 Rtg-Tag

Die Routing-Tag des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.8 Gegenstelle

Die Gegenstelle, die über diese Route erreicht werden kann.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.10 VLAN-ID

Die VLAN-ID des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.11 Netzwerkname

Der Name des Netzwerks, zu dem die Route gehört.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.8.9.12 Port

Das (logische) LAN-Interface, über das die Route gelernt wurde.

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **Alle-Routen**

2.8.9 1-N-NAT

Dieses Menü enthält die Konfiguration des 1-N-NAT für ihren IP-Router.

SNMP-ID: 2.8.9

Pfad Telnet: /Setup/IP-Router

2.8.9.1 TCP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer TCP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

SNMP-ID: 2.8.9.1

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- 0 bis 65.535

Default: 300 Sek.

2.8.9.2 UDP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer UDP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

SNMP-ID: 2.8.9.2

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- 0 bis 65.535

Default: 20 Sek.

2.8.9.3 ICMP-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer ICMP-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

SNMP-ID: 2.8.9.3

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- 0 bis 65.535

Default: 10 Sek.

2.8.9.4 Service-Tabelle

Wenn Sie einzelne Dienste auf bestimmten Stationen auch ausserhalb Ihres Netzes verfügbar machen wollen (z. B. einen WebServer), dann tragen Sie die Stationen und die Dienste in diese Tabelle ein.

SNMP-ID: 2.8.9.4

Pfad Telnet: /Setup/IP-Router/1-N-NAT

2.8.9.4.1 D-Port-von

Geben Sie hier den Port des gewünschten Services an.

SNMP-ID: 2.8.9.4.1

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.8.9.4.2 Intranet-Adresse

Geben Sie hier die Adresse des Rechners im Intranet an, der den Service zur Verfügung stellt.

SNMP-ID: 2.8.9.4.2

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.9.4.3 D-Port-bis

Geben Sie hier den Port des gewünschten Services an.

SNMP-ID: 2.8.9.4.3

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.8.9.4.4 Map-Port

Port mit dem das Paket weitergeleitet wird.

SNMP-ID: 2.8.9.4.4

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.8.9.4.5 Aktiv

Sie können diesen Eintrag vorübergehend inaktiv schalten, ohne ihn löschen zu müssen.

SNMP-ID: 2.8.9.4.5

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- aktiv
- inaktiv

Default: Aktiv

2.8.9.4.6 Kommentar

Dieses Feld steht für einen Kommentar zur Verfügung.

SNMP-ID: 2.8.9.4.6

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- max. 64 Zeichen

Default: /

2.8.9.4.7 Gegenstelle

Wählen Sie hier die Gegenstelle, für die dieser Eintrag gültig ist.

SNMP-ID: 2.8.9.4.7

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen.

2.8.9.4.8 Protokoll

Stellen Sie hier ein für welches Protokoll der Datensatz gelten soll.

SNMP-ID: 2.8.9.4.8

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- TCP
- UDP
- TCP + UDP

Default: TCP + UDP

2.8.9.4.9 WAN-Adresse

Stellen Sie hier ein, für welche WAN-Adresse der Datensatz gelten soll. Hat man mehr als eine statische IP-Adresse, kann man durch Angabe dieser Adresse ein gezieltes Portforwarding für diese Adresse erzielen. Bei Angabe der Adresse 0.0.0.0 wird weiterhin die der Verbindung zugewiesene Adresse verwendet.

SNMP-ID: 2.8.9.4.9

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Service-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.9.5 Tabelle-1-N-NAT

Die 1-N-NAT-Tabelle zeigt die maskierten Verbindungen.

SNMP-ID: 2.8.9.5

Pfad Telnet: /Setup/IP-Router/1-N-NAT

2.8.9.5.1 Intranet-Adresse

Zeigt die interne IP-Adresse der Station, zu der eine maskierte Verbindung gespeichert wurde.

SNMP-ID: 2.8.9.5.1

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

Mögliche Werte:

- Gültige IP-Adresse.

2.8.9.5.2 S-Port

Quell-Port der maskierten Verbindung.

SNMP-ID: 2.8.9.5.2

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

2.8.9.5.3 Protokoll

Protokoll (UDP/TCP), das auf der maskierten Verbindung verwendet wird.

SNMP-ID: 2.8.9.5.3

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

2.8.9.5.4 Timeout

Gültigkeitsdauer der maskierten Verbindung in Sekunden (Einstellbar unter TCP-Aging, UDP-Aging oder ICMP-Aging).

SNMP-ID: 2.8.9.5.4

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

2.8.9.5.5 Handler

Handler, der zur Maskierung benötigt wird, z. B. FTP

SNMP-ID: 2.8.9.5.5

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

2.8.9.5.6 Remote-Adresse

Entfernte IP-Adresse, zu der die maskierte Verbindung aufgebaut wurde.

SNMP-ID: 2.8.9.5.6

Pfad Telnet: /Setup/IP-Router/1-N-NAT/Tabelle-1-N-NAT

Mögliche Werte:

- Gültige IP-Adresse.

2.8.9.6 Fragmente

Diese Einstellung kontrolliert das Verhalten der Firewall bei fragmentierten IP-Paketen.

SNMP-ID: 2.8.9.6

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- Filtern: Die Fragmente werden immer verworfen (gefiltert).

- Routen: Die Fragmente werden demaskiert. Dazu müssen die Fragmente allerdings in der ursprünglichen Reihenfolge empfangen werden. Ausserdem werden in dieser Einstellung nur die einzelnen Fragmente von der Firewall überprüft, nicht aber das gesamte IP-Paket.
- Reassemblieren: Die einzelnen Fragmente werden so lange zwischengespeichert, bis das IP-Paket komplett reassembliert ist. Die Fragmente können dabei in beliebiger Reihenfolge empfangen werden. Ausserdem überprüft die Firewall den Inhalt des reassemblierten IP-Pakets.

Default: Reassemblieren

2.8.9.7 Fragment-Aging-Sekunden

Wenn ein IP-Paket nicht vollständig demaskiert werden kann, weil nicht alle Fragmente empfangen wurden, dann werden die unvollständigen Fragmente nach der hier eingestellten Zeit in Sekunden verworfen.

SNMP-ID: 2.8.9.7

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- 1 bis 255

Default: 5

2.8.9.8 IPSec-Aging-Sekunden

Geben Sie hier an, nach welcher Zeit der Inaktivität einer IPSec-Verbindung der entsprechende Eintrag in der Masquerading-Tabelle entfernt werden soll.

SNMP-ID: 2.8.9.8

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- 0 bis 65.535

Default: 2000

2.8.9.9 IPSec-Table

Die IPSec-Tabelle zeigt die maskierten IPSec-Verbindungen an inkl. einiger Parameter der Verbindung.

SNMP-ID: 2.8.9.9

Pfad Telnet: /Setup/IP-Router/1-N-NAT

2.8.9.9.1 Remote-Adresse

Adresse des entfernten VPN-Gateways

SNMP-ID: 2.8.9.9.1

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

Mögliche Werte:

- Gültige IP-Adresse.

2.8.9.9.2 Lokale-Adresse

Adresse des lokalen VPN-Gateways (i.A. ist das ein VPN-Client im lokalen Netz)

SNMP-ID: 2.8.9.9.2

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

Mögliche Werte:

- Gültige IP-Adresse.

2.8.9.9.3 rc-hi

Höchstwertige 32 Bit des IKE Cookies des entfernten VPN-Gateways

SNMP-ID: 2.8.9.9.3

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.4 rc-lo

Niederwertige 32 Bit des IKE Cookies des entfernten VPN-Gateways.

SNMP-ID: 2.8.9.9.4

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.5 lc-hi

Höchstwertige 32 Bit des IKE Cookies des lokalen VPN-Gateways.

SNMP-ID: 2.8.9.9.5

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.6 lc-lo

Niederwertige 32 Bit des IKE Cookies des lokalen VPN-Gateways.

SNMP-ID: 2.8.9.9.6

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.7 remoter-SPI

Vom entfernten VPN Gateway verwendeter SPI.

SNMP-ID: 2.8.9.9.7

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.8 lokaler-SPI

Vom lokalen VPN Gateway verwendeter SPI.

SNMP-ID: 2.8.9.9.8

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.9 Timeout

Timeout in Sekunden bis der Eintrag gelöscht wird. Der Wert ist unter IPSec-Aging-Seconds einstellbar und der Default beträgt 2000 Sekunden.

SNMP-ID: 2.8.9.9.9

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.10 Flags

Flags, die den Zustand der Verbindung beschreiben:

0x01 Verbindung ist invers maskiert

0x02 Verbindung wartet auf SPI

0x04 andere Verbindungen warten auf SPI

0x08 Aggressive-Mode Verbindung

0x10 NAT-Traversal-Verbindung

0x20 Session-Recovery

SNMP-ID: 2.8.9.9.10

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.11 CO

Connect-Timeout - läuft direkt nachdem der Eintrag angelegt wurde. Wenn innerhalb von 30 Sekunden keine SA ausgehandelt wurde (d.h.es wurde kein ESP Paket gesendet oder empfangen) wird der Eintrag wieder gelöscht

SNMP-ID: 2.8.9.9.11

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.12 NL

Lokaler Notification Timeout: wenn vom lokalen VON-Gateway eine IKE Notification empfangen wurde wird dieser Timer gestartet. Wird innerhalb von 30 Sekunden kein IKE oder ESP-Paket von der remoten Seite empfangen, so wird der Eintrag gelöscht

SNMP-ID: 2.8.9.9.12

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.13 NR

Remoter Notification Timeout: entspricht dem lokalen Notification Timeout, nur dass hier die Notification vom remoten VPN-Gateway empfangen wurde.

SNMP-ID: 2.8.9.9.13

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.9.14 DP

DPD-Timeout: wenn von einer Seite ein DPD-Paket empfangen wurde, wird dieser Timer gestartet. Wenn innerhalb von 30 Sekunden kein DPD-Paket von der anderen Seite empfangen wird, dann wird der Eintrag entfernt.

SNMP-ID: 2.8.9.9.14

Pfad Telnet: /Setup/IP-Router/1-N-NAT/IPSec-Table

2.8.9.10 ID-Spoofing

Bei der Verwendung von NAT werden in den abgehenden Paketen die Paket-IDs ersetzt (ID-Spoofing), um einerseits auch fragmentierte Pakete übertragen zu können und andererseits ein Ausspähen des internen Netzes über die Paket-IDs zu verhindern. Bei der Nutzung von AH ist dieser Vorgang unerwünscht, da die Pakete-ID von AH genutzt wird. Für die korrekte Funktion von AH kann das ID-Spoofing hier deaktiviert werden.

SNMP-ID: 2.8.9.10

Pfad Telnet: /Setup/IP-Router/1-N-NAT

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.8.10 Firewall

Dieses Menü enthält die Konfiguration der Firewall.

SNMP-ID: 2.8.10

Pfad Telnet: /Setup/IP-Router

2.8.10.1 Objekt-Tabelle

In der Objekttabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regeltabelle der Firewall verwendet werden sollen. Objekte können sein:

- einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- ganze Netze
- Protokolle
- Dienste (Ports oder Port-Bereiche, z. B. HTTP, Mail&News, FTP, ...)

SNMP-ID: 2.8.10.1

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.1.1 Name

Geben Sie hier einen eindeutigen Namen für dieses Objekt an.

SNMP-ID: 2.8.10.1.1

Pfad Telnet: /Setup/IP-Router/Firewall/Objekt-Tabelle

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.8.10.1.2 Beschreibung

SNMP-ID: 2.8.10.1.2

Pfad Telnet: /Setup/IP-Router/Firewall/Objekt-Tabelle

Die Elemente der Objkt-Tabelle lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z.B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man drauf aufbauend Objekte z.B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

Mögliche Werte:

In der Objekttabelle können die Stationen und Dienste nach folgenden Regeln beschrieben werden:

Tabelle 6: Objekte für Firewall-Aktionen

Beschreibung	Objekt-ID	Beispiele und Bemerkungen
lokales Netz	%L	
Gegenstellen	%H	Name muss in DSL-/ISDN-/PPTP- oder VPN-Gegenstellenliste stehen
Hostname	%D	
MAC-Adresse	%E	`00:A0:57:01:02:03`
IP-Adresse	%A	`%A10.0.0.1, 10.0.0.2`; `%A0` (alle Adressen)

Beschreibung	Objekt-ID	Beispiele und Bemerkungen
Netzmaske	%M	%M255.255.255.0
Protokoll (TCP/UDP/ICMP etc.)	%P	%P6 (für TCP)
Dienst (Port)	%S	%S20-25 (für Ports 20 bis 25)

Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen. Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt.

Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Ziel, Quelle) jeweils in Anführungszeichen (Zollzeichen: ") eingeschlossen werden.

Default: Leer

2.8.10.2 Regel-Tabelle

In der Regel-Tabelle werden verschiedene Informationen zu einer Firewall-Regel verknüpft. Die Regel enthält das zu filternde Protokoll, die Quelle, das Ziel sowie die auszuführende Firewall-Aktion. Zusätzlich gibt es für jede Firewall-Regel einen Ein-/Ausschalter, eine Priorität, die Option für eine Verknüpfung mit anderen Regeln und eine Aktivierung der Regel für VPN-Verbindungen.

Zur Beschreibung der Firewall-Regeln gibt es im LCOS eine spezielle Syntax. Diese Syntax erlaubt es, auch komplexe Zusammenhänge für die Prüfung und Behandlung von Datenpaketen in der Firewall mit wenigen Zeichen darzustellen. Die Regeln werden in der Regel-Tabelle definiert. Damit häufig verwendete Objekte nicht jedesmal wieder neu in der LCOS-Syntax eingetragen werden müssen, können in zwei weiteren Tabellen vordefinierte Objekte gespeichert werden:

In der Aktionstabelle sind die Firewall-Aktionen enthalten

In der Objekttabelle sind die Stationen und Dienste enthalten

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekttabelle für Protokolle, Dienste, Stationen und der Aktionstabelle für die Firewall-Aktionen bestehen, als auch direkte Beschreibungen in der entsprechenden LCOS-Syntax enthalten (z. B. %P6 für TCP).

SNMP-ID: 2.8.10.2

Pfad Telnet: /Setup/IP-Router/Firewall

Die Objekte aus diesen Tabellen können bei der Regeldefinition verwendet werden, müssen es aber nicht! Sie erleichtern lediglich die Verwendung von häufiger verwendeten Objekten. Bei der direkten Eingabe der Pegel-Parameter in der LCOS-Syntax gelten die gleichen Regeln, wie sie in den folgenden Abschnitten für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

2.8.10.2.1 Name

Geben Sie hier einen eindeutigen Namen für diese Firewall-Regel an.

SNMP-ID: 2.8.10.2.1

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.8.10.2.2 Prot.

Angabe der Protokolle, für welche dieser Eintrag gelten soll.

SNMP-ID: 2.8.10.2.2

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Direkte Eingabe nach der LCOS-Syntax wie in der *Objekttabelle* beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

Default: Leer

2.8.10.2.3 Quelle

Angabe der Quell-Stationen, für welche dieser Eintrag gelten soll.

SNMP-ID: 2.8.10.2.3

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Direkte Eingabe nach der LCOS-Syntax wie in der *Objekttabelle* beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

Default: Leer

2.8.10.2.4 Ziel

Angabe der Ziel-Stationen, für welche dieser Eintrag gelten soll.

SNMP-ID: 2.8.10.2.4

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Direkte Eingabe nach der LCOS-Syntax wie in der *Objekttabelle* beschrieben.
- Verweis auf einen Eintrag der Objekttabelle.

Default: Leer

2.8.10.2.7 Aktion

Aktion, die ausgeführt werden soll, wenn die Firewall-Regel auf ein Paket zutrifft.

SNMP-ID: 2.8.10.2.7

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Direkte Eingabe nach der LCOS-Syntax wie in der *Aktionstabelle* beschrieben.
- Verweis auf einen Eintrag der Aktionstabelle.

Default: Leer

2.8.10.2.8 verknuepft

Verbindet die Regel mit weiteren Regeln.

SNMP-ID: 2.8.10.2.8

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.8.10.2.9 Prio

Priorität der Regel.

SNMP-ID: 2.8.10.2.9

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- 0 bis 255

Default: Leer

2.8.10.2.10 Aktiv

Schaltet die Regel ein oder aus.

SNMP-ID: 2.8.10.2.10

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.8.10.2.11 VPN-Regel

Aktiviert die Regel für das Erstellen von VPN-Regeln.

SNMP-ID: 2.8.10.2.11

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.8.10.2.12 Stateful

Wenn diese Option aktiviert ist, wird geprüft, ob ein Verbindungaufbau korrekt abläuft. Fehlerhafte Pakete im Verbindungsaufbau werden verworfen. Ist diese Option nicht aktiviert, dann werden alle Pakete akzeptiert, auf die diese Regel zutrifft.

Desweiteren wird über diese Option die automatische Protokollerkennung für FTP, IRC und PPTP aktiviert, die benötigt wird, um für die jeweiligen Datenverbindungen einen Port in der Firewall öffnen zu können.

Auch die Prüfung auf Portscans/SYN-Floodings wird über diese Option aktiviert oder deaktiviert. Damit können bestimmte, stark frequentierte Server von der Prüfung ausgenommen werden, ohne die Limits für halboffene Verbindungen (DOS) oder Portanfragen (IDS) so hoch einzustellen, dass sie letztendlich unwirksam werden.

SNMP-ID: 2.8.10.2.12

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.8.10.2.13 Kommentar

Kommentar für diesen Eintrag.

SNMP-ID: 2.8.10.2.13

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- max. 64 Stellen

Default: Leer

2.8.10.2.14 Rtg-Tag

Routing-Tag für die Regel.

SNMP-ID: 2.8.10.2.14

Pfad Telnet: /Setup/IP-Router/Firewall/Regel-Tabelle

Mögliche Werte:

- 0 bis 65535

Default: 0

2.8.10.2.15 Quell-Tag

Das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) dient zur Identifikation des ARF-Kontextes aus dem ein Paket empfangen wurde. Dieses kann zur Einschränkung von Firewall-Regeln auf bestimmte ARF-Kontexte verwendet werden.

Pfad Telnet:

Setup > **IP-Router** > **Firewall** > **Regel-Tabelle**

Mögliche Werte:

0…65535

Erläuterung:

- 65535: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 0 ist.
- 1…65534: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 1…65534 ist.
- 0: Wildcard. Die betreffende Firewall-Regel wird auf alle ARF-Kontexte angewandt (erwartetes Schnittstellen- bzw. Routing-Tag 0…65535).

Default:

0

2.8.10.3 Filter-Liste

Die Filterliste wird aus den Regeln der Firewall erzeugt. Die darin enthaltenen Filter sind statisch und ändern sich nur beim Hinzufügen, Bearbeiten oder Löschen von Firewall-Regeln.

SNMP-ID: 2.8.10.3

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.3.1 Idx.

Index zu diesem Eintrag in der Liste.

SNMP-ID: 2.8.10.3.1

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.2 Prot.

TCP-Protokoll für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.2

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.3 Quell-Adresse

Quell-IP-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.3

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.3.4 Quell-Netz-Maske

Quell-IP-Netzmaske für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.4

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.3.5 Q-Von

Anfangsadresse eines Bereiches von Quell-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.5

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.6 Q-Bis

Endadresse eines Bereiches von Quell-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.6

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.7 Ziel-Adresse

Ziel-IP-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.7

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.3.8 Ziel-Netz-Maske

Ziel-IP-Netzmaske für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.8

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.3.9 Z-Von

Anfangsadresse eines Bereiches von Ziel-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.9

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.10 Z-Bis

Endadresse eines Bereiches von Ziel-IP-Adressen, deren Datenpakete von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.10

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.11 Aktion

Aktion, die für Datenpakete ausgeführt wird, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.11

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.13 Quell-MAC

Quell-MAC-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.13

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.14 Ziel-MAC

Ziel-MAC-Adresse für Datenpakete, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.14

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.15 verknuepft

Zeigt an, ob nach dieser Aktion noch weitere Firewall-Regeln angewendet werden.

SNMP-ID: 2.8.10.3.15

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.16 Prio

Priorität für diesen Eintrag.

SNMP-ID: 2.8.10.3.16

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.17 Rtg-tag

Dieses Routing-Tag wird Datenpaketen hinzugefügt, die von diesem Eintrag erfasst werden.

SNMP-ID: 2.8.10.3.17

Pfad Telnet: /Setup/IP-Router/Firewall/Filter-Liste

2.8.10.3.18 Quell-Tag

Das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) dient zur Identifikation des ARF-Kontextes aus dem ein Paket empfangen wurde.

Pfad Telnet:

Setup > **IP-Router** > **Firewall** > **Filter-Liste**

2.8.10.4 Aktions-Tabelle

Eine Firewall-Aktion besteht aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen.

Die Firewall-Aktionen können wie bereits die Elemente der Objekt-Tabelle mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden.

SNMP-ID: 2.8.10.4

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.4.1 Name

Geben Sie hier einen eindeutigen Namen für diese Aktion an.

SNMP-ID: 2.8.10.4.1

Pfad Telnet: /Setup/IP-Router/Firewall/Aktions-Tabelle

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.8.10.4.2 Beschreibung

SNMP-ID: 2.8.10.4.2

Pfad Telnet: /Setup/IP-Router/Firewall/Aktions-Tabelle

In der Aktionstabelle werden die Firewall-Aktionen als beliebige Kombinationen aus Bedingungen, Limits, Paket-Aktionen und weiteren Maßnahmen zusammengestellt.

Mögliche Werte:

Eine Firewall-Aktion besteht aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen. In der Aktionstabelle werden die Firewall-Aktionen als beliebige Kombinationen aus den folgenden Elementen zusammengestellt.

Bedingungen

Tabelle 7: Bedingungen für Firewall-Aktionen

Bedingung	Beschreibung	Objekt-ID
Connect-Filter	Der Filter ist aktiv, wenn keine physikalische Verbindung zum Ziel des Pakets besteht	`@c`
DiffServ-Filter	Der Filter ist aktiv, wenn das Paket den angegebenen Differentiated Services Code Point (DSCP) enthält	`@d`
Internet-Filter	Der Filter ist aktiv, wenn das Paket über die Defaultroute empfangen wurde oder gesendet werden soll	`@i`
VPN-Filter	Der Filter ist aktiv, wenn das Paket über eine VPN-Verbindung empfangen wurde oder gesendet werden soll	`@v`

Wenn zum "Connect-" oder "Internet-" Filter keine weitere Aktion angegeben wird, dann wird implizit eine Kombination dieser Filter mit der "Reject" Aktion angenommen.

Limits

Jede Firewall-Aktion kann mit einem Limit verknüpft werden, dessen Überschreitung zur Auslösung der Aktion führt. Über mehrere Limits für einen Filter sind dadurch auch Aktionsketten möglich. Limit-Objekte werden dabei allgemein mit %L eingeleitet, gefolgt von:

- Bezug: verbindungsbezogen (c) oder global (g)
- Art: Datenrate (d), Anzahl der Pakete (p) oder Paketrate (b)
- Wert des Limits
- Weitere Parameter (z.B. Zeitraum und Größe)

Es stehen folgende Limitierungen zur Verfügung:

Tabelle 8: Limits für Firewall-Aktionen

Limit	Beschreibung	Objekt-ID
Data (abs)	Absolute Anzahl von Kilobytes auf der Verbindung nach denen die Aktion ausgeführt wird	`%lcd`
Data (rel)	Anzahl von Kilobytes/Sekunde, Minute, Stunde auf der Verbindung nach denen die Aktion ausgeführt wird	`%lcds, %lcdm, %lcdh`
Packet (abs)	Absolute Anzahl von Paketen auf der Verbindung nach denen die Aktion ausgeführt wird	`%lcp`
Packet (rel)	Anzahl von Paketen/Sekunde Minute, Stunde oder absolut auf der Verbindung nach denen die Aktion ausgeführt wird	`%lcps, %lcpm, %lcph`
global Data (abs)	Absolute Anzahl von Kilobytes, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	`%lgd`
global Data (rel)	Anzahl von Kilobytes/Sekunde, Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	`%lgds, %lgdm, %lgdh`
global Packet (abs)	Absolute Anzahl von Paketen, die an den Zielrechner gesendet oder von diesem empfangen wurde, nach denen die Aktion ausgeführt wird	`%lgp`

Limit	Beschreibung	Objekt-ID
global Packet (rel)	Anzahl von Paketen/Sekunde Minute oder Stunde, die an den Zielrechner gesendet oder von diesem empfangen wurden, nach denen die Aktion ausgeführt wird	%lgps, %lgpm, %lgph
receive Option	Beschränkung des Limits auf die Empfangsrichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdsr, %lcdsr
transmit Option	Beschränkung des Limits auf die Senderichtung (dies wirkt im Zusammenhang mit obigen Limitierungen). In der Object-ID Spalte sind Beispiele angegeben	%lgdst, %lcdst

Wird eine Aktion ohne Limit angegeben, so wird implizit ein Paket-Limit angenommen, welches sofort beim ersten Paket überschritten wird.

Quality-of-Servic-Objekte

Eine weiteres Limit-Objekt ist das "Quality-of-Service-Objekt" oder QoS-Objekt, das es erlaubt, einen minimalen Durchsatz bzw. eine Minimale Bandbreite für eine Verbindung oder global zu definieren. Es können sämtliche Begrenzungen angegeben werden, die auch bei normalen Limit-Objekten möglich sind, also verbindungsorientierte oder globale Minima, absolute oder zeitabhängige (relative) Minima, paket- oder datenbezogene Minima. Es gelten die gleichen Konventionen wie bei den Limit-Objekten.

QoS-Objekte werden durch das Token %q eingeleitet und unterscheiden sich von Limit-Objekten nur dadurch, dass sie zunächst eine implizite "Accept" Aktion besitzen, d.h. nach überschreiten der Schwelle werden die folgenden Pakete weiterhin akzeptiert.

- Alle Pakete, die einen mit einem QoS-Objekt belegten Filter durchlaufen, werden vom Gerät bevorzugt versendet (das entspricht einem gesetzten "Low Delay" Flag im TOS-Feld des IP-Headers), solange die Anzahl der übertragenen Pakete oder Daten unterhalb der angegebenen Schwelle liegt.
- Wird die Schwelle überschritten, so werden die hinter dem QoS-Objekt angegebenen Aktionen ausgeführt. So kann für einen Dienst durch Kombination von QoS- und Limit-Objekt eine minimale und maximale Bandbreite vorgegeben werden.

So ergibt z.B. aus einer minimalen Bandbreite von 32 kBit/s pro Verbindung und einer maximalen Bandbreite von 256 kBit/s für alle Verbindungen die folgende Beschreibung:

```
%a %qcds32%a %lgds256%d
```

Hier kann die explizite Angabe der Accept-Aktion, sowohl als Haupt-Aktion, als auch als getriggerte Aktion unterbleiben und die Beschreibung entsprechend abgekürzt werden:

```
%qcds32 %lgds256%d
```

Wenn die minimale und maximale Bandbreite eines Kanals gleich sein soll, so kann an die Drop-Aktion auch direkt im QoS-Objekt angegeben werden (direkt in abgekürzter Schreibweise):

```
%qcds32%d
```

Hier wird eine minimale Bandbreite von 32 kBit/s reserviert und gleichzeitig alle Pakete, die über diese Bandbreite hinaus übertragen werden sollen, verworfen. Diese Formulierung ist somit gleichbedeutend mit %a %qcds32%a %lgds32%d.

Es stehen folgende Objekte zur Verfügung:

Tabelle 9: QoS-Objekte für Firewall-Aktionen

QoS-Objekt	Beschreibung	Objekt-ID
Minimale bzw. maximale Bandbreite reservieren	Reserviert die angegebene Bandbreite entsprechende der weiteren Parameter entweder global oder pro Verbindung	%q

QoS-Objekt	Beschreibung	Objekt-ID
Minimale bzw. maximale Bandbreite erzwingen	Erzwingt die angegebene Bandbreite. Falls die geforderte Bandbreite nicht zur Verfügung steht, lehtn das Gerät die Verbindung ab.	%qf

Paket-Aktionen

Tabelle 10: Paket-Aktionen für Firewall-Aktionen

Paket-Aktion	Beschreibung	Objekt-ID
Accept	Das Paket wird angenommen	%a
Reject	Das Paket wird mit einer passenden Fehlermeldung zurückgewiesen	%r
Drop	Das Paket wird stillschweigend verworfen	%d
Externe Prüfung	Das Paket wird einem anderen Modul für eine externe Prüfung übergeben. Dem %x folgt ein Kennzeichner für das Modul, welches die Prüfung durchführt. Mögliche Werte: ■ %xc für den Contentfilter, gefolgt von einem zuvor definierten Contentfilter-Profil, z.B. %xcCF-BASIC-PROFILE.	%x

Diese Pakete-Aktionen sind beliebig miteinander kombinierbar, wobei bei widersinnigen oder nicht eindeutigen Aktionen (z.B.: Accept + Drop) die sicherere, d.h. im Beispiel "Drop" genommen wird.

Sonstige Maßnahmen

Über die Paket-Aktionen hinaus kann die Firewall weitere Maßnahmen ausführen, sobald die gesetzten Limits erreicht wurden. So kann die Firewall z.B. Benachrichtigungen über verschiedene Kanäle versenden oder Ports sowie Hosts für bestimmte Zeit sperren.

Es stehen folgende Maßnahmen zur Verfügung:

Tabelle 11: Sonstige Maßnahmen für Firewall-Aktionen

Maßnahmen	Beschreibung	Objekt-ID
Syslog	Gibt eine detaillierte Meldung über Syslog aus	%s
Mail	Schickt eine E-Mail an den Administrator	%m
SNMP	Sendet einen SNMP-Trap	%n
Close-Port	Schließt den Zielport des Pakets für eine einstellbare Zeit	%p
Deny-Host	Sperrt die Absender-Adresse des Pakets für eine einstellbare Zeit	%h
Disconnect	Trennt die physikalische Verbindung zur Gegenstelle, über die das Paket empfangen wurde oder gesendet werden sollte	%t
Zero-Limit	Setzt den Limit-Counter (s.u.) bei überschreiten der Trigger-Schwelle wieder auf 0	%z
Fragmentierung	Erzwingt die Fragmentierung aller nicht auf die Regel passenden Pakete	%f

Wenn die "Close-Port" Aktion ausgeführt wird, wird ein Eintrag in einer Sperrliste vorgenommen, durch den alle Pakete, die an den jeweiligen Rechner und Port gesendet werden, verworfen werden. Für das "Close-Port"-Objekt kann eine Sperrzeit in Sekunden, Minuten oder Stunden angegeben werden, die direkt hinter der Objekt-ID vermerkt wird. Diese Zeitangabe baut sich zusammen aus dem Bezeichner für die Zeiteinheit (h, m, s für Stunde, Minute und Sekunde) sowie der eigentlichen Zeitangabe. So sperrt z.B. %pm10 den Port für 10 Minuten. Wird

keine Zeiteinheit angegeben, so wird “Minuten” als Einheit angenommen. (damit ist `%p10` gleichbedeutend mit `%pm10`).

Wird die “Deny-Host” Aktion ausgeführt, so wird der Absender des Pakets in eine Sperrliste eingetragen. Ab diesem Moment werden alle Pakete, die von dem gesperrten Rechner empfangen werden verworfen. Auch das “Deny-Host”-Objekt kann mit einer Sperrzeit versehen werden, die wie bei der “Close-Port” Option beschrieben gebildet wird.

Wird die Aktion "Fragmentieren" ausgeführt, so kann diese zum einen richtungsabhängig wirken (`%ft512`, `%fr512` fragmentiert gesendete bzw. empfangene Pakte auf 512 Bytes) oder statt einer harten Fragmentierung nur die PTMU senken (`%fp512` reduziert die PMTU auf 512 Bytes). Auch die PMTU-Reduktion kann richtungabhängig definiert werden (`%fpt512`, `%fpr512`). Die Aktion "Fragmentieren" gilt zudem immer - unabhängig davon, ob ein Limit überschritten wurde.

Default: Leer

2.8.10.5 Verbindungsliste

In der Verbindungsliste wird für jede aufgebaute Verbindung ein Eintrag vorgenommen, wenn das geprüfte Paket von der Filterliste akzeptiert wird. In der Verbindungsliste wird festgehalten, von welcher Quelle zu welchem Ziel, über welches Protokoll und welchen Port eine Verbindung aktuell erlaubt ist. Darüber hinaus wird in dieser Liste festgehalten, wie lange der Eintrag noch in der Liste stehen bleibt und welche Firewall-Regel den Eintrag erzeugt hat. Diese Liste ist sehr dynamisch und permanent “in Bewegung”.

SNMP-ID: 2.8.10.5

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.5.1 Quell-Adresse

IP-Adresse der Station, die eine Verbindung aufgebaut hat.

SNMP-ID: 2.8.10.5.1

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.5.2 Ziel-Adresse

Ziel-IP-Adresse, zu der eine Verbindung aufgebaut wurde.

SNMP-ID: 2.8.10.5.2

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.5.3 Prot.

Protokoll, das auf dieser Verbindung zugelassen ist.

SNMP-ID: 2.8.10.5.3

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.4 Quell-Port

Quell-Port der Station, die eine Verbindung aufgebaut hat.

SNMP-ID: 2.8.10.5.4

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.5 Ziel-Port

Ziel-Port, zu der eine Verbindung aufgebaut wurde.

SNMP-ID: 2.8.10.5.5

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.6 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

SNMP-ID: 2.8.10.5.6

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.7 Flags

In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert.

Als Zustände sind folgende Werte möglich: new, establish, open, closing, closed, rejected (entsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST).

UDP-Verbindungen kennen nun die Zustände new, open und closing (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z. B. beim Protokoll H.323 der Fall).

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

Mögliche Werte:

- 00000001 TCP: SYN gesendet
- 00000002 TCP: SYN/ACK empfangen
- 00000004 TCP: warte auf ACK des Servers
- 00000008 alle: Verbindung offen
- 00000010 TCP: FIN empfangen
- 00000020 TCP: FIN gesendet
- 00000040 TCP: RST gesendet oder empfangen
- 00000080 TCP: Sitzung wird wiederhergestellt
- 00000100 FTP: passive FTP-Verbindung wird aufgebaut
- 00000400 H.323: zugehörige T.120-Verbindung
- 00000800: Verbindung über Loopback-Interface
- 00001000: prüfe verkettete Regeln
- 00002000: Regel ist verkettet
- 00010000: Ziel ist auf "lokaler Route"
- 00020000: Ziel ist auf Default-Route
- 00040000: Ziel ist auf VPN-Route
- 00080000: physikalische Verbindung ist nicht aufgebaut
- 00100000: Quelle ist auf Default-Route
- 00200000: Quelle ist auf VPN-Route
- 00800000: keine Route zum Ziel
- 01000000: enthält globale Aktion mit Bedingung

2.8.10.5.8 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

SNMP-ID: 2.8.10.5.8

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.9 Quell-Route

Quell-Route, über welche diese Verbindung aufgebaut wurde.

SNMP-ID: 2.8.10.5.9

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.10 Ziel-Route

Ziel-Route, zu der diese Verbindung aufgebaut wurde.

SNMP-ID: 2.8.10.5.10

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.5.11 Rtg-tag

Routing-Tag der Verbindung.

SNMP-ID: 2.8.10.5.11

Pfad Telnet: /Setup/IP-Router/Firewall/Verbindungsliste

2.8.10.6 Hostsperrliste

In der Hostsperrliste werden die Stationen aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Die Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

SNMP-ID: 2.8.10.6

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.6.1 Quell-Adresse

Quell-IP-Adresse, die durch diesen Eintrag gesperrt ist.

SNMP-ID: 2.8.10.6.1

Pfad Telnet: /Setup/IP-Router/Firewall/Hostsperrliste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.6.2 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

SNMP-ID: 2.8.10.6.2

Pfad Telnet: /Setup/IP-Router/Firewall/Hostsperrliste

2.8.10.6.3 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

SNMP-ID: 2.8.10.6.3

Pfad Telnet: /Setup/IP-Router/Firewall/Hostsperrliste

2.8.10.7 Portsperrliste

In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

SNMP-ID: 2.8.10.7

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.7.1 Ziel-Adresse

Ziel-IP-Adresse, die durch diesen Eintrag gesperrt ist.

SNMP-ID: 2.8.10.7.1

Pfad Telnet: /Setup/IP-Router/Firewall/Portsperrliste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.7.2 Prot.

Protokoll, das durch diesen Eintrag gesperrt ist.

SNMP-ID: 2.8.10.7.2

Pfad Telnet: /Setup/IP-Router/Firewall/Portsperrliste

2.8.10.7.3 Ziel-Port

Ziel-Port, der durch diesen Eintrag gesperrt ist.

SNMP-ID: 2.8.10.7.3

Pfad Telnet: /Setup/IP-Router/Firewall/Portsperrliste

2.8.10.7.4 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

SNMP-ID: 2.8.10.7.4

Pfad Telnet: /Setup/IP-Router/Firewall/Portsperrliste

2.8.10.7.5 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

SNMP-ID: 2.8.10.7.5

Pfad Telnet: /Setup/IP-Router/Firewall/Portsperrliste

2.8.10.8 Max.-Halb-Offene-Verb.

Denial-Of-Service Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen aus. Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z. B. SYN-Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop) oder mit gefälschten Absenderadressen arbeiten (z. B. Land). Ihr Gerät erkennt die meisten dieser Angriffe und kann mit einer hier konfigurierbaren gezielten Gegenmaßnahme reagieren.

SNMP-ID: 2.8.10.8

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- 100 bis 9999

Default: 100

2.8.10.9 DoS-Aktion

Hier bestimmen Sie, wie mit den Paketen verfahren werden soll, welche den Trigger ausgelöst oder überschritten haben. Sie können die Pakete übertragen, unkommentiert verwerfen oder mittels ICMP-Reject (der Absender wird informiert) zurückweisen.

SNMP-ID: 2.8.10.9

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- Übertragen
- Verwerfen
- Zurückweisen

Default: Verwerfen

2.8.10.10 Admin-Email

Wenn sie über definierte Ereignisse (DoS. IDS oder das Überschreiten von Limitierungen) benachrichtigt werden wollen, müssen Sie hier eine gültige E-Mail-Adresse angeben.

SNMP-ID: 2.8.10.10

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- max. 255 Zeichen

Für E-Mail-Benachrichtigung müssen Sie außerdem die notwendigen Einstellungen in der Hauptgruppe 'Meldungen' in der Untersektion 'SMTP' vornehmen.

2.8.10.11 Aktiv

Hier können Sie die gesamte Firewall an- oder abschalten. Die Firewall überprüft und zählt alle ein- und ausgehenden Pakete. Sie öffnet in Abhängigkeit vom jeweiligen Protokoll vorübergehend nur jene Kanäle, die von einer lokalen Station zur Abwicklung einer Anfrage erforderlich sind. Außerdem können bestimmte Netze oder Stationen, Dienste oder Protokolle bevorzugt, limitiert oder verboten werden.

SNMP-ID: 2.8.10.11

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- aktiv
- inaktiv

Default: Aktiv

Bei abgeschalteter Firewall werden definierte VPN-Regeln weiterhin beachtet.

2.8.10.12 Port-Scan-Schwelle

Intrusion-Detection-System (IDS). Ihr Gerät erkennt die meisten unberechtigten Eindringversuche und kann mit einer hier konfigurierbaren gezielten Gegenmaßnahme reagieren.

SNMP-ID: 2.8.10.12

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- 50 bis 9999

Default: 50

2.8.10.13 IDS-Aktion

Hier bestimmen Sie, wie mit den Paketen verfahren werden soll, welche den Trigger ausgelöst oder überschritten haben. Sie können die Pakete übertragen, unkommentiert verwerfen oder mittels ICMP-Reject (der Absender wird informiert) zurückweisen.

SNMP-ID: 2.8.10.13

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- Übertragen
- Verwerfen
- Zurückweisen

Default: Verwerfen

2.8.10.14 Ping-Block

Eine umstrittene Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers, indem Ping- und Traceroute-Anfragen nicht mehr beantwortet werden (Ping-Blocking). Dies ist insofern umstritten, weil auch ein Nichtantworten auf die Existenz eines Gerätes schließen lässt. Ist nämlich wirklich kein Gerät vorhanden, so beantwortet der jeweils vorherige Router die entsprechenden Pakete mit "nicht zustellbar", da er sie wirklich nicht zustellen kann. Antwortet hingegen der jeweils vorherige Router nicht mit einer entsprechenden Ablehnung, so war das Paket für ihn zustellbar und unabhängig vom darauf folgenden Verhalten des Empfängers ist dieser auf jeden Fall vorhanden. Das Verhalten des jeweils vorherigen Routers kann nicht simuliert werden, ohne Ihr Gerät wirklich offline (und damit auch für selbst angeforderte Dienste unerreichbar) zu halten oder abzuschalten.

SNMP-ID: 2.8.10.14

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- Aus
- Immer
- Nur WAN
- Nur für Default-Route

Default: Aus

2.8.10.15 Stealth-Mode

Eine umstrittene Methode, die Sicherheit zu erhöhen, ist das Verstecken des Routers. indem TCP- und UDP-Anfragen nicht mehr normgerecht abgelehnt, sondern ignoriert werden (Stealth-Modus). Dies ist insofern umstritten, als auch ein Nichtantworten auf die Existenz eines Gerätes schließen lässt. Ist nämlich wirklich kein Gerät vorhanden, so beantwortet der jeweils vorherige Router die entsprechenden Pakete mit "nicht zustellbar", da er sie wirklich nicht zustellen kann. Antwortet hingegen der jeweils vorherige Router nicht mit einer entsprechenden Ablehnung, so war das Paket für ihn zustellbar und unabhängig vom darauf folgenden Verhalten des Empfängers ist dieser auf jeden Fall vorhanden. Das Verhalten des jeweils vorherigen Routers kann nicht simuliert werden, ohne Ihr Gerät wirklich offline (und damit auch für selbst angeforderte Dienste unerreichbar) zu halten oder abzuschalten.

SNMP-ID: 2.8.10.15

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- Aus
- Immer
- Nur WAN
- Nur für Default-Route

Default: Aus

2.8.10.16 Auth-Port

Werden TCP- oder UDP-Ports versteckt, so entsteht auf maskierten Verbindungen das Problem, dass die sogenannten "Authenticate"- bzw. "Idenf-Anfragen", welche von einigen Mail- oder News-Servern dazu benutzt werden etwaige zusätzliche Informationen vom User anzufordern, nicht mehr korrekt abgelehnt werden. Diese Server laufen dann in einen Timeout, was dazu führt, dass die Mailzustellung erheblich verzögert wird. Um dieses Problem bei eingeschaltetem Stealth-Modus zu umgehen, wird für den betroffenen Port vorübergehend der Stealth-Modus aufgehoben. Die Firewall erkennt die Absicht einer internen Station zu einem Mail- (SMTP, POP3, IMAP2) oder News-Server (NNTP) Kontakt aufzunehmen und öffnet den Port für 20 Sekunden. Sie können hier die kurzfristige Aufhebung des Stealth-Modus für den Authentifizierungs-Port unterdrücken.

SNMP-ID: 2.8.10.16

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.10.17 Sitzungswiederherst.-Verb.

Die Firewall öffnet für jede begonnene Sitzung und deren Verbindungen (z. B. FTP mit Kontroll- und Datenverbindung) für eine bestimmte Zeit für jede Verbindung einen entsprechenden Kanal. Findet über einen definierten Zeitraum hinaus (Einstellung in IP-Router-Maskierung) auf den Verbindungen keine Kommunikation statt, so wird die Sitzung als beendet betrachtet und die den Verbindungen zugehörigen Kanäle geschlossen. Die Auswahl 'Sitzungs-Wiederherstellung' bestimmt das Verhalten der Firewall beim Empfang von Paketen, die auf eine ehemalige Sitzung schließen lassen. Die Pakete werden entweder verworfen oder es wird davon ausgegangen, dass eine Sitzung bestand, auf dieser aber zu lange keine Kommunikation stattfand. Dann kann eine gleichwertige Sitzung wiederhergestellt werden. Letzteres Verhalten kann generell erlaubt oder verboten werden. Ein Verbot kann auf die Default-Route oder auf WAN-Sitzungen eingeschränkt werden.

SNMP-ID: 2.8.10.17

Pfad Telnet: /Setup/IP-Router/Firewall

Mögliche Werte:

- Immer erlaubt
- Immer verboten
- Nicht über WAN
- Nicht über Default-Route

Default: Nicht über Default-Route

Wenn die Default-Route ins LAN weist, hat diese Einstellung keine Auswirkung.

2.8.10.19 Open-Port-Liste

In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit geöffnet sind. Diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

SNMP-ID: 2.8.10.19

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.19.1 Quell-Adresse

Quell-IP-Adresse, welche die geöffneten Ports und Protokolle aus diesem Eintrag nutzen kann.

SNMP-ID: 2.8.10.19.1

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.19.2 Ziel-Adresse

Ziel-IP-Adresse, zu der über die geöffneten Ports und Protokolle aus diesem Eintrag Verbindungen aufgebaut werden können.

SNMP-ID: 2.8.10.19.2

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.8.10.19.3 Prot.

Protokoll, das durch diesen Eintrag geöffnet ist.

SNMP-ID: 2.8.10.19.3

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

2.8.10.19.5 Ziel-Port

Ziel-Port, der durch diesen Eintrag geöffnet ist.

SNMP-ID: 2.8.10.19.5

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

2.8.10.19.6 Timeout

Gültigkeitsdauer dieses Eintrags in der Tabelle.

SNMP-ID: 2.8.10.19.6

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

2.8.10.19.8 Filterregel

Zeigt die Filterregel, die diesen Eintrag erzeugt hat.

SNMP-ID: 2.8.10.19.8

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

2.8.10.19.9 Quell-Route

Quell-Route, über welche diese Verbindung aufgebaut wurde.

SNMP-ID: 2.8.10.19.9

Pfad Telnet: /Setup/IP-Router/Firewall/Open-Port-Liste

2.8.10.20 Anwendungen

Dieses Menü enthält die Konfiguration einzelner Anwendungen für ihre Firewall.

SNMP-ID: 2.8.10.20

Pfad Telnet: /Setup/IP-Router/Firewall

2.8.10.20.1 FTP

Dieses Menü enthält die Konfiguration von FTP für ihre Firewall.

SNMP-ID: 2.8.10.20.1

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen

2.8.10.20.1.1 FTP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf jede FTP-Session reagieren' gibt an, ob und auf welchen Routen jede Art von FTP sonderbehandelt werden soll.

SNMP-ID: 2.8.10.20.1.1

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/FTP

Mögliche Werte:

- Aus
- Immer
- WAN
- Default-Route

Default: Nein

2.8.10.20.1.2 Actives-FTP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf aktives FTP reagieren' gibt an, ob und auf welchen Routen aktives FTP sonderbehandelt werden soll.

SNMP-ID: 2.8.10.20.1.2

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/FTP

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nein

2.8.10.20.1.3 Min-Port

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. "Die kleinste erlaubte Port-Nummer" gibt den kleinsten zulässigen Port beim aktiven FTP an.

SNMP-ID: 2.8.10.20.1.3

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/FTP

Mögliche Werte:

- 1024 bis 9999

Default: 1024

2.8.10.20.1.4 Host-IP-Pruefen

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Stations-IP-Adresse prüfen' gibt an, ob und auf welchen Routen die im FTP-Kommando-Kanal übermittelte Adresse gegen die Quelladresse des FTP-Clients geprüft werden soll. Stimmt sie nicht, werden die unten konfigurierten Gegenmaßnahmen ergriffen. Wenn ein Site-To-Site-Transfers stattfinden soll und auch erlaubt ist, dann wird diese Überprüfung natürlich nicht durchgeführt.

SNMP-ID: 2.8.10.20.1.4

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/FTP

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nur für Default-Route

2.8.10.20.1.5 FXP-Blockieren

Wenn eine FTP-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf FXP-Sessions reagieren' gibt an, ob Site-To-Site-Transfers (FXP) sonderbehandelt werden soll.

SNMP-ID: 2.8.10.20.1.5

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/FTP

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nur für Default-Route

2.8.10.20.2 IRC

Dieses Menü enthält die Konfiguration von IRC für ihre Firewall.

SNMP-ID: 2.8.10.20.2

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen

2.8.10.20.2.1 IRC-Blockieren

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf IRC reagieren' gibt an, ob und auf welchen Routen jede Art von IRC sonderbehandelt werden.

SNMP-ID: 2.8.10.20.2.1

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/IRC

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nein

2.8.10.20.2.2 DDC-Blockieren

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Auf DDC reagieren' gibt an, ob und auf welchen Routen Direct-Data-Connect (private Chats und Filetransfers) sonderbehandelt werden sollen.

SNMP-ID: 2.8.10.20.2.2

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/IRC

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nein

2.8.10.20.2.3 Min-Port

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Kleinste erlaubte Port-Nummer" gibt den kleinsten zulässigen Port beim DDC an.

SNMP-ID: 2.8.10.20.2.3

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/IRC

Mögliche Werte:

- 1024 bis 9999

Default: 1024

2.8.10.20.2.4 Host-IP-Pruefen

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen. 'Stations-IP-Adresse prüfen' gibt an, ob und auf welchen Routen die im DDC-Kommando übermittelte Adresse gegen die Quelladresse des IRC-Clients geprüft werden soll.

SNMP-ID: 2.8.10.20.2.4

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen/IRC

Mögliche Werte:

- Nein
- Immer
- Nur für WAN-Route
- Nur für Default-Route

Default: Nur für Default-Route

2.8.10.20.10 Anw.-Aktion

Wenn eine IRC-Session auf einem beliebigen Port erkannt wird, werden die konfigurierbaren Gegenmaßnahmen ergriffen.

SNMP-ID: 2.8.10.20.10

Pfad Telnet: /Setup/IP-Router/Firewall/Anwendungen

Mögliche Werte:

- Übertragen
- Verwerfen
- Zurückweisen

Default: Zurückweisen

2.8.11 Start-WAN-Pool

Geben Sie hier einen Bereich von IP-Adressen ein, der Benutzern zugewiesen werden soll, die sich auf dem Gerät einwählen.

Das Gerät verwendet automatisch für jeden Benutzer eine freie Adresse aus diesem Bereich. Sobald ein Benutzer die Verbindung zum Gerät wieder trennt, wird die ihm zugewiesene Adresse wieder frei und steht anderen Benutzern zur Verfügung.

SNMP-ID: 2.8.11

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.12 Ende-WAN-Pool

Geben Sie hier einen Bereich von IP-Adressen ein, der Benutzern zugewiesen werden soll, die sich auf dem Gerät einwählen.

Das Gerät verwendet automatisch für jeden Benutzer eine freie Adresse aus diesem Bereich. Sobald ein Benutzer die Verbindung zum Gerät wieder trennt, wird die ihm zugewiesene Adresse wieder frei und steht anderen Benutzern zur Verfügung.

SNMP-ID: 2.8.12

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.13 Default-Zeit-Liste

Über die zeitabhängige Steuerung können Sie, abhängig vom Wochentag und von der Uhrzeit, verschiedene Ziele für die Default-Route angeben.

SNMP-ID: 2.8.13

Pfad Telnet: /Setup/IP-Router

2.8.13.1 Index

Index für diesen Eintrag in der Liste.

SNMP-ID: 2.8.13.1

Pfad Telnet: /Setup/IP-Router/Default-Zeit_Liste

2.8.13.2 Tage

Wählen Sie die Tage, wann dieser Eintrag verwendet werden soll.

SNMP-ID: 2.8.13.2

Pfad Telnet: /Setup/IP-Router/Default-Zeit_Liste

Mögliche Werte:

- Mo
- Di
- Mi
- Do
- Fr
- Sa
- So
- Feiertags

Default: Es sind keine Tage markiert

2.8.13.3 Start

Wählen Sie den Zeitraum, wann dieser Eintrag verwendet werden soll.

SNMP-ID: 2.8.13.3

Pfad Telnet: /Setup/IP-Router/Default-Zeit_Liste

Mögliche Werte:

- 00:00 bis 23:59

Default: 0

2.8.13.4 Stop

Wählen Sie den Zeitraum, wann dieser Eintrag verwendet werden soll.

SNMP-ID: 2.8.13.4

Pfad Telnet: /Setup/IP-Router/Default-Zeit_Liste

Mögliche Werte:

- 00:00 bis 23:59

Default: 0.999305556

2.8.13.5 Gegenstelle

Sobald dieser Eintrag gültig wird, weil der angegebene Zeitraum erreicht ist, wird die hier angegebene Gegenstelle als Ziel der Default-Route verwendet. Wählen Sie dazu den Namen einer Gegenstelle aus der Liste der Gegenstellen aus.

SNMP-ID: 2.8.13.5

Pfad Telnet: /Setup/IP-Router/Default-Zeit_Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

2.8.14 Nutzung-Default-Listen

Aktivieren Sie hier die zeitabhängige Steuerung der Default-Route. Über die Default-Route wird üblicherweise die Verbindung zu einem Internet-Anbieter herestellt. Mit der Zeitsteuerung können Sie zeitabhängig verschiedene Internet-Anbieter auswählen, z. B. um den zu der jeweiligen Uhrzeit preisgünstigsten Anbieter zu verwenden.

SNMP-ID: 2.8.14

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

Um diesen Mechanismus zu nutzen, müssen Sie in der Routing-Tabelle eine Default-Route angegeben haben. Der in der Default-Route angegebene Router wird nur in den Zeiten verwendet, welche nicht von der Zeitsteuerungs-Tabelle abgedeckt werden.

2.8.19 N-N-NAT

Die N:N-NAT-Tabelle enthält Regeln, auf welche IP-Adressen die Quell-Adressen einzelner Stationen oder ganzer IP-Netze umgesetzt werden sollen. Diese Regeln müssen für jede Gegenstelle gesondert spezifiziert werden, da die Umsetzung nach dem Routen erfolgt. Für die Gegenstelle sind die Stationen oder Netzwerke unter ihrer angegebenen umgesetzten IP-Adresse erreichbar.

SNMP-ID: 2.8.19

Pfad Telnet: /Setup/IP-Router

2.8.19.1 Idx.

Eindeutiger Index des Eintrags.

SNMP-ID: 2.8.19.1

Pfad Telnet: /Setup/IP-Router/N-N-NAT

Mögliche Werte:

- max. 4 Zeichen

Default: Leer

2.8.19.2 Quell-Adresse

IP-Adresse des Rechners oder Netzes, dass eine alternative IP-Adresse erhalten soll.

SNMP-ID: 2.8.19.2

Pfad Telnet: /Setup/IP-Router/N-N-NAT

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.19.3 Quell-Maske

Netzmaske des Quell-Bereiches.

SNMP-ID: 2.8.19.3

Pfad Telnet: /Setup/IP-Router/N-N-NAT

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.19.4 Ziel-Gegenstelle

Name der Gegenstelle, über die das entfernte Netzwerk erreicht werden kann.

SNMP-ID: 2.8.19.4

Pfad Telnet: /Setup/IP-Router/N-N-NAT

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen.

Default: Leer

2.8.19.5 Neue-Netz-Adr.

IP-Adresse oder -Adressebereich, der für die Umsetzung verwendet werden soll.

SNMP-ID: 2.8.19.5

Pfad Telnet: /Setup/IP-Router/N-N-NAT

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

Für die neue Netzadresse wird jeweils die gleiche Netzmaske verwendet, die auch schon die Quell-Adresse verwendet. Für die Zuordnung von Quell- und Mapping-Adresse gelten folgende Hinweise:

- Bei der Umsetzung von einzelnen Adressen können Quelle und Mapping beliebig zugeordnet werden.
- Bei der Umsetzung von ganzen Adressbereichen wird der rechnerbezogene Teil der IP-Adresse direkt übernommen und nur an den netzbezogenen Teil der Mapping-Adresse angehängt. Bei einer Zuweisung von 10.0.0.0/255.255.255.0 nach 192.168.1.0 wird also dem Server im LAN mit der IP-Adresse 10.1.1.99 zwangsweise die Mapping-Adresse 192.168.1.99 zugewiesen.

Der Adressbereich für die Umsetzung muss mindestens so groß sein wie der Quell-Adressbereich.

Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist.

2.8.20 Load-Balancer

Dieses Menü enthält die Konfiguration von Load-Balancing für ihren IP-Router.

SNMP-ID: 2.8.20

Pfad Telnet: /Setup/IP-Router

2.8.20.1 Aktiv

Hier werden die Load-Balancing (Last-Verteilung) Parameter eingestellt. Load-Balancing kann genutzt werden, wenn Ihr Provider keine echte Kanal-Bündelung anbietet. Mindestens eine virtuelle Verbindung muss dafür in der Load-Balancing-Tabelle festgelegt werden. Wieviele Gegenstellen maximal gebündelt weden können hängt davon ab, wie viele DSL-Ports der verwendete Gerätetyp zur Verfügung stellt.

SNMP-ID: 2.8.20.1

Pfad Telnet: /Setup/IP-Router/Load-Balancer

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.20.2 Buendel-Gegenstellen

Wenn Ihr Internet-Anbieter keine echte Kanal-Bündelung zur Verfügung stellt, ist es möglich mehrere Verbindungen mit Hilfe des Load-Balancing zusammenzufassen.

SNMP-ID: 2.8.20.2

Pfad Telnet: /Setup/IP-Router/Load-Balancer

2.8.20.2.1 Gegenstelle

Eindeutiger Name für eine virtuelle Load-Balancing-Gegenstelle. Diese Gegenstelle kann dann in der Routing-Tabelle verwendet werden.

SNMP-ID: 2.8.20.2.1

Pfad Telnet: /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

Default: leer

2.8.20.2.2 Buendel-GgSt.-1

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

SNMP-ID: 2.8.20.2.2

Pfad Telnet: /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.8.20.2.3 Buendel-GgSt.-2

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

SNMP-ID: 2.8.20.2.3

Pfad Telnet: /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.8.20.2.4 Buendel-GgSt.-3

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

SNMP-ID: 2.8.20.2.4

Pfad Telnet: /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.8.20.2.5 Buendel-GgSt.-4

Name einer bereits konfigurierten Gegenstelle zu der weitere hinzugebündelt werden sollen.

SNMP-ID: 2.8.20.2.5

Pfad Telnet: /Setup/IP-Router/Load-Balancer/Buendel-Gegenstellen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.8.20.2.10 Client-Binding

Aktivieren oder deaktivieren Sie hier das Client-Binding je Load-Balancer.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Buendel-Gegenstellen**

Mögliche Werte:

Ja

Das Client-Binding ist aktiv.

Nein

Das Client-Binding ist nicht aktiv.

Default-Wert:

Nein

2.8.20.3 Client-Binding

In diesem Menü konfigurieren Sie das Client-Binding.

Der Einsatz von Load-Balancing führt bei Servern zu Problemen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden. Wählt der Load-Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen (Policy Based Routing). Damit ist jedoch der gesamte Datenverkehr zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt. Außerdem lassen sich so keine Backup-Verbindung aufbauen, falls die erste Verbindung gestört ist.

Das Client-Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions ebenfalls über diese Internetverbindung, was im Prinzip dem zuvor angesprochenen Policy Based Routing entspricht. Das erfolgt protokollabhängig, d. h., es überträgt nur Daten des selben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Verbindung.

Um zu vermeiden, dass nun auch Daten über diese Internetverbindung fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer**

2.8.20.3.1 Protokolle

In dieser Tabelle definieren Sie die vom Client-Binding überwachten Protokolle sowie deren Ports.

Die Tabelle enthält bereits die Standard-Einträge

- HTTPS
- HTTP
- ANY

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

2.8.20.3.1.1 Name

Vergeben Sie einen aussagekräftigen Namen für diesen Eintrag.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

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

Default-Wert:

leer

2.8.20.3.1.2 Protokoll

Wählen Sie die IP-Protokollnummer aus.

Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank* der IANA.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

max. 3 Zeichen von `[0-255]`

Besondere Werte:

0
alle Protokolle

Default-Wert:

0

2.8.20.3.1.3 Port

Wählen Sie den Port aus.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

max. 5 Zeichen von `[0-65535]`

Besondere Werte:

0
alle Ports

Default-Wert:

0

2.8.20.3.1.4 Aktiv

Aktivieren oder deaktivieren Sie das Client-Binding für diesen Eintrag.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

Ja
Aktiviert den Eintrag

Nein
Deaktiviert den Eintrag

Default-Wert:

Ja

2.8.20.3.2 Bindung-Minuten

Definieren Sie die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

Mögliche Werte:

max. 3 Zeichen von `[0-999]`

Besondere Werte:

0

Binding-Einträge sind dauerhaft gültig.

Default-Wert:

30

2.8.20.3.3 Balance-Sekunden

Um zu vermeiden, dass Daten über diese Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

Mögliche Werte:

max. 3 Zeichen von `[0-999]`

Besondere Werte:

0

Der Timer ist deaktiviert. Alle Sessions sind fest an die bestehende Internetverbindung gebunden.

Default-Wert:

10

2.8.21 VRRP

Dieses Menü enthält die Konfiguration von VRRP für ihren IP-Router.

SNMP-ID: 2.8.21

Pfad Telnet: /Setup/IP-Router

2.8.21.1 Aktiv

Das Virtual-Router-Redundancy-Protocol dient dazu, mehrere physikalische Router wie einen einzigen "virtuellen" Router erscheinen zu lassen. Von den vorhandenen physikalischen Routern ist immer einer der sogenannte Master. Dieser Master ist der einzige, der wirklich eine Verbindung z. B. ins Internet hat und Daten überträgt. Erst wenn der Master ausfällt, weil z. B. die Spannungsversorgung unterbrochen oder seine Internetanbindung ausgefallen ist, werden die anderen Router aktiv. Über das Protokoll VRRP, handeln sie nun aus, wer als nächster die Rolle des Masters zu übernehmen hat. Der neue Master übernimmt vollständig die Aufgaben des bisherigen Masters.

SNMP-ID: 2.8.21.1

Pfad Telnet: /Setup/IP-Router/VRRP

Mögliche Werte:

- aktiv
- inaktiv

Default: inaktiv

2.8.21.2 VRRP-Liste

In der VRRP-Liste können Sie virtuelle Router definieren und konfigurieren.

SNMP-ID: 2.8.21.2

Pfad Telnet: /Setup/IP-Router/VRRP

2.8.21.2.1 Router-ID

Eindeutige ID des virtuellen Routers.

SNMP-ID: 2.8.21.2.1

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- 0 bis 255

Default: 1

2.8.21.2.2 virt.-Adresse

IP-Adresse des virtuellen Routers. Alle Router auf denen der virtuelle Router eingerichtet ist, müssen diesem die gleiche IP-Adresse zuweisen.

SNMP-ID: 2.8.21.2.2

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.8.21.2.3 Prio

Haupt-Priorität des virtuellen Routers. Es sind Werte zwischen 0 und 255 zulässig. Die Priorität ist proportional zum eingetragenen Wert. Dabei haben die Werte 0 und 255 eine besondere Bedeutung. Der Wert 0 schaltet den virtuellen Router aus. Der Wert 255 wird nur akzeptiert, wenn die Adresse des virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. Ist das nicht der Fall, wird der Router von allen anderen Routern im Event-Log gemeldet.

SNMP-ID: 2.8.21.2.3

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- 0 bis 255

Default: 0

2.8.21.2.4 B-Prio

Backup-Priorität des virtuellen Routers. Es sind Werte zwischen 0 und 255 zulässig. Die Priorität ist proportional zum eingetragenen Wert. Dabei haben die Werte 0 und 255 eine besondere Bedeutung. Der Wert 0 deaktiviert den virtuellen Router im Backup-Fall. Es wird in regelmäßigen Intervallen geprüft, ob die Hauptverbindung wieder aufgebaut werden kann. Das Intervall legt der Reconnect-Delay-Parameter fest. Der Wert 255 wird nur akzeptiert, wenn die Adresse des

virtuellen Routers gleich der Adresse des Interfaces ist, an das der Router gebunden ist. Ist das nicht der Fall, wird der Router von allen anderen Routern im Event-Log gemeldet. Wenn im Backup-Fall auch die Backup-Verbindung nicht aufgebaut werden kann, geht der virtuelle Router vollständig in den Stand-by-Modus und versucht in Intervallen entweder die Haupt- oder die Backup-Verbindung erneut aufzubauen.

SNMP-ID: 2.8.21.2.4

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- 0 bis 255

Default: 0

2.8.21.2.5 Gegenstelle

Der Eintrag des Gegenstellennamens ist optioal. Wird hier eine Gegenstelle eingetragen, so steuert diese das VRRP. Verliert diese Gegenstelle bspw. Ihre Internetanbindung, so tritt der Backup-Fall ein. Wird keine eingetragen, so kann man VRRP dazu nutzen einen Hardware-Ausfall abzudecken. Die Gegenstelle kann auch weiteren virtuellen Routern zugeordnet werden.

SNMP-ID: 2.8.21.2.5

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen.

Default: leer

2.8.21.2.6 Kommentar

Hier können Sie einen Kommentar zur Beschreibung des virtuellen Routers einfügen.

SNMP-ID: 2.8.21.2.6

Pfad Telnet: /Setup/IP-Router/VRRP/VRRP-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: leer

2.8.21.3 Reconnect-Verz.

Wenn die Backup-Verbindung eines Routers nicht aufgebaut werden konnte, wird der Router nicht mehr propagiert. Das Reconnect-Delay gibt an, nach wie vielen Minuten ein solcher Router in diesem Fall versucht, seine Haupt- oder Backup-Verbindung erneut aufzubauen. Während dieses Versuchs wird dieser Router weiterhin nicht propagiert.

SNMP-ID: 2.8.21.3

Pfad Telnet: /Setup/IP-Router/VRRP

Mögliche Werte:

- 0 bis 999 Minuten

Default: 30 Min.

2.8.21.4 Anz.-IntervallInterne-Dienste

Das Advertising-Intervall gibt an nach wie vielen Sekunden ein Router neu propagiert wird. Alle Router des Virtuellen-Router-Systems müssen den gleichen Wert konfiguriert haben

SNMP-ID: 2.8.21.4

Pfad Telnet: /Setup/IP-Router/VRRP

Mögliche Werte:

- 0 bis 999 Sekunden

Default: 1 Sek.

2.8.21.5 Interne-Dienste

Der Schalter "Interne Dienste" steuert das Verhalten des Routers, wenn er unter der Adresse eines virtuellen Routers angesprochen wird. In der Default-Einstellung "on" reagiert der Router bei den Diensten DNS und NETBIOS genau so, als wäre er unter seiner realen Adresse angesprochen worden. Dies funktioniert jedoch nur, wenn der Router selbst Master des virtuellen Routers ist. Die Einstellung "off" bewirkt RFC konformes Verhalten, d.h. entsprechende Pakete werden verworfen.

SNMP-ID: 2.8.21.5

Pfad Telnet: /Setup/IP-Router/VRRP

Mögliche Werte:

- ein
- aus

Default: ein

2.8.22 WAN-Tag-Erzeugung

Mit der WAN-Tag-Erzeugung wird die Quelle für die Zuordnung von Schnittstellen-Tags definiert. Neben der Zuordnung über die Firewall oder direkte Zuordnung über die Tag-Tabelle kann das Schnittstellen-Tag auch anhand der effektiven Routing-Tabelle gewählt werden (statische Routing-Einträge plus Routen, die über RIP gelernt wurden). Aus dieser Routing-Tabelle wird das Tag derjenigen Route gewählt, die sowohl auf die Gegenstelle als auch auf das zugehörige Netzwerk passt. Enthält die effektive Routing-Tabelle mehrere Einträge für eine Gegenstelle mit gleichem Netzwerk, so wird das kleinste Tag verwendet.

SNMP-ID: 2.8.22

Pfad Telnet: /Setup/IP-Router

Mögliche Werte:

- Manual: In dieser Einstellung werden die Schnittstellen-Tags ausschließlich über einen Eintrag in der Tag-Tabelle bestimmt. Die Routing-Tabelle hat keine Bedeutung für die Zuordnung der Schnittstellen-Tags.
- Auto: In dieser Einstellung werden die Schnittstellen-Tags zunächst über einen Eintrag in der Tag-Tabelle bestimmt. Wird dort kein passender Eintrag gefunden, so wird das Tag anhand der Routing-Tabelle ermittelt .

Default: Manual

Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

2.8.23 Tag-Tabelle

Über die Tag-Tabelle kann den eingehenden Datenpaketen anhand der Gegenstelle direkt ein Schnittstellen-Tag zugewiesen werden.

SNMP-ID: 2.8.23

Pfad Telnet: /Setup/IP-Router

2.8.23.1 Gegenstelle

Name der Gegenstelle, zu deren Paketen beim Empfang Schnittstellen-Tags hinzugefügt werden sollen.

SNMP-ID: 2.8.23.1

Pfad Telnet: /Setup/IP-Router/Tag-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

Default: Leer

Besondere Werte: Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen (RAS-Benutzer) einer Firma getaggt werden, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "Firma1_" bekommen. In der Tag-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "Firma1_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

2.8.23.2 Rtg-Tag

Dieses Schnittstellen-Tag wird den eingehenden Paketen der Gegenstelle zugewiesen.

SNMP-ID: 2.8.23.2

Pfad Telnet: /Setup/IP-Router/Tag-Tabelle

Mögliche Werte:

- 0 bis 65535

Default: 0

2.8.23.3 Start-WAN-Pool

Der Start-WAN-Pool stellt den Beginn des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

SNMP-ID: 2.8.23.3

Pfad Telnet: /Setup/IP-Router/Tag-Tabelle

Mögliche Werte:

- Gültige IP-Adresse

Default: 0.0.0.0

2.8.23.4 Ende-WAN-Pool

Der End-WAN-Pool stellt das Ende des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

SNMP-ID: 2.8.23.4

Pfad Telnet: /Setup/IP-Router/Tag-Tabelle

Mögliche Werte:

- Gültige IP-Adresse

Default: 0.0.0.0

Besondere Werte: Wenn der Pool leer ist (Start- und End-Adresse sind 0.0.0.0), dann wird der globale Pool verwendet.

2.8.23.5 DNS-Default

Über diesen Eintrag konfigurieren Sie die Adresse, die die Gegenstelle als DNS-Server zugewiesen bekommt.

Sofern der eingetragene Wert `0.0.0.0` ist, weist Ihr Gerät den im Setup-Menü unter **TCP-IP/DNS-Default** konfigurierten DNS-Server zu. Steht dort ebenfalls `0.0.0.0`, weist sich Ihr Gerät selbst als DNS-Server zu.

Pfad Telnet:

Setup > **IP-Router** > **Tag-Tabelle**

Mögliche Werte:

Gültige IPv4-Adresse

Default:

0.0.0.0

2.8.23.6 DNS-Backup

Über diesen Eintrag konfigurieren Sie die Adresse, die die Gegenstelle als alternativen DNS-Server zugewiesen bekommt.

Sofern der eingetragene Wert `0.0.0.0` ist, weist Ihr Gerät den im Setup-Menü unter **TCP-IP/DNS-Backup** konfigurierten alternativen DNS-Server zu.

Pfad Telnet:

Setup > **IP-Router** > **Tag-Tabelle**

Mögliche Werte:

Gültige IPv4-Adresse

Default:

0.0.0.0

2.8.23.7 NBNS-Default

Über diesen Eintrag konfigurieren Sie die Adresse, die die Gegenstelle als NBNS-Server zugewiesen bekommt.

Sofern der eingetragene Wert `0.0.0.0` ist, weist Ihr Gerät den im Setup-Menü unter **TCP-IP/NBNS-Default** konfigurierten NBNS-Server zu. Steht dort ebenfalls `0.0.0.0`, weist sich Ihr Gerät selbst als NBNS-Server zu, wenn der NetBIOS-Proxy aktiv ist.

Pfad Telnet:

Setup > **IP-Router** > **Tag-Tabelle**

Mögliche Werte:

Gültige IPv4-Adresse

Default:

0.0.0.0

2.8.23.8 NBNS-Backup

Über diesen Eintrag konfigurieren Sie die Adresse, die die Gegenstelle als alternativen NBNS-Server zugewiesen bekommt.

Sofern der eingetragene Wert `0.0.0.0` ist, weist Ihr Gerät den im Setup-Menü unter **TCP-IP/NBNS-Backup** konfigurierten alternativen DNS-Server zu.

Pfad Telnet:

Setup > **IP-Router** > **Tag-Tabelle**

Mögliche Werte:

Gültige IPv4-Adresse

Default:

0.0.0.0

2.9 SNMP

Dieses Menü enthält die Konfiguration von SNMP.

SNMP-ID: 2.9

Pfad Telnet: /Setup

2.9.1 Traps-senden

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

SNMP-ID: 2.9.1

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.9.2 IP-Traps

Hier können Sie SNMP-Manager eintragen.

SNMP-ID: 2.9.2

Pfad Telnet: /Setup/SNMP

2.9.2.1 Trap-IP

Geben Sie hier die IP-Adresse des Computers ein, auf dem ein SNMP-Manager installiert ist.

SNMP-ID: 2.9.2.1

Pfad Telnet: /Setup/SNMP/IP-Traps

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.9.2.3 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

SNMP-ID: 2.9.2.3

Pfad Telnet: /Setup/SNMP/IP-Traps

Mögliche 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

Default: Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehorige IP-Adresse verwendet.

2.9.2.4 Version

Gibt die SNMP-Version an, die für die Traps an diesen Empfänger verwendet werden soll.

SNMP-ID: 2.9.2.4

Pfad Telnet: /Setup/SNMP/IP-Traps

Mögliche Werte:

- SNMPv1
- SNMPv2

Default: SNMPv2

2.9.2.5 Port

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

Pfad Telnet:

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

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

0 … 65535

Default-Wert:

leer

2.9.3 Administrator

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

SNMP-ID: 2.9.3

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.4 Standort

Standortangabe zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.4

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.5 Register-Monitor

Mit dieser Aktion können sich SNMP-Agenten bei einem Gerät anmelden, um anschließend SNMP-Traps zu erhalten. Zu dem Kommando werden dazu die IP-Adresse, der Port und die MAC-Adresse des SNMP-Agenten angegeben. Alle drei Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

SNMP-ID: 2.9.5

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- <IP-Adresse|*>:<Port|*> <MAC-Adresse|*> <W>

Default: Leer

Besondere Werte: <W> am Ende des Kommandos ist für eine Registrierung über eine WAN-Verbindung erforderlich.

Ein LANmonitor muss nicht explizit am Gerät angemeldet werden. Der LANmonitor überträgt bei der Suche nach neuen Geräten automatisch die Anmeldeinformationen an das Gerät.

2.9.6 Loesche-Monitor

Mit dieser Aktion können angemeldete SNMP-Agenten aus der Monitor-Liste entfernt werden. Zu dem Kommando werden dazu die IP-Adresse und der Port des SNMP-Agenten angegeben. Alle drei Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

SNMP-ID: 2.9.6

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- <IP-Adresse|*>:<Port|*>

Default: Leer

2.9.7 Monitor-Tabelle

Die Monitor-Tabelle zeigt alle am Gerät angemeldeten SNMP-Agenten.

SNMP-ID: 2.9.7

Pfad Telnet: /Setup/SNMP

2.9.7.1 IP-Adresse

IP-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.1

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

2.9.7.2 Port

Port, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.2

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.7.3 Timeout

Timeout in Minuten, bis die Gegenstelle aus der Monitor-Tabelle entfernt wird.

SNMP-ID: 2.9.7.3

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.7.4 MAC-Adresse

MAC-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.4

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.7.5 Gegenstelle

Name der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.5

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen.

2.9.7.6 Loopback-Addr.

Loopback-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.6

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

Mögliche 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

2.9.7.7 VLAN-ID

VLAN-ID, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.7

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.7.8 LAN-Ifc

LAN-Ifc, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.8

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.7.9 Ethernet-Port

Ethernet-Port, über den die Gegenstelle mit einem SNMP-Agent auf das Gerät zugreift.

SNMP-ID: 2.9.7.9

Pfad Telnet: /Setup/SNMP/Monitor-Tabelle

2.9.10 Passw.Zwang-fuer-SNMP-Lesezugriff

Über diese Einstellung legen Sie fest, ob das Lesen von SNMP-Meldungen über einen SNMP-Agenten (z. B. LANmonitor) die Eingabe eines Passwort erfordert.

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

nein

In dieser Einstellung lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. öffentlich via SNMP auslesen (Ready-Only Community 'public' aktiviert).

ja

In dieser Einstellung lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentisiert hat (Ready-Only Community 'public' daktiviert). Die Authorisierung kann wahlweise über die Zugangsdaten für den Administrator-Account oder über den in der individuellen SNMP-Community definierten Zugang derfolgen.

Default-Wert:

nein

2.9.11 Kommentar-1

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.11

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.12 Kommentar-2

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.12

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.13 Kommentar-3

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.13

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.14 Kommentar-4

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.14

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 Zeichen

Default: Leer

2.9.15 Read-Only-Community

Über diesen Parameter definieren Sie eine individuelle SNMP-Community für den Lesezugriff. Geben Sie dazu entweder ein Master-Passwort oder ein Benutzername:Passwort-Paar ein. Lassen Sie das Feld leer, um keine weitere schreibgeschützte Community ausser 'public' zu verwenden (sofern aktiviert).

Das deaktivieren der Community 'public' hat keine Auswirkung auf den Zugriff über die hier angelegte Community. Eine individuelle SNMP Read-Only Community bleibt stets ein alternativer Zugangsschlüssel, welcher nicht an ein Administratorkonto gebunden ist.

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

Keine direkte Abhängigkeit von anderen Werten. **Read-Only-Community** aus **Setup** > **SNMP** > **Read-Only-Communities** erweitert jedoch den hier definierten Parameter um weitere schreibgeschützte Communities.

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

Default-Wert:

leer

2.9.16 Kommentar-5

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.16

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 alphanumerische Zeichen

Default: Leer

2.9.17 Kommentar-6

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.17

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 alphanumerische Zeichen

Default: Leer

2.9.17 Kommentar-7

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.17

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 alphanumerische Zeichen

Default: Leer

2.9.17 Kommentar-8

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

SNMP-ID: 2.9.17

Pfad Telnet: /Setup/SNMP

Mögliche Werte:

- max. 255 alphanumerische Zeichen

Default: Leer

2.9.20 Volle-Host-MIB

Wählen Sie hier aus, ob für das Gerät eine volle Host-MIB genutzt wird.

SNMP-ID: 2.9.20

Pfad Telnet: /Setup/SNMP/Volle-Host-MIB

Mögliche Werte:

- Nein
- Ja

Default: Nein

2.9.21 Port

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

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

0 … 65535

Default-Wert:

161

2.9.22 Read-Only-Communities

In dieser Tabelle definieren Sie weitere schreibgeschützte Communities für den SNMP-Zugriff.

Pfad Telnet:

Setup > **SNMP**

2.9.22.1 Read-Only-Community

Über diesen Parameter definieren Sie eine zusätzliche individuelle SNMP-Community für den Lesezugriff. Geben Sie dazu entweder ein Master-Passwort oder ein Benutzername:Passwort-Paar ein.

Das deaktivieren der Community 'public' hat keine Auswirkung auf den Zugriff über die hier angelegte Community. Eine individuelle SNMP Read-Only Community bleibt stets ein alternativer Zugangsschlüssel, welcher nicht an ein Administratorkonto gebunden ist.

Pfad Telnet:

Setup > **SNMP** > **Read-Only-Communities**

Mögliche Werte:

Keine direkte Abhängigkeit von anderen Werten. Dieser Parameter erweitert jedoch die **Read-Only-Community** aus **Setup** > **SNMP** um weitere schreibgeschützte Communities.

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

Default-Wert:

leer

2.9.23 Oefftl-Kommentar-1

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

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

Default-Wert:

leer

2.9.24 Oefftl-Kommentar-2

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

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

Default-Wert:

leer

2.9.25 Oefftl-Kommentar-3

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

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

Default-Wert:

leer

2.9.26 Oefftl-Kommentar-4

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

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

Default-Wert:

leer

2.10 DHCP

Dieses Menü enthält die Einstellungen für DHCP.

SNMP-ID: 2.10

Pfad Telnet: /Setup

2.10.6 Max.-Gueltigkeit-Minuten

Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

SNMP-ID: 2.10.6

Pfad Telnet: /Setup/DHCP

Mögliche Werte:

- max. 10 Zeichen

Default: 6000

2.10.7 Default-Gueltigkeit-Minuten

Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeitsdauer der hier eingestellte Wert zugewiesen.

SNMP-ID: 2.10.7

Pfad Telnet: /Setup/DHCP

Mögliche Werte:

- max. 10 Zeichen

Default: 500

2.10.8 DHCP-Tabelle

Die DHCP-Tabelle gibt eine Übersicht über die in den IP-Netzwerken verwendeten IP-Adressen. Bei der DHCP-Tabelle handelt es sich um eine reine Status-Tabelle, in der keine Parameter konfiguriert werden können.

SNMP-ID: 2.10.8

Pfad Telnet: /Setup/DHCP

2.10.8.1 IP-Adresse

IP-Adresse, die von der Station verwendet wird.

SNMP-ID: 2.10.8.1

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

2.10.8.2 MAC-Adresse

MAC-Adresse der Station.

SNMP-ID: 2.10.8.2

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.3 Timeout

Gültigkeitsdauer der Adresszuweisung in Minuten.

SNMP-ID: 2.10.8.3

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.4 Rechnername

Name der Station, sofern dieser ermittelt werden konnte.

SNMP-ID: 2.10.8.4

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.5 Typ

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

neu: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.

unbek.: Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

stat.: Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr für andere Stationen im Netz verwendet werden.

dyn.: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

SNMP-ID: 2.10.8.5

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.7 Ethernet-Port

Physikalisches Interface, über das die Station mit dem Gerät verbunden ist.

SNMP-ID: 2.10.8.7

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.8 VLAN-ID

Die von dieser Station verwendete VLAN-ID.

SNMP-ID: 2.10.8.8

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.9 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

SNMP-ID: 2.10.8.9

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle

2.10.8.10 LAN-Ifc

Die LAN-Schnittstelle, auf die sich dieser Eintrag bezieht.

SNMP-ID: 2.10.8.10

Pfad Telnet: /Setup/DHCP/DHCP-Tabelle/LAN-Ifc

2.10.8.11 Zuweisung

Diese Spalte zeigt den Zeitstempel (Datum und Uhrzeit in der Form "dd.mm.yyyy "hh:mm:ss") an, zu dem die DHCP-Zuweisung für die betreffende IP-Adresse erfolgte.

Pfad Telnet:

Setup > **DHCP** > **DHCP-Tabelle**

2.10.9 Hosts

Über das Bootstrap-Protokoll (BOOTP) können einer Station beim Starten eine IP-Adresse und weitere Parameter übermittelt werden. Dazu wird die MAC-Adresse der Station in die Host-Tabelle eingetragen.

SNMP-ID: 2.10.9

Pfad Telnet: /Setup/DHCP

2.10.9.1 MAC-Adresse

Geben Sie hier die MAC-Adresse der Station ein, der eine IP-Adresse zugewiesen werden soll.

SNMP-ID: 2.10.9.1

Pfad Telnet: /Setup/DHCP/Hosts

Mögliche Werte:

- Gültige MAC-Adresse.

Default: 000000000000

2.10.9.2 IP-Adresse

Geben Sie hier die IP-Adresse der Station ein, die der Station zugewiesen werden soll.

SNMP-ID: 2.10.9.2

Pfad Telnet: /Setup/DHCP/Hosts

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.9.3 Rechnername

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

SNMP-ID: 2.10.9.3

Pfad Telnet: /Setup/DHCP/Hosts

Mögliche Werte:

- max. 30 Zeichen

Default: Leer

2.10.9.4 Image-Alias

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

SNMP-ID: 2.10.9.4

Pfad Telnet: /Setup/DHCP/Hosts

Mögliche Werte:

- max. 16 Zeichen

Default: Leer

Den Server, der das Boot-Image zur Verfügung stellt, sowie den Namen der Datei auf dem Server müssen Sie in der Boot-Image-Tabelle eingeben.

2.10.9.5 Netzwerkname

Hier wird der Name eines konfigurierten IP-Netzwerks eingetragen. Nur wenn sich die anfragende Station in diesem IP-Netzwerk befindet, wird der Station die für die MAC-Adresse definierte IP-Adresse zugewiesen.

SNMP-ID: 2.10.9.5

Pfad Telnet: /Setup/DHCP/Hosts

Mögliche Werte:

- max. 16 Zeichen

Default: Leer

Besondere Werte: Leer: Passt die in diesem Eintrag definierte IP-Adresse zu dem Adresskreis des IP-Netzwerks, in dem sich die anfragende Station befindet, dann wird die IP-Adresse zugewiesen.

Befindet sich die anfragende Station in einem IP-Netzwerk, zu dem es keinen passenden Eintrag in der HostTabelle gibt, so wird der Station dynamisch eine IP-Adresse aus dem IP-Adress-Pool des jeweiligen IP-Netzwerks zugewiesen.

2.10.10 Alias-Liste

In der Alias-Liste werden die Bezeichnungen für die Boot-Images definiert, über welche die Images in der Host-Tabelle referenziert werden können.

SNMP-ID: 2.10.10

Pfad Telnet: /Setup/DHCP

2.10.10.1 Image-Alias

Geben Sie eine beliebige Bezeichnung für dieses Boot-Image ein. Diese Bezeichnung wird verwendet, wenn Sie in der Stations-Liste ein Boot-Image einer bestimmten Station zuordnen.

SNMP-ID: 2.10.10.1

Pfad Telnet: /Setup/DHCP/Alias-Liste

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.10.10.2 Image-File

Geben Sie den Namen der Datei auf dem Server an, die das Boot-Image enthält.

SNMP-ID: 2.10.10.2

Pfad Telnet: /Setup/DHCP/Alias-Liste

Mögliche Werte:

- max. 60 Zeichen

Default: leer

2.10.10.3 Image-Server

Geben Sie die IP-Adresse des Servers ein, der das Boot-Image zur Verfügung stellt.

SNMP-ID: 2.10.10.3

Pfad Telnet: /Setup/DHCP/Alias-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.18 Ports

In der Port-Tabelle wird der DHCP-Server für die jeweiligen logischen Interfaces des Geräts freigegeben.

SNMP-ID: 2.10.18

Pfad Telnet: /Setup/DHCP

2.10.18.2 Port

Auswahl des logischen Interfaces, für das der DHCP-Server aktiviert bzw. deaktiviert werden soll.

SNMP-ID: 2.10.18.2

Pfad Telnet: /Setup/DHCP/Ports

Mögliche Werte:

- Auswahl aus der Liste der logischen Interfaces in diesem Gerät, z. B. LAN-1, WLAN-1, P2P-1-1 etc.

2.10.18.3 DHCP-Freigeben

Aktiviert bzw. deaktiviert den DHCP-Server für das gewählte logische Interface.

SNMP-ID: 2.10.18.3

Pfad Telnet: /Setup/DHCP/Ports

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.10.19 User-Class-Identifier

Der DHCP-Client im Gerät kann in den versendeten DHCP-Requests zusätzliche Angaben einfügen, die eine Erkennung der Requests im Netzwerk erleichtern. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt den Gerätetyp an. Die Vendor-Class-ID wird immer übertragen. Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an. Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

SNMP-ID: 2.10.19

Pfad Telnet: /Setup/DHCP

Mögliche Werte:

- max. 63 Zeichen

Default: leer

2.10.20 Netzliste

In dieser Tabelle werden die DHCP-Einstellungen zu den IP-Netzwerken definiert. Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann "verteilen" sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der Geräte löst allerdings nur die Namen der Stationen richtig auf, denen der eigene DHCP-Server die Adressinformationen zugewiesen

hat. Damit der DNS-Server auch die Namen anderer DHCP-Server auflösen kann, können die DHCP-Server im Cluster betrieben werden. In dieser Betriebsart verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern im Cluster angemeldet haben.

Der Betrieb eines DHCP-Servers im Cluster kann für jedes einzelne ARF-Netz in den zugehörigen DHCP-Einstellungen aktiviert bzw. deaktiviert werden.

SNMP-ID: 2.10.20

Pfad Telnet: /Setup/DHCP/Netzliste

2.10.20.1 Netzwerkname

Name des Netzwerks, für das die Einstellungen des DCHP-Servers gelten sollen.

SNMP-ID: 2.10.20.1

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.10.20.2 Start-Adress-Pool

Erste IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die erste freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

SNMP-ID: 2.10.20.2

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.3 Ende-Adress-Pool

Letzte IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die letzte freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

SNMP-ID: 2.10.20.3

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.4 Netz-Maske

Zugehörige Netzmaske für den Adressbereich, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die Netzmaske aus dem zugehörigen Netzwerk.

SNMP-ID: 2.10.20.4

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.5 Broadcast-Adresse

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z. B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.

SNMP-ID: 2.10.20.5

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0 (Broadcast-Adresse wird automatisch ermittelt)

Wir empfehlen Änderungen der voreingestellten Broadcast-Adresse nur für erfahrene Netzwerk-Spezialisten. Fehlkonfigurationen können zu unerwünschten, gebührenpflichtigen Verbindungen führen!

2.10.20.6 Gateway-Adresse

Der DHCP-Server weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechenden IP-Adresse auch ein anderes Gateway übertragen werden.

SNMP-ID: 2.10.20.6

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.7 DNS-Default

IP-Adresse des DNS-Nameservers, den die anfragenden Arbeitsstation verwenden soll.

SNMP-ID: 2.10.20.7

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

Wenn weder ein Default- noch ein Backup-DNS-Server eingetragen wurde, weist das Gerät der anfragenden Arbeitsstation seine eigene IP-Adresse im jeweiligen ARF-Netz als (primären) DNS-Server zu.

2.10.20.8 DNS-Backup

IP-Adresse des Backup-DNS-Nameservers. Diesen DNS-Nameserver verwendet die Arbeitsstation, wenn der erste DNS-Nameserver ausfällt.

SNMP-ID: 2.10.20.8

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

Wenn weder ein Default- noch ein Backup-DNS-Server eingetragen wurde, weist das Gerät der anfragenden Arbeitsstation seine eigene IP-Adresse im jeweiligen ARF-Netz als (primären) DNS-Server zu.

2.10.20.9 NBNS-Default

IP-Adresse des NBNS-Nameservers, den die anfragende Arbeitsstation verwenden soll.

SNMP-ID: 2.10.20.9

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.10 NBNS-Backup

IP-Adresse des Backup-NBNS-Nameservers. Diesen NBNS-Nameserver verwendet die Arbeitsstation, wenn der erste NBNS-Nameserver ausfällt.

SNMP-ID: 2.10.20.10

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.11 Aktiv

Betriebsart des DHCP-Servers für dieses Netzwerk. Je nach Betriebsart kann sich der DHCP-Server selbst aktivieren bzw. deaktivieren. Ob der DHCP-Server aktiv ist, kann den DHCP-Statistiken entnommen werden.

SNMP-ID: 2.10.20.11

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Nein: Der DHCP-Server ist dauerhaft abgeschaltet.
- Ja: Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft. Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an. Bei einer fehlerhaften Konfiguration (z. B. ungültige Pool-Grenzen) wird der DHCP-Server für das Netzwerk deaktiviert. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das kein anderer DHCP-Server im LAN aktiv ist.
- Automatisch: In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED. Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für das Gerät noch keine IP-Adresse konfiguriert, dann wechselt es in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u. a. verhindert, dass ein unkonfiguriertes Gerät nach dem Einschalten im Netz unerwünscht Adressen vergibt. Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem späteren Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wird der DHCP-Server im Gerät deaktiviert.
- 'Anfragen Weiterleiten': Der DHCP-Server ist eingeschaltet, das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter (Betriebsart DHCP-Relay-Agent).

- 'Client-Modus': Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN. Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

Default: Nein

Verwenden Sie die Einstellung "Ja" nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist. Verwenden Sie die Einstellung "Client-Modus" nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

2.10.20.12 Broadcast-Bit

Wählen Sie hier, ob das von den Clients gemeldete Broadcast-Bit ausgewertet wird oder nicht. Wenn das Bit nicht ausgewertet wird, werden alle DHCP-Nachrichten als Broadcast versendet.

SNMP-ID: 2.10.20.12

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.10.20.13 Master-Server

Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

SNMP-ID: 2.10.20.13

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.14 Cache

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers im Gerät gespeichert werden. Spätere Anfragen können dann vom Gerät selbst beantwortet werden. Diese Option ist nützlich, wenn der übergeordnete DHCP-Server nur über eine kostenpflichtige Verbindung erreicht werden kann.

SNMP-ID: 2.10.20.14

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.10.20.15 Anpassung

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers an das lokale Netzwerk angepasst werden. Bei aktiviert Anpassung ersetzt das Gerät in den Antworten des übergeordneten DHCP-Servers folgende Einträge durch seine eigene Adresse (bzw. lokal konfigurierte Adressen):

- Gateway
- Netzmaske
- Broadcast-Adresse
- DNS-Server
- NBNS-Server
- Server-ID

Diese Option ist sinnvoll, wenn der übergeordnete DHCP-Server keine getrennte Konfiguration für DHCP-Clients in einem anderen Netzwerk zulässt.

SNMP-ID: 2.10.20.15

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.10.20.16 Cluster

Wählen Sie hier aus, ob der DHCP-Server für dieses ARF-Netz im Cluster oder separat betrieben werden soll.

SNMP-ID: 2.10.20.16

Pfad Telnet: /Setup/DHCP/Netzliste

Mögliche Werte:

- Ja: Wenn der Cluster-Betrieb aktiviert ist, verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern in Cluster angemeldet haben. Diese Stationen werden in der DHCP-Tabelle mit dem Flag "cache" gekennzeichnet.
- Nein: Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

Default:

Nein

Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request). Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage nach einer neuen DHCP-Anbindung (Rebinding Request) als Broadcast an alle erreichbaren DHCP-Server. Renew-Requests werden von den DHCP-Servern im Cluster ignoriert – so wird ein Rebinding erzwungen, damit alle im Cluster vorhandenen DHCP-Server über den Broadcast ihren Eintrag für die Station erneuern können. Auf den Rebind-Request antwortet zunächst nur der DHCP-Server, bei dem die Station ursprünglich registriert war. Wird der Rebind-Request von einer Station wiederholt, dann gehen alle DHCP-Server im Cluster davon aus, das der ursprünglich zuständige DHCP-Server im Cluster nicht mehr aktiv ist und beantworten die Anfrage. Diese Antwort enthält zwar die gleiche IP-Adresse für die Station, kann aber unterschiedliche Gateway- und DNS-Serveradressen enthalten. Die Station sucht sich nun aus den Antworten einen neuen DHCP-Server aus, an den sie von nun an gebunden ist und übernimmt von ihm Gateway und DNS-Server (sowie alle anderen zugewiesenen Parameter).

2.10.20.17 2ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

SNMP-ID: 2.10.20.17

Pfad Telnet: /Setup/DHCP/Netzliste/2ter-Master-Server

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.18 3ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

SNMP-ID: 2.10.20.18

Pfad Telnet: /Setup/DHCP/Netzliste/2ter-Master-Server

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.20.19 4ter-Master-Server

Hier wird die IP-Adresse eines alternativen DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

SNMP-ID: 2.10.20.19

Pfad Telnet: /Setup/DHCP/Netzliste/2ter-Master-Server

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.10.21 Zusaetzliche-Optionen

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.

SNMP-ID: 2.10.21

Pfad Telnet: /Setup/DHCP

2.10.21.1 Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. "17" (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

SNMP-ID: 2.10.21.1

Pfad Telnet: /Setup/DHCP/Zusaetzliche-Optionen

Mögliche Werte: max. 3 Zeichen

Default: Leer

Eine Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

2.10.21.2 Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

SNMP-ID: 2.10.21.2

Pfad Telnet: /Setup/DHCP/Zusaetzliche-Optionen

Mögliche Werte:

- Auswahl aus der Liste der definierten IP-Netzwerke.

Default: Leer

Besondere Werte: Leer: Wird kein Netzwekname angegeben, so wird die in diesem Eintrag definierte DHCP-Option in allen IP--Netzwerken verwendet.

2.10.21.3 Options-Wert

In diesem Feld wird der Inhalt der DHCP-Option definiert. IP-Adressen gibt man normalerweise in der üblichen IPv4-Notation an, z. B. `123.123.123.100`. Integer-Typen geben Sie in Dezimalzahlen an, String-Typen als Simple Text. Verschiedene Werte in einem Textfeld werden mit Kommas getrennt, z. B. `123.123.123.100, 123.123.123.200`.

Die mögliche Länge des Optionswertes hängt von der gewählten Optionsnummer ab. Der RFC 2132 listet für jede Option ein zulässige Länge auf.

Pfad Telnet:

Setup > **DHCP** > **Zusaetzliche-Optionen**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.10.21.4 Typ

Typ des Eintrags.

SNMP-ID: 2.10.21.4

Pfad Telnet: /Setup/DHCP/Zusaetzliche-Optionen

Dieser Wert ist abhängig von der jeweiligen Option. Für die Option "35" wird hier im RFC 2132 z. B. der ARP Cache Timeout so definiert (in englischer Sprache):

ARP Cache Timeout Option

This option specifies the timeout in seconds for ARP cache entries.

The time is specified as a 32-bit unsigned integer.

The code for this option is 35, and its length is 4.

Code	Len	Time			
35	4	t1	t2	t3	t4

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ "32-Bit-Integer" verwendet wird.

Mögliche Werte:

- String
- Integer8
- Integer16
- Integer32

- IP-Adresse

Default: String

Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

2.10.22 Vendor-Class-Identifier

Der Vendor-Class-Identifier (DHCP-Option 60) zeigt den Gerätetyp an. Die Vendor-Class-ID wird immer übertragen.

Pfad Telnet:

Setup > **DHCP** > **Vendor-Class-Identifier**

Mögliche Werte:

max. 63 Zeichen

Default:

Leer

2.11 Config

Enthält die allgemeinen Konfigurationseinstellungen.

SNMP-ID: 2.11

Pfad Telnet: /Setup

2.11.3 Pass.Zwang-fuer-SNMP-Lesezugriff

Wenn diese Option eingeschaltet ist und noch kein Passwort vergeben ist, werden Sie immer wenn Sie sich auf das Gerät einloggen aufgefordert ein Passwort zu setzen.

SNMP-ID: 2.11.3

Pfad Telnet: /Setup/Config

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.11.4 max. Verbindungen

max. Anzahl von Konfigurationsverbindungen, die gleichzeitig zu diesem Gerät bestehen dürfen.

SNMP-ID: 2.11.4

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: 0 schaltet die Begrenzung aus.

2.11.5 Config-Aging-Minutes

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

SNMP-ID: 2.11.5

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 15

2.11.6 Sprache

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. Er wird werkseitig auf Englisch als Konsolensprache eingestellt.

SNMP-ID: 2.11.6

Pfad Telnet: /Setup/Config

Mögliche Werte:

- Deutsch
- Englisch

Default: Englisch

Bitte beachten Sie, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da ansonsten die Kommandos der Zeitautomatik nicht beachtet werden.

2.11.7 Login-Fehler

Um die Konfiguration Ihres Gerätes vor unberechtigtem Zugriff zu schützen, kann sich das Gerät nach mehreren fehlerhaften Anmelde-Versuchen automatisch sperren. Geben Sie hier ein, nach wieviel Fehlversuchen die Sperre aktiviert werden soll.

SNMP-ID: 2.11.7

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 10

2.11.8 Sperr-Minuten

Um die Konfiguration Ihres Gerätes vor unberechtigtem Zugriff zu schützen, kann sich das Gerät nach mehreren fehlerhaften Anmelde-Versuchen selber sperren. Geben Sie hier den Zeitraum ein, für den die Sperre aktiv bleiben soll. Erst nach Ablauf dieses Zeitraums kann wieder auf das Gerät zugegriffen werden.

SNMP-ID: 2.11.8

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 45

Besondere Werte: 0 schaltet die Sperre aus.

2.11.9 Admin.-EAZ-MSN

Wenn der LANCAPI-Server auch ankommende Rufe entgegen nehmen soll, so geben Sie im Feld 'Rufnummern (MSN/EAZ)' alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegennehmen soll. Mehrere Rufnummern werden voneinander durch Semikola getrennt. Wenn Sie hier keine Rufnummer eingeben, nimmt die LANCAPI Anrufe aller eigenen ISDN-Rufnummern entgegen.

SNMP-ID: 2.11.9

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 31 Zeichen

Default: leer

2.11.10 Display-Kontrast

Stellen Sie hier den Kontrast für das Display des Geräts ein.

SNMP-ID: 2.11.10

Pfad Telnet: /Setup/Config/Display-Kontrast

Mögliche Werte:

- K1 (geringer Kontrast) bis K8 (hoher Kontrast).

Default: K4

2.11.12 WLAN-Nur-Authentifizierung

Mit dieser Einstellung haben Sie die Möglichkeit, den Gerätezugriff über Public Spot-Interfaces auf die Public Spot-Authentisierungsseiten zu beschränken und automatisch alle anderen Konfigurationsprotokolle zu sperren.

Der Zugriff aus einem Public Spot-Netzwerk auf die Konfiguration eines Public Spots (WEBconfig) sollte aus Sicherheitsgründen immer ausgeschlossen sein. Die Aktivierung dieser Einstellung ist für Public Spot-Szenarien daher dringend zu empfehlen!

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

nein

ja

Default:

nein

2.11.15 Zugriffstabelle

Hier können Sie für jedes Netz und jedes unterstützte Konfigurationsprotokoll gesondert die Zugriffsrechte einstellen. Außerdem können Sie den Zugriff auf bestimmte Stationen einschränken.

SNMP-ID: 2.11.15

Pfad Telnet: /Setup/Config

2.11.15.1 Ifc.

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

SNMP-ID: 2.11.15.1

Pfad Telnet: /Setup/Config/Zugriffstabelle

2.11.15.2 Telnet

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET-Protokoll ein. Dieses Protokoll wird für die textbasierte und Betriebssystem-unabhängige Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.3 TFTP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TFTP-Protokoll (Trivial File Transfer Protocol) ein. Dieses Protokoll wird zum Beispiel für die Konfiguration mit dem Programm LANconfig benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.4 HTTP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das HTTP-Protokoll (Hypertext Transfer Protocol) ein. Dieses Protokoll wird für die Betriebssystem-unabhängige Konfiguration dieses Gerätes über das implementierte Web-Browser-Interface benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.5 SNMP

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das SNMP-Protokoll (Simple Network Management Protocol) ein. Dieses Protokoll wird zum Beispiel für die Überwachung des Gerätes mit dem Programm LANmonitor benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.6 HTTPS

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das HTTPS-Protokoll (Hypertext Transfer Protocol Secure oder HTTP über SSL) ein. Dieses Protokoll wird für die Betriebssystem-unabhängige und sichere Konfiguration dieses Gerätes über das implementierte Web-Browser-Interface benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.7 Telnet-SSL

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET-Protokoll ein. Dieses Protokoll wird für die textbasierte und Betriebssystem-unabhängige Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.8 SSH

Stellen Sie hier das Zugriffsrecht für die Konfiguration des Gerätes über das TELNET/SSH-Protokoll ein. Dieses Protokoll wird für die textbasierte, Betriebssystem-unabhängige und sichere Konfiguration dieses Gerätes über die implementierte Telnet-Konsole benötigt.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.15.10 Config-Sync

Gibt an, ob über diese Schnittstelle ein Config-Sync (eingeschränkt) möglich ist.

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN

Zugriff ist nur über VPN möglich.

Nur bei VPN-fähigen Geräten.

ja

Zugriff ist generell möglich.

Standardeinstellung bei allen Schnittstellen außer WAN.

Read

Zugriff ist nur lesend möglich.

nein

Zugriff ist nicht möglich.

Standardeinstellung bei der WAN-Schnittstelle.

Default-Wert:

ja

nein

2.11.16 Bildschirmhoehe

Gibt die maximale Höhe des Bildschirms in Zeilen an. Wenn Sie hier eine 0 eingeben, dann bestimmt das Gerät beim Einloggen die optimale Bildschirmhöhe automatisch.

SNMP-ID: 2.11.16

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 24

Besondere Werte: 0

2.11.17 Prompt

Mit diesem Wert definieren Sie den Prompt (die Eingabeaufforderung) an der Kommandozeile.

SNMP-ID: 2.11.17

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 31 Zeichen mit den folgenden Variablen:
- %f: Gibt ein [Test] aus, wenn Sie an der Kommandozeile zuvor den Befehl 'flash no' eingegeben haben. Mit dem Befehl 'flash no' aktivieren Sie den Testmodus für die folgenden Konfigurationsänderungen. Bei aktiviertem Testmodus speichert das Gerät die Änderungen an der Konfiguration nur im RAM. Da das Gerät den RAM bei einem Neustart (Boot) löscht, gehen die Konfigurationsänderungen im Testmodus beim Booten verloren. Die Anzeige [Test] warnt den Administrator vor diesem möglichen Verlust der Konfigurationsänderungen.
- %u: Benutzername
- %n: Gerätename
- %p: aktueller Pfad
- %t: aktuelle Uhrzeit
- %o: aktuelle Betriebszeit

Default: leer

2.11.18 LED-Test

Aktiviert den Testmodus für die LEDs, bei der die Funktion der LEDs in verschiedenen Farben getestet wird.

SNMP-ID: 2.11.18

Pfad Telnet: /Setup/Config

Mögliche Werte:

- Aus: Schaltet alle LEDs aus
- Rot: Schaltet alle LEDs ein, die rot leuchten können
- Grün: Schaltet alle LEDs ein, die grün leuchten können
- Orange: Schaltet alle LEDs ein, die orange leuchten können
- Kein_Test: Normaler Betriebszustand der LEDs

Default: Kein_Test

2.11.20 Cron-Tabelle

Mit Hilfe von CRON-Jobs lassen sich regelmäßige Aktionen zu bestimmten Zeiten automatisch auf einem Gerät ausführen. Sind in einer Installation sehr viele Geräte aktiv, die zu einem gemeinsamen Zeitpunkt über einen CRON-Job die gleiche Aktion ausführen (z. B. eine Konfiguration per Script aktualisieren), kann das zu unerwünschten Effekten führen, weil z. B. alle Geräte gleichzeitig die VPN-Verbindungen abbauen. Um diesen Effekt zu vermeiden, können die CRON-Jobs mit einer zufälligen Verzögerungszeit von 0 bis 59 Minuten definiert werden.

SNMP-ID: 2.11.20

Pfad Telnet: /Setup/Config

2.11.20.1 Index

Index für diesen Eintrag.

SNMP-ID: 2.11.20.1

Pfad Telnet: /Setup/Config/Cron-Tabelle

2.11.20.2 Minute

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als “Minimalwert-max.wert”) eingegeben werden.

SNMP-ID: 2.11.20.2

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- max. 50 Zeichen

Default: leer

2.11.20.3 Stunde

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber einen Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

SNMP-ID: 2.11.20.3

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- max. 50 Zeichen

Default: leer

2.11.20.4 Wochentag

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber einen Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

SNMP-ID: 2.11.20.4

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- 0: Sonntag
- 1: Montag
- 2: Dienstag
- 3: Mittwoch
- 4: Donnerstag
- 5: Freitag
- 6: Samstag

Default: leer

2.11.20.5 Tag

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

SNMP-ID: 2.11.20.5

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- max. 50 Zeichen

Default: leer

2.11.20.6 Monat

Der Wert definiert den Zeitpunkt, an dem ein Kommando ausgeführt werden soll. Wird kein Wert angegeben, so wird er auch nicht in die Steuerung einbezogen. Es kann auch eine Komma-separierte Liste von Werten, oder aber ein Bereich (angegeben als "Minimalwert-max.wert") eingegeben werden.

SNMP-ID: 2.11.20.6

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- 0: Sonntag
- 1: Montag
- 2: Dienstag
- 3: Mittwoch
- 4: Donnerstag
- 5: Freitag
- 6: Samstag

Default: leer

2.11.20.7 Kommando

Das auszuführende Kommando oder eine Komma-separierte Kommando-Liste. Ausgeführt werden kann dabei jede beliebige Kommandozeilenfunktion.

SNMP-ID: 2.11.20.7

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- max. 100 Zeichen

Default: leer

2.11.20.8 Basis

Bestimmt ob die zeitliche Steuerung auf Grundlage der Echtzeit oder auf Grundlage der Betriebszeit des Gerätes ausgeführt werden soll.

SNMP-ID: 2.11.20.8

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- Echtzeit: Diese Regeln werten alle Zeit-/Datumsangaben aus. Echtzeit-basierte Regel können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.
- Betriebszeit: Diese Regeln werten nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.

Default: Echtzeit

2.11.20.9 Aktiv

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.11.20.9

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.11.20.10 Besitzer

Als Besitzer des Cron-Jobs kann ein im Gerät definierter Administrator ausgewählt werden. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.

SNMP-ID: 2.11.20.10

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.11.20.11 Variation

Dieser Parameter gibt eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der definierten Startzeit maximal verzögert wird. Die tatsächliche Verzögerungszeit wird zufällig ermittelt und liegt zwischen Null und der hier eingetragenen Zeit.

SNMP-ID: 2.11.20.11

Pfad Telnet: /Setup/Config/Cron-Tabelle

Mögliche Werte:

- 0 bis 65535 Sekunden

Default: 0

Besondere Werte: Bei einer Variation von Null wird der CRON-Job exakt zur definierten Zeit ausgeführt.

Echtzeit-basierte Regeln können nur ausgeführt werden, sofern das Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.

2.11.20.12 Kommentar

Über diesen Parameter lässt sich zu dem Eintrag in der CRON-Tabelle ein Kommentar hinterlegen.

Pfad Telnet:

Setup > **Config** > **Cron-Tabelle**

Mögliche Werte:

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

Default-Wert:

leer

2.11.21 Admins

Hier können Sie weitere Admin-Benutzerkonten anlegen.

SNMP-ID: 2.11.21

Pfad Telnet: /Setup/Config

2.11.21.1 Administrator

In der Konfiguration des Gerätes können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für ein Gerät können bis zu 16 verschiedene Administratoren eingerichtet werden.

SNMP-ID: 2.11.21.1

Pfad Telnet: /Setup/Config/Admins

Mögliche Werte:

- max. 16 Zeichen

Default: leer

Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den „root"-Administrator mit dem Haupt-Geräte-Passwort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht gelöscht oder umbenannt werden. Um sich als root-Administrator anzumelden, geben Sie im Login-Fenster den Benutzernamen „root" ein oder Sie lassen dieses Feld frei. Sobald in der Konfiguration des Gerätes ein Passwort für den „root"-Administrator gesetzt ist, erscheint beim Aufruf von WEBconfig auf der Startseite die Schaltfläche Login, mit dem das Fenster zur Anmeldung eingeblendet wird. Nach Eingabe von korrektem Benutzernamen und Passwort erscheint das Hauptmenü der WEBconfig. In diesem Menü sind nur die Punkte vorhanden, für die der Administrator Zugriffs- bzw. Funktionsberechtigungen hat. Ist mindestens ein weiterer Administrator in der Admin-Tabelle eingerichtet, so enthält das Hauptmenü zusätzlich eine Schaltfläche Administrator wechseln, der es erlaubt zu einer anderen Benutzerkennung (mit ggf. anderen Rechten) zu wechseln.

2.11.21.2 Passwort

Kennwort für diesen Eintrag.

SNMP-ID: 2.11.21.2

Pfad Telnet: /Setup/Config/Admins

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.11.21.3 Funktionsrechte

Jeder Administrator verfügt über "Funktionsrechte", die den persönlichen Zugriff auf bestimmte Funktionen wie z. B. die Setup-Assistenten bestimmen. Diese Funktionsrechte vergeben Sie beim Anlegen eines neuen Administrators.

Wenn Sie einen neuen Administrator per Telnet anlegen, stehen Ihnen die unten genannten Hexadezimalwerte zur Verfügung. Durch die Eingabe eines oder mehrerer dieser Werte im Zusammenhang mit **set** legen Sie die Funktionsrechte fest.

Bei der Konfiguration über Webconfig weisen Sie die Funktionsrechte zu, indem Sie im unten aufgeführten Menü die entsprechenden Kontrollkästchen aktivieren.

Pfad Telnet:

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

Mögliche Werte:

- 0x00000001 Der Benutzer darf den Grundeinstellungs-Assistenten ausführen.
- 0x00000002 Der Benutzer darf den Sicherheits-Assistenten ausführen.
- 0x00000004 Der Benutzer darf den Internet-Assistenten ausführen.
- 0x00000008 Der Benutzer darf den Assistenten zur Auswahl von Internet-Providern ausführen.
- 0x00000010 Der Benutzer darf den RAS-Assistenten ausführen.
- 0x00000020 Der Benutzer darf den LAN-LAN-Kopplungs-Assistenten ausführen.
- 0x00000040 Der Benutzer darf die Uhrzeit und das Datum stellen (gilt auch für Telnet und TFTP).
- 0x00000080 Der Benutzer darf nach weiteren Geräten suchen.
- 0x00000100 Der Benutzer darf den WLAN-Linktest ausführen (gilt auch für Telnet).
- 0x00000200 Der Benutzer darf den a/b-Assistenten ausführen.

- 0x00000400 Der Benutzer darf den WTP-Zuordnungs-Assistenten ausführen.
- 0x00000800 Der Benutzer darf den Public-Spot-Assistenten ausführen.
- 0x00001000 Der Benutzer darf den WLAN-Assistenten ausführen.
- 0x00002000 Der Benutzer darf den Rollout-Assistenten ausführen.
- 0x00004000 Der Benutzer darf den Dynamic-DNS-Assistenten ausführen.
- 0x00008000 Der Benutzer darf den VoIP-CallManager-Assistenten ausführen.
- 0x00010000 Der Benutzer darf den WLC-Profil-Assistenten ausführen.
- 0x00020000 Der Benutzer darf den eingebauten Telnet- bzw. SSH-Client benutzen.
- 0x00100000 Der Benutzer darf den Public-Spot-Benutzerverwaltungs-Assistenten ausführen.

Default:

leer

2.11.21.4 Aktiv

Aktiviert bzw. Deaktiviert die Funktion.

SNMP-ID: 2.11.21.4

Pfad Telnet: /Setup/Config/Admins

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.11.21.5 Zugriffsrechte

Der Zugriff auf die internen Funktionen kann wie folgt getrennt nach Interfaces getrennt konfiguriert werden:

- ISDN-Aministrationszugang

- LAN

- Wireless LAN (WLAN)

- WAN (z. B. ISDN, DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z. B. dass nur die Konfiguration von bestimmten IP-Adressen oder LANCAPI-Clients vorgenommen werden darf. Ferner sind die folgenden internen Funktionen getrennt schaltbar:

- LANconfig (TFTP)

- WEBconfig (HTTP, HTTPS)

- SNMP

- Terminal/Telnet

Bei Geräten mit VPN-Unterstützung kann die Nutzung der einzelnen internen Funktionen über WAN-Interfaces auch nur auf VPN-Verbindungen beschränkt werden.

SNMP-ID: 2.11.21.5

Pfad Telnet: /Setup/Config/Admins

Mögliche Werte:

- Kein
- Admin-RO-Limit

- Admin-RW-Limit
- Admin-Ro
- Admin-RW
- Supervisor

Default: leer

2.11.23 Telnet-Port

Dieser Port wird für unverschlüsselte Konfigurationsverbindungen über Telnet verwendet.

SNMP-ID: 2.11.23

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 23

2.11.25 SSH-Port

Dieser Port wird für Konfigurationsverbindungen über SSH verwendet.

SNMP-ID: 2.11.25

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 22

2.11.26 SSH-Authentisierungs-Methoden

Legen Sie hier fest welche Authentizifierungsmethoden für SSH verwendet werden sollen.

SNMP-ID: 2.11.26

Pfad Telnet: /Setup/Config

2.11.26.1 Ifc.

Die zulässigen Authentifizierungs-Methoden für den SSH-Zugang können für LAN, WAN und WLAN getrennt eingestellt werden.

SNMP-ID: 2.11.26.1

Pfad Telnet: /Setup/Config/SSH-Authentisierungs-Methoden

Mögliche Werte:

- LAN
- WAN
- WLAN

2.11.26.2 Methoden

Das SSH-Protokoll erlaubt grundsätzlich zwei verschiedene Authentifizierungs-Mechanismen: Benutzername und Kennwort, mit Hilfe eines öffentlichen Schlüssels (Public Key) oder oder interaktiv über die Tastatur .

SNMP-ID: 2.11.26.2

Pfad Telnet: /Setup/Config/SSH-Authentisierungs-Methoden

Mögliche Werte:

- Public Key: Erlaubt nur die Authentifizierung über Zertifikat.
- Keyboard-Interactive: Erlaubt nur die interaktive Authentifizierung über die Tastatur.
- Password: Erlaubt nur die Authentifizierung über Kennwort.
- Password und Keyboard-Interactive: Erlaubt die Authentifizierung über Kennwort oder interaktiv über die Tastatur.
- Password und Public Key: Erlaubt die Authentifizierung über Kennwort oder über Zertifikat.
- Keyboard-Interactive und Public Key: Erlaubt nur die interaktive Authentifizierung über die Tastatur oder über Zertifikat.
- Alle: Erlaubt die Authentifizierung über alle Methoden.

Default: Alle

2.11.27 Predef.-Admins

Hier finden Sie den vordefinierten Admin-Account des Gerätes. Dieser Admin-Account wird verwendet, wenn beim Login kein Benutzername angegeben wird.

SNMP-ID: 2.11.27

Pfad Telnet: /Setup/Config/Predef.-Admins

2.11.27.1 Name

Geben Sie hier den Namen für den vordefinierten Admin-Account ein.

SNMP-ID: 2.11.27.1

Pfad Telnet: /Setup/Config/Predef.-Admins/Name

Mögliche Werte Telnet:

- maximal 16 Zeichen

Default: leer

2.11.28 SSH

Verwalten Sie hier die erlaubten Mechanismen der SSH-Verschlüsselung. Die Auswahl legt fest, welche Algorithmen sowohl im Server- als auch im Client-Modus unterstützt werden.

Pfad Telnet:

Setup > **Config**

2.11.28.1 Cipher-Algorithmen

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

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

Default:

3des-cbc,3des-ctr,arcfour,arcfour128,arcfour256,blowfish-cbc,blowfish-ctr,aes128-cbc,
aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr

2.11.28.2 MAC-Algorithmen

Die MAC-Algorithmen dienen der Integritätsprüfung von Nachrichten. Wählen Sie aus den verfügbaren Algorithmen einen oder mehrere aus.

Pfad Telnet:

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

Mögliche Werte:

hmac-md5-96

hmac-md5

hmac-sha1-96

hmac-sha1

hmac-sha2-256-96

hmac-sha2-256

hmac-sha2-512-96

hmac-sha2-512

Default:

hmac-md5-96,hmac-md5,hmac-sha1-96,hmac-sha1,hmac-sha2-256-96,
hmac-sha2-256,hmac-sha2-512-96,hmac-sha2-512

2.11.28.3 Schluesselaustausch-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

2.11.28.4 Hostkey-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

ssh-rsa

ssh-dss

2.11.28.5 Min-Hostkey-Laenge

Dieser Parameter definiert die minimale Länge der Hostkeys.

Pfad Telnet:

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

Mögliche Werte:

max. 5 Ziffern

Default:

512

2.11.28.6 Max-Hostkey-Laenge

Dieser Parameter definiert die maximale Länge der Hostkeys.

Pfad Telnet:

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

Mögliche Werte:

max. 5 Ziffern

Default:

8192

2.11.28.7 DH-Gruppen

Die Diffie-Hellman-Gruppen dienen dem Schlüsselaustausch. Wählen Sie aus den verfügbaren Gruppen eine oder mehrere aus.

Pfad Telnet:

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

Mögliche Werte:

Gruppe-1

Gruppe-5

Gruppe-14

Gruppe-15

Gruppe-16

Default:

Gruppe-1,Gruppe-5,Gruppe-14

2.11.28.8 Kompression

Über diese Einstellung aktivieren bzw. deaktivieren Sie die Kompression der Datenpakete für Verbindungen über SSH.

Pfad Telnet:

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

Mögliche Werte:

ja

nein

Default:

ja

2.11.28.9 Elliptic-Curves

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

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

Pfad Telnet:

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

Mögliche Werte:

nistp256
nistp384
nistp521

Default-Wert:

nistp256

nistp384

nistp521

2.11.28.10 SFTP-Server

In diesem Menü finden Sie die Einstellungen zum SFTP-Server.

Pfad Telnet:

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

2.11.28.10.1 In-Betrieb

Über diese Einstellung aktivieren bzw. deaktivieren Sie den SFTP-Server.

Pfad Telnet:

Setup > **Config** > **SSH** > **SFTP-Server**

Mögliche Werte:

ja

nein

Default:

ja

2.11.28.11 Keepalive-Intervall

Über diesen Parameter konfigurieren Sie die SSH-Keepalives für serverseitige Verbindungen. Der Parameter definiert das Intervall, in dem der LCOS-interne SSH-Server regelmäßig Keepalives verschickt, um eine Verbindung aufrecht zu erhalten.

Pfad Telnet:

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

Mögliche Werte:

0 … 99999 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Funktion.

Default-Wert:

60

2.11.29 Telnet-SSL

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

Pfad Telnet:

Setup > **Config**

2.11.29.2 Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

Pfad Telnet:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

TLSv1

2.11.29.3 Schluesselaustausch-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

2.11.29.4 Krypto-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.11.29.5 Hash-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

2.11.29.6 PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

Pfad Telnet:

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

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

2.11.29.7 Neuverhandlungen

Mit dieser Einstellung steuern Sie, ob der Client eine Neuverhandlung von SSL/TLS auslösen kann.

Pfad Telnet:

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

Mögliche Werte:

verboten
Das Gerät bricht die Verbindung zur Gegenstelle ab, falls diese eine Neuverhandlung anfordert.

erlaubt
Das Gerät lässt Neuverhandlungen mit der Gegenstelle zu.

ignoriert
Das Gerät ignoriert die Anforderung der Gegenseite zur Neuverhandlung.

Default-Wert:

erlaubt

2.11.29.10 PORT

Dieser Port wird für verschlüsselte Konfigurationsverbindungen über Telnet verwendet.

Pfad Telnet:

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

Mögliche Werte:

0 … 65535

Default-Wert:

992

2.11.31 Standortverifikation

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen. Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

GPS-Standort-Verifikation

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten aktiviert das Gerät bei Bedarf automatisch das GPS-Modul und prüft, ob es sich an der „richtigen" Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet. Nach Abschluss der Standort-Verifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist. ISDN-Standort-Verifikation Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet.

ISDN-Standort-Verifikation

Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

SNMP-ID: 2.11.31

Pfad Telnet: /Setup/Config

2.11.31.1 In-Betrieb

Mit der Option 'Standort-Überprüfung einschalten' aktivieren Sie die Standort-Verifikation. Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet. Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation: Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

SNMP-ID: 2.11.31.1

Pfad Telnet: /Setup/Config/Standortverifikation

2.11.31.2 Abgehende Rufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN als ausgehende Rufnummer verwendet.

SNMP-ID: 2.11.31.2

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- max. 14 Zeichen

Default: leer

2.11.31.3 Zielrufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN angerufen.

SNMP-ID: 2.11.31.3

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- max. 14 Zeichen

Default: leer

2.11.31.4 Erwartete-abgehende-Rufnummer

Diese Rufnummer wird bei einem Anruf zur Standortverifikation über ISDN als eingehende Rufnummer erwartet.

SNMP-ID: 2.11.31.4

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- max. 14 Zeichen

Default: leer

2.11.31.6 Methode

Wählen Sie die Methode für die Standort-Überprüfung.

SNMP-ID: 2.11.31.6

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- Basic-Call: Selbst-Anruf für die Überprüfung über ISDN mit einem Rückruf.
- Facility: Rufweiterleitungs-Überprüfung für die Überprüfung über ISDN durch Abfrage der Rufnummer aus der Vermittlungsstelle. Hierbei ist kein Rückruf erforderlich.
- GPS: GPS-Verifikation für die Überprüfung über die Geo-Koordinaten.

Für die Standort-Überprüfung über GPS muss eine entsprechende GPS-Antenne an den AUX-Anschluss des Gerätes angeschlossen werden. Zusätzlich muss eine SIM-Karte für den Mobilfunkbetrieb eingelegt werden und das Gerät muss in ein Mobilfunknetz eingebucht sein. Für eine erfolgreiche ISDN-Standort-Verifikation muss das Gerät aus dem öffentlichen ISDN-Netz erreichbar sein. Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

2.11.31.7 ISDN-Ifc

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

SNMP-ID: 2.11.31.7

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- S0-1
- S0-2

2.11.31.8 Abweichung

Abweichung von der erlaubten Position in Metern

SNMP-ID: 2.11.31.8

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- 50

2.11.31.9 Laengengrad

Längengrad des Standortes, an dem das Gerät in Betrieb genommen wird.

SNMP-ID: 2.11.31.9

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- leer

2.11.31.10 Breitengrad

Breitengrad des Standortes, an dem das Gerät in Betrieb genommen wird.

SNMP-ID: 2.11.31.10

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- leer

2.11.31.12 GPS-Position-holen

Mit dieser Option kann das Gerät die Geo-Koordinaten für den aktuellen Standort selbst ermitteln. Nach dem Rückschreiben der Konfiguration in das Gerät werden automatisch die aktuellen Längen- und Breitengrade eingetragen, wenn die Standortverifikation aktiv ist und gültige GPS-Daten vorliegen. Anschließend wird diese Option selbsttätig wieder deaktiviert.

Pfad Telnet: /Setup/Config/Standortverifikation

Mögliche Werte:

- Ja
- Nein

2.11.32 Reset-Knopf

Der Reset-Taster hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Tasters gesteuert werden.

SNMP-ID: 2.11.32

Pfad Telnet: /Setup/Config

Mögliche Werte:

- Ignorieren: Der Taster wird ignoriert.
- Nur-Booten: Beim Druck auf den Taster wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.
- Reset-oder-Booten (Standardeinstellung): In dieser Einstellung hat der Reset-Taster verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:
  - Weniger als 5 Sekunden: Booten (Neustart), dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.
  - Mehr als 5 Sekunden bis zum ersten Aufleuchten aller LEDs am Gerät: Konfigurations-Reset (Löschen des Konfigurationsspeichers) und anschließender Neustart. Damit werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.
  - Mehr als 15 Sekunden bis zum zweiten Aufleuchten aller LEDs am Gerät: Aktivieren der Rollout-Konfiguration und Löschen der benutzerdefinierten Konfiguration. Nach dem Neustart wird die Rollout-Konfiguration (zweiter Speicherplatz) geladen. Das Laden der Rollout-Konfiguration wird angezeigt, indem alle LEDs des Geräts zweimal kurzzeitig rot aufleuchten. Wenn der zweite Speicherplatz leer ist, werden die Werkseinstellungen geladen.

Weitere Informationen zu den verschiedenen Boot-Konfigurationen finden Sie im Referenzhandbuch.

Default: reset-oder-booten

Ein Access Point befindet sich nach dem Reset wieder im „Managed-Modus“, in dem kein direkter Zugriff über die WLAN-Schnittstelle zur Konfiguration möglich ist!

Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, alle Einstellungen gehen dabei verloren. Sichern Sie daher vor dem Reset nach Möglichkeit die aktuelle Konfiguration des Geräts!

Mit der Einstellung 'Ignorieren' oder 'Nur-Booten' wird das Rücksetzen der Konfiguration auf den Auslieferungszustand sowie das Laden der Rollout-Konfiguration durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort nicht mehr vorliegt, gibt es keine Möglichkeit mehr, auf das Gerät zuzugreifen! In diesem Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden – dabei wird das Gerät in den Auslieferungszustand zurückgesetzt, und die bisherige Konfiguration wird gelöscht. Hinweise zum Firmware-Upload über die serielle Konfigurationsschnittstelle finden Sie im LCOS-Referenzhandbuch.

2.11.33 Outband-Aging-Minutes

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

SNMP-ID: 2.11.33

Pfad Telnet: /Setup/Config

Mögliche Werte:

- max. 10 Zeichen

Default: 1

2.11.35 Monitortrace

Dieses Menü enthält die Einstellungen für Monitor-Tracing

SNMP-ID: 2.11.35

Pfad Telnet: /Setup/Config

2.11.35.1 Tracemask1

Dieser Parameter wird nur für Supportzwecke gebraucht.

SNMP-ID: 2.11.35.1

Pfad Telnet: /Setup/Config/Monitortrace

2.11.35.2 Tracemask2

Dieser Parameter wird nur für Supportzwecke benötigt.

SNMP-ID: 2.11.35.2

Pfad Telnet: /Setup/Config/Monitortrace

2.11.39 Lizenzablauf-Email

Die Nutzung einer Lizenz kann auf einen bestimmten Zeitraum begrenzt sein. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz mit einer Nachricht an die hier eingestellte E-Mail-Adresse an die auslaufende Lizenz erinnert.

Pfad Telnet: /Setup/Config/Lizenzablauf-Email

Mögliche Werte:

- Gültige E-Mail-Adresse

Default: leer

2.11.40 Crash-Meldung

Legen Sie hier die Meldung fest, die beim Absturz des Geräts im Bootlog erscheint.

SNMP-ID: 2.11.40

Pfad Telnet: /Setup/Config/Crash-Meldung

Mögliche Werte:

- maximal 32 alphanumerische Zeichen

Default: LCOS-Watchdog

2.11.41 Admin-Geschlecht

Geben Sie hier das Geschlecht des Admins an.

SNMP-ID: 2.11.41

Pfad Telnet: /Setup/Config/Admin-Geschlecht

Mögliche Werte:

- unbekannt
- maennlich
- weiblich

Default: unbekannt

2.11.42 Assert-Action

Dieser Parameter beeinflusst das Verhalten des Geräts bei der Prüfung des Firmware-Codes.

SNMP-ID: 2.11.42

Pfad Telnet: /Setup/Config/Assert-Action

Mögliche Werte:

- log_only
- reboot

Default: log_only

Die Einstellungen für diesen Parameter werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.11.43 Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

SNMP-ID: 2.11.43

Pfad Telnet: /Setup/Config

2.11.43.1 Taste

Bezeichnung der Funktionstaste.

SNMP-ID: 2.11.43.1

Pfad Telnet: /Setup/Config/Funktionstasten

Mögliche Werte:

- Auswahl aus den Funktionstasten F1 bis F12.

Default: F1

2.11.43.2 Abbildung

Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

SNMP-ID: 2.11.43.2

Pfad Telnet: /Setup/Config/Funktionstasten

Mögliche Werte:

- Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

Default: Leer

Besondere Werte: Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.^a

^A steht für Strg-A (ASCII 1)

^Z steht für Strg-Z (ASCII 26)

^[steht für Escape (ASCII 27)

^M steht für Return/Enter erwähnen. Dieses Zeichen ist z. B. dann nützlich, wenn Sie ein Kommando mit der Funktionstaste nicht nur eingeben, sondern auch direkt abschicken möchten.

^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst ^.

Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von Caret-Zeichen + A macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein. Aus Caret-Zeichen + Leerzeichen + A wird dann die Sequenz ^A.

2.11.45 Konfigurations-Datum

Über diesen Parameter kann LANconfig das Datum einer Konfiguration setzen.

Dieser Wert existiert nur in der SNMP-Verkettung.

Pfad Telnet:

Setup > **Config** > **Config-Date**

Mögliche Werte:

gültiges Konfigurationsdatum

2.11.50 LL2M

Dieses Menü enthält die Einstellungen für LANCOM Layer-2 Management.

SNMP-ID: 2.11.50

Pfad Telnet: /Setup/Config

2.11.50.1 In-Betrieb

Schaltet den LL2M-Server ein oder aus. Ein aktivierter LL2M-Server kann nach dem Booten/Einschalten des Gerätes für die Dauer des Zeit-Limits von einem LL2M-Client angesprochen werden.

SNMP-ID: 2.11.50.1

Pfad Telnet: /Setup/Config/LL2M

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.11.50.2 Zeit-Limit

Definiert die Zeitspanne in Sekunden, in der ein aktivierter LL2M-Server nach dem Booten/Einschalten des Gerätes von einem LL2M-Client angesprochen werden kann. Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert.

SNMP-ID: 2.11.50.2

Pfad Telnet: /Setup/Config/LL2M

Mögliche Werte:

- 0 bis 4294967295

Default: 0

Besondere Werte: 0 deaktiviert das Zeit-Limit, in diesem Zustand bleibt der LL2MServer dauerhaft aktiv.

2.11.51 Sync

In diesem Verzeichnis konfigurieren Sie den automatischen Konfigurationsabgleich.

Pfad Telnet:

Setup > **Config**

2.11.51.1 Aktiv

Aktiviert oder deaktiviert den automatischen Konfigurationsabgleich.

Pfad Telnet:

Setup > **Config** > **Sync**

Mögliche Werte:

Nein
ja

Default-Wert:

Nein

2.11.51.2 Neuer-Cluster

Hier konfigurieren Sie den Umfang eines Konfigurationsabgleiches.

Pfad Telnet:

Setup > **Config** > **Sync**

2.11.51.2.1 Name

Vergeben Sie eine Bezeichnung für diesen Eintrag.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

Mögliche Werte:

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

Default-Wert:

Default

2.11.51.2.2 Gruppen-Mitglieder

Diese Tabelle listet Geräte auf, die am automatischen Konfigurationsabgleich teilnehmen.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

2.11.51.2.2.1 Idx.

Index zu diesem Eintrag in der Liste.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

2.11.51.2.2.2 Adresse

IP-Adresse des entsprechenden Gerätes.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

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

Mögliche Argumente:

IPv4-Adresse
IPv6-Adresse

Default-Wert:

leer

2.11.51.2.3 Menueknoten

Hier konfigurieren Sie, welche Konfigurationselemente der automatische Konfigurationsabgleich enthalten soll. Sie können dabei Werte, Tabellen und ganze Menüs einbeziehen oder ausschließen.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

2.11.51.2.3.1 Idx.

Index zu diesem Eintrag in der Liste.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

2.11.51.2.3.2 Enthalten

Bestimmen Sie hier, ob der angegebene Menüknoten im automatischen Konfigurationsabgleich enthalten oder ausgenommen ist.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

Enthalten
Ausgenommen

Default-Wert:

Enthalten

2.11.51.2.3.3 Pfad

Geben Sie den Pfad zum Menüknoten an. Es kann sich hierbei um einen Wert, eine Tabelle oder um ein komplettes Menü handeln.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

/Setup

2.11.51.2.3.4 SNMP-OID

Zeigt die SNMP-ID des angegebenen Menüknotens an.

Die Anzeige aktualisiert sich nach dem Speichern des Eintrages.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

2

Default-Wert:

2

2.11.51.2.4 Ignorierte-Zeilen

Wenn Sie eine Tabelle in den automatischen Konfigurationsabgleich übernehmen, bestimmen Sie hier, welche Zeilen dieser Tabelle davon ausgenommen sein sollen.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

2.11.51.2.4.1 Idx.

Index zu diesem Eintrag in der Liste.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

2.11.51.2.4.2 Zeilenindex

Geben Sie hier die Zeilennummer (Index) an, die vom automatischen Konfigurationsabgleich ausgenommen sein soll.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.11.51.2.4.3 Pfad

Geben Sie den Pfad zum Knoten der Tabelle an, die im automatischen Konfigurationsabgleich enthalten ist.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

/Setup

2.11.51.2.4.4 SNMP-OID

Zeigt die SNMP-ID des angegebenen Tabellenknotens an.

Die Anzeige aktualisiert sich nach dem Speichern des Eintrages.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

2

Default-Wert:

2

2.11.51.2.5 Start

Startet den automatischen Konfigurationsabgleich für diesen Eintrag.

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

2.11.51.3 TLS-Verbindungen

In diesem Verzeichnis legen Sie fest, über welche Adresse und auf welchem Port das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

Pfad Telnet:

Setup > **Config** > **Sync**

2.11.51.3.1 Port

Geben Sie den Port an, auf dem das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

Pfad Telnet:

Setup > **Config** > **Sync** > **TLS-Verbindungen**

Mögliche Werte:

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

0 … 65535

Default-Wert:

1941

2.11.51.3.2 Loopback-Adresse

Geben Sie die Loopback-Adresse an, auf der das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

Pfad Telnet:

Setup > **Config** > **Sync** > **TLS-Verbindungen**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][a-z][0-9].-:%`

Mögliche Argumente:

Namen der IP-Netzwerke, deren Adresse eingesetzt werden soll
„INT" für die Adresse des ersten Intranets
„DMZ" für die Adresse der ersten DMZ
LBO ... LBF für die 16 Loopback-Adressen
beliebige gültige IPv4- oder IPv6-Adresse

Default-Wert:

leer

2.11.51.4 Schnappschuss-erneuern

In diesem Verzeichnis konfigurieren Sie die Schnappschüsse für das High Availability Clustering.

Pfad Telnet:

Setup > **Config** > **Sync**

2.11.51.4.1 Aenderungs-Limit

Geben Sie hier das Änderungs-Limit an.

Pfad Telnet:

Setup > **Config** > **Sync** > **Schnappschuss-erneuern**

Mögliche Werte:

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

Besondere Werte:

0

Dieser Wert deaktiviert die Funktion.

Default-Wert:

2048

2.11.51.4.2 Verbleibende-Aenderungen

Dieser Wert gibt die Anzahl der verbleibenden Änderungen an.

Pfad Telnet:

Setup > **Config** > **Sync** > **Schnappschuss-erneuern**

Mögliche Werte:

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

0 … 4294967295 Zweierpotenzen

Besondere Werte:

0

Dieser Wert deaktiviert die Funktion.

Default-Wert:

256

2.11.51.4.3 Schnappschuss-erneuern

Mit dieser Aktion erneuern Sie den Schnappschuss.

Pfad Telnet:

Setup > **Config** > **Sync** > **Renew-Snapshot**

2.11.51.5 Lokale-Konfiguration

In diesem Verzeichnis bestimmen Sie die Anzahl der angewandten und beobachteten Änderungen.

Pfad Telnet:

Setup > **Config** > **Sync**

2.11.51.5.1 Beobachtete-Aenderungen

Geben Sie die Anzahl der beobachteten Änderungen an.

Pfad Telnet:

Setup > **Config** > **Sync** > **Lokale-Konfiguration**

Mögliche Werte:

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

2.11.51.5.2 Angewandte-Aenderungen

Geben Sie die Anzahl der angewandten Änderungen an.

Pfad Telnet:

Setup > **Config** > **Sync** > **Lokale-Konfiguration**

Mögliche Werte:

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

2.11.60 CPU-Last-Intervall

Hier können Sie die den Zeitraum zur Mittelung der CPU-Lastanzeige auswählen. Die Anzeige der CPU-Last im LANmonitor, im Status-Bereich, im Display (sofern vorhanden) sowie in evtl. genutzten SNMP-Tools basiert auf dem hier eingestellten Mittelungszeitraum. Im Status-Bereich unter WEBconfig oder CLI werden zusätzlich die CPU-Lastwerte für alle vier möglichen Mittelungszeiträume angezeigt.

Mittlere Werte für den CPU-Load sind verfügbar über die folgenden Zeitintervalle:

SNMP-ID: 2.11.60

Pfad Telnet: /Setup/Config

Mögliche Werte:

T1s (arithmetisches Mittel)

T5s (arithmetisches Mittel)

T60s (gleitender Mittelwert)

T300s (gleitender Mittelwert)

Default: T60s

2.11.65 Error-Aging-Minutes

Bestimmen Sie die Zeitspanne in Minuten, nach der das Gerät aufgetretene VPN-Fehler aus der Status-Tabelle löscht.

Um sporadisch auftretende Fehler zu dokumentieren, deaktivieren Sie diese Option mit dem Eintrag `0`.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert diese Option. Aufgetretene Fehler verbleiben in der Status-Tabelle.

2.11.70 Firmware-Check

Mit dieser Einstellung legen Sie fest, ob das Gerät beim Systemstart eine SYSLOG-Warnung ausgibt, wenn eine nicht zertifizierte Firmware eingespielt wurde.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

- **only-certified**: Das Gerät akzeptiert nur zertifizierte Firmwares. Bei Verwendung einer nicht-zertifizierten Firmware wird eine SYSLOG-Meldung erzeugt.
- **any**: Das Gerät erzeugt bei jedem Einspielen einer neuen Firmware eine SYSLOG-Meldung.

Default:

only-certified

2.11.71 Bootlog-sichern

Dieser Parameter aktiviert oder deaktiviert das persistente Speichern der Bootlog-Nachrichten im Flash des Gerätes. Die Informationen aus dem Bootlog bleiben damit auch bei Neustart mit einer Trennung des Gerätes vom Stromnetz erhalten. Der Bootlog umfasst Informationen über die Boot-Vorgänge des Gerätes.

Bei Bedarf löschen Sie den persistenten Bootlog-Speicher durch Eingabe des Befehls `deletebootlog` an einer beliebigen Stelle auf der Kommandozeile.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

ja

nein

Default:

ja

2.11.72 Eventlog-sichern

Dieser Parameter aktiviert oder deaktiviert das persistente Speichern der Eventlog-Nachrichten im Flash des Gerätes. Die Informationen aus dem Eventlog bleiben damit auch bei Neustart mit einer Trennung des Gerätes vom Stromnetz erhalten. Der Eventlog umfasst alle Informationen aus der Tabelle unter **Status** > **Config** > **Eventlog**. Diese Tabelle speichert Informationen übeer An- und Abmeldevorgänge der Administratoren sowie Upload- und Download-Vorgänge von Konfigurationen und Firmware-Dateien

Bei Bedarf löschen Sie den persistenten Eventlog-Speicher durch Eingabe des Befehls `deleteeventlog` an einer beliebigen Stelle auf der Kommandozeile.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

ja

nein

Default:

ja

2.11.73 Menue-sortieren

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

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.11.80 Authentifizierung

Um sich für die Anmeldung an der Verwaltungsoberfläche des Geräts zu authentifizieren, stehen verschiedene Möglichkeiten zur Verfügung:

- **intern**: Das Gerät verwaltet die Anwender intern in der Tabelle **Setup** > **Config** > **Admins**.
- **Radius**: Ein RADIUS-Server übernimmt die Verwaltung der Anwender.
- **Tacacs+**: Ein TACACS+-Server übernimmt die Verwaltung der Anwender.

Die notwendigen Daten für den RADIUS-Server verwalten Sie unter **Setup** > **Config** > **Radius** > **Server**. Die notwendigen Daten für den TACACS+-Server verwalten Sie unter **Setup** > **Tacacs+** > **Server**.

Da das RADIUS-Protokoll keine Änderung von Passworten zulässt, kann der per RADIUS eingeloggte Anwender sein Passwort im Gerät nicht ändern.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

Intern

Radius

Tacacs+

Default:

Intern

2.11.81 Radius

Wenn sich der Anwender für die Anmeldung an der Verwaltungsoberfläche über einen RADIUS-Server authentifizieren soll, geben Sie hier die notwendigen Server-Daten sowie zusätzliche Verwaltungs-Daten an.

Pfad Telnet:

Setup > **Config**

2.11.81.1 Server

Diese Tabelle enthält die Einstellungen für den RADIUS-Server

Pfad Telnet:

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

2.11.81.1.1 Name

Vergeben Sie hier einen Namen für den RADIUS-Server.

Pfad Telnet:

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

Mögliche Werte:

max. 16 Zeichen

Default:

Leer

2.11.81.1.2 Server

Vergeben Sie hier die IPv4-Adresse des RADIUS-Server.

Pfad Telnet:

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

Mögliche Werte:

Max. 64 Zeichen

Default:

Leer

2.11.81.1.3 Port

Geben Sie hier den Port an, über den der RADIUS-Server mit dem Gerät kommuniziert.

Pfad Telnet:

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

Mögliche Werte:

Max. 5 Zeichen

Default:

1812

2.11.81.1.4 Protokoll

Geben Sie hier das Protokoll an, mit dem der RADIUS-Server mit dem Gerät kommuniziert.

Pfad Telnet:

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

Mögliche Werte:

RADIUS

RADSEC

Default:

RADIUS

2.11.81.1.5 Loopback-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.

Pfad Telnet:

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

Mögliche Werte:

Name der IP-Netzwerke, deren Adresse das Gerät einsetzen soll.

"INT" für die Adresse des ersten Intranets.

"DMZ" für die Adresse der ersten DMZ.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen "DMZ" vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

LB0 bis LBF für eine der 16 Loopback-Adressen.

Eine beliebige gültige IP-Adresse.

Default:

Leer

2.11.81.1.6 Secret

Geben Sie hier das Kennwort für den Zugang zum RADIUS-Server an und wiederholen Sie es im zweiten Eingabefeld.

Pfad Telnet:

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

Mögliche Werte:

Max. 64 Zeichen

Default:

Leer

2.11.81.1.7 Backup

Geben Sie den Namen des alternativen RADIUS-Servers an, an den das Gerät Anfragen weiterleitet, wenn der erste RADIUS-Server nicht erreichbar ist.

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

Pfad Telnet:

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

Mögliche Werte:

Max. 16 Zeichen

Default:

Leer

2.11.81.1.8 Kategorie

Bestimmen Sie, für welche Kategorie der RADIUS-Server gelten soll.

Sie können keine, eine oder beide Kategorien auswählen.

Pfad Telnet:

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

Mögliche Werte:

Authentifizierung

Accounting

Default:

Authentifizierung

2.11.81.1.9 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.11.81.2 Zugriffsrechte-Uebertragung

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

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

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

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

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

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

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

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

Pfad Telnet:

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

Mögliche Werte:

Herstellerabhaengig
Mapped
Shell-Privileg

Default-Wert:

Herstellerabhaengig

2.11.81.3 Accounting

Hier bestimmen Sie, ob das Gerät die Sitzung des Anwenders aufzeichnen soll. In diesem Fall speichert es die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

Pfad Telnet:

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

Mögliche Werte:

Nein

Ja

Default:

Nein

2.11.90 LED-Modus

Bestimmen Sie die Betriebsart der Geräte-LEDs.

Die Funktion "LED-Test" lässt sich trotz deaktivierter LEDs ausführen.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

An

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Zeitgesteuert-Aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

Default-Wert:

An

2.11.91 LED-Ausschalten-Sekunden

Bestimmen Sie die Dauer in Sekunden, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

Wenn Sie diesen Wert innerhalb der zuvor eingestellten Dauer ändern und speichern, starten Sie den Timer neu.

Pfad Telnet:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen `0123456789`

Default-Wert:

300

2.12 WLAN

Dieses Menü enthält die Einstellungen für kabellose Netzwerke (WLAN)

SNMP-ID: 2.12

Pfad Telnet: /Setup

2.12.3 Heap-Reserve

Die Heap-Reserve gibt an, wie viele Blöcke des LAN-Heaps für die direkte Kommunikation (Telnet) mit dem Gerät reserviert werden. Wenn die Anzahl der Blöcke im Heap unter den angegebenen Wert fällt, dann werden empfangene Pakete sofort verworfen (außer bei TCP-Paketen, die direkt an das Gerät gerichtet sind).

SNMP-ID: 2.12.3

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 3 Ziffern

Default: 10

2.12.8 Zugriffsmodus

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

SNMP-ID: 2.12.8

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Daten von den aufgeführten Stationen ausfiltern, alle anderen Stationen übertragen
- Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern

Default: Daten von den aufgeführten Stationen ausfiltern, alle anderen Stationen übertragen

2.12.12 IAPP-Protokoll

Über das Inter Access Point Protocol (IAPP) tauschen die Access Points untereinander Informationen über die eingebuchten Clients aus. Diese Informationen werden beim Roaming von Clients zwischen verschiedenen Access Points verwendet. Der neue Access Point informiert den bisherigen Access Point über den Roaming-Vorgang, damit der bisherige Access Point den Client aus seiner Stationstabelle löschen kann.

SNMP-ID: 2.12.12

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.12.13 IAPP-Announce-Interval

In diesem Intervall (in Sekunden) geben die Access Points ihre SSIDs bekannt.

SNMP-ID: 2.12.13

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 10 Ziffern

Default: 120

2.12.14 IAPP-Handover-Timeout

Bei einem erfolgreichen Roaming-Vorgang (Handover) informiert der neue Access Point den bisherigen Access Point darüber, dass ein bestimmter Client jetzt bei einem anderen Access Point angemeldet ist. Mit dieser Information kann der alte Access Point den Client aus seiner Stationstabelle austragen und leitet nicht mehr (unnötigerweise) Pakete für diesen Client in seine Funkzelle weiter. Für diesen Zeitraum (in Millisekunden) wartet der neue Access Point, bis er versucht, den bisherigen Access Point noch einmal zu kontaktieren. Nach fünf Versuchen gibt der neue Access Point diese Versuche auf.

SNMP-ID: 2.12.14

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 10 Ziffern

Default: 1000

2.12.26 Inter-SSID-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Die Kommunikation der Clients in unterschiedlichen SSIDs kann mit dieser Option erlaubt oder verhindert werden. Bei Modellen mit mehreren WLAN-Modulen gilt diese Einstellung global für allem WLANs aller Module.

SNMP-ID: 2.12.26

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Ja
- Nein

Default: Ja

Die Kommunikation der Clients innerhalb eines logischen WLANs wird separat bei den logischen WLAN-Einstellungen gesteuert (Inter-Station-Verkehr). Wenn der Inter-SSID-Verkehr aktiviert ist und der Inter-Station-Verkehr deaktiviert, kann ein Client aus einem logischen WLAN mit den Clients in anderen logischen WLANs kommunizieren. Diese Möglichkeit kann über VLAN-Einstellungen oder Protokollfilter verhindert werden.

2.12.27 Ueberwachung-Stationen

Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der Access Point zur Überwachung in regelmäßigen Abständen Pakete an die eingebuchten Stationen schicken. Kommen von einer Station keine Antworten mehr auf diese Pakete, wird sie als nicht mehr aktiv an das Abrechnungssystem gemeldet.

SNMP-ID: 2.12.27

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.12.29 RADIUS-Zugriffspruefung

Dieses Menü enthält die Einstellungen für die RADIUS-Zugriffsprüfung

SNMP-ID: 2.12.29

Pfad Telnet: /Setup/WLAN

2.12.29.2 Auth.-Port

Port zur Kommunikation mit dem RADIUS-Server bei der Authentifizierung

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- Gültige Port-Angabe

Default: 1812

2.12.29.3 Schluessel

Kennwort für den Zugang zum RADIUS-Server

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.12.29.5 Backup-Auth.-Port

Port zur Kommunikation mit dem Backup-RADIUS-Server bei der Authentifizierung

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- Gültige Port-Angabe

Default: 1812

2.12.29.6 Backup-Schluessel

Kennwort für den Zugang zum Backup-RADIUS-Server

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.12.29.7 Antwort-Lebenszeit

Mit diesem Wert definieren Sie die Lebensdauer einer im Gerät gespeicherten, abgelehnten MAC-Prüfung über den RADIUS-Server.

Wenn zur Prüfung der MAC-Adressen der WLAN-Clients ein RADIUS-Server eingesetzt wird, sendet das Gerät alle Verbindungsanfragen von WLAN-Clients an den RADIUS-Server weiter. Ist eine MAC-Adresse in diesem RADIUS-Server gesperrt, dann wird die ablehnende Antwort des RADIUS-Servers für die hier eingestellte Zeit im Gerät zwischengespeichert. So wird verhindert, dass das Gerät die wiederholten Anfragen einer gesperrten MAC-Adresse nicht immer wieder an den RADIUS-Server weitergeleitet.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- maximal 10 numerische Zeichen im Bereich von 0 bis 4294967295 (2^32-1)

Default: 15

Die aktuellen Einträge der zwischengespeicherten MAC-Adressen können Sie in der Tabelle '1.3.48 RADIUS-Cache' einsehen.

2.12.29.8 Passwort-Quelle

Legen Sie hier fest, ob das Gerät bei der Autenthifizierung mit dem RADIUS-Server das Shared Secret oder die MAC-Adresse als Passwort einsetzt.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- Secret
- MAC-Adresse

Default: Secret

2.12.29.9 Pruef-Zyklus

Wenn Sie einen Wert größer als Null wählen, überprüft das Gerät Ihre MAC-Adresse sowohl beim Anmelden, als auch während der Verbindung im angegebenen Zyklus in Sekunden. Wenn Sie Null angeben, wird die MAC-Adresse nur beim Anmelden überprüft. Eine zyklische Überprüfung ermöglicht es dem Gerät zu erkennen, wenn sich für eine MAC-Adresse z. B. die Bandbreiten-Limits ändern. In diesem Fall bleibt der Client angemeldet und die Verbindung bleibt bestehen.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- maximal 10 numerische Zeichen im Bereich von 0 - 4294967295 (2^32-1)

Default: 0

2.12.29.10 Server-Datenbank-liefern

Aktivieren Sie diese Option, wenn ein RADIUS-Server die MAC-Adressliste zur Verfügung stellt.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- nein
- ja

Default: ja

2.12.29.11 Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche 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

Default: Leer

Wenn es eine Schnittstelle mit Namen "DMZ" gibt, dann wird deren Adresse verwendet.

2.12.29.12 Backup-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Default: Leer

2.12.29.13 Protokoll

Protokoll für die Kommunikation zwischen dem RADIUS-Server und den Clients.

SNMP-ID: 2.12.29.13

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung

Mögliche Werte:

- RADSEC
- RADIUS

Default: RADIUS

2.12.29.14 Backup-Protokoll

Protokoll für die Kommunikation zwischen dem Backup-RADIUS-Server und den Clients.

Pfad Telnet: /Setup/WLAN/RADIUS-Zugriffspruefung/Backup-Protokoll

Mögliche Werte:

- RADIUS

- RADSEC

Default: RADIUS

2.12.29.15 Pruefen-erzwingen

Über diese Aktion erwirken Sie manuell eine sofortige Ausführung der RADIUS-Zugriffsprüfung. Über das Eingabefeld haben Sie die Möglichkeit, optionale Parameter für das Kommando einzugeben. Das Kommando erwartet als Argument eine oder mehrere MAC-Adressen von eingebuchten Clients. Für diese Clients wird die initiale Überprüfung ihrer MAC-Adresse über den RADIUS-Server wiederholt. Mehrere MAC-Adressen trennen Sie mittels Leerzeichen.

Pfad Telnet:

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

Mögliche Werte:

MAC-Adresse(n) eingebuchter Clients, durch Leerzeichen getrennt

2.12.29.16 Server-Hostname

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

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

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.29.17 Backup-Server-Hostname

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.29.18 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.29.19 Backup-Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.36 Land

Damit Ihr Wireless-Netz mit den richtigen Parametern betrieben werden kann, muss das Gerat seinen nationalen Standort kennen.

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

Auswahl aus der Liste der angebotenen Länder

Wenn Sie den Wert **unbekannt** wählen, lässt das Gerät lässt nur jene Parameter zu, die weltweit zugelassen sind!

Default:

Europa

2.12.38 ARP-Behandlung

Will eine Station im LAN eine Verbindung zu einer Station im WLAN aufbauen, die im Stromspar-Modus ist, so klappt dies häufig entweder gar nicht oder nur mit großen Verzögerungen. Der Grund ist, dass die Auslieferung von Broadcasts, z. B. ARP-Anfragen, an im Powersave befindliche Stationen von der Basisstation nicht garantiert werden kann.

Wenn Sie die ARP-Behandlung einschalten, beantwortet die Basisstation ARP-Anfragen für bei ihr eingebuchte Stationen selber und damit in solchen Fällen zuverlässiger.

SNMP-ID: 2.12.38

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Ein
- Aus

Default: Ein

Ab der LCOS-Version 8.00 wird mit diesem Schalter eine analoge Behandlung für IPv6-Neighbor-Solicitations aktiviert.

2.12.41 Mail-Adresse

An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet.

SNMP-ID: 2.12.41

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Gültige E-Mail-Adresse

Default: Leer

Zur Nutzung der E-Mail-Benachrichtigung muss ein SMTP-Konto eingerichtet sein.

2.12.44 Erlaube-illegale-Assoziation-ohne-Authentifizierung

Dieser Parameter aktiviert oder deaktiviert die Möglichkeit, dass das Gerät sich mit einem WLAN ohne Authentifizierung verbindet.

SNMP-ID: 2.12.44

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- ja
- nein

Default: nein

2.12.45 RADIUS-Accounting

Die Accounting-Funktion im Gerät kann u. a. dazu genutzt werden, das Budget von angeschlossenen WLAN-Clients zu kontrollieren. Wireless Internet Service Provider (WISPs) nutzen diese Möglichkeit teilweise zur Abrechnung ihrer Kunden. Da die Abrechnungsintervalle üblicherweise zum Monatsende wechseln, kann über eine entsprechende Aktion der Neustart aller aktuellen Accounting-Sitzungen ausgelöst werden – die eigentliche WLAN-Verbindung bleibt dabei bestehen. Mit Hilfe eines Cron-Jobs kann dieser Neustart komfortabel automatisiert werden.

SNMP-ID: 2.12.45

Pfad Telnet: /Setup/WLAN

2.12.45.8 Interim-Update-Periode

Geben Sie hier das Zeitintervall in Sekunden an, in dem das Gerät ein Interim-Update an den Accounting-Server sendet.

SNMP-ID: 2.12.45.8

Pfad Telnet: /Setup/WLAN/RADIUS-Accounting

Mögliche Werte:

- maximal 10 numerische Zeichen im Bereich von 0 bis 4289999999

Default: 0

2.12.45.9 Ausgeschlossenes-VLAN

Geben Sie hier die ID des VLANs ein, welches das Gerät vom RADIUS-Accounting ausschließen soll. Der RADIUS-Server erhält dann keine Informationen über den Verkehr dieses VLANs.

SNMP-ID: 2.12.45.9

Pfad Telnet: /Setup/WLAN/RADIUS-Accounting

Mögliche Werte:

- maximal 4 numerische Zeichen im Bereich von 0 bis 9999
- 0 deaktiviert diese Funktion.

Default: 0

2.12.45.14 Neustart-Accounting

Mit dieser Funktion beendet das Gerät alle aktuell laufenden WLAN-Accounting-Sessions mit einem Accounting-Stop zum RADIUS-Server. Hilfreich ist dies z. B. am Ende eines Abrechungszeitraums.

Pfad Telnet: /Setup/WLAN/RADIUS-Accounting/Neustart-Accounting

2.12.45.17 Server

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

Pfad Telnet:

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

2.12.45.17.1 Name

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.45.17.3 Port

Port zur Kommunikation mit dem RADIUS-Server beim Accounting.

Pfad Telnet:

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

Mögliche Werte:

0 … 65535

Default-Wert:

0

2.12.45.17.4 Schluessel

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.45.17.5 Loopback-Addr.

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

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

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

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.45.17.6 Protokoll

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

Pfad Telnet:

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

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

2.12.45.17.7 Backup

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

Pfad Telnet:

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

Mögliche Werte:

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

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

Default-Wert:

leer

2.12.45.17.8 Host-Name

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.45.17.9 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.12.46 Nur-Indoor-Betrieb

Bei aktiviertem Indoor-Only Modus werden im 5 GHz Band in ETSI-Ländern die Kanäle auf den Bereich 5,15 bis 5,25 GHz (Kanäle 36-48) beschränkt. Die Radarerkennung (DFS) wird ausgeschaltet und es entfällt die Zwangsunterbrechung alle 24 Stunden. In dieser Betriebsart ist daher das Risiko von Unterbrechungen durch (falsche) Radarerkennungen reduziert. Im 2,4 GHz Band in Frankreich werden die Kanäle 8 bis 13 freigegeben, wodurch mehr Kanäle zur Verfügung stehen.

SNMP-ID: 2.12.46

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Ein
- Aus

Default: Aus

Die Aktivierung des Indoor-Only-Modus ist nur erlaubt, wenn die Basisstation und alle Stationen in einem geschlossenen Raum betrieben werden.

Die Aktivierung des Indoor-Only Modus ist nur erlaubt, wenn die Basisstation und alle Stationen in einem geschlossenen Raum betrieben werden.

2.12.47 Idle-Timeout

Das ist die Zeit in Sekunden, nach der ein Client getrennt wird, wenn der Aceess Point keine Pakete von ihm empfangen hat.

SNMP-ID: 2.12.47

Pfad Telnet: /Setup/WLAN/Idle-Timeout

Mögliche Werte Telnet:

- Max. 10 numerische Zeichen

Default: 3600 Sekunden

2.12.50 Signalmittelung

Dieses Menü enthält die Einstellungen für die Signalmittelung.

SNMP-ID: 2.12.50

Pfad Telnet: /Setup/WLAN

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.50.1 Methode

Methode zur Signalmittelung.

SNMP-ID: 2.12.50.1

Pfad Telnet: /Setup/WLAN/Signalmittelung

Mögliche Werte:

- Standard
- Gefiltert

Default: Standard

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.50.2 Standard-Parameter

Dieses Menü enthält die Konfiguration der Standard-Parameter für die Signalmittelung.

SNMP-ID: 2.12.50.2

Pfad Telnet: /Setup/WLAN/Signalmittelung

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.50.2.1 Faktor

Faktor für die Signalmittelung.

Pfad Telnet: /Setup/WLAN/Signalmittelung/Standard-Parameter

Mögliche Werte:

- maximal 3 numerische Zeichen

Default: 4

Die Einstellungen zur Signalmittelung werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.51 Raten-Adaption

Dieses Menü enthält die Einstellungen für den Ratenadaptionsalgorithmus.

SNMP-ID:

2.12.51

Pfad Telnet:

Setup > **WLAN**

2.12.51.2 Initiale Rate

Die Initiale Rate bestimmt, bei welcher Bitrate der Algorithmus beginnt die optimale Bitrate zu bestimmen.

Pfad Telnet:

Setup > **WLAN** > **Raten-Adaption**

Mögliche Werte:

Minimum

RSSI-abhaengig

Default:

Minimum

2.12.51.3 Ministrel-Glaettungsfaktor

Der Glättungsfaktor, der bei der Neuberechnung der Nettoraten pro Bitrate nach der Methode Ministrel zum Tragen kommt.

Pfad Telnet:

Setup > **WLAN** > **Raten-Adaption**

Mögliche Werte:

0 bis 99

Default:

75

2.12.51.4 Standard-Glaettungsfaktor

Der Glättungsfaktor, der bei der Neuberechnung der Nettoraten pro Bitrate nach der Methode Standard zum Tragen kommt.

Pfad Telnet:

Setup > **WLAN** > **Raten-Adaption**

Mögliche Werte:

0 bis 99

Default:

0

2.12.51.5 Methode

Bestimmt die Methode zur Raten-Adaption.

Pfad Telnet:

Setup > **WLAN** > **Raten-Adaption** > **Methode**

Mögliche Werte:

Standard

Minstrel

Default:

Minstrel

2.12.60 IAPP-IP-Netzwerk

Wählen Sie hier aus, welches ARF-Netzwerk als IAPP-IP-Netzwerk verwendet werden soll.

SNMP-ID: 2.12.60

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Auswahl aus der Liste der im Gerät definierten ARF-Netzwerke
- maximal 16 alphanumerische Zeichen

Default: leer

Besondere Werte: leer: Wenn kein IAPP-IP-Netzwerk definiert ist, werden die IAPP-Announces in alle definierten ARF-Netze versendet.

2.12.70 VLAN-Gruppenschluessel-Abbildung

Die Tabelle enthält die Zuordnungen der VLAN-Gruppenschlüssel zu den logischen WLAN-Netzen.

Pfad Telnet:

Setup > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

2.12.70.1 Netzwerk

Enthält den Namen eines im Gerät registrierten WLAN-Netzes.

Pfad Telnet:

Setup > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

2.12.70.2 VLAN-Id

Enthält die dem logischen WLAN-Netz zugeordnete VLAN-ID.

Pfad Telnet:

Setup > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

Mögliche Werte:

1 bis 4094

Default:

1

2.12.70.3 Gruppenschluessel-Index

Die Tabelle enthält den Gruppenschlüssel-Index.

Pfad Telnet:

Setup > **WLAN** > **VLAN-Gruppenschluessel-Abbildung**

Mögliche Werte:

1 bis 3

2.12.80 Dual-Roaming

Verwalten Sie hier das Roaming-Verhalten von Geräten mit mehreren WLAN-Modulen.

Pfad Telnet:

Setup > **WLAN** > **Dual-Roaming**

2.12.80.1 Gruppe

Bestimmt, ob alle WLAN-Module am Dual-Roaming teilnehmen.

Pfad Telnet:

Setup > **WLAN** > **Dual-Roaming**

Mögliche Werte:

Aus

WLAN-1 + WLAN-2

Default:

Aus

2.12.80.2 Sperrzeit-ms

Über diese Einstellung setzen Sie die Sperrzeit für das zeitversetzte Roaming von Dual Radio Client WLAN-Modulen.

Wenn Sie Dual-Roaming aktivieren, betreibt Ihr Dual-Radio-Gerät beide WLAN-Module im Client-Modus. Mit Dual-Roaming erhöht sich die Wahrscheinlichkeit, dass beim Wechsel zwischen zwei Funkzellen mindestens eines der Module eine Konnektivität besitzt, über die das Gerät Datenpakete übertragen kann. Die Sperrzeit beschreibt dabei die Zeit (in Milisekunden), in der ein WLAN-Modul keinen Roaming-Vorgang und kein Background-Scanning durchführt, nachdem das andere WLAN-Modul erfolgreich eine neue Konnektivität hergestellt hat.

Pfad Telnet:

Setup > **WLAN** > **Dual-Roaming**

Mögliche Werte:

0 bis 4294967295

Default:

100

2.12.85 PMK-Caching

Verwalten Sie hier das PMK-Caching.

Pfad Telnet:

Setup > **WLAN** > **PMK-Caching**

2.12.85.1 Vorgabe-Lebenszeit

Definiert die Dauer in Sekunden, für welche der WLAN-Client den ausgehandelten PMK speichert.

Stellen Sie sicher, dass die hier eingestellte Dauer mit dem Session-Timeout übereinstimmt, welche der Access Point oder ein RADIUS-Server in der Accept-Nachricht an den WLAN-Client übermittelt. Nach dieser Zeit erfordert der Access Point oder ein RADIUS-Server eine erneute Authentifizierung.

Pfad Telnet:

Setup > **WLAN** > **PMK-Caching**

Mögliche Werte:

0 bis 4294967295

Default:

0

Besondere Werte:

0: Der ausgehandelte PMK läuft sofort ab.

2.12.86 Paket-Capture

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

Pfad Telnet:

Setup > **WLAN**

2.12.86.1 WLAN-Capture-Format

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

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

Pfad Telnet:

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

Mögliche Werte:

Radiotap

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

AVS

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

PPI

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

PRISM

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

Plain

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

Default-Wert:

Radiotap

2.12.87 Client-Steering

Hier bestimmen Sie die Einstellungen für das 'WLAN Band Steering' der am Access Point angemeldeten WLAN-Clients.

Pfad Telnet:

Setup > **WLAN**

2.12.87.1 In-Betrieb

Mit dieser Option aktivieren Sie das 'Client Steering' im Access Point.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

2.12.87.3 Bevorzugtes-Band

Bestimmen Sie hier, in welches Frequenzband der Access Point den WLAN-Client bevorzugt leiten soll.

Pfad Telnet:

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

Mögliche Werte:

5GHz

2,4GHz

Default:

5GHz

2.12.87.4 Probe-Request-Herausaltern

Bestimmen Sie hier die Zeit in Sekunden, für die die Verbindung eines WLAN-Clients im Access Point gespeichert bleiben soll. Nach Ablauf dieser Zeit löscht der Access Point den Eintrag in der Tabelle.

Wenn Sie Clients im WLAN benutzen, die z. B. oft von Dual-Band- auf Single-Band-Modus umschalten, sollten Sie diesen Wert entsprechend niedrig ansetzen.

Pfad Telnet:

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

Mögliche Werte:

max. 10 Zeichen

aus 0 bis 9

Besondere Werte:

0: Die gesehenen Probe Requests werden sofort als ungültig betrachtet.

Default:

120

2.12.87.5 Initiale Block-Zeit

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

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

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

Pfad Telnet:

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

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Besondere Werte:

0

Dieser Wert deaktiviert die Verzögerung.

Default-Wert:

10

2.12.89 Zugriffsregeln

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

Pfad Telnet:

Setup > **WLAN**

2.12.89.1 MAC-Adress-Muster

Geben Sie hier die MAC-Adresse einer Station ein.

Die Verwendung von Wildcards ist möglich.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Mögliche Argumente:

MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressenbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

2.12.89.2 Name

Sie können zu jeder Station einen beliebigen Namen eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

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

2.12.89.3 Kommentar

Sie können zu jeder Station einen beliebigen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

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

2.12.89.4 WPA-Passphrase

Hier können Sie optional für jeden Eintrag eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

Bei WEP gesicherten Netzwerken hat dieses Feld keine Bedeutung.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

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

2.12.89.5 Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.12.89.6 Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.12.89.7 VLAN-Id

Das Gerät weist diese VLAN-ID den Paketen zu, die der WLAN-Client mit der eingetragenen MAC-Adresse empfängt.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

0 … 4096

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.12.89.9 SSID-Muster

Dieser Eintrag reduziert oder erlaubt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen für diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Besondere Werte:

*****

Platzhalter für beliebig viele Zeichen

?

Platzhalter für genau ein Zeichen

Default-Wert:

leer

2.12.100 Karten-Reinit-Zyklus

In diesem Intervall (in Sekunden) werden die internen WLAN-Karten bei älteren Access Points reinitialisiert, um Point-to-Point-Verbindungen aufrecht zu erhalten. Diese Funktion wird bei aktuelleren Modellen über den "Alive-Test" ersetzt.

SNMP-ID: 2.12.100

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 10 Ziffern

Default: 0

Besondere Werte: 0: Deaktiviert diese Funktion.

2.12.101 Rausch-Messzyklus

In diesem Intervall (in Sekunden) wird bei WLAN-Karten mit Atheros-Chipsatz der Rauschpegel auf dem Medium gemessen.

SNMP-ID: 2.12.101

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 10 Ziffern

Default: 0

Besondere Werte: 0: Deaktiviert diese Funktion.

2.12.103 Trace-MAC

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Client eingestellt werden, dessen WLAN-MAC-Adresse hier eingetragen wird.

SNMP-ID: 2.12.103

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 12 hexadezimale Zeichen

Default: 000000000000

Besondere Werte: 000000000000: Deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

2.12.105 Therm.-Rekal.-Messzyklus

In diesem Intervall (in Sekunden) wird bei älteren WLAN-Karten mit Atheros-Chipsatz die Sendeleistung korrigiert, um thermische Schwankungen auszugleichen.

SNMP-ID: 2.12.105

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- max. 10 Ziffern

Default: 20

Besondere Werte: 0: Deaktiviert diese Funktion.

Bitte beachten Sie, dass die Hardware der WLAN-Karte bei deaktiviertem Therm.-Rekal.-Messzyklus nicht mehr auf thermische Schwankungen reagieren kann!

2.12.109 Rausch-Offsets

In dieser Tabelle werden Korrekturfaktoren definiert, mit der die angezeigten Signalwerte angepasst werden.

SNMP-ID: 2.12.109

Pfad Telnet: /Setup/WLAN

2.12.109.1 Band

Auswahl des Frequenzbands für die Rauschwertanpassung.

SNMP-ID: 2.12.109.1

Pfad Telnet: /Setup/WLAN/Rausch-Offsets

Mögliche Werte:

- Auswahl aus den im Gerät unterstützten Frequenzbändern, z. B. 2,4 GHz oder 5 GHz

Default: 2,4 GHz

2.12.109.2 Kanal

Auswahl des Kanals für die Rauschwertanpassung.

SNMP-ID: 2.12.109.2

Pfad Telnet: /Setup/WLAN/Rausch-Offsets

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: leer

2.12.109.3 Schnittstelle

Auswahl der WLAN-Schnittstelle für die Rauschwertanpassung.

SNMP-ID: 2.12.109.3

Pfad Telnet: /Setup/WLAN/Rausch-Offsets

Mögliche Werte:

- je nach Ausstattung der Hardware, z. B. WLAN-1 oder WLAN-2

Default: WLAN-1

2.12.109.4 Wert

Dieser numerische Wert wird zum aktuellen Rauschwert addiert.

SNMP-ID: 2.12.109.4

Pfad Telnet: /Setup/WLAN/Rausch-Offsets

Mögliche Werte:

- maximal 3 numerische Zeichen im Bereich von 0 bis 127

Default: 0

2.12.110 Trace-Stufe

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Die Meldungen werden dazu in Form einer Bit-Maske eingetragen.

SNMP-ID: 2.12.110

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- 0 bis 255.
- 0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde
- 1: zusätzlich die physikalischen Parameter der Pakete /Datenrate, Signalstärke...)
- 2: zusätzlich der MAC-Header
- 3: zusätzlich der Layer3-Header (z. B. IP/IPX)
- 4: zusätzlich der Layer4-Header (TCP, UDP...)
- 5: zusätzlich die TCP/UDP-Payload

Default: 255

2.12.111 Rausch-Immunitaet

Hier können Sie Einstellungen für die Rausch-Immunität (Adaptive Noise Immunity - ANI) vornehmen.

SNMP-ID: 2.12.111

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.1 Rausch-Immunitaet

Definieren Sie hier den Schwellwert für die Rausch-Immunität.

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet/Rausch-Immunitaet

Mögliche Werte:

- Numerische Zeichen von 0 bis 255

Default: 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.2 OFDM-Schwache-Signale-Erkennung

Definieren Sie hier den Schwellwert für die Erkennung von schwachen OFDM-Signalen.

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet/OFDM-Schwache-Signale-Erkennung

Mögliche Werte:

- Numerische Zeichen von 0 bis 255

Default: 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.3 CCK-Schwaches-Signal-Erkennungs-Schwellwert

Definieren Sie hier den Schwellwert für die Erkennung von schwachen CCK-Signalen.

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet/CCK-Schwaches-Signal-Erkennungs-Schwellwert

Mögliche Werte

- Numerische Zeichen von 0 bis 255

Default: 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.4 Fir-Step

Definieren Sie hier den Wert für den Fir-Step.

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet/Fir-Step

Mögliche Werte:

- Numerische Zeichen von 0 bis 255

Default: 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.5 Spurious-Immunitaet

Definieren Sie hier den Schwellwert für die Spurious-Immunität.

Pfad Telnet: /Setup/WLAN/Rausch-Immunitaet/Spurious-Immunitaet

Mögliche Werte

- Numerische Zeichen von 0 bis 255

Default: 255

Die Einstellungen für Rausch-Immunitaet werden in der Regel vom Treiber des WLAN-Moduls automatisch anhand der Funkfeldsituation geregelt. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.12.111.6 MRC-CCK

Über diesen Parameter schalten Sie auf Geräten mit Osprey-WLAN-Modul (AR93xx) das Maximum Ratio Combining (MRC) für 802.11b-Raten (1 bis 11 Mbit) ein (Wert != `0`) oder aus (Wert = `0`). Der Standardwert von `255` bedeutet, dass die Vorgabe des WLAN-Treibers für diese Einstellung nicht übersteuert wird. In Einzelfällen kann es sinnvoll sein, diesen Wert auf `0` zu setzen, um den Empfänger im Gerät künstlich zu vertauben.

Pfad Telnet:

Setup > **WLAN** > **Rausch-Immunitaet**

Mögliche Werte:

0 bis 255

Default:

255

2.12.114 Aggregat-Wiederholungs-Limit

Dieser Parameter gibt an, wie viele Male ein Aggregat von zu sendenden Paketen von der Hardware wiederholt werden darf, bis es erst einmal wieder zurückgestellt wird und andere zu sendende Pakete zum Zuge kommen können. Mit der Begrenzung auf wenige Wiederholungen wird so z. B. in VoIP-Umgebungen die maximale Verzögerung von VoIP-Paketen begrenzt.

SNMP-ID: 2.12.114

Pfad Telnet: /Setup/WLAN/Aggregat-Wiederholungs-Limit

Mögliche Werte:

- 0 bis 255

Default: 255

Das unter 'Hard-Retries' eingestellte absolute Limit für Sendeversuche bleibt von diesem Wert unbeeinflusst.

2.12.115 Globale-Krypto-Sequenz-Pruefung-auslassen

Stellen Sie hier die globale Prüfung der Krypto-Sequenz ein.

SNMP-ID: 2.12.115

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Auto
- Ja
- Nein

Default: Auto

Besondere Werte: Auto: LCOS enthält eine Liste der für diese Verhalten bekannten Geräte und schaltet in der Einstellung 'Auto' die globale Sequenzprüfung ab. Für andere, noch nicht in der Liste enthaltenen Geräte muss die globale Sequenzprüfung manuell deaktiviert werden.

2.12.116 Trace-Pakete

Ähnlich wie bei der Trace-MAC und der Trace-Stufe lassen sich die Ausgaben im WLAN-DATA-Traces anhand des Typs der empfangenen bzw. gesendeten Pakete einschränken, z. B. Management (Authenticate, Association, Action, Probe-Request/Response), Control (z. B. Powersave-Poll), EAPOL (802.1x-Verhandlung, WPA-Key-Handshake).

SNMP-ID: 2.12.116

Pfad Telnet: /Setup/WLAN

Mögliche Werte:

- Einer oder mehrere Werte aus Management, Control, Daten, EAPOL, Alle

Default: Alle

2.12.117 WPA-Handshake-Verzoegerung-ms

Mit dieser Einstellung legen Sie die Zeit (in Millisekunden) fest, mit der das Gerät den WPA-Handshake beim Roaming verzögert. Ein Wert von `0` bedeutet, dass keine Verzögerung stattfindet.

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.12.118 WPA-Handshake-Timeout-Uebersteuerung-ms

Mit dieser Einstellung legen Sie die Zeit (in Millisekunden) fest, mit der das Gerät den Timeout des WPA-Handshakes übersteuert. Ein Wert von `0` bedeutet, dass keine Übersteuerung stattfindet.

Pfad Telnet:

Setup > **WLAN** > **WPA-Handshake-Timeout-Uebersteuerung-ms**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.12.120 Rx-Aggregat-Flush-Timeout-ms

Über diese Einstellung setzen sie die Zeit (in Millisekunden), nach der das Gerät nicht empfangene Teile von Aggregaten als 'verloren' betrachtet und nachfolgende Datenpakete nicht mehr zurückhält.

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

0 bis 4294967295

Default:

40

2.12.121 HT-Fairness

Wenn Sie HT-Fairness aktivieren, benutzt das Gerät bei der Auswahl zu versendenden Pakete eine andere Strategie, welche bei einem Mischbetrieb von 802.11n-fähigen und 802.11n-unfähigen Clients versucht, beiden Arten von Clients einen in etwa gleichen Zugang zum Funkmedium zu gewähren.

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

ja

nein

Default:

ja

2.12.124 Trace-Mgmt-Pakete

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

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

Assoziierung

(Re)Association Request/Response

Disassociate

Authentisierung

Authentication

Deauthentication

Probes

Probe Request

Probe Response

Action

Beacon

Andere

alle restlichen Management-Frametypen

Default-Wert:

Assoziierung

Authentisierung

Probes

Action

Andere

2.12.125 Trace-Daten-Pakete

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

Pfad Telnet:

Setup > **WLAN**

Mögliche Werte:

normal
Alle normalen Daten-Pakete

NULL
Alle leeren Daten-Pakete

andere
alle restlichen Daten-Pakete

2.12.130 DFS

In diesem Menü konfigurieren Sie die Dynamic Frequency Selection (DFS). Mit DFS kann ein Access Point einen Kanalwechsel durchführen, wenn auf dem aktuellen Kanal ein anderes System wie z. B. Wetterradar aktiv ist.

Pfad Telnet:

Setup > **WLAN**

2.12.130.1 Benutze-vollen-Kanalsatz

Dieser Parameter erlaubt bei Benutzung von 5 GHz und DFS die Verwendung der ansonsten wegen "Wetterradars" gesperrten Kanäle 120, 124 und 128, sofern Sie EN 301893-1.3 oder älter als DFS-Version verwenden. Für EN 301893 ist gegenwärtig keine Unterstützung dieser Kanäle implementiert; der Parameter hat keine Wirkung.

Beachten Sie, dass die Aktivierung dieser Option eine Verletzung der ETSI-Bestimmungen darstellt, da für LCOS keine Zulassungen dieser Kanäle besteht.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein
Der Access Point ignoriert die Kanäle 120, 124 und 128 bei einem Kanalwechsel.

ja
Der Access Point nutzt bezieht die Kanäle 120, 124 und 128 bei einem Kanalwechsel mit ein.

Default-Wert:

nein

2.12.130.2 Radar-Last-Schwellwert

Dieser Wert gibt die prozentuale Auslastung des WLAN-Moduls an, bei dem der Access Point die Genauigkeit der Radarerkennung reduziert.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

0 … 100 Prozent

Default-Wert:

80

2.12.130.3 Direkter-Kanalwechsel

Über diesen Parameter bestimmen Sie, wie das Gerät den bei DFS erforderlichen Channel Availability Check (CAC) durchführt.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein

Das Gerät beobachtet einen zufällig ausgewählten Kanal (landesspezifische Wahl) für mindestens 60 Sekunden auf Radarfreiheit, bevor es auf diesem Kanal sendet. Um im späteren Betrieb bei Erkennen eines Radars rasch auf einen anderen Kanal wechseln zu können, ermittelt das Gerät zusätzlich eine Mindestanzahl an voraussichlich freien Alternativkanälen (siehe *2.23.20.8.27 DFS-Rescan-Kanalzahl* auf Seite 488).

ja

Das Gerät springt innerhalb von 60 Sekunden im 500ms-Zeitraster über sämtliche Kanäle und erhält damit Informationen über diese Kanäle. Erkennt das Gerät im späteren im Betrieb einen Radar, wechselt das Gerät sofort auf einen anderen Kanal.

Beachten Sie, dass diese Betriebsart gegenwärtig nicht mehr zulassungskonform ist, weswegen der Schalter standardmäßig deaktiviert ist.

Default-Wert:

nein

2.12.130.4 DFS-Testmodus

Über diese Einstellung aktivieren bzw. deaktivieren Sie den DFS-Testmodus. Ist er eingeschaltet, beschränkt sich das Gerät auf die Meldung erkannter Radar-Bursts und wechselt – im Gegensatz zum Normalbetrieb – nicht den Funkkanal.

Dieser Parameter ist ausschließlich für Entwicklungstests von Bedeutung und für den normalen Betriebsablauf nicht relevant. Verändern Sie die Standardeinstellung niemals!

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein

Der DFS-Testmodus ist deaktiviert.

ja
Der DFS-Testmodus ist aktiviert.

Default-Wert:

nein

2.12.130.5 Ignoriere-CRC-Fehler

Über diesen Parameter legen Sie fest, ob das Gerät Radarpulse ignoriert, die das System parallel zu einem CRC-Fehler meldet.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.12.130.6 Melde-ignorierte-Pulse

Dieser Parameter legt fest, ob LCOS im DFS-Pulse-Trace Radarpulse meldet, die zwar von der WLAN-Hardware gemeldet, jedoch als ungültig von der Software verworfen wurden.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.12.130.7 Strebe-hoechste-Bandbreite-an

Über diesen Parameter legen Sie fest, ob das Gerät bei der Kanalwahl die Verwendung der höchsten Bandbreite anstrebt, sofern die dafür in Frage kommenden Kanäle noch als Radar-frei gespeichert sind.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein

Das Gerät nimmt den Betrieb sofort auf, jedoch mit reduzierter Kanalbreite (z. B. 20 statt 40 MHz).

ja

Das Gerät führt zunächst einen Channel Availibity Check durch, um weitere Kanalgruppen zu finden, auf denen Betrieb mit voller oder zumindest erhöhter Kanalbreite möglich ist.

Default-Wert:

ja

2.12.130.8 Schnellen-Wechsel-bevorzugen

Dieser Parameter ist ein Platzhalter und hat derzeit keine Funktion.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.12.130.9 Kanalwechsel-Verzoegerung

Geben Sie hier an, wie lange der Access Point bei Erkennen eines Radars warten soll, bis er auf einen anderen Kanal wechselt.

Pfad Telnet:

Setup > **WLAN** > **DFS**

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Bei Wert 0 ist diese Funktion deaktiviert.

2.12.130.10 Radar-Muster-Schwellwerte

In dieser Tabelle definieren Sie die Grenzwerte für die Radar-Erkennung.

Pfad Telnet:

Setup > **WLAN** > **DFS**

2.12.130.10.1 Muster-pps

Wählen Sie hier eines der vordefinierten Radarmuster, um den Schwellwert bei der Radarmustererkennung zu ändern.

Pfad Telnet:

Setup > **WLAN** > **DFS** > **Radar-Muster-Schwellwert**

Mögliche Werte:

Muster-pps

EN301893-1.2-700pps
EN301893-1.2-1800pps
EN301893-1.2-330pps
EN301893-1.3-750pps
EN301893-1.3-200pps
EN301893-1.3-300pps
EN301893-1.3-500pps
EN301893-1.3-800pps
EN301893-1.3-1000pps
EN301893-1.3-1200pps
EN301893-1.3-1500pps
EN301893-1.3-1600pps
EN301893-1.3-2000pps
EN301893-1.3-2300pps
EN301893-1.3-3000pps
EN301893-1.3-3500pps
EN301893-1.3-4000pps
EN302502-200pps
EN302502-300pps
EN302502-500pps
EN302502-750pps
EN302502-800pps
EN302502-1000pps
EN302502-1200pps
EN302502-1500pps
EN302502-1600pps
EN302502-2000pps
EN302502-2300pps
EN302502-3000pps
EN302502-3500pps
EN302502-4000pps

EN302502-4500pps

2.12.130.10.2 Schwellwert

Der eingetragene Wert beschreibt die Genauigkeit, mit der der Access Point das entsprechende Radarmuster erkennt.

Wenn Sie die voreingestellten Werte verändern, verletzt das Gerät im Betrieb möglicherweise den Standard ETSI EN 301 893 Version 1.3.

Pfad Telnet:

Setup > **WLAN** > **DFS** > **Radar-Muster-Schwellwerte**

Mögliche Werte:

0 … 4294967295

Default-Wert:

abhängig vom gewählten Radarmuster

2.13 LANCAPI

Die LANCAPI von LANCOM ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z. B. ein Fax oder einen Anrufbeantworter, bereit.

SNMP-ID: 2.13

Pfad Telnet: /Setup

2.13.1 Zugangs-Liste

In dieser Tabelle können Sie Adressen oder Adressbereiche eintragen, die Zugang zu dem Server haben sollen. Wenn die Tabelle leer ist, hat automatisch jeder Zugang.

SNMP-ID: 2.13.1

Pfad Telnet: /Setup/LANCAPI/Zugangs-Liste

2.13.1.1 IP-Adresse

Geben Sie hier eine IP-Adresse ein, die Zugang erhalten soll.

Pfad Telnet: /Setup/LANCAPI/Zugangs-Liste/IP-Adresse

Mögliche Werte: max. 15 Zeichen

Default: Leer

2.13.1.2 IP-Netzmaske

Geben Sie hier die zugehörige Netzmaske ein.

Wenn Sie nur eine einzelne Station mit der zuvor angegebenen Adresse freischalten wollen, geben Sie **255.255.255.255** ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie die zugehörige Netzmaske ein.

Pfad Telnet: /Setup/LANCAPI/Zugangs-Liste/IP-Netzmaske

Mögliche Werte: max. 15 Zeichen

Default: Leer

2.13.1.3 Rtg-Tag

Wenn sie ein Routing-Tag für diese Zugriffs-Regel angeben, so werden nur solche Pakete angenommen, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden. Wenn als Routing-Tag 0 angegeben ist, wird jeder Zugriff einer passenden IP-Adresse zugelassen.

Pfad Telnet: /Setup/LANCAPI/Zugangs-Liste/Rtg-Tag

Mögliche Werte: max. 5 Zeichen

Default: Leer

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechend begleitenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

2.13.3 UDP-Port

Hier können Sie die UDP-Port-Nummer des LANCAPI-Servers ändern.

SNMP-ID: 2.13.3

Pfad Telnet: /Setup/LANCAPI/UDP-Port

Mögliche Werte: max. 5 Zeichen

Default: 75 (any private telephony service)

2.13.6 Interface-Liste

Diese Liste enthält einen Eintrag für jedes Interface Ihres Gerätes. Für jedes S_0-Interface ist einstellbar, ob es für LANCAPI-Clients verfügbar ist und welche Rufnummern verwendet werden sollen.

Pfad Telnet:

Setup > **LANCAPI**

2.13.6.1 Ifc

Dies ist die Bezeichnung des Interface (z. B. S0-1).

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

2.13.6.2 Aktiv

Wählen Sie aus, ob und wie dieses Interface für LANCAPI-Clients verfügbar ist.

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

Mögliche Werte:

ja
Das Gerät lässt über das ausgewählte Interface sämtliche Rufe zu.

nein
Das Gerät lässt über das ausgewählte Interface keine Rufe zu.

Abgehend
Das Gerät lässt über das ausgewählte Interface ausschließlich abgehende Rufe zu.

Ankommend
Das Gerät lässt über das ausgewählte Interface ausschließlich ankommende Rufe zu.

Default-Wert:

nein

2.13.6.3 EAZ-MSN(s)

In diesem Eingabefeld geben Sie alle eigenen ISDN-Rufnummern an, auf denen die LANCAPI Anrufe entgegen nimmt. Mehrere Rufnummern trennen Sie durch eine semikolon-separierte Liste.

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

Mögliche Werte:

gültige ISDN-Rufnummer, max. 30 Zeichen aus `[0-9]#;?`

Besondere Werte:

leer
Wenn Sie keine spezifische(n) Rufnummer(n) angeben, nimmt die LANCAPI Anrufe an allen eigenen ISDN-Rufnummern entgegen.

Default-Wert:

leer

2.13.6.5 Erzw.-Out-MSN

Wenn bei einem abgehenden Ruf die eigene Rufnummer nicht gesetzt ist, dann bestimmt diese Option, dass die Rufnummer dieses Interfaces als eigene Rufnummer eingetragen wird. Aktivieren Sie diese Option, wenn Ihre Telefonanlage keine abgehenden Rufe ohne gesetzte eigene Rufnummer zulässt.

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

Mögliche Werte:

ja
Das Gerät versieht abgehende Rufe bei fehlender Rufnummer ersatzweise mit der Interface-Rufnummer.

nein
Das Gerät versieht abgehende Rufe bei fehlender Rufnummer mit keiner Ersatz-Rufnummer.

Default-Wert:

nein

2.13.6.6 Max-Verbindungen

Über diese Einstellung begrenzen Sie die maximale Anzahl der Verbindungen pro S_0-Bus.

Pfad Telnet:

Setup > **LANCAPI** > **Interface-Liste**

Mögliche Werte:

0 … 255

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung (unlimitiert).

Default-Wert:

0

2.13.7 Prioritaeten-Liste

In dieser Tabelle definieren Sie die Prioritäten der ISDN-Schnittstellen für abgehende Rufe über die LANCAPI.

Pfad Telnet: /Setup/LANCAPI/Prioritaeten-Liste

2.13.7.1 Ifc

Wählen Sie hier die ISDN-Schnittstelle, für welche Sie die Priorität festlegen wollen.

Pfad Telnet: /Setup/LANCAPI/Prioritaeten-Liste/Ifc

Mögliche Werte:

- Auswahl aus den im Gerät vorhandenen ISDN-Schnittstellen, z. B. S0-1

2.13.7.2 Prio-ab

Wählen Sie hier die Priorität der ISDN-Schnittstelle für abgehende Rufe über die LANCAPI.

Pfad Telnet: /Setup/LANCAPI/Prioritaeten-Liste/Prio-ab

Mögliche Werte:

- P1 (hohe Priorität) bis P3 (niedrige Priorität)

Default: P3

2.14 Zeit

Dieses Menü enthält die Konfiguration der Zeit-Einstellungen im Gerät.

SNMP-ID: 2.14

Pfad Telnet: /Setup

2.14.1 Hol-Methode

Wählen Sie hier aus, ob und wie das Gerät seine interne Echtzeit-Uhr synchronisiert.

Pfad Telnet:

Setup > **Zeit**

Mögliche Werte:

keine

ISDN

NTP

GPS

Default:

NTP

2.14.2 Aktuelle-Zeit

Anzeige der aktuellen Zeit.

SNMP-ID: 2.14.2

Pfad Telnet: /Setup/Zeit

2.14.3 Zeit-Rufnummer

Geben Sie hier eine beliebige Telefonnummer ein, die das Gerät anrufen soll, um Zeitinformationen aus dem ISDN zu erhalten. Das Gerät wird unmittelbar nach dem Einschalten diese Nummer anwählen und die Verbindung anschließend sofort wieder trennen. Dabei wird von der ISDN-Vermittlungsstelle die aktuelle Zeit übermittelt.

SNMP-ID: 2.14.3

Pfad Telnet: /Setup/Zeit

Mögliche Werte:

- max. 39 Zeichen

Default: Leer

2.14.5 Anwahl-Versuche

Legen Sie fest, wie oft maximal versucht werden soll, die angegebene Rufnummer zum Zwecke der Zeitinitialisierung.

SNMP-ID: 2.14.5

Pfad Telnet: /Setup/Zeit

Mögliche Werte:

- max.3 Ziffern

Default: 3

2.14.7 UTC-in-Sekunden

Dieser Parameter wird von LANmonitor zum Auslesen der Uhrzeit genutzt.

Pfad Telnet:

Setup > **Zeit**

2.14.10 Zeitzone

Stellen Sie hier die Zeitzone Ihres Gerätestandorts ein. Die Zeitzone ist die Differenz aus der lokalen Zeit und der koordinierten Weltzeit (UTC) in Stunden. Diese Angabe ist insbesondere für das Netzwerk-Zeit-Protokoll (NTP) wichtig

SNMP-ID: 2.14.10

Pfad Telnet: /Setup/Zeit

Mögliche Werte:

- 0
- +1
- +2
- +3
- +4
- +5
- +6
- +7
- +8
- +9
- +10
- +11
- +12
- +13
- +14
- -1
- -2
- -3
- -4
- -5
- -6
- -7
- -8
- -9
- -10
- -11
- -12

Default: +1

2.14.11 Sommerzeit

Die Zeitumstellung zwischen lokaler Normal- und Sommerzeit kann hier manuell vorgenommen werden oder automatisch erfolgen. Stellen Sie für eine automatische Zeitumstellung die passende Zeit-Region des Standorts Ihres Gerätes ein. Nur, wenn Ihr Gerät außerhalb der aufgeführten Zeit-Regionen steht, ist es für eine automatische Zeitumstellung notwendig, die Auswahl 'Benutzer definiert' zu treffen und in der folgenden Tabelle die Werte für die automatische Zeitumstellung anzugeben.

SNMP-ID: 2.14.11

Pfad Telnet: /Setup/Zeit

Mögliche Werte:

- Ja
- Nein

- Europa (EU)
- Russland
- USA
- Benutzerdefiniert

Default: Europa (EU)

2.14.12 Umstellungen-Sommerzeit

Konfigurieren Sie hier individuelle Werte für die automatischen Zeitumstellungen zwischen Normal- und Sommerzeit, wenn in der Auswahlliste für Sommerzeit-Einstellungen 'Benutzer definiert' ausgewählt ist.

SNMP-ID: 2.14.12

Pfad Telnet: /Setup/Zeit

2.14.12.1 Ereignis

Definiert den Anfang bzw. das Ende der Sommerzeit

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.2 Index

Erster oder letzter Tag des Monats, in dem die Sommerzeitumstellung ausgeführt wird.

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.3 Tag

Definiert an welchem wiederkehrenden Wochentag des Monats die Umstellung ausgeführt wird.

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.4 Monat

Definiert den Monat in dem die Umstellung ausgeführt wird.

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.5 Stunde

Definiert die Stunde in der die Umstellung ausgeführt wird.

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.6 Minute

Definiert die Minute in der die Umstellung ausgeführt wird.

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.12.7 Zeit-Typ

Zeit-Standard, z. B. UTC (Universal Time Coordinated).

Pfad Telnet: /Setup/Zeit/Umstellungen-Sommerzeit

2.14.13 Zeit-holen

Dieser Befehl veranlasst das Gerät sich die aktuelle Zeit von dem eingetragenen Zeitserver zu holen.

SNMP-ID: 2.14.13

Pfad Telnet: /Setup/Zeit

2.14.15 Feiertage

In dieser Tabelle finden Sie die definierten Feiertage.

SNMP-ID: 2.14.15

Pfad Telnet: /Setup/Zeit/Feiertage

2.14.15.1 Index

Index des Eintrags, der dessen Position in der Tabelle beschreibt.

SNMP-ID: 2.14.15.1

Pfad Telnet: /Setup/Zeit/Feiertage/Index

Mögliche Werte:

- 0 bis 9999

Default: leer

2.14.15.2 Datum

Wenn Sie in der Least-Cost-Tabelle oder in der Zeitsteuerungs-Tabelle Einträge angelegt haben, die an Feiertagen gelten sollen, dann tragen Sie diese Tage hier ein.

SNMP-ID: 2.14.15.2

Pfad Telnet: /Setup/Zeit/Feiertage/Datum

Mögliche Werte:

- Gültiges Datum

Default: Leer

2.14.16 Zeitrahmen

Zeitrahmen werden verwendet, um die Gültigkeitsdauer von Content-Filter-Profilen zu definieren. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d.h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

SNMP-ID: 2.14.16

Pfad Telnet: /Setup/Zeit

2.14.16.1 Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er im Content-Filter-Profil referenziert wird.

SNMP-ID: 2.14.16.1

Pfad Telnet: /Setup/Zeit/Zeitrahmen

Mögliche Werte:

- Name eines Zeitrahmens
- maximal 31 Zeichen

Default: leer

2.14.16.2 Start

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

SNMP-ID: 2.14.16.2

Pfad Telnet: /Setup/Zeit/Zeitrahmen

Mögliche Werte:

- max. 5 Zeichen
- Format HH:MM

Default: 00:00

2.14.16.3 Stopp

Hier kann die Endzeit (Tageszeit) angegeben werden, bis zu der das gewählte Profil gelten soll.

SNMP-ID: 2.14.16.3

Pfad Telnet: /Setup/Zeit/Zeitrahmen

Mögliche Werte:

- max. 5 Zeichen
- Format HH:MM

Default: 23:59

2.14.16.4 Wochentage

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

SNMP-ID: 2.14.16.4

Pfad Telnet: /Setup/Zeit/Zeitrahmen

Mögliche Werte:

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

Default: Aktiviert für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

2.15 LCR

Dieses Menü enthält die Konfiguration des Least-Cost-Routers.

SNMP-ID: 2.15

Pfad Telnet: /Setup

2.15.1 Router-Nutzung

Ein Router ist eine intelligente Netzwerkkomponente; vergleichbar mit einer Poststelle, die aufgrund von logischer Zieladresse eines Paketes entscheiden kann, an welche nächste Netzwerkkomponente dieses Paket übertragen wird; kennt die gesamte Topologie des Netzes. Wenn Sie diese Option aktivieren, dann werden alle Verbindungen, die der Router aufbaut, vom Least-Cost-Routing gesteuert.

SNMP-ID: 2.15.1

Pfad Telnet: /Setup/LCR

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.15.2 Lancapi-Nutzung

Wenn Sie diese Option aktivieren, dann werden alle Verbindungen, die von CAPI-Clients aufgebaut werden, vom Least-Cost-Routing gesteuert.

SNMP-ID: 2.15.2

Pfad Telnet: /Setup/LCR

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.15.4 Zeit-Liste

In dieser Tabelle können Sie abhängig von der Uhrzeit, dem Tag und der gewählten Vorwahl angeben, über welche Call-by-Call-Nummern ein Anruf umgeleitet werden soll.

SNMP-ID: 2.15.4

Pfad Telnet: /Setup/LCR

2.15.4.1 Index

Index für diesen Eintrag in der Tabelle.

SNMP-ID: 2.15.4.1

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.15.4.2 Praefix

Geben Sie hier die Vorwahl oder die ersten Ziffern einer Gruppe von Vorwahlen ein, für die dieser Eintrag gelten soll. Wenn Sie beispielsweise 030 für Berlin eingeben, dann werden alle Anrufe mit dieser Vorwahl wie hier angegeben umgeleitet. Sie können aber auch nur 03 eingeben, dann werden alle Anrufe zu Orten, deren Vorwahl mit 03 beginnt, umgeleitet.

SNMP-ID: 2.15.4.2

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- max. 10 Zeichen

Default: leer

2.15.4.3 Tage

Die Tage an denen dieser Eintrag verwendet werden soll. Sie können mehrere Einträge fiir die gleiche Vorwahl anlegen, die jedoch zu verschiedenen Zeiten oder an verschiedenen Tagen gelten.

SNMP-ID: 2.15.4.3

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

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

Default: leer

2.15.4.4 Start

Gibt den Anfang des Zeitraums an, in dem der Eintrag verwendet werden soll.

SNMP-ID: 2.15.4.4

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- max. 5 Zeichen

Default: leer

2.15.4.5 Stop

Gibt das Ende des Zeitraums an, in dem der Eintrag verwendet werden soll.

SNMP-ID: 2.15.4.5

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- max. 5 Zeichen

Default: leer

2.15.4.6 Nummernliste

Tragen Sie hier die Vorwahl des Call-by-Call Anbieters ein, über den die zu diesem Eintrag passenden Rufe umgeleitet werden sollen.

Sie können auch mehrere Vorwahlen durch Semikolon getrennt eingeben. Wenn mit der ersten Vorwahl keine Verbindung aufgebaut werden kann, dann werden anschließend die anderen Nummern nacheinander versucht.

Lassen Sie dieses Feld leer, wenn Sie die zu diesem Eintrag passenden Rufe nicht umleiten wollen.

SNMP-ID: 2.15.4.6

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- max. 29 Zeichen

Default: leer

2.15.4.7 Rueckfall

Automatischer Rückfall: Wenn über keine der eingetragenen Call-by-Call-Nummern eine Verbindung hergestellt werden kann, baut der Least-Cost-Router die Verbindung über Ihren regulären Telefonanbieter auf. Wenn Sie dies nicht wünschen, dann schalten Sie diese Option aus.

SNMP-ID: 2.15.4.7

Pfad Telnet: /Setup/LCR/Zeit-Liste

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.16 NetBIOS

Dieses Menü enthält die Konfiguration des NetBIOS.

SNMP-ID: 2.16

Pfad Telnet: /Setup

2.16.1 Aktiv

Wenn Sie diese Option aktivieren, kann der Gerät auch NetBIOS-Pakete gezielt an die richtigen Gegenstellen in entfernten Netzen weiterleiten. Ohne diese Option verursachen diese Pakete oft unnötige Verbindungen, da die einzelnen Rechner in einem auf NetBIOS basierenden Netzwerk (zum Beispiel Microsoft Windows Netzwerke) ständig Status-Informationen austauschen.

SNMP-ID: 2.16.1

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.16.2 Scope-ID

Diese Zeichenkette hängt das Gerät in allen TCP-IP-Verbindungen über NetBIOS an den NetBIOS-Namen an.

SNMP-ID: 2.16.2

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- max. 64 Zeichen

Default: leer

2.16.4 Gegenstellen

Geben Sie in dieser Liste die Gegenstellen ein, zu denen NetBIOS über IP übertragen werden soll. Diese Gegenstellen müssen ebenfalls in der IP-Routing-Tabelle vorhanden sein.

SNMP-ID: 2.16.4

Pfad Telnet: /Setup/NetBIOS

2.16.4.1 Name

Geben Sie hier den Namen einer Gegenstelle ein. Diese Gegenstelle muss ebenfalls in der Routing-Tabelle des IP- Routers vorhanden sein.

SNMP-ID: 2.16.4.1

Pfad Telnet: /Setup/NetBIOS/Gegenstellen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.16.4.3 Typ

Geben Sie an, ob es sich bei der Gegenstelle auch um einen Router handelt, oder ob dies ein einzelner Rechner ist, der sich für Fernzugriff einwählt.

SNMP-ID: 2.16.4.3

Pfad Telnet: /Setup/NetBIOS/Gegenstellen

Mögliche Werte:

- Workstation
- Router

Default: Router

2.16.5 Gruppen-Liste

Diese Liste zeigt Ihnen alle NetBIOS-Gruppen an.

SNMP-ID: 2.16.5

Pfad Telnet: /Setup/NetBIOS

2.16.5.1 Gruppe/Domaene

Name der Arbeitsgruppe, der über NetBIOS übermittelt wurde.

SNMP-ID: 2.16.5.1

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.5.2 Typ

NetBIOS legt eine bestimmte Menge von Servertypen fest, die durch hexadezimale Zahlen dargestellt werden. Die wichtigsten dieser Typen sind:

- Standard-Workstation 00
- Win-PopUp Dienst 03
- RAS-Server 06
- Domain Master-Browser oder PDC 1B
- Master-Browser 1D
- NetDDE Dienst 1F
- Datei- oder Druckerdienst 20
- RAS-Client 21
- Network Monitor Agent BE
- Network Monitor Utility BF

SNMP-ID: 2.16.5.2

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.5.3 IP-Addresse

IP-Adresse der Station.

SNMP-ID: 2.16.5.3

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.16.5.4 Gegenstelle

Name der Gegenstelle, über welche diese NetBIOS-Gruppe erreicht werden kann.

SNMP-ID: 2.16.5.4

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

2.16.5.5 Timeout

Gültigkeitsdauer für diesen Eintrag in Minuten.

SNMP-ID: 2.16.5.5

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.5.6 Flags

Flags zur weiteren Kennzeichnung der Station oder Gruppe.

SNMP-ID: 2.16.5.6

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.5.7 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

SNMP-ID: 2.16.5.7

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.5.8 Rtg-Tag

Routing-Tag für diesen Eintrag.

SNMP-ID: 2.16.5.8

Pfad Telnet: /Setup/NetBIOS/Gruppen-Liste

2.16.6 Host Liste

Diese Liste zeigt Ihnen alle NetBIOS-Hosts an.

SNMP-ID: 2.16.6

Pfad Telnet: /Setup/NetBIOS

2.16.6.1 Name

Name der Station, der über NetBIOS übermittelt wurde.

SNMP-ID: 2.16.6.1

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.6.2 Typ

NetBIOS legt eine bestimmte Menge von Servertypen fest, die durch hexadezimale Zahlen dargestellt werden. Die wichtigsten dieser Typen sind:

- Standard-Workstation 00
- Win-PopUp Dienst 03
- RAS-Server 06
- Domain Master-Browser oder PDC 1B
- Master-Browser 1D
- NetDDE Dienst 1F
- Datei- oder Druckerdienst 20
- RAS-Client 21
- Network Monitor Agent BE
- Network Monitor Utility BF

SNMP-ID: 2.16.6.2

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.6.3 IP-Addresse

IP-Adresse der Station.

SNMP-ID: 2.16.6.3

Pfad Telnet: /Setup/NetBIOS/Host-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.16.6.4 Gegenstelle

Name der Gegenstelle, über welche diese Station erreicht werden kann.

SNMP-ID: 2.16.6.4

Pfad Telnet: /Setup/NetBIOS/Host-Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

2.16.6.5 Timeout

Gültigkeitsdauer für diesen Eintrag in Minuten.

SNMP-ID: 2.16.6.5

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.6.6 Flags

Flags zur weiteren Kennzeichnung der Station oder Gruppe.

SNMP-ID: 2.16.6.6

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.6.7 Netzwerkname

Name des IP-Netzwerks, in dem sich die Station befindet.

SNMP-ID: 2.16.6.7

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.6.8 Rtg-Tag

Routing-Tag für diesen Eintrag.

SNMP-ID: 2.16.6.8

Pfad Telnet: /Setup/NetBIOS/Host-Liste

2.16.7 Server-Liste

Diese Liste zeigt Ihnen alle NetBIOS-Server an.

SNMP-ID: 2.16.7

Pfad Telnet: /Setup/NetBIOS

2.16.7.1 Host

Zeigt den NetBIOS-Namen des Hosts.

SNMP-ID: 2.16.7.1

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.2 Gruppe/Domaene

Zeigt die Arbeitsgruppe/Domäne, in dem sich der NetBIOS-Host befindet.

SNMP-ID: 2.16.7.2

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.4 IP-Addresse

Zeigt die IP-Adresse des NetBIOS-Hosts.

SNMP-ID: 2.16.7.4

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.5 OS-Ver.

Zeigt das Betriebssystem des NetBIOS-Hosts.

SNMP-ID: 2.16.7.5

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.6 SMB-Ver.

Zeigt die SMB-Version des NetBIOS-Hosts.

SNMP-ID: 2.16.7.6

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.7 Server-Typ

Zeigt den Servertyp des NetBIOS-Hosts.

SNMP-ID: 2.16.7.7

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.8 Gegenstelle

Gegenstelle, über welche der NetBIOS-Host erreicht werden kann.

SNMP-ID: 2.16.7.8

Pfad Telnet: /Setup/NetBIOS/Server-Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

2.16.7.9 Timeout

Zeigt die Dauer in Minuten bevor die NetBIOS-Information aktualisiert wird.

SNMP-ID: 2.16.7.9

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.10 Flags

Zeigt die für den NetBIOS-Host ermittelten NetBIOS-Flags.

SNMP-ID: 2.16.7.10

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.11 Netzwerkname

Zeigt das IP-Netzwerk, in dem sich der NetBIOS-Host befindet.

SNMP-ID: 2.16.7.11

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.7.12 Rtg-Tag

Routing-Tag für die Verbindung zum NetBIOS-Host.

SNMP-ID: 2.16.7.12

Pfad Telnet: /Setup/NetBIOS/Server-Liste

2.16.8 Watchdogs

Manche Stationen versenden von Zeit zu Zeit Watchdog-Pakete, um zu prüfen, ob andere Stationen im Netzwerk noch erreichbar sind. Solche Watchdogs können unnötige Verbindungsaufbauten verursachen. Hier können Sie festlegen, ob das Gerät solche Watchdogs abfangen und selber beantworten soll, um diese Verbindungsaufbauten zu vermeiden.

SNMP-ID: 2.16.8

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- spoof
- route

Default: spoof

2.16.9 Abgleich

Das Gerät muss mit anderen NetBIOS-Routern von Zeit zu Zeit Routing-Informationen austauschen. Um unnötige Verbindungsaufbauten zu vermeiden, können Sie auswählen, wann dies geschehen soll.

SNMP-ID: 2.16.9

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- pBack
- Trig
- Zeit

Default: pBack

2.16.10 WAN-Update-Minuten

Wenn Sie festgelegt haben, dass Routing-Informationen in bestimmten Intervallen ausgetauscht werden sollen, dann geben Sie hier dieses Intervall in Minuten an.

SNMP-ID: 2.16.10

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- max. 10 Zeichen

Default: 60

2.16.11 Gültigkeit

Die maximale Zeit in Minuten, für die NetBIOS-Namen gültig sind.

Ein Host registriert sich mit einem NetBIOS-Namen im Gerät. Wenn diese Zeitspanne abgelaufen ist, dann ist für den Host eine erneute Registrierung mit seinem Namen erforderlich.

SNMP-ID: 2.16.11

Pfad Telnet: /Setup/NetBIOS

Mögliche Werte:

- max. 10 numerische Zeichen

Default: 500

2.16.12 Netzwerke

In dieser Tabelle können Sie NetBIOS Einstellungen vornehmen und auswählen für welches Netzwerk diese gelten sollen.

SNMP-ID: 2.16.12

Pfad Telnet: /Setup/NetBIOS

2.16.12.1 Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

SNMP-ID: 2.16.12.1

Pfad Telnet: /Setup/NetBIOS/Netzwerke

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.16.12.2 Aktiv

Wählen Sie hier aus, ob der NetBIOS-Proxy für das gewählte Netzwerk verwendet wird oder nicht.

SNMP-ID: 2.16.12.2

Pfad Telnet: /Setup/NetBIOS/Netzwerke

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.16.12.3 NT-Domaene

Geben Sie hier den Namen der Arbeitsgruppe ein, die von den Rechnern in Ihrem Netz verwendet wird. Wenn in Ihrem Netz mehrere Arbeitsgruppen existieren, dann reicht es, eine von diesen anzugeben.

SNMP-ID: 2.16.12.3

Pfad Telnet: /Setup/NetBIOS/Netzwerke

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.16.13 Browser-Liste

Diese Tabelle zeigt Ihnen die Übersicht der Masterbrowser, die dem NetBIOS-Proxy bekannt sind.

Pfad Telnet:

Setup > **NetBIOS**

2.16.13.1 Browser

Dieser Eintrag zeigt die Computernamen (Master Browser) an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.2 Gruppe/Domaene

Dieser Eintrag zeigt die Arbeitsgruppen/Domänen an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.4 IP-Adresse

Dieser Eintrag zeigt die IP-Adressen an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.5 OS-Ver.

dieser Eintrag zeigt die OS-Version an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.7 Server-Typ

Dieser Eintrag zeigt den Server-Typ an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.8 Gegenstelle

Dieser Eintrag zeigt den Namen der Gegenstelle an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.9 Timeout

Dieser Eintrag zeigt die Anzahl der Timeouts an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.10 Flags

Dieser Eintrag zeigt die Flags an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.11 Netzwerkname

Dieser Eintrag zeigt den Netzwerknamen an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.13.12 Rtg-Tag

Dieser Eintrag zeigt das verwendete Routing-Tag an.

Pfad Telnet:

Setup > **NetBIOS** > **Browser-Liste**

2.16.14 Suchdienst-Unterstuetzung

Windows nutzt den sog. Browser oder Suchdienst, um die Netzwerkumgebung aufzubauen. Da der Browserservice mit Broadcasts arbeitet, ist die Netzwerkumgebung in gerouteten Netzen unvollständig, wenn keine Domänen verwendet werden. Die Suchdienst-Unterstützung schließt diese Lücke, indem sie für jede lokale Arbeitsgruppe den zuständigen Masterbrowser auf die remote Seite propagiert, bzw. von der remoten Seite empfangene Masterbrowser im LAN per Broadcast propagiert. Die Liste der dem NetBIOS-Proxy bekannten Masterbrowser kann unter /Status/TCP-IP/NetBIOS/Browser-List eingesehen werden. Die Suchdienst-Unterstuetzung muß nur in Arbeitsgruppennetzen aktiviert werden. In Domänennetzen wird ohne Broadcasts gearbeitet und der Master-Browser ist immer der Domänen-Controler.

Pfad Telnet: /Setup/NetBIOS/Suchdienst-Untersuetzung

Mögliche Werte:

- ja
- nein

Default: ja

2.17 DNS

Dieses Menü enthält die Konfiguration des Domain-Name-System (DNS).

SNMP-ID: 2.17

Pfad Telnet: /Setup

2.17.1 Aktiv

Aktiviert oder deaktiviert DNS.

SNMP-ID: 2.17.1

Pfad Telnet: /Setup/DNS/Aktiv

Mögliche Werte:

- ja
- nein

Default: ja

2.17.2 Domain

Eigene Domäne des Gerätes.

SNMP-ID: 2.17.2

Pfad Telnet: /Setup/DNS

Mögliche Werte:

- max. 64 Zeichen

Default: intern

2.17.3 DHCP-verwenden

Der DNS-Server kann die Namen der Stationen auflösen, die über DHCP eine IP-Adresse angefordert haben.

Mit diesem Schalter können Sie diese Option aktivieren.

SNMP-ID: 2.17.3

Pfad Telnet: /Setup/DNS

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.17.4 NetBIOS-verw.

Der DNS-Server kann die Namen der Stationen auflösen, die dem NetBIOS-Router bekannt sind.

Mit diesem Schalter können Sie diese Option aktivieren.

SNMP-ID: 2.17.4

Pfad Telnet: /Setup/DNS

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.17.5 DNS-Liste

Tragen Sie hier Stations-Namen und die zugehörigen IP-Adressen ein.

SNMP-ID: 2.17.5

Pfad Telnet: /Setup/DNS

2.17.5.1 Rechnername

Tragen Sie hier den Namen einer Station ein.

Wenn Sie beispielsweise einen Rechner mit dem Namen myhost haben und der Name Ihrer Domäne myhome.intern lautet, dann müssen Sie hier als Stationsnamen myhost.myhome.intern eingeben.

SNMP-ID: 2.17.5.1

Pfad Telnet: /Setup/DNS/DNS-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.5.2 IP-Adresse

Tragen Sie hier die IP-Adresse der Station ein.

Wenn ein Client den Namen einer Station auflösen möchte, dann schickt er eine Anfrage mit diesem Namen an den DNS-Server. Der Server beantwortet diese Anfrage mit der hier eingegebenen IP-Adresse.

SNMP-ID: 2.17.5.2

Pfad Telnet: /Setup/DNS/DNS-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.17.5.3 IPV6-Adresse

Tragen Sie hier die IPv6-Adresse der Station ein.

Wenn ein Client den Namen einer Station auflösen möchte, dann schickt er eine Anfrage mit diesem Namen an den DNS-Server. Der Server beantwortet diese Anfrage mit der hier eingegebenen IPv6-Adresse.

SNMP-ID: 2.17.5.3

Pfad Telnet: /Setup/DNS/DNS-Liste

Mögliche Werte:

- Gültige IPv6-Adresse.

Default: leer

2.17.5.4 Rtg-Tag

Das Routing-Tag legt bei einer Station fest, in welchem Tag-Kontext das Gerät den Stationsnamen auflöst.

Pfad Telnet:

Setup > **DNS** > **DNS-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

2.17.6 Filter-Liste

Benutzen Sie den DNS-Filter, um den Zugriff auf bestimmte Stationen oder Domänen zu unterbinden.

SNMP-ID: 2.17.6

Pfad Telnet: /Setup/DNS

2.17.6.1 Idx.

Index für die Filtereinträge.

SNMP-ID: 2.17.6.1

Pfad Telnet: /Setup/DNS/Filter-Liste

Mögliche Werte:

- max. 4 Zeichen

Default: Leer

2.17.6.2 Domain

Tragen Sie hier den Namen einer Station oder einer Domäne ein, die Sie sperren wollen. Die Zeichen '*' und '?' können als Wildcards verwendet werden.

SNMP-ID: 2.17.6.2

Pfad Telnet: /Setup/DNS/Filter-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.6.3 IP-Adresse

Wenn die Zugriffs-Einschränkung nur für einen bestimmten Rechner oder für ein Teilnetz gelten soll, dann geben Sie hier die IP-Adresse des Rechners bzw. des Netzes ein.

SNMP-ID: 2.17.6.3

Pfad Telnet: /Setup/DNS/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.17.6.4 Netzmaske

Wenn Sie für die Zugriffs-Einschränkung die Adresse eines Teilnetzes angegeben haben, dann müssen Sie hier die zugehörige Netzmaske eingeben.

SNMP-ID: 2.17.6.4

Pfad Telnet: /Setup/DNS/Filter-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.17.6.5 IPv6-Prefix

Über diesen Einträg legen Sie fest, für welche IPv6-Absenderadressen das Gerät die Domain filtert. Sofern Sie den Filter auf alle IPv6-Adressen anwenden wollen, wählen Sie den Präfix `::/0`.

Pfad Telnet:

Setup > **DNS** > **Filter-Liste**

Mögliche Werte:

Gültiger IPv6-Präfix

Default:

2.17.6.6 Rtg-Tag

Das Routing-Tag legt fest, welche Filter im jeweiligen Tag-Kontext gelten.

Pfad Telnet:

Setup > **DNS** > **Filter-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

2.17.7 Gueltigkeit

Manche Computer speichern die Namen und Adressen der Stationen, die sie beim DNS-Server angefragt haben, um später schneller auf diese Informationen zugreifen zu können.

Geben Sie hier ein, wie lange diese Daten gespeichert bleiben dürfen, bevor sie ungültig werden. Danach muss der betreffende Computer die Informationen erneut anfragen.

SNMP-ID: 2.17.7

Pfad Telnet: /Setup/DNS

Mögliche Werte:

- max. 10 Zeichen

Default: 2000

2.17.8 Dyn.-DNS-Liste

Die Dyn-DNS-Liste nimmt Namen auf die, über einen Register-Request angemeldet wurden. Das macht z. B. Windows, wenn unter den erweiterten TCP/IP-Einstellungen einer Netzwerkverbindung unter "DNS" die Optionen bei "Adressen dieser Verbindung in DNS registrieren" und "DNS-Suffix dieser Verbindung in DNS-Registrierung verwenden" aktiviert sind und sich die Station in der Domäne anmeldet.

SNMP-ID: 2.17.8

Pfad Telnet: /Setup/DNS

2.17.8.1 Rechnername

Name der Station, die sich über Register-Request angemeldet hat.

SNMP-ID: 2.17.8.1

Pfad Telnet: /Setup/DNS/Dyn.-DNS-Liste

2.17.8.2 IP-Adresse

IP-Adresse der Station, die sich über Register-Request angemeldet hat.

SNMP-ID: 2.17.8.2

Pfad Telnet: /Setup/DNS/Dyn.-DNS-Liste

Mögliche Werte:

- Gültige IP-Adresse.

2.17.8.3 Timeout

Gültigkeitsdauer für diesen Eintrag.

SNMP-ID: 2.17.8.3

Pfad Telnet: /Setup/DNS/Dyn.-DNS-Liste

2.17.8.4 IPV6-Adresse

Zeigt die IPv6-Adresse des betreffenden Hosts an (sofern vorhanden).

Pfad Telnet:

Setup > **DNS** > **Dyn.-DNS-Liste**

2.17.8.5 Netzwerkname

Zeigt den Namen des Netzes an, in dem sich der Host befindet.

Pfad Telnet:

Setup > **DNS** > **Dyn.-DNS-Liste**

2.17.9 DNS-Weiterleitungen

Sie können Anfragen für bestimmte Domänen explizit an bestimmte Gegenstellen weiterleiten.

SNMP-ID: 2.17.9

Pfad Telnet: /Setup/DNS

2.17.9.1 Domainname

Um Namen einer bestimmten Domäne von einem anderen DNS-Server auflösen zu lassen, können Sie hier die Domäne eintragen und dieser eine Gegenstelle bzw. einen DNS-Server dediziert zuweisen.

SNMP-ID: 2.17.9.1

Pfad Telnet: /Setup/DNS/DNS-Weiterleitungen

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.9.2 Gegenstelle

Gegenstelle, an die Anfragen für die definierte Domäne weitergeleitet werden sollen.

SNMP-ID: 2.17.9.2

Pfad Telnet: /Setup/DNS/DNS-Weiterleitungen

Mögliche Werte:

- max. 31 Zeichen

Default: Leer

2.17.9.3 Rtg-Tag

Das Routing-Tag ermöglicht es, mehrere voneinander unabhängige Forwarding-Definitionen zu bestimmen (insbesondere allgemeine Wildcard-Definitionen mit "*"). Abhängig vom Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit "0" gekennzeichneten Einträge.

Pfad Telnet:

Setup > **DNS** > **DNS-Weiterleitungen**

Mögliche Werte:

0 bis 65535

Default:

0

2.17.10 Service-Location-Liste

Konfigurieren Sie hier ob und wohin bestimmte Dienste aufgelöst werden sollen.

SNMP-ID: 2.17.10

Pfad Telnet: /Setup/DNS

2.17.10.1 Service-Name

Definieren Sie hier welcher Dienst vom DNS wie aufgelöst werden soll.

Der Dienst-Bezeichner ist der aufzulösende Dienst nach RFC 2782.

Zur Veranschaulichung werden in folgendem Beispiel einige Einträge zur Auflösung von SIP-Diensten aufgelistet: (Dienst-ID, Stations-Name, Port)

- _sips._tcp.myhome.intern . 0
- _sip._tcp.myhome.intern myhost.myhome.intern 5060
- _sip._udp.myhome.intern [self] 5060

Pfad Telnet: /Setup/DNS/Service-Location-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.10.2 Rechnername

Der Stationsname gibt den Namen der Station an, die den angegebenen Dienst bereitstellt. Wenn Sie beispielsweise einen Rechner mit dem Namen myhost haben und der Name Ihrer Domäne myhome.intern lautet, dann müssen Sie hier als Stationsnamen myhost.myhome.intern eingeben. Der Stationsname '[self]' kann als Name angegeben werden, wenn es sich um dieses Gerät selbst handelt. Ein Punkt '.' kann angegeben werden, wenn dieser Dienst gesperrt ist und demzufolge nicht aufgelöst werden soll (In diesem Fall wird eine Angabe im nachfolgenden Port-Feld ignoriert).

Pfad Telnet: /Setup/DNS/Service-Location-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.10.3 Port

Der Dienst-Port bezeichnet die verwendete Port-Nummer des angegebenen Dienstes an der genannten Station.

Pfad Telnet: /Setup/DNS/Service-Location-Liste

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.17.10.4 Rtg-Tag

Das Routing-Tag legt fest, ob und wie das Gerät bestimmte Dienstanfragen im jeweiligen Tag-Kontext auflösen soll.

Pfad Telnet:

Setup > **DNS** > **Service-Location-Liste**

Mögliche Werte:

0 bis 65535

Default:

0

2.17.11 Dynamische-SRV-Liste

In der Dynamic-SRV-List werden Service-Location-Records abgelegt, die das Gerät selbst verwendet. Hier trägt sich z. B. das VoIP-Modul ein.

SNMP-ID: 2.17.11

Pfad Telnet: /Setup/DNS

2.17.11.1 Service-Name

Name des Dienstes.

SNMP-ID: 2.17.11.1

Pfad Telnet: /Setup/DNS/Dynamische-SRV-Liste

2.17.11.2 Rechnername

Name der Station, die diesen Dienst anbietet.

SNMP-ID: 2.17.11.2

Pfad Telnet: /Setup/DNS/Dynamische-SRV-Liste

2.17.11.3 Port

Port, über den dieser Dienst angemeldet wird.

SNMP-ID: 2.17.11.3

Pfad Telnet: /Setup/DNS/Dynamische-SRV-Liste

2.17.12 Domain-aufloesen

Wenn diese Option aktiviert ist, werden Anfragen nach der eigenen Domäne mit der eigenen IP-Adresse beantwortet.

SNMP-ID: 2.17.12

Pfad Telnet: /Setup/DNS

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.17.13 Sub-Domains

Hier kann für jedes logische Netzwerk eine separate Domäne konfiguriert werden.

SNMP-ID: 2.17.13

Pfad Telnet: /Setup/DNS

2.17.13.1 Netzwerkname

IP-Netzwerk, für das eine eigene Subdomäne definiert werden soll.

SNMP-ID: 2.17.13.1

Pfad Telnet: /Setup/DNS/Sub-Domains

Mögliche Werte:

- Auswahl aus der Liste der definierten IP-Netzwerke.

Default: Leer

2.17.13.2 Sub-Domain

Sub-Domäne, die für das gewählte IP-Netzwerk verwendet werden soll.

SNMP-ID: 2.17.13.2

Pfad Telnet: /Setup/DNS/Sub-Domains

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.17.14 Forwarder

Über diese Einstellung legen Sie fest, ob Ihr Gerät ihm unbekannte DNS-Anfragen weiterleitet (forwardet) oder verwirft.

Um zu entscheiden, ob das Gerät eine Adresse kennt oder nicht, prüft der DNS-Server unter **Setup** > **DNS** die Tabellen

- **DNS-Liste**
- **Dyn.-DNS-Liste**
- **Service-Location-Liste**
- **Dynamische-SRV-Liste**

und erfragt die betreffenden Adressen ggf. beim DHCP-Server und beim NetBIOS-Proxy, sofern Sie dies erlauben.

Pfad Telnet:

Setup > **DNS**

Mögliche Werte:

ja

nein

Default:

ja

2.17.15 Tag-Konfiguration

In dieser Tabelle verwalten Sie die spezifischen DNS-Einstellungen für die einzelnen Tag-Kontexte. Wenn ein Eintrag für einen Tag-Kontext existiert, dann gelten für diesen Kontext nur die DNS-Einstellungen in dieser Tabelle. Existiert hingegen kein Eintrag in dieser Tabelle, dann gelten die globalen Einstellungen des DNS-Servers.

Pfad Telnet:

Setup > **DNS**

2.17.15.1 Rtg-tag

Eindeutiges Schnittstellen- bzw. Routing-Tag, dessen Einstellungen die globalen Einstellungen des DNS-Servers überschreiben sollen.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

Gültiges Routing-Tag, 1 bis 65534

Default:

2.17.15.2 Aktiv

Aktiviert den DNS-Server des Gerätes für den betreffenden Tag-Kontext.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

nein

ja

Default:

ja

2.17.15.3 Forwarder

Über diese Einstellung legen Sie fest, ob Ihr Gerät für den betreffenden Tag-Kontext ihm unbekannte DNS-Anfragen weiterleitet (forwardet) oder verwirft.

Um zu entscheiden, ob das Gerät eine Adresse kennt oder nicht, prüft der DNS-Server unter **Setup** > **DNS** die Tabellen

- **DNS-Liste**
- **Dyn.-DNS-Liste**
- **Service-Location-Liste**
- **Dynamische-SRV-Liste**

und erfragt die betreffenden Adressen ggf. beim DHCP-Server und beim NetBIOS-Proxy, sofern Sie dies erlauben.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

nein

ja

Default:

ja

2.17.15.4 DHCP-verwenden

Aktiviert bzw. deaktiviert – für den betreffenden Tag-Kontext – die Auflösung von Stations-Namen, die über DHCP eine IP-Adresse angefordert haben.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

nein

ja

Default:

ja

2.17.15.5 NetBIOS-verw.

Aktiviert bzw. deaktiviert – für den betreffenden Tag-Kontext – die Auflösung von Stations-Namen, die dem NetBIOS-Router bekannt sind.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

nein

ja

Default:

ja

2.17.15.6 Domain-aufloesen

Aktiviert bzw. deaktiviert – für den betreffenden Tag-Kontext – die Beantwortung von DNS-Anfragen an die eigene Domäne mit der IP-Adresse des Routers.

Pfad Telnet:

Setup > **DNS** > **Tag-Konfiguration**

Mögliche Werte:

nein

ja

Default:

ja

2.18 Accounting

Dieses Menü enthält die Konfiguration des Accounting.

SNMP-ID: 2.18

Pfad Telnet: /Setup

2.18.1 Aktiv

Accounting ein- oder ausschalten.

SNMP-ID: 2.18.1

Pfad Telnet: /Setup/Accounting

Mögliche Werte:

- Ja
- Nein

2.18.2 Speichern-Flashrom

Accounting-Daten im Flashspeicher ein- oder ausschalten. Wenn die Accounting-Daten im Flash gespeichert werden, gehen sie auch bei einem Stromausfall nicht verloren.

SNMP-ID: 2.18.2

Pfad Telnet: /Setup/Accounting

Mögliche Werte:

- Ja
- Nein

2.18.3 Sortieren-nach

Wählen Sie hier aus, ob die Daten in der Accounting-Tabelle nach Verbindungszeiten oder Datenvolumen sortiert werden sollen.

SNMP-ID: 2.18.3

Pfad Telnet: /Setup/Accounting

Mögliche Werte:

- Zeit
- Daten

2.18.4 Aktuelle-User

Zeigt Ihnen eine Accounting-Liste aller aktuellen Benutzer.

SNMP-ID: 2.18.4

Pfad Telnet: /Setup/Accounting

2.18.4.1 Username

Zeigt den Benutzernamen an.

SNMP-ID: 2.18.4.1

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

SNMP-ID: 2.18.4.3

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

SNMP-ID: 2.18.4.4

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

SNMP-ID: 2.18.4.5

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.6 Tx-KBytes

Zeigt die gesendeten Bytes an

SNMP-ID: 2.18.4.6

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

SNMP-ID: 2.18.4.8

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.4.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

SNMP-ID: 2.18.4.9

Pfad Telnet: /Setup/Accounting/Aktuelle-User

2.18.5 Accounting-Liste

In der Accounting-Tabelle werden Informationen über die Verbindungen der Clients im eigenen Netzwerk zu verschiedenen Gegenstellen mit Angabe der Verbindungszeit und der übertragenen Datenvolumen gespeichert. Mit Hilfe von Accounting-Snapshots können die Accounting-Daten zu bestimmten Zeitpunkten regelmäßig für eine weitere Auswertung festgehalten werden.

SNMP-ID: 2.18.5

Pfad Telnet: /Setup/Accounting

2.18.5.1 Username

Zeigt den Benutzernamen an.

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.6 Tx-KBytes

Zeigt die gesendeten Bytes an

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.5.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

Pfad Telnet: /Setup/Accounting/Accounting-Liste

2.18.6 Loeschen-Accounting-Liste

Hier haben Sie die Möglichkeit Parameter zu löschen.

SNMP-ID: 2.18.6

Pfad Telnet: /Setup/Accounting

2.18.8 Zeit-Schnappschuss

Bei der Konfiguration des Snapshots wird das Interval festgelegt, in dem die Accounting-Daten in einem Snapshot zwischengespeichert werden.

SNMP-ID: 2.18.8

Pfad Telnet: /Setup/Accounting

2.18.8.1 Index

Zeigt den systeminternen Index an.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Default: 1

2.18.8.2 Aktiv

Zwischenspeichern der Accounting-Daten ein- oder ausschalten.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.18.8.3 Type

Hier können Sie das Intervall einstellen in dem der Zeit-Schnappschuss erstellt wird.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- täglich
- wöchentlich
- monatlich

Default: monatlich

2.18.8.4 Tag

Der Tag im Monat, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'monatlich' von Bedeutung.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- 0 bis 31

Default: 1

2.18.8.5 Wochentag

Der Wochentag, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'wöchentlich' von Bedeutung.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- 0 bis 7

Default: unbekannt

2.18.8.6 Stunde

Die Stunde, zu der die Zwischenspeicherung vorgenommen wird.

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- 0 bis 23

Default: 0

2.18.8.7 Minute

Die Minute, zu der die Zwischenspeicherung vorgenommen wird

Pfad Telnet: /Setup/Accounting/Zeit-Schnappschuss

Mögliche Werte:

- 0 bis 59

Default: 0

2.18.9 Letzter Schnappschuss

Zeigt Ihnen den letzten Schnappschuss.

SNMP-ID: 2.18.9

Pfad Telnet: /Setup/Accounting

2.18.9.1 Username

Zeigt den Benutzernamen an.

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.3 Gegenstelle

Zeigt den Namen der Gegenstelle an.

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.4 Verbindungs-Typ

Zeigt den Verbindungs-Typ an (z. B. DSL-Verbindung)

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.5 Rx-KBytes

Zeigt die empfangenen Bytes an.

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.6 Tx-KBytes

Zeigt die gesendeten Bytes an

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.8 Gesamt-Zeit

Zeigt die Gesamtzeit der jeweiligen Verbindung an.

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.9.9 Verbindungen

Zeigt die Anzahl der Verbindungen an.

Pfad Telnet: /Setup/Accounting/Letzter-Schnappschuss

2.18.10 Diskriminator

Hier können Sie das Merkmal auswählen, nach dem die Accounting-Daten kumuliert werden. MAC-Adresse: Die Daten werden anhand der MAC-Adresse der Clients gesammelt. IP-Adresse: Die Daten werden anhand der IP-Adresse der Clients gesammelt. --> siehe Info

SNMP-ID: 2.18.10

Pfad Telnet: /Setup/Accounting

Mögliche Werte:

- MAC-Adresse
- IP-Adresse

Die Option 'IP-Adresse' kann bei wechselnden IP-Adressen, z. B. bei Verwendung eines DHCP-Servers, zu ungenauen Accounting-Daten führen. Eine Zuordnung der Daten zu Benutzern ist dann ggf. nicht exakt möglich. Auf der anderen Seite können mit dieser Einstellung die Daten von Clients separiert werden, die sich hinter einem weiteren Router befinden und daher mit der gleichen MAC-Adresse des Routers in der Accounting-Liste auftauchen.

2.19 VPN

Dieses Menü enthält die Konfiguration des Virtual-Private-Network (VPN).

Pfad Telnet:

Setup

2.19.3 Isakmp

Dieses Menü enthält die Konfiguration des Isakmp.

Pfad Telnet:

Setup > **VPN**

2.19.3.4 Timer

Diese Tabelle enthält Werte, die das Timing von IKE-Verhandlungen beeinflussen.

Die Werte werden bei jeder VPN-Vollkonfiguration (Aufsetzen aller VPN-Regeln) an den IKE-Job übergeben. Der IKE-Job liest diese Werte bei jeder Verwendung direkt aus seiner Konfiguration. Dadurch wird der Expiry-Timeout bei jeder neuen Verhandlung (inkl. Rekeying alter Verbindungen) sofort verwendet. Ebenso wird das Retry-Limit sofort verwendet, dieses sogar bei schon laufenen Wiederholungen von Verhandlungspaketen.

SNMP-ID: 2.19.3.4

Pfad Telnet: /Setup/VPN/Isakmp

2.19.3.4.1 Retr-Lim

Das Retry-Limit gibt an, wie oft ein IKE-Verhandlungspaket maximal wiederholt wird, wenn keine Antwort darauf empfangen wird. Der Defaultwert ist 5. Die Zeitabstände der Wiederholungen sind derzeit nicht konfigurierbar und betragen 5, 7, 9, 11, 13, ... Sekunden. Die Gesamtdauer einer IKE-Verhandlung wird zusätzlich durch das Expiry-Limit beschränkt.

SNMP-ID: 2.19.3.4.1

Pfad Telnet: /Setup/VPN/Isakmp/Timer

Mögliche Werte:

- Maximal 5 Zeichen

Default: 5

2.19.3.4.2 Retr-Tim

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

SNMP-ID: 2.19.3.4.2

Pfad Telnet: /Setup/VPN/Isakmp/Timer

2.19.3.4.3 Retr-Tim-Usec

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

SNMP-ID: 2.19.3.4.3

Pfad Telnet: /Setup/VPN/Isakmp/Timer

2.19.3.4.4 Retr-Tim-Max

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

SNMP-ID: 2.19.3.4.4

Pfad Telnet: /Setup/VPN/Isakmp/Timer

2.19.3.4.5 Exp-Tim

Maximale Dauer einer IKE-Verhandlungs-Phase in Sekunden.

SNMP-ID: 2.19.3.4.5

Pfad Telnet: /Setup/VPN/Isakmp/Timer

Mögliche Werte:

- 0 bis 65535

Default: 30 Sekunden

Diese Einstellungen sind nur aus Gründen der Kompatibilität zu früheren Firmware-Versionen enthalten. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.19.3.4.6 Idx.

Die Tabelle enthält nur eine Zeile, daher hat der Index nur den Wert '1'.

SNMP-ID: 2.19.3.4.6

Pfad Telnet: /Setup/VPN/Isakmp/Timer

2.19.3.29 DH-Gruppen

Dieses Menü enthält die Konfiguration zur Vorberechnung von DH-Schlüsseln.

Pfad Telnet:

Setup > **VPN** > **Isakmp**

2.19.3.29.1 Vorberechnung

Diese Option aktiviert bzw. deaktiviert die Vorberechnung von DH-Schlüsseln.

Pfad Telnet:

Setup > **VPN** > **Isakmp** > **DH-Gruppen**

Mögliche Werte:

Ja

Nein

Default:

Ja

2.19.3.29.2 Gruppenkonfig

Diese Tabelle legt die Anzahl der zu berechnenden DH-Schlüssel je DH-Gruppe fest.

Pfad Telnet:

Setup > **VPN** > **Isakmp** > **DH-Gruppen**

2.19.3.29.2.1 DH-Gruppe

Dieser Wert zeigt die jeweilige DH-Gruppe an.

Pfad Telnet:

Setup > **VPN** > **Isakmp** > **DH-Gruppen** > **Gruppenkonfig**

Mögliche Werte:

Auswahl aus der Liste vorgegebener DH-Gruppen

2.19.3.29.2.2 Vorberechnungsziel

Mit diesem Wert bestimmen Sie die Anzahl der für diese DH-Gruppe zu berechnenden DH-Schlüssel.

Wenn Sie hier den Wert `0` angeben, aber die Vorberechnung aktiviert haben, verwendet das Gerät die Anzahl der in der SPD-Tabelle (Security Policy Database) gespeicherten Policies als Berechnungsgrundlage.

Pfad Telnet:

Setup > **VPN** > **Isakmp** > **DH-Gruppen** > **Gruppenkonfig**

Mögliche Werte:

0 bis 999999999

Default:

0

2.19.4 Proposals

Dieses Menü enthält die Konfiguration der Proposals.

SNMP-ID: 2.19.4

Pfad Telnet: /Setup/VPN

2.19.4.9 IKE-Proposal-Listen

Hier können Sie IKE-Proposal-Listen anzeigen und hinzufügen.

SNMP-ID: 2.19.4.9

Pfad Telnet: /Setup/VPN/Proposals

2.19.4.9.1 IKE-Proposal-Listen

Name für die Zusammenstellung von IKE-Proposals

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.4.9.2 IKE-Proposal-1

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.3 IKE-Proposal-2

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.4 IKE-Proposal-3

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.5 IKE-Proposal-4

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.6 IKE-Proposal-5

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.7 IKE-Proposal-6

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.8 IKE-Proposal-7

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.9.9 IKE-Proposal-8

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IKE-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IKE-Proposals

Default: Leer

2.19.4.10 IPSEC-Proposal-Listen

Kombinieren Sie hier die zuvor definierten Proposals zu Proposal-Listen.

SNMP-ID: 2.19.4.10

Pfad Telnet: /Setup/VPN/Proposals

2.19.4.10.1 IPSEC-Proposal-Listen

Name für die Zusammenstellung von IPSec-Proposals

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.4.10.2 IPSEC-Proposal-1

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.3 IPSEC-Proposal-2

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.4 IPSEC-Proposal-3

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.5 IPSEC-Proposal-4

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.6 IPSEC-Proposal-5

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.7 IPSEC-Proposal-6

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.8 IPSEC-Proposal-7

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.10.9 IPSEC-Proposal-8

Proposal, welches für diese Liste verwendet werden soll.

Pfad Telnet: /Setup/VPN/Proposals/IPSEC-Proposal-Listen

Mögliche Werte:

- Auswahl aus den definierten IPSec-Proposals

Default: Leer

2.19.4.11 IKE

In dieser Tabelle können Sie Proposals zur Verwaltung der SA-Aushandlung definieren.

SNMP-ID: 2.19.4.11

Pfad Telnet: /Setup/VPN/Proposals

2.19.4.11.1 Name

Name für die Kombination von IKE-Parametern, die als Proposal verwendet werden soll.

SNMP-ID: 2.19.4.11.1

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

Der Internet Key Exchange (IKE) ist ein Authentisierungs- und Schlüsselaustauschprotokoll.

2.19.4.11.2 IKE-Crypt-Alg

Verschlüsselungsalgorithmus für dieses Proposal

SNMP-ID: 2.19.4.11.2

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NULL

Default: AES-CBC

2.19.4.11.3 IKE-Crypt-Keylen

Schlüssellänge für dieses Proposal

SNMP-ID: 2.19.4.11.3

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- 0 bis 65535

Default: 128

2.19.4.11.4 IKE-Auth-Alg

Hash-Verfahren zur Abbildung der Verschlüsselung. Die zur Verfügung stehenden Werte sind abhängig von dem zu konfigurierenden Gerät.

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IKE**

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384
SHA2-512

Default-Wert:

MD5

2.19.4.11.5 IKE-Auth-Mode

Authentifizierungsverfahren für dieses Proposal

SNMP-ID: 2.19.4.11.5

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- Preshared Key: Beim symmetrischen PSK-Verfahren muss der verwendete Schlüssel vorher beiden Seiten bekannt sein.
- RSA-Signature: Asymmetrisches Verfahren mit privatem und öffentlichem Schlüssel, benannt nach Rivest, Shamir Adleman.

Default: Preshared Key

2.19.4.11.6 Lifetime-Sec

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die Verbindungsdauer.

SNMP-ID: 2.19.4.11.6

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- 0 bis 65535

Default: 8000 Sekunden

Besondere Werte: 0: Keine Einschränkung der Verbindungszeit.

2.19.4.11.7 Lifetime-KB

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die übertragene Datenmenge.

SNMP-ID: 2.19.4.11.7

Pfad Telnet: /Setup/VPN/Proposals/IKE

Mögliche Werte:

- 0 bis 65535

Default: 0 kBytes

Besondere Werte: 0: Keine Einschränkung des Datenvolumens

2.19.4.12 IPSEC

Hier können Sie Vorgaben für Verschlüsselung, Authentifizierung oder Kompression festlegen.

SNMP-ID: 2.19.4.12

Pfad Telnet: /Setup/VPN/Proposals

2.19.4.12.1 Name

Name für die Kombination von IPSec-Parametern, die als Proposal verwendet werden soll.

SNMP-ID: 2.19.4.12.1

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

IPSec steht für „IP Security Protocol“ und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der Internet Engineering Task Force. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

2.19.4.12.2 Encaps-Mode

Auswahl des Verbindungsmodus

SNMP-ID: 2.19.4.12.2

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- Transport: Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt. Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.
- Tunnel: Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

Default: Tunnel

2.19.4.12.3 ESP-Crypt-Alg

Verschlüsselungsalgorithmus für dieses Proposal

SNMP-ID: 2.19.4.12.3

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- AES
- Blowfish
- CAST128
- 3DES
- DES
- NULL

Default: AES-CBC

2.19.4.12.4 ESP-Crypt-Keylen

Schlüssellänge für dieses Proposal

SNMP-ID: 2.19.4.12.4

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- 0 bis 65535

Default: 128

2.19.4.12.5 ESP-Auth-Alg

ESP-Authentifizierungsverfahren für dieses Proposal

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IPSEC**

Mögliche Werte:

Keine Authentifizierung

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

Keine Authentifizierung

2.19.4.12.6 AH-Auth-Alg

AH-Authentifizierungsverfahren für dieses Proposal

Pfad Telnet:

Setup > **VPN** > **Proposals** > **IPSEC**

Mögliche Werte:

Keine Authentifizierung

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

Keine Authentifizierung

2.19.4.12.7 IPCOMP-Alg

Kompressionsverfahren für dieses Proposal

SNMP-ID: 2.19.4.12.7

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- Kein IPCOMP
- Deflate
- LZS

Default: Kein IPCOMP

2.19.4.12.8 Lifetime-Sec

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die Verbindungsdauer.

SNMP-ID: 2.19.4.12.8

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- 0 bis 65535

Default: 8000 Sekunden

Besondere Werte: 0: Keine Einschränkung der Verbindungszeit.

2.19.4.12.9 Lifetime-KB

Gültigkeit der mit diesem Proposal ausgehandelten Verbindungen in Bezug auf die übertragene Datenmenge.

SNMP-ID: 2.19.4.12.9

Pfad Telnet: /Setup/VPN/Proposals/IPSEC

Mögliche Werte:

- 0 bis 65535

Default: 0 kBytes

Besondere Werte: 0: Keine Einschränkung des Datenvolumens

2.19.5 Zertifikate-Schluessel

Dieses Menü enthält die Konfiguration der Zertifikate und Schlüssel.

SNMP-ID: 2.19.5

Pfad Telnet: /Setup/VPN

2.19.5.3 IKE-Keys

Hier werden die gemeinsamen Schlüssel für die Authentifizierung nach dem Preshared-Key-Verfahren und die Identitäten für die Authentifizierung nach dem Preshared-Key- und dem RSA-Signature-Verfahren eingegeben.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel

2.19.5.3.1 Name

Name für die Kombination von Identitäten und Schlüsseln

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.5.3.2 Remote-Identity

Entfernte Identität, für die der eingetragene Schlüssel gelten soll.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.5.3.3 Shared-Sec

Schlüssel, der für diese Kombination gelten soll.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.5.3.4 Shared-Sec-File

[obsolet, nicht verwendet: Datei mit PSK]

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

2.19.5.3.5 Remote-ID-Type

Typ der entfernten Identität, für die der eingetragene Schlüssel gelten soll.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- Keine Identität
- IP-Adresse
- Domänen-Name (FQDN)
- E-Mail-Adresse (FQUN)
- ASN.1-Distinguished Name

Default: Keine Identität

2.19.5.3.6 Local-ID-Type

Typ der lokalen Identität, für die der eingetragene Schlüssel gelten soll.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- Keine Identität
- IP-Adresse
- Domänen-Name (FQDN)
- E-Mail-Adresse (FQUN)
- ASN.1-Distinguished Name

Default: Keine Identität

2.19.5.3.7 Local-Identity

Lokale Identität, für die der eingetragene Schlüssel gelten soll.

Pfad Telnet: /Setup/VPN/Zertifikate-Schluessel/IKE-Keys

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.7 Layer

Definieren Sie hier weitere Parameter für die einzelnen VPN-Verbindungen.

Pfad Telnet:

Setup > **VPN**

2.19.7.1 Name

Name für die Kombination der Verbindungs-Parameter

SNMP-ID: 2.19.7.1

Pfad Telnet: /Setup/VPN/Layer

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.7.3 PFS-Grp

Perfect Forward Secrecy (PFS) ist ein Sicherheitsmerkmal von Verschlüsselungsverfahren. Die PFS-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

Pfad Telnet:

Setup > **VPN** > **Layer**

Mögliche Werte:

0
Kein PFS

1
MODP-768

2
MODP-1024

5
MODP-1536

14
MODP-2048

15
MODP-3072

16
MODP-4096

Default-Wert:

2

2.19.7.4 IKE-Grp

Die IKE-Gruppe gibt an, wie lang der Diffie-Hellmann Key ist, der zur Verschlüsselung der IKE-Verhandlung verwendet wird.

Pfad Telnet:

Setup > **VPN** > **Layer**

Mögliche Werte:

1
MODP-768

2
MODP-1024

5
MODP-1536

14
MODP-2048

15
MODP-3072

16
MODP-4096

Default-Wert:

2

2.19.7.5 IKE-Prop-Liste

IKE-Proposal-Liste für diese Verbindung.

SNMP-ID: 2.19.7.5

Pfad Telnet: /Setup/VPN/Layer

Mögliche Werte:

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

Default: Leer

2.19.7.6 IPSEC-Prop-Liste

IKE-Schlüssel für diese Verbindung.

SNMP-ID: 2.19.7.6

Pfad Telnet: /Setup/VPN/Layer

Mögliche Werte:

- Auswahl aus der Liste der definierten IKE-Schlüssel.

Default: Leer

2.19.7.7 IKE-Key

IPSec-Proposal-Liste für diese Verbindung.

SNMP-ID: 2.19.7.7

Pfad Telnet: /Setup/VPN/Layer

Mögliche Werte:

- Auswahl aus der Liste der definierten IPSec-Proposal-Listen.

Default: Leer

2.19.8 Aktiv

Schaltet das VPN-Modul ein bzw. aus.

SNMP-ID: 2.19.8

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Aktiviert
- Deaktiviert

Default: Deaktiviert

2.19.9 VPN-Gegenstellen

In dieser Tabelle definieren Sie die VPN-Verbindungen, die Ihr Gerät aufbauen soll.

SNMP-ID: 2.19.9

Pfad Telnet: /Setup/VPN

2.19.9.1 Gegenstelle

Name der VPN-Verbindung.

SNMP-ID: 2.19.9.1

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

Default: Leer

2.19.9.2 Extranet-Adresse

In LCOS-Versionen vor 9.10 enthielt dieses Feld die IPv4-Adresse, die die lokalen Stationen in speziellen Szenarien zur Maskierung ihrer eigenen IP-Adresse nutzten.

Ab LCOS-Version 9.10 erfolgt die Maskierung unter **Setup** > **WAN** > **IP-Liste** im Feld **Masq.-IP-Addr.**.

Pfad Telnet:

Setup > **VPN** > **VPN-Gegenstellen**

Mögliche Werte:

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

Default-Wert:

leer

2.19.9.4 Layer

Kombination von Verbindungs-Parametern (PFS-, IKE- und IPSec-Parameter), die für diese Verbindung verwendet werden sollen.

SNMP-ID: 2.19.9.4

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Auswahl aus der Liste der definierten Verbindungs-Parameter

Default: Leer

2.19.9.5 dynamisch

Dynamic VPN ist eine Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen.

SNMP-ID: 2.19.9.5

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Kein dynamisches VPN

- Dynamisches VPN: Es wird eine Verbindung aufgebaut, um IP-Adressen zu übermitteln
- Dynamisches VPN: IP-Adressen werden nach Möglichkeit ohne Verbindungsaufbau übermittelt:
- Dynamisches VPN: Ein ICMP-Paket wird an die Gegenstelle gesendet um die IP-Adresse zu übermitteln
- Dynamisches VPN: Ein UDP-Paket wird an die Gegenstelle gesendet um die IP-Adresse zu übermitteln

Default: Kein dynamisches VPN

2.19.9.6 SH-Zeit

Geben Sie an, nach wieviel Sekunden die Verbindung zu dieser Gegenstelle getrennt werden soll, wenn in dieser Zeit keine Daten mehr übertragen worden sind.

SNMP-ID: 2.19.9.6

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- 0 bis 9999

Default: 0

Besondere Werte: Der Wert 9999 sorgt für einen sofortigen Verbindungsaufbau ohne zeitliche Begrenzung.

2.19.9.7 IKE-Exchange

Auswahl des IKE-Exchange-Modus

SNMP-ID: 2.19.9.7

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Main Mode
- Aggressive Mode

Default: Main Mode

Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode. Der Main Mode ist daher wesentlich sicherer als der Aggressive Mode.

2.19.9.8 Entferntes-Gw

DNS-Name oder IP-Adresse des entfernten Gateways, über das die VPN-Verbindung aufgebaut werden soll.

SNMP-ID: 2.19.9.8

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.9.9 Regelerzegung

Ein-/Ausschalter und Art der VPN-Regelerzeugung

SNMP-ID: 2.19.9.9

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Aus: Es wird keine VPN-Regel für die Gegenstelle erzeugt.

- Automatisch: Automatisch erzeugte VPN-Regeln verbinden die lokalen IP-Netze mit den in der Routing-Tabelle für die Gegenstelle eingetragenen IP-Netzen.
- Manuell: VPN-Regeln werden nur für die in der Firewall-Konfiguration „manuell“ angegebenen IP-Netzbeziehungen für die Gegenstelle angelegt.

Default: Automatisch

2.19.9.10 DPD-Inakt-Timeout

Die Dead Peer Detection wird bei der Einwahl von VPN-Clients in ein VPN-Gateway oder bei Verbindungen von 2 VPN-Gateways eingesetzt. Damit soll sichergestellt werden, das eine Gegenstelle ausgebucht wird, wenn die VPN-Verbindung z. B. durch kurzzeitigen Ausfall der Internetverbindung gestört wurde. Ohne eine entsprechende Leitungsüberwachung würde das VPN-Gateway den Client oder das andere VPN-Gateway weiter in der Liste der eingebuchten Gegenstellen führen. Eine erneute Einwahl der Gegenstelle würde damit verhindert, weil z. B. beim LANCOM Advanced VPN Client eine erneute Einwahl mit der gleichen Seriennummer nicht möglich ist.

Bei der Dead-Peer-Detection tauschen Gateway und Gegenstelle während der Verbindung regelmäßig „Keep-Alive“-Pakete aus. Bleiben die Antworten aus, bucht das Gateway die Gegenstelle aus und ermöglicht so nach wiederherstellen der VPN-Verbindung eine erneute Anmeldung mit der gleichen Identity. Für VPN-Clients wird die DPD-Zeit üblicherweise auf 60 Sekunden eingestellt.

SNMP-ID: 2.19.9.10

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- 0 bis 9999 numerische Zeichen

Default: 0

Ohne Leitungsüberwachung würde z. B. die Einwahl eines Benutzers mit gleicher "Identity" – also gleichem Usernamen – verhindert, da der entsprechende Benutzer weiterhin in der Liste der eingebuchten Gegenstellen geführt würde.

2.19.9.11 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 angegeben.

SNMP-ID: 2.19.9.11

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Aus: Ist der IKE-CFG-Modus ausgeschaltet, werden keine IP-Adressen für die Verbindung zugewiesen. Auf beiden Seiten der VPN-Strecke muss fest konfiguriert sein, welche IP-Adressen für diese Verbindung zu verwenden sind.
- Client: In dieser Einstellung fungiert das Gerät als Client für diese VPN-Verbindung und fordert eine IP-Adresse für die Verbindung von der Gegenstelle (Server) an. Das Gerät verhält sich also so ähnlich wie ein VPN-Client.
- Server: In dieser Einstellung fungiert das Gerät als Server für diese VPN-Verbindung. Für die Zuweisung der IP-Adresse an den Client gibt es zwei Möglichkeiten:
- Wenn die Gegenstelle in der Routing-Tabelle eingetragen ist, wird ihr die dort konfigurierte IP-Adresse zugewiesen.
- Wenn die Gegenstelle nicht in der Routing-Tabelle eingetragen ist, wird eine freie IP-Adresse aus dem IP-Pool für die Einwahlzugänge entnommen.

Default: Aus

In der Einstellung als Server muss die Gegenstelle als IKE-CFG-Client konfiguriert sein und so vom Server eine IP-Adresse für die Verbindung anfordern. Für die Einwahl mit einem LANCOM Advanced VPN Client aktivieren Sie im Verbindungsprofil die Option "IKE Config Mode verwenden".

2.19.9.12 XAUTH

Aktiviert die Verwendung von XAUTH für die gewählte VPN-Gegenstelle.

SNMP-ID: 2.19.9.12

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- Client: In der Betriebsart als XAUTH-Client startet das Gerät die erste Phase der IKE-Verhandlung (Main Mode oder Aggressive Mode) und wartet dann auf den Authentifizierungs-Request vom XAUTH-Server. Auf diesen Request antwortet der XAUTH-Client mit dem Benutzernamen und dem Kennwort aus dem Eintrag der PPP-Tabelle, in dem die PPP-Gegenstelle der hier definierten VPN-Gegenstelle entspricht. Zu der VPN-Gegenstelle muss es also eine gleichnamige PPP-Gegenstelle geben. Der in der PPP-Tabelle definierte Benutzername weicht üblicherweise von dem Gegenstellennamen ab.
- Server: In der Betriebsart als XAUTH-Server startet das Gerät nach erfolgreicher Verhandlung der ersten IKE-Verhandlung die Authentifizierung mit einem Request an den XAUTH-Client, der daraufhin mit seinem Benutzernamen und Kennwort antwortet. Der XAUTH-Server sucht den übermittelten Benutzernamen in den Gegenstellennamen der PPP-Tabelle und prüft bei Übereinstimmung das Kennwort. Der Benutzername für diesen Eintrag in der PPP-Tabelle wird nicht verwendet.
- Aus: Bei der Verbindung zu dieser Gegenstelle wird keine XAUTH-Authentifizierung durchgeführt.

Default: Aus

Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

2.19.9.13 SSL-Encaps.

Mit dieser Option aktivieren Sie die Nutzung der IPsec over HTTPS-Technologie beim aktiven Verbindungsaufbau zu dieser Gegenstelle.

SNMP-ID: 2.19.9.13

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- ja, nein

Default: nein

Bitte beachten Sie, dass bei eingeschalteter IPsec over HTTPS-Option die VPN-Verbindung nur aufgebaut werden kann, wenn die Gegenstelle diese Technologie ebenfalls unterstützt und die Annahme von passiven VPN-Verbindungen mit IPsec over HTTPS bei der Gegenstelle aktiviert ist.

2.19.9.15 Rtg-Tag

Routing-Tags werden im Gerät genutzt, um neben der IP-Adresse weitere Kriterien zur Auswahl der Zielroute auswerten zu können. Aus der Routing-Tabelle werden nur die Routen mit übereinstimmendem Routing-Tag verwendet. Hier kann für jede VPN-Verbindung das Routing-Tag angegeben werden, das verwendet werden soll, um die Route zum entfernten Gateway zu ermitteln.

SNMP-ID: 2.19.9.15

Pfad Telnet: /Setup/VPN/VPN-Gegenstellen

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.9.16 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.

Beachten Sie, dass die Prüfung via OCSP allein den Sperrstatus eines Zertifikates abfragt, jedoch nicht die mathematische Korrektheit seiner Signatur, seine Gültigkeitsdauer oder sonstige Nutzungsbeschränkungen prüft.

Pfad Telnet:

Setup > **VPN** > **VPN-Gegenstellen**

Mögliche Werte:

nein

ja

Default:

nein

2.19.10 AggrMode-Proposal-List-Default

Diese IKE-Proposal-Liste wird für Aggressive-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

SNMP-ID: 2.19.10

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

Default: IKE_RSA_SIG

2.19.11 AggrMode-IKE-Group-Default

Diese IKE-Gruppe wird für Aggressive-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

1
MODP-768

2
MODP-1024

5
MODP-1536

14
MODP-2048

15
MODP-3072

16
MODP-4096

Default-Wert:

2

2.19.12 Zusaetzliche-Gateway-Liste

In dieser Tabelle wird für jede Gegenstelle eine Liste der möglichen Gateways angegeben.

SNMP-ID: 2.19.12

Pfad Telnet: /Setup/VPN

2.19.12.1 Gegenstelle

Name der VPN-Verbindung, für welche die hier definierten zusätzlichen Gateways gelten sollen.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- Auswahl aus der Liste der definierten VPN-Verbindungen.

Default: Leer

2.19.12.2 Entferntes-Gateway-1

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.3 Entferntes-Gateway-2

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.4 Entferntes-Gateway-3

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.5 Entferntes-Gateway-4

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.6 Entferntes-Gateway-5

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.7 Entferntes-Gateway-6

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.8 Entferntes-Gateway-7

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.9 Entferntes-Gateway-8

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.10 Anfangen-mit

Auswahl des Gateways, über das zuerst der Aufbau der VPN-Verrbindung versucht werden soll.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- Erstem: Beginnt mit dem ersten Eintrag in der Liste.

- Zufaelligem: Wählt zufällig einen Eintrag aus der Liste.
- Zuletzt-verwendetem: Beginnt mit dem Eintrag, über den zuletzt eine Verbindung erfolgreich aufgebaut werden konnte.

Default: Zuletzt-verwendetem

2.19.12.11 Rtg-Tag-1

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.12 Rtg-Tag-2

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.13 Rtg-Tag-3

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.14 Rtg-Tag-4

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.15 Rtg-Tag-5

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.16 Rtg-Tag-6

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.17 Rtg-Tag-7

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.18 Rtg-Tag-8

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.19 Entferntes-Gateway-9

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 64 Zeichen

Default: Leer

2.19.12.20 Entferntes-Gateway-10

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.21 Entferntes-Gateway-11

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.22 Entferntes-Gateway-12

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.23 Entferntes-Gateway-13

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.24 Entferntes-Gateway-14

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.25 Entferntes-Gateway-15

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.26 Entferntes-Gateway-16

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.27 Rtg-Tag-9

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.28 Rtg-Tag-10

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.29 Rtg-Tag-11

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.30 Rtg-Tag-12

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.31 Rtg-Tag-13

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.32 Rtg-Tag-14

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.33 Rtg-Tag-15

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.34 Rtg-Tag-16

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/VPN/Zusaetzliche-Gateway-Liste

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.35 Gateway-17

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-17

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.36 Rtg-Tag-17

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-17

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.37 Gateway-18

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-18

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.38 Rtg-Tag-18

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-18

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.39 Gateway-19

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-19

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.40 Rtg-Tag-19

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-19

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.41 Gateway-20

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-20

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.42 Rtg-Tag-20

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-20

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.43 Gateway-21

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-21

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.44 Rtg-Tag-21

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-21

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.45 Gateway-22

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-22

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.46 Rtg-Tag-22

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-22

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.47 Gateway-23

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-23

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.48 Rtg-Tag-23

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-23

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.49 Gateway-24

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-24

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.50 Rtg-Tag-24

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-24

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.51 Gateway-25

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-25

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.52 Rtg-Tag-25

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-25

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.53 Gateway-26

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-26

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.54 Rtg-Tag-26

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-26

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.55 Gateway-27

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-27

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.56 Rtg-Tag-27

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-27

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.57 Gateway-28

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-28

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.58 Rtg-Tag-28

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-28

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.59 Gateway-29

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-29

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.60 Rtg-Tag-29

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-29

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.61 Gateway-30

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-30

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.62 Rtg-Tag-30

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-30

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.63 Gateway-31

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-31

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.64 Rtg-Tag-31

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-31

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.12.65 Gateway-32

DNS-Name oder IP-Adresse des entfernten Gateways, welches als Alternative für die Verbindung genutzt werden kann.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Gateway-32

Mögliche Werte:

- max. 63 Zeichen

Default: Leer

2.19.12.66 Rtg-Tag-32

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen Gateway ermittelt wird.

Pfad Telnet: /Setup/Vpn/Zertifikate-Schluessel/Zusaetzliche-Gateway-Liste/Rtg-Tag-32

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.13 MainMode-Proposal-List-Default

Diese IKE-Proposal-Liste wird für Main-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

SNMP-ID: 2.19.13

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Auswahl aus der Liste der definierten IKE-Proposal-Listen.

Default: IKE_PRESH_KEY

2.19.14 MainMode-IKE-Group-Default

Diese IKE-Gruppe wird für Main-Mode-Verbindungen genutzt, wenn die Gegenstelle nicht anhand der IP-Adresse, sondern anhand einer später übermittelten Identität identifiziert werden kann.

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

1
MODP-768

2
MODP-1024

5
MODP-1536

14
MODP-2048

15
MODP-3072

16
MODP-4096

Default-Wert:

2

2.19.16 NAT-T-Aktiv

Aktiviert die Verwendung von NAT-Traversal. NAT Traversal überwindet die Probleme beim VPN-Verbindungsaufbau an den Endpunkten der VPN-Tunnel.

SNMP-ID: 2.19.16

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Ein
- Aus

Default: Aus

NAT-T kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert.

Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das Gerät als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

2.19.17 Vereinfachtes-Zertifikats-RAS-Aktiv

Erlaubt die vereinfachte Einwahl mit Zertifikaten. Die Vereinfachung besteht darin, dass für ankommende Verbindungen eine gemeinsame Konfiguration vorgenommen werden kann, wenn die Zertifikate der Gegenstellen vom Herausgeber

des im Gerät befindlichen Root-Zertifikats signiert sind. In diesem Fall muss keine Konfiguration pro Gegenstelle erfolgen. Die dafür nötige gemeinsame Konfiguration finden Sie bei den Einstellungen der Default-Parameter. Einzelne Gegenstellen können von dieser Funktionalitat nur ausgenommen werden, indem ihre Zertifikate mit Hilfe einer CRL (Certificate Revocation List) zurückgezogen werden.

SNMP-ID: 2.19.17

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.19.19 QuickMode-Proposal-List-Default

Diese IPSec-Proposal-Liste bei der vereinfachten Einwahl mit Zertifikaten genutzt.

SNMP-ID: 2.19.19

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Auswahl aus der Liste der definierten IPSec-Proposal-Listen.

Default: ESP_TN

2.19.20 QuickMode-PFS-Group-Default

Diese IPSec-Gruppe wird bei der vereinfachten Einwahl mit Zertifikaten genutzt.

Pfad Telnet:

Setup > **VPN**

Mögliche Werte:

0
Kein PFS

1
MODP-768

2
MODP-1024

5
MODP-1536

14
MODP-2048

15
MODP-3072

16
MODP-4096

Default-Wert:

2

2.19.21 QuickMode-Shorthold-Zeit-Default

Diese Haltezeit wird für Verbindungen bei der vereinfachten Einwahl mit Zertifikaten genutzt.

SNMP-ID: 2.19.21

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- 0 bis 65535

Default: 0

2.19.22 Erlaube-Entferntes-Netzwerk-Auswahl

Wenn die vereinfachte Einwahl mit Zertifikaten für ein Gerät in der Zentrale aktiviert ist, können die entfernten Router während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, dass für die Anbindung verwendet werden soll. Dieses Netzwerk wird z. B. bei der Einrichtung der VPN-Verbindung in den entfernten Router eingetragen. Das Gerät in der Zentrale akzeptiert das vorgeschlagene Netzwerk, wenn diese Option aktiviert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

SNMP-ID: 2.19.22

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Ein
- Aus

Default: Aus

Achten Sie bei der Konfiguration der einwählenden Gegenstellen darauf, dass jede Gegenstelle ein spezielles Netzwerk anfordert, damit es nicht zu Konflikten der Netzwerkadressen kommt.

2.19.23 SA-Aufbau-gemeinsam

Die Basis für den Aufbau eines VPN-Tunnels zwischen zwei Netzwerken stellen die „Security Associations" (SAs) dar. Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestoßen, dass vom Quell- ins Zielnetz übertragen werden soll.

Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestoßen, dass vom Quell- ins Zielnetz übertragen werden soll. Daher kann der Aufbau der Netzbeziehungen je nach Anwendung gezielt gesteuert werden.

SNMP-ID: 2.19.23

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Einzeln: Nur die explizit durch ein zu übertragenes Paket angesprochene SA wird aufgebaut.
- Gemeinsam: Alle im Gerät definierten SAs werden aufgebaut.
- Gemeinsam für KeepAlive: Alle definierten SAs werden aufgebaut, für deren Gegenstelle in der VPN-Verbindungsliste eine Haltezeit von '9999' eingestellt ist (Keep Alive).

Default: Einzeln

2.19.24 Max-gleichzeitige-Verbindungen

Stellen Sie hier ein, wie viele VPN-Verbindungen das Gerät aufbauen darf.

Pfad Telnet: /Setup/Vpn/Max-gleichzeitige-Verbindungen

Mögliche Werte:

- Der Maximalwert ist durch die jeweilige Lizenz begrenzt.

Default: 0

Bei einem Wert von 0 darf das Gerät den durch die Lizenz begrenzten Maximalwert voll ausnutzen. Werte oberhalb der Lizenzgrenze werden ignoriert.

2.19.25 Flexibler-ID-Vergleich

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

SNMP-ID: 2.19.25

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- ja
- nein

Default: nein

Der flexible Identitätsvergleich wird sowohl bei der Prüfung der (empfangenen) entfernten Identität als auch bei der Zertifikatsauswahl durch die lokale Identität eingesetzt.

2.19.26 NAT-T-Port-fuer-Rekeying

Stellen Sie hier ein, ob bei einem Rekeying die IKE-Pakete an den Port 500 (nein) oder den Port 4500 (ja) geschickt werden.

Pfad Telnet: /Setup/Vpn/NAT-T-Port-fuer-Rekeying

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.19.27 SSL- Encaps. erlaubt

Für den passiven Verbindungsaufbau zu einem VPN-Gerät von einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie (VPN-Gerät oder LANCOM Advanced VPN Client) aktivieren Sie die Option SSL-Encaps in den allgemeinen VPN-Einstellungen.

SNMP-ID: 2.19.27

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- ja, nein

Default: nein

Der LANCOM Advanced VPN Client unterstützt einen automatischen Fallback auf IPSec over HTTPS. In dieser Einstellung versucht der VPN-Client zunächst eine Verbindung ohne die zusätzliche SSL-Kapselung aufzubauen.

Falls diese Verbindung nicht aufgebaut werden kann, versucht das Gerät im zweiten Schritt eine Verbindung mit der zusätzlichen SSL-Kapselung aufzubauen.

2.19.28 myVPN

Die Funktion "myVPN" dient dazu, auf Endgeräten mit iOS-Betriebsystem VPN-Profile automatisch zu beziehen und die Konfiguration des internen VPN-Clients zu übernehmen. Auf Seiten des Routers konfigurieren Sie dazu das VPN-Profil und die myVPN-Parameter. Mit der LANCOM myVPN App und einer passenden PIN können Sie Ihr Endgerät in wenigen Schritten für eine VPN-Einwahl konfigurieren.

Weitere Informationen zur myVPN-App finden Sie auf der *LANCOM-Homepage*.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

2.19.28.1 Aktiv

Mit diesem Schalter können Sie myVPN für dieses Gerät aktivieren.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Ja

Nein

Default:

Nein

2.19.28.2 PIN-Laenge

Hier können Sie die PIN-Länge angeben, mit der der Setup-Assistent neue PINs generiert.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Maximale Länge: 12

Minimale Länge: 4

Default:

4

2.19.28.3 Geraetename

Geben Sie hier den Gerätenamen an, wenn ein vertrauenswürdiges SSL-Zertifikat auf diesem Gerät eingerichtet ist und bei dem Bezug des Profils auf dem iOS-Gerät keine Warnmeldung bezüglich eines nicht vertrauenswürdigen Zertifikats auftauchen soll.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 31 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

leer

2.19.28.4 Mapping

In dieser Tabelle erfolgt die Zuordnung der myVPN-PIN zu den angelegten VPN-Profilen.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

2.19.28.4.1 PIN

Hinterlegen Sie hier die PIN zum Profilbezug der myVPN-App.

Der myVPN-Setup-Assistent benutzt diese PIN auch in der PPP-Liste für den eigentlichen VPN-Login. Sollten Sie also die PIN hier ändern, müssen Sie sie auch mit LANconfig unter **Kommunikation** > **Protokolle** > **PPP-Liste** ändern, sofern Sie keine unterschiedliche PIN wünschen.

Sicherheitshinweis: Um das myVPN-Feature abzusichern, deaktiviert das Gerät bei der wiederholten Falscheingabe einer spezifischen PIN temporär den Profilbezug und versendet ggf. eine entsprechende Benachrichtigung sowohl per SYSLOG als auch per E-Mail. Nach den ersten drei Fehlversuchen sperrt das Gerät den Profilbezug für 15 Minuten. Drei weitere Fehlversuche sperren den Profilbezug für 24 Stunden. Bei weiteren Fehlversuchen alternieren die Zeitspannen. Eine manuelle Entsperrung setzt den entsprechenden Zähler wieder zurück. Hierbei ist auch zu beachten, dass das Gerät einen versuchten Profilbezug bei einem deaktiviertem Zugang (z. B. durch vorherigen erfolgreichen Profilbezug) ebenfalls als Fehlversuch wertet.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

max. 12 Ziffern aus 1234567890

Default:

leer

2.19.28.4.2 VPN-Profil

Bestimmen Sie hier das VPN-Profil, dessen Daten die myVPN-App beim Profilbezug laden soll.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

16 Zeichen aus

0-9

a-z

A-Z

@{|}~!$%&'()+-,/:;<=>?[\]^_.

Default:

leer

2.19.28.4.3 Aktiv

Mit diesem Schalter können sie den Profilbezug mit Hilfe der myVPN-App aktivieren. Nach einem erfolgreichen Profilbezug deaktiviert das Gerät das entsprechende Profil automatisch, um den wiederholten Download von einem anderen Gerät zu vermeiden.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

Nein

Ja

Default:

Nein

2.19.28.5 Loginsperre-aufheben

Mit dem Befehl `do Loginsperre-aufheben` können Sie eine durch Fehlversuche hervorgerufene Loginsperre aufheben. Ggf. erzeugt die Aufhebung eine Nachricht über SYSLOG oder E-Mail.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

2.19.28.6 E-Mail-Benachrichtigung

Aktivieren Sie diese Option, um Nachrichten der myVPN-App an eine bestimmte E-Mail-Adresse zu versenden. Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für myVPN aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

2.19.28.7 E-Mail-Adresse

Bestimmen Sie hier die E-Mail-Adresse, an die die myVPN-App Nachrichten versenden soll.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

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

Default:

leer

2.19.28.8 SYSLOG

Aktivieren Sie diese Option, um Nachrichten der myVPN-App an SYSLOG zu versenden. Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für myVPN aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

2.19.28.9 Remote-Gateway

Bestimmen Sie hier die WAN-Adresse oder den über öffentliche DNS-Server auflösbaren Namen dieses Routers. Geben Sie das Remote-Gateway zusätzlich in der myVPN-App an, sofern die App das Gateway nicht über die automatische Suche findet.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

leer

2.19.28.10 Anzahl-Fehler-fuer-Loginsperre

Dieser Parameter begrenzt die Anzahl der fehlerhaften Logins der myVPN App.

Wenn der Benutzer die maximale Anzahl der Fehlversuche überschreitet, sperrt das Gerät den Zugang bei der ersten Überschreitung für 15 Minuten, ab der zweiten Überschreitung für 24 Stunden.

Der Konsolenbefehl `Loginsperre-aufheben` hebt diese Sperrung wieder auf (siehe *Loginsperre-aufheben*).

Pfad Telnet:

Setup > **Vpn** > **myVPN**

Mögliche Werte:

5-30

Default:

5

2.19.28.11 Zugriff-vom-WAN-erlauben

Dieser Parameter erlaubt oder unterbindet das Laden des myVPN App-Profils durch den Benutzer vom WAN aus.

Pfad Telnet:

Setup > **Vpn** > **myVPN**

Mögliche Werte:

ja

nein

Default:

ja

2.19.30 Anti-Replay-Window-Size

Dieser Parameter definiert die Breite des Fensters, in dem ein VPN-Gerät im Rahmen der Replay-Detection die empfangenen Sequenznummern der Pakete als aktuell ansieht. Das VPN-Gerät verwirft Pakete mit einer Sequenznummer vor diesem Bereich und doppelt empfangene Pakete innerhalb dieses Bereiches.

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 5 Ziffern

Default:

0

Besondere Werte:

Der Wert 0 deaktiviert die Replay-Detection.

2.19.64 OCSP-Client

In diesem Menü finden Sie die Einstellungen für den OCSP-Client.

Pfad Telnet:

Setup > **VPN**

2.19.64.1 OCSP-Client Aktiv

Mit dieser Einstellung aktivieren Sie den OSCP-Client.

SNMP-ID: 2.19.64.1

Pfad Telnet: /Setup/VPN

Mögliche Werte:

- Nein
- Ja

Default: Nein

2.20 LAN-Bridge

Dieses Menü enthält die Einstellungen für die LAN-Bridge.

SNMP-ID: 2.20

Pfad Telnet: /Setup

2.20.1 Protokoll-Version

Wählen Sie hier das gewünschte Protokoll aus. Je nach Wahl verwendet das Gerät entweder das Classic- oder das Rapid-Protokoll, welche in der IEEE 802.1D-1998 chapter 8, bzw. IEEE 802.1D-2004 chapter 17 definiert sind.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Version

Mögliche Werte:

- Klassisch
- Rapid

Default: Klassisch

2.20.2 Bridge-Prioritaet

Dieser Wert legt die Priorität der Bridge im LAN fest. Sie beeinflussen damit, welche Bridge das Spanning- Tree-Protokoll bevorzugt als Root-Bridge verwendet. Es handelt sich hier um einen 16-Bit-Wert (0...65535), wobei höhere Werte eine niedrigere Priorität bedeuten. Ändern Sie den voreingestellten Wert nur dann, wenn Sie eine bestimmte Bridge bevorzugen.

Auch mit gleichen Werten funktioniert das Auswahlverfahren, da das Gerät die MAC-Adresse der Bridge bei gleicher Priorität zur Entscheidung heranzieht.

Pfad Telnet: /Setup/LAN-Bridge/Bridge-Prioritaet

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 32768

Obwohl für die Konfiguration dieses Parameters ein ganzer 16-Bit Wert zur Verfügung steht, sollte bei neueren Versionen des Rapid-, bzw. Multiple-Spanning-Tree Protokolles darauf geachtet werden, den Prioritätswert nur in Schritten von 4096 zu verändern, da hier die unteren 12-Bit für andere Zwecke verwendet werden und deshalb von künftigen Firmware-Releases vielleicht ignoriert werden könnten.

2.20.4 Verkapselungs-Tabelle

In dieser Tabelle können Sie Verkapselungen hinzufügen.

SNMP-ID: 2.20.4

Pfad Telnet: /Setup/LAN-Bridge

2.20.4.1 Protokoll

Ein Protokoll wird als 16-bit Protokoll ausgewiesen, und in ein Ethernet II/SNAP Feld gebracht. Der Protokoll Typ ist eine Hexadezimalzahl von 0001 bis ffff. Auch wenn die Tabelle leer ist, implizieren einige Protokolle eine Annahme, die in der Tabelle als SNAP (namely, IPX und AppleTalk) aufgelistet sind. Das kann durch die Protokoll Einstellung zu Ethernet II überschrieben werden.

Pfad Telnet: /Setup/LAN-Bridge/Verkapselungs-Tabelle

2.20.4.2 Verkapselung

Hier können Sie angeben, ob die Datenpakete bei der Übertragung mit einem Ethernet-Header versehen werden sollen oder nicht. Normalerweise sollten Sie hier "Transparent" auswählen. Nur wenn Sie einen Layer zur Verwendung mit der Bridge zusammenstellen, sollten Sie "Ethernet" auswählen.

Pfad Telnet: /Setup/LAN-Bridge/Verkapselungs-Tabelle

Mögliche Werte:

- Transparent
- Ethernet

Default: Transparent

2.20.5 Max-Age

Dieser Wert bestimmt die Zeit (in Sekunden), nach der eine Bridge über Spanning Tree empfangene Nachrichten als 'veraltet' verwirft. Damitt legt man fest, wie schnell der Spanning-Tree Algorithmus auf Änderungen z. B. durch fortgefallene Bridges reagiert. Es handelt sich hier um einen 16-Bit-Wert (0...65535).

SNMP-ID: 2.20.5

Pfad Telnet: /Setup/LAN-Bridge/Max-Age

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 20

2.20.6 Hello-Time

Dieser Parameter legt fest, in welchem zeitlichen Abstand in Sekunden ein als Root-Bridge ausgewähltes Gerät Informationen ins LAN schickt.

SNMP-ID: 2.20.6

Pfad Telnet: /Setup/LAN-Bridge/Hello-Time

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 2

2.20.7 Forward-Delay

Dieser Wert bestimmt die Zeit (in Sekunden), die mindestens vergeht, bevor ein Port von 'listening' nach 'learning' bzw. von 'learning' nach 'forwarding' wechseln darf. Seit es beim Rapid-Spanning-Tree jedoch eine Methode gibt, um festzustellen, wann ein Port in den 'Forwarding-Zustand' versetzt werden kann ohne lange zu warten, hat diese Einstellung in vielen Fällen keinen Effekt mehr.

SNMP-ID: 2.20.7

Pfad Telnet: /Setup/LAN-Bridge/Forward-Delay

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 6

2.20.8 Isolierter-Modus

Hier können die Verbindungen, zum Beispiel zwischen Layer-2 Forwarding und den LAN Schnittstellen an- oder ausgeschaltet werden.

SNMP-ID: 2.20.8

Pfad Telnet: /Setup/LAN-Bridge

Mögliche Werte:

- Bridge oder Router (Isolierter Modus)

Default: Bridge

Beachten Sie, dass andere konfigurierte Funktionen der Verbindung (wie zum Beispiel Spanning Tree, Packet Filters) bestehen bleiben / unabhängig davon, ob die Schnittstellen an- oder ausgeschaltet sind.

2.20.10 Protokoll-Tabelle

Hier können Sie Protokolle zur Verwendung durch die LAN-Bridge hinzufügen.

SNMP-ID: 2.20.10

Pfad Telnet: /Setup/LAN-Bridge

2.20.10.1 Name

Dieser Name sollte die Regel beschreiben. Beachten Sie, dass es sich hier gleichzeitig um die Inhaltsspalte (index column) der Tabelle handelt, d.h. der Tabelleninhalt ist eine Reihe (String).

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- max. 15 Zeichen

Default: leer

2.20.10.2 Protokoll

Hier wird die Kennung des Protokolls eingegeben. Die Kennung ist eine 4-stellige Hexadezimalzahl, die jedes Protokoll eindeutig kennzeichnet. Einige häufig vorkommende Protokolle sind z. B. 0800, 0806 für IP und ARP (Internet), E0E0, 8137 für IPX (Novell Netware), F0F0 für NetBEUI (Windows Netzwerk) oder 809B, 80F3 für Apple Talk (Apple Netzwerk). Wenn Sie das Protokoll-Feld auf Null setzen, betrifft diese Regel alle Pakete. Weitere Protokolle entnehmen Sie bitte der Dokumentation.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- 4-stellige Hexadezimalzahl

Default: leer

2.20.10.3 Unterprotokoll

Geben Sie hier das Unter-Protokoll ein. Gängige Unterprotokolle innerhalb des IP-Protokolls (0800) sind z. B. 1 ICMP, 6 TCP, 17 UDP, 50 ESP (IPSec). Für ARP-Pakete gibt dieses Feld den ARP-Rahmen-Typ an (ARP request/reply, RARP request/reply). Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 Paket handelt und das IP-Protokoll (UDP, TCP, ICMP,...) auf den gegebenen Wert passt, oder wenn es ein ARP Paket ist und der gegebene Wert mit dem ARP-Typ übereinstimmt. Wenn das Protokoll-Feld gesetzt ist, jedoch das Unterprotokoll-Feld auf Null steht, trifft diese Regel auf alle Pakete des angegebenen Protokolls zu, z. B. auf alle IP-Pakete für Protokoll 0800. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.20.10.4 Port

Geben Sie hier für TCP- oder UDP-Protokolle den Port-Nummern-Bereich an. Beispielsweise entspricht der UDP-Port 500 dem bei IPSec verwendeten IKE.

Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 TCP oder ein UDP-Paket handelt oder die Quelle des Ziel-TCP/UDP-Ports in einem Bereich liegt, der durch diese beiden Werte definiert wird.

Falls Sie als End-Port eine Null angeben, gilt die Regel nur für den Anfangs-Port. Der Portnummern-Vergleich wird sowohl beim Empfangs- als auch beim Ziel-Port vorgenommen und eine Regel trifft zu, wenn auch nur einer der beiden im angegebenen Bereich liegt. Wenn das Protokoll- und das Unter-Protokoll-Feld gesetzt sind, jedoch die Port-Felder auf Null stehen, trifft diese Regel auf alle Pakete des angegebenen UnterProtokolls zu, z. B. auf alle Pakete für Protokoll 0800/6. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.20.10.5 Port-Ende

Geben Sie hier für TCP- oder UDP-Protokolle den Port-Nummern-Bereich an. Beispielsweise entspricht der UDP-Port 500 dem bei IPSec verwendeten IKE.

Wenn dieser Wert ungleich 0 ist, trifft die Regel nur zu, wenn es sich um ein IPv4 TCP oder ein UDP-Paket handelt oder die Quelle des Ziel-TCP/UDP-Ports in einem Bereich liegt, der durch diese beiden Werte definiert wird.

Falls Sie als End-Port eine Null angeben, gilt die Regel nur für den Anfangs-Port. Der Portnummern-Vergleich wird sowohl beim Empfangs- als auch beim Ziel-Port vorgenommen und eine Regel trifft zu, wenn auch nur einer der beiden im angegebenen Bereich liegt. Wenn das Protokoll- und das Unter-Protokoll-Feld gesetzt sind, jedoch die Port-Felder auf Null stehen, trifft diese Regel auf alle Pakete des angegebenen UnterProtokolls zu, z. B. auf alle Pakete für Protokoll 0800/6. Hinweis: Weitere Informationen finden Sie unter der URL www.iana.org, Rubrik "Protocol Number Assignment Services", Dokumente "Protocol Numbers" und "Port Numbers".

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- max. 65.535

Default: 0

2.20.10.6 Ifc-Liste

Diese Liste enthält die LAN-Interfaces, für welche die Regel angewendet wird. Die Syntax der Schnittstellen-Liste ist in Ergänzungen/Nachträgen/Anhängen angegeben.

In Abhängigkeit von den tatsächlich vorhandenen Interfaces können folgende vordefinierte Interface-beschreibende Bezeichner in einem Komma-separierten Ausdruck verwendet werden, um die betroffenen Interfaces zu spezifizieren:

- LAN-1,
- WLAN-1, WLAN-1-2, WLAN-1-3, WLAN-1-4, WLAN-1-5, WLAN-1-6, WLAN-1-7, WLAN-1-8, WLAN-2, WLAN-2-2, WLAN-2-3, WLAN-2-4, WLAN-2-5, WLAN-2-6, WLAN-2-7, WLAN-2-8,
- P2P-n-m ('n' bezeichnet die Schnittstelle des WLANs und 'm' die Nummer der P2P-Verbindung auf diesem WLAN).

Numerisch aufeinanderfolgende Interface-Bezeichner können durch folgende Notation verkürzt beschrieben werden: P2P-4~P2P-10. Wird hier kein Interface spezifiziert, wird die gewählte Aktion auch nie ausgeführt.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- alle LAN-Interfaces
- DMZ-Interfaces
- die logischen WLAN-Netze und die Point-to-Point-Strecken im WLAN

Default: leer

2.20.10.7 Aktion

Hier können Sie eine Aktion auswählen, die mit einem Paket durchgeführt wird, das dieser Regel entspricht. Mögliche Aktionen sind Übertragen, Verwerfen oder Umleiten. Im Falle einer Umleitung muss im darauffolgenden Feld angegeben werden, zu welcher IP-Adresse das Paket umgeleitet werden soll. Die Umleitungseigenschaft ist nur für Pakete möglich, die TCP, UDP oder ICMP "echo requests" unterstützen. Das Gerät kann die Ziel-MAC- und IP-Adresse verändern, bevor das Paket weitergeleitet und wird so eine Eingabe in die Connection-Tabelle vornehmen, die eine Übersetzung der möglichen Antworten erlaubt.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- Übertragen
- Verwerfen

- Umleiten

Default: Pakete verwerfen

2.20.10.8 Umleite-IP-Adresse

Falls die Regel eine Umleitungsregel darstellt, muss in diesem Feld angegeben werden, zu welcher IP-Adresse die passenden Pakete umgeleitet werden sollen.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0.

2.20.10.9 Ziel-MAC-Adr.

Hier wird die physikalische Adresse (MAC) einer Ziel-WLAN-Station eingegeben. Jede Netzwerkkarte hat eine eigene weltweit eindeutige MAC-Adresse. Diese Adresse ist eine 12stellige Hexadezimalzahl (z. B. 00A057010203). Sie finden diese Adresse meistens als Aufdruck auf der Netzwerkkarte selbst. Wenn Sie keine MAC-Adresse (oder 0) spezifizieren, betrifft diese Regel alle Pakete.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- 12-stellige Hexadezimalzahl

Default: leer

2.20.10.10 IP-Netzwerk

Wenn der Wert im ersten Feld ungleich 0.0.0.0 ist, trifft eine Regel auf ein Paket zu, wenn es sich um ein IPv4 Paket handelt und entweder die Quell- oder Zieladresse des Pakets im IP-Netzwerk vorkommt und durch diese beiden Werte definiert wird.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0.

2.20.10.11 IP-Netzmaske

Wenn der Wert im ersten Feld ungleich 0.0.0.0 ist, trifft eine Regel auf ein Paket zu, wenn es sich um ein IPv4 Paket handelt und entweder die Quell- oder Zieladresse des Pakets im IP-Netzwerk vorkommt und durch diese beiden Werte definiert wird.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0.

2.20.10.12 DHCP-Src-MAC

meine Übersetzung: Diese Einstellungsregel hängt von der Quelle der MAC-Adresse ab, da diese ihre IP-Adresse über DHCP zugewiesen bekommt.

Aus anderer Quelle (Aurelia): DHCP-Tracking auf einer bestimmten (W)LAN-Schnittstelle findet nur statt, wenn Protokollfilter für die Schnittstelle definiert wurden, die den Parameter "Per DHCP zugewiesene IP" auf Ja oder Nein eingestellt haben. Für eine Filterregel kann zusätzlich ein Netz spezifiziert werden. Wenn eine Regel allerdings den Parameter "Per DHCP zugewiesene IP" auf Ja eingestellt hat, wird ein eventuell angegebenes Netz ignoriert.

Pfad Telnet: /Setup/LAN-Bridge/Protokoll-Tabelle

Mögliche Werte:

- Irrelevant
- Nein
- Ja

Default: Irrelevant

2.20.11 Port-Daten

In dieser Tabelle kann man weitere Bridge-Parameter pro Port einstellen.

SNMP-ID: 2.20.11

Pfad Telnet: /Setup/LAN-Bridge

2.20.11.2 Port

Auswahl des Ports, für den die Spanning-Tree-Parameter eingestellt werden sollen.

SNMP-ID: 2.20.11.2

Pfad Telnet: /Setup/LAN-Bridge/Port-Daten

Mögliche Werte:

- Auswahl aus der Liste der logischen Schnittstellen des Geräts, z. B. LAN-1, WLAN-1 oder P2P-1-1

2.20.11.3 aktiv

Hier können Sie einen Port komplett sperren, d.h. der Port wird nie den Status disabled (gesperrt) verlassen.

SNMP-ID: 2.20.11.3

Pfad Telnet: /Setup/LAN-Bridge/Port-Daten

Mögliche Werte:

- aktiv
- inaktiv

Default: aktiviert

2.20.11.5 Bridge-Gruppe

Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu dieser logischen Interface über die LAN-Bridge. Durch die Zuordnung zu einer gemeinsamen Bridge-Gruppe können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für das Gerät wie ein einzelnes Interface – z. B. für die Nutzung im Zusammenhang mit Advanced Routing and Forwarding.

SNMP-ID: 2.20.11.5

Pfad Telnet: /Setup/LAN-Bridge/Port-Daten

Mögliche Werte:

- BRG-1 bis BRG-8
- keine

Default: BRG - 1

Besondere Werte: Wird das Interface über die Einstellung 'keine' aus allen Bridge-Gruppen entfernt, so findet keine Übertragung über die LAN-Bridge zwischen LAN und WLAN statt (isolierter Modus). In dieser Einstellung ist eine Datenübertragung zwischen LAN und WLAN für dieses Interface nur über den Router möglich.

Voraussetzung für die Datenübertragung von/zu einem logischen interface über die LAN-Bridge ist die Deaktivierung des globalen „Isolierten Modus“, der für die gesamte LAN-Bridge gilt. Außerdem muss das logische Interface einer Bridge-Gruppe zugeordnet sein – in der Einstellung 'keine' ist keine Übertragung über die LAN-Bridge möglich.

2.20.11.6 DHCP-Limit

Anzahl der Clients, die über DHCP zugewiesen werden können. Bei Überschreiten des Limits wird der jeweils älteste Eintrag verworfen. Dies kann in Kombination mit der Protokoll-Filter-Tabelle genutzt werden, um den Zugang auf ein logisches Interface zu begrenzen.

SNMP-ID: 2.20.11.6

Pfad Telnet: /Setup/LAN-Bridge/Port-Daten

Mögliche Werte:

- 0 bis 255

Default: 0

2.20.11.7 Point-To-Point-Port

Dieser Wert beschreibt die in der IEEE 802.1D definierte "adminPointToPointMAC"-Einstellmöglichkeit. Standardmäßig wird die "Point-to-Point"-Einstellung der LAN-Schnittstelle automatisch aufgrund der Technologie und des momentanen Status hergeleitet:

Ein Ethernet Port wird als P2P-Port angenommen, wenn er im Full-Duplex-Modus betrieben wird.

Ein Token Ring Port wird als P2P-Port angenommen, wenn er im Full-Duplex-Modus betrieben wird.

Eine WLAN SSID wird niemals als P2PPort betrachtet.

Eine WLAN P2P-Verbindung wird immer als P2P-Port angenommen.

Es ist jedoch möglich diese automatisch getroffene Einstellung zu revidieren, falls diese z. B. nicht brauchbar für die vorliegende Konfiguration erscheint. Schnittstellen im "Point-to-Point"-Modus haben besondere Fähigkeiten, die benutzt werden können um z. B. im Rapid-Spanning-Tree-Verfahren die Port-Status-Wechsel zu beschleunigen.

SNMP-ID: 2.20.11.7

Pfad Telnet: /Setup/LAN-Bridge/Port-Daten

Mögliche Werte:

- automatisch
- ein
- aus

Default: automatisch

2.20.11.9 Privater-Modus

Sie haben die Möglichkeit, für jede einzelne Schnittstelle den privaten Modus zu aktivieren oder zu deaktivieren.

Pfad Telnet:

Setup > **LAN-Bridge** > **Port-Daten**

Mögliche Werte:

nein
Der private Modus ist deaktiviert.

ja
Der private Modus ist aktiviert.

Default-Wert:

nein

2.20.12 Alterungs-Zeit

Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Der Wert der maximalen Gültigkeit kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf. Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeitsdauer der Wert der Standard Gültigkeit zugewiesen.

SNMP-ID: 2.20.12

Pfad Telnet: /Setup/LAN-Bridge

Mögliche Werte:

- 1 bis 99.999 Minuten

Default: max. Gültigkeit: 6.000 Min., Standard Gültigkeit: 500 Min.

2.20.13 Prioritaets-Zuordnung

Ordnen Sie über diese Tabelle jedem zu sendenden IP-Paket anhand eines ToS/DSCP-Wertes eine User-Priority gemäß 802.1D zu. Das Gerät nutzt die User-Priority z. B. im WLAN bei aktiviertem QoS, um Pakete einzelnen Access Categories zuzuordnen (Voice/Video/Best-Effort/Background).

Pfad Telnet: /Setup/LAN-Bridge/Prioritaets-Zuordnung

2.20.13.1 Name

Geben Sie hier einen Namen für eine Kombination von DSCP-Wert und Priorität an.

Pfad Telnet: /Setup/LAN-Bridge/Prioritaets-Zuordnung/Name

Mögliche Werte:

- maximal 16 alphanumerische Zeichen

Default: leer

2.20.13.2 DSCP-Wert

Geben Sie hier den DSCP-Wert an, der für diese Prioritätszuordnung verwendet wird.

Pfad Telnet: /Setup/LAN-Bridge/Prioritaets-Zuordnung/DSCP-Wert

Mögliche Werte:

- Numerische Zeichen von 0 bis 255

Default: 0

2.20.13.3 Prioritaet

Geben Sie hier die Priorität an, die für diese Prioritätszuordnung verwendet wird.

Pfad Telnet: /Setup/LAN-Bridge/Prioritaets-Zuordnung/Prioritaet

Mögliche Werte:

- Best-Effort
- Background
- Two
- Excellent-Erffort
- Controlled-Latency
- Video
- Voice
- Network-Control

Default: Best-Effort

2.20.20 Spannning-Tree

Dieses Menü enthält die Einstellungen des Spanning-Tree.

SNMP-ID: 2.20.20

Pfad Telnet: /Setup/LAN-Bridge

2.20.20.1 Aktiv

Hier können Sie die Unterstützung für Spanning-Tree ein- und ausschalten. Bei ausgeschaltetem Spanning-Tree verschickt der Router keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete weiter, anstatt sie selber zu verarbeiten.

SNMP-ID: 2.20.20.1

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- aktiv
- inaktiv

Default: deaktiviert

2.20.20.2 Bridge-Priotitaet

Dieser Wert legt die Priorität der Bridge im LAN fest. Man kann damit beeeinflußen, welche Bridge vom Spanning-Tree-Protokoll bevorzugt zur Root-Bridge gemacht wird. Es handelt sich hier um einen 16-Bit-Wert (0…65535), wobei höhere Werte eine niedrigere Priorität bedeuten. Eine Änderung des voreingestellten Wertes sollte nur erfolgen, wenn eine bestimmte Bridge bevorzugt werden soll. Auch mit gleichen Werten funktioniert das Auswahlverfahren, da die MAC-Adresse der Bridge bei gleicher Priorität zur Entscheidung herangezogen wird. Obwohl für die Konfiguration eines Parameters ein ganzer 16-Bit Wert zur Verfügung steht, sollte bei neueren Versionen des Rapid- bzw. Multiple-Spanning-Tree Protokolls darauf geachtet werden, den Prioritätswert nur in Schritten von 4096 zu verändern, da hier die unteren 12-Bit für andere Zwecke verwendet werden und deshalb von künftigen Firmware-Releases vielleicht ignoriert werden könnten.

SNMP-ID: 2.20.20.2

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- max. 65.535

Default: 32768

2.20.20.5 Max-Age

Dieser Wert bestimmt die Zeit (in Sekunden) nach der eine Bridge über Spanning Tree empfangene Nachrichten als "veraltet" verwirft. Man legt damit folglich fest, wie schnell der Spanning-Tree Algorithmus auf Änderungen z. B. durch fortgefallene Bridges reagiert.

SNMP-ID: 2.20.20.5

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- max. 65535 Sekunden

Default: 20 Sekunden

2.20.20.6 12 Sekunden

Die Hello-Zeit legt fest, in welchem Intervall (in Sekunden) die Root-Bridge Informationen ins LAN schickt. Beachte, dass die Non-Root-Bridge Werte der Root-Bridge übernehmen kann. Daher kann der Wert, abhängig von der Struktur des Netzwerks ignoriert werden.

SNMP-ID: 2.20.20.6

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- max. 32768 Sekunden

Default: 2 Sekunden

2.20.20.7 Forward-Delay

Bestimmt die Zeit (in Sekunden) die mindestens vergehen muss, bevor ein Port von "listening" auf "learning" bzw. von "learning" auf "forwarding" wechseln darf. Seit es beim Rapid-Spanning-Tree jedoch eine Methode gibt um festzustellen, wann ein Port in den "Forwarding-Zustand" versetzt werden kann ohne lange zu warten, hat diese Einstellung in vielen Fällen keinen Effekt mehr." Ändern Sie diesen Wert ohne ausreichendes Wissen über Spanning-Trees nicht, da er das Risiko einer vorübergehenden Schleife im Netzwerk beeinflusst.

SNMP-ID: 2.20.20.7

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- max. 32768 Sekunden

Default: 6 Sekunden

2.20.20.11 Port-Daten

In dieser Tabelle kann man weitere Spanning-Tree-Parameter pro Port einstellen.

SNMP-ID: 2.20.20.11

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

2.20.20.11.2 Port

Der Name der LAN-Schnittstelle.

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

2.20.20.11.4 Priorität

Die Priorität des Ports, vorliegend als 8-Bit Wert. Wenn mehr als ein Port verfügbar ist als Pfad zu einem LAN, und die Pfade zu beiden Ports die gleiche Länge haben, dann fungiert dieser Wert als Entscheidungsregel um einen Port auszuwählen. Wenn zwei Ports die gleiche Priorität haben, dann wird der Port mit der kleineren Nummer ausgewählt.

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

Mögliche Werte:

- max. 255

Default: 128

Für Rapid-Spanning-Tree benutzt das Gerät nur die oberen 4 Bits dieses Wertes, z. B. wenn ein Wert sich in 16 Schritten erhöht und erniedrigt. Niedriger Werte bringen eine höhere Priorität.

2.20.20.11.6 Kanten-Port

Ein Port kann als Edge-Port gekennzeichnet werden

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

Mögliche Werte:

- an
- aus

Default: Kennzeichnung aus

2.20.20.11.7 Pfadkosten-Uebersteuerung

Gibt die Pfadkosten-Beeinflussung an.

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree/Port-Daten

Mögliche Werte:

- max. 4.294.967.295

Default: 0

2.20.20.12 Protokoll-Version

Hier kann das Protokoll gewählt werden. Je nach Wahl wird entweder das Classic- oder das Rapid-Protokoll verwendet, welche in der IEE 802.1D-1998 chapter 8 bzw. in der IEEE 802.1D-2004 chapter 17 definiert ist.

SNMP-ID: 2.20.20.12

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- classic
- rapid

Default: classic

Beachten Sie die Aufwärtskompatibilität dieses Protokolls. Wird eine Komponente erkannt die kein Rapid-Spanning-Tree unterstützt, werden automatisch Classic-Spannning-Tree Datenelemente und Methoden verwendet.

2.20.20.13 Transmit-Hold-Count

Bestimmt die Anzahl BPDUs (Bridge-Protocol-Data-Units), die bei der Verwendung von Rapid-Spanning-Tree gesendet werden dürfen, bevor eine Sekunde Pause eingelegt wird. (Bei Classic-Spanning-Tree hat dieser Wert keinen Einfluss.)

SNMP-ID: 2.20.20.13

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- max. 999

Default: 6

2.20.20.14 Pfadkosten-Berechnung

Hier kann eingestellt werden, nach welchem Protokoll die Pfadkosten berechnet werden. Während beim Rapid-Spanning-Tree Verfahren der volle 32-Bit Wertebereich ausgenutzt wird, findet beim Classic-Algorithmus nur ein 16-Bit Wertebereich Anwendung. Das Rapid-Spanning-Tree Verfahren ist aber nur sinnvoll, wenn es von allen Bridges im Netzwerk unterstützt wird und auch bei allen konsistent konfiguriert ist.

SNMP-ID: 2.20.20.14

Pfad Telnet: /Setup/LAN-Bridge/Spanning-Tree

Mögliche Werte:

- classic
- rapid

Default: classic

2.20.30 IGMP-Snooping

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

2.20.30.1 In-Betrieb

Aktiviert oder deaktiviert IGMP-Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP-Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicasts auf alle Ports weiter.

Wenn diese Funktion deaktiviert ist, sendet die Bridge alle IP-Multicast-Pakete auf alle Ports. Bei einer Änderung des Betriebszustandes setzt das Gerät die IGMP-Snooping-Funktion vollständig zurück, d. h. es löscht alle dynamisch gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften).

Pfad Telnet:

Setup > **LAN-Bridge** > **IGMP-Snooping**

Mögliche Werte:

nein

ja

Auto

Default:

nein

2.20.30.2 Port-Einstellungen

In dieser Tabelle werden die Port-bezogenen Einstellungen für IGMP Snooping vorgenommen.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

2.20.30.2.1 Port

Auf diesen Port beziehen sich die Einstellungen.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Port-Einstellungen/Port

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports

2.20.30.2.2 Router-Port

Diese Option definiert das Verhalten des Ports.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Port-Einstellungen/Router-Port

Mögliche Werte:

- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die auf diesem Port evtl. empfangen werden.
- Auto: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn für die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfangen wurden.

Default: Auto

2.20.30.3 Unregistrierte-Datenpakete-Behandlung

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches "224.0.0.x", für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Mögliche Werte:

- Nur-Router-Ports: Sendet diese Pakete an alle Router-Ports.
- Fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

Default: Nur-Router-Ports

2.20.30.4 Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können mehrere unabhängige Querier definiert werden, welche dann die entsprechenden VLAN-IDs nutzen.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default: Leer

In-Betrieb

Aktiviert oder deaktiviert die Querier-Instanz.

Mögliche Werte:

- Ja
- Nein

Default: Nein

Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen, keine.

Default: keine

Besondere Werte: Wenn “keine” Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

VLAN-Id

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096.

Default: 0

Besondere Werte: Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

2.20.30.4.1 Name

Name der Querier-Instanz.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/Name

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default: Leer

2.20.30.4.2 In-Betrieb

Aktiviert oder deaktiviert die Querier-Instanz.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/In-Betrieb

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.20.30.4.3 Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/Bridge-Gruppe

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen
- keine.

Besondere Werte: Wenn “keine” Bridge-Gruppe gewählt wird, werden die IGMP-Anfragen auf allen Brigde-Gruppen ausgegeben.

Default: keine

2.20.30.4.4 VLAN-Id

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Simulierte-Anfrager/VLAN-Id

Mögliche Werte:

- 0 bis 4096

Besondere Werte: Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Default: 0

2.20.30.5 Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse 224.0.0.1 schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen “altern” und gelöscht werden.

Ein Querier sendet nach der Anfangsphase IGMP-Anfragen in diesem Intervall.

Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von “Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)”.

Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von “Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)”.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0

Default: 125

Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

2.20.30.6 Anfrage-Antwort-Intervall

Intervall in Sekunden, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen “altern” und gelöscht werden.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0

Default: 10

Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

2.20.30.7 Robustheit

Dieser Wert bestimmt die Robustheit des IGMP-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0

Default: 2

2.20.30.8 Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z. B. nicht automatisch gelernt werden können oder sollen.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse

Default: Leer

VLAN-Id

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

Mögliche Werte:

- 0 bis 4096

Default: 0

Besondere Werte: Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Lernen-erlauben

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

Mögliche Werte:

- Ja
- Nein

Default: Ja

Statische-Mitglieder

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen

Default: Leer

2.20.30.8.1 Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Adresse

Mögliche Werte:

- Gültige IP-Multicast-Adresse

Default: Leer

2.20.30.8.2 Statische-Mitglieder

An diese Ports werden die Pakete mit der entsprechenden IP-Multicast-Adresse immer zugestellt, unabhängig von empfangenen Join-Nachrichten.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Statische-Mitglieder

Mögliche Werte:

- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen

Default: Leer

2.20.30.8.3 VLAN-Id

Die VLAN-ID, auf welche diese statische Mitgliedschaft angewendet werden soll. Für eine IP-Multicast-Adresse können durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs gemacht werden.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/VLAN-Id

Mögliche Werte:

- 0 bis 4096

Besondere Werte: Wenn "0" als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Default: 0

2.20.30.8.4 Lernen-erlauben

Mit dieser Option wird das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe aktiviert. Wenn das automatische Lernen deaktiviert ist, werden die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports verschickt.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping/Statische-Mitglieder/Lernen-erlauben

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.20.30.9 Werbe-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP Snooping-fähige Geräte schneller lernen, welche ihrer Ports als Router-Ports verwendet werden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende

Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP-Anfragen.

Pfad Telnet: /Setup/LAN-Bridge/IGMP-Snooping

Webconfig englisch: Setup/LAN-Bridge/IGMP-Snooping

Mögliche Werte:

- 4 bis 180 Sekunden

Default: 20

2.20.40 DHCP-Snooping

Hier können Sie das DHCP-Snooping je Schnittstelle konfigurieren.

Pfad Telnet:

Setup > **LAN-Bridge**

2.20.40.1 Port

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

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen

WLAN-x
Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen

P2P-x-x
Alle logischen P2P-Schnittstellen

WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

2.20.40.2 Agent-Info-hinzufuegen

Bestimmen Sie hier, ob der DHCP-Relay-Agent den ankommenden DHCP-Paketen die DHCP-Option "Relay Agent Info" (Option 82) anfügen bzw. eine vorhandene "Relay Agent Info" bearbeiten soll, bevor er die Anfrage an einen DHCP-Server weiterleitet.

Mit dieser Option übermittelt der Relay-Agent dem DHCP-Server zusätzliche Informationen über die Schnittstelle, über die der Client die Anfrage gestellt hat.

Die "Relay Agent Info" setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Sollten diese beiden Felder leer sein, fügt der DHCP-Relay-Agent auch keine "Relay Agent Info" in die Datenpakete ein.

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

Ja

Fügt den DHCP-Paketen die "Relay Agent Info" an.

Nein

Diese Einstellung deaktiviert das DHCP-Snooping für diese Schnittstelle.

Default-Wert:

Nein

2.20.40.3 Behandle-existierendes-Agent-Info

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

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

beibehalten

In dieser Einstellung leitet der DHCP-Relay-Agent ein DHCP-Paket mit vorhandener "Relay Agent Info" ohne Veränderung an den DHCP-Server weiter.

ersetzen

In dieser Einstellung ersetzt der DHCP-Relay-Agent eine vorhandene "Relay Agent Info" durch die in den Feldern **Remote-Id** und **Circuit-Id** vorgegebenen Werte.

verwerfen

In dieser Einstellung löscht der DHCP-Relay-Agent ein DHCP-Paket, das eine "Relay Agent Info" enthält.

Default-Wert:

beibehalten

2.20.40.4 Remote-Id

Die Remote-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig den Client, der einen DHCP-Request stellt.

Sie können die folgenden Variablen verwenden:

- `%%`: fügt ein Prozent-Zeichen ein.
- `%c`: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- `%i`: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- `%n`: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.

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

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

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

Default-Wert:

leer

2.20.40.5 Circuit-Id

Die Circuit-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen DHCP-Request stellt.

Sie können die folgenden Variablen verwenden:

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

Pfad Telnet:

Setup > **LAN-Bridge** > **DHCP-Snooping**

Mögliche Werte:

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

Default-Wert:

leer

2.20.41 DHCPv6-Snooping

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

Pfad Telnet:

Setup > **LAN-Bridge**

2.20.41.1 Port

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

Pfad Telnet:

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

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen

WLAN-x
Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen

P2P-x-x
Alle logischen P2P-Schnittstellen

WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

2.20.41.2 Orientierung

Aktivieren bzw. deaktivieren Sie hier das DHCPv6-Snooping.

Pfad Telnet:

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

Mögliche Werte:

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

Client-seitig
Aktiviert das DHCPv6-Snooping für dieses Interface.

Default-Wert:

Netz-seitig

2.20.41.3 Typ

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

Pfad Telnet:

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

Mögliche Werte:

vertrauenswuerdig

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

nicht-vertrauenswuerdig

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

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

Default-Wert:

vertrauenswuerdig

2.20.41.4 Remote-Id

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

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

Sie können die folgenden Variablen verwenden:

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.20.41.5 Interface-Id

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

Sie können die folgenden Variablen verwenden:

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.20.41.6 Server-Adresse

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

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

Pfad Telnet:

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

Mögliche Werte:

max. 39 Zeichen `0123456789ABCDEFabcdef:.`

Default-Wert:

leer

2.20.42 RA-Snooping

Hier können Sie den das RA-Snooping konfigurieren.

Pfad Telnet:

Setup > **LAN-Bridge**

2.20.42.1 Port

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

Pfad Telnet:

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

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen

WLAN-x
Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen

P2P-x-x
Alle logischen P2P-Schnittstellen

WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

2.20.42.3 Orientierung

Bestimmen Sie hier den bevorzugten Schnittstellen-Typ.

Pfad Telnet:

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

Mögliche Werte:

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

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

Default-Wert:

Router

2.20.42.4 Router-Adresse

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

Pfad Telnet:

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

Mögliche Werte:

max. 39 Zeichen `0123456789ABCDEFabcdef:.`

Default-Wert:

leer

2.20.43 PPPoE-Snooping

Hier konfigurieren Sie das PPPoE-Snooping je Schnittstelle.

Pfad Telnet:

Setup > **LAN-Bridge**

2.20.43.1 Port

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

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen

WLAN-x
Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen

P2P-x-x
Alle logischen P2P-Schnittstellen

WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

GRE-TUNNEL-x
Alle virtuellen GRE-Tunnel

2.20.43.2 Agent-Info-hinzufuegen

Bestimmen Sie hier, ob der PPPoE-Intermediate-Agent den ankommenden PPPoE-Paketen einen Hersteller spezifischen PPPoE-Tag mit Vendor-ID „3561“ hinzufügen soll, bevor er die Anfrage an einen PPPoE-Server weiterleitet.

Mit dieser Option übermittelt der PPPoE-Intermediate-Agent dem PPPoE-Server zusätzliche Informationen über die Schnittstelle, über die der Client die Anfrage gestellt hat.

Der PPPoE-Tag setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Sollten diese beiden Felder leer sein, fügt der PPPoE-Intermediate-Agent auch keinen PPPoE-Tag in die Datenpakete ein.

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

Ja

Fügt den PPPoE-Paketen die „Relay Agent Info“ an.

Nein

Diese Einstellung deaktiviert das PPPoE-Snooping für diese Schnittstelle.

Default-Wert:

Nein

2.20.43.3 Remote-Id

Die Remote-ID ist eine Unteroption der PPPoE-Intermediate-Agent-Option und kennzeichnet eindeutig den Client, der einen PPPoE-Request stellt.

Sie können die folgenden Variablen verwenden:

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

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

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

Default-Wert:

leer

2.20.43.4 Circuit-Id

Die Circuit-ID ist eine Unteroption der PPPoE-Intermediate-Agent-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen PPPoE-Request stellt.

Sie können die folgenden Variablen verwenden:

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

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

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

Default-Wert:

leer

2.20.43.5 verwerfe-Server-Pakete

Hier bestimmen Sie, ob der PPPoE-Intermediate-Agent bereits vorhandene PPPoE-Tags behalten oder verwerfen soll.

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

Ja

Der PPPoE-Intermediate-Agent entfernt vorhandene PPPoE-Tags und lässt sowohl „Circuit-ID“ als auch „Remote-ID“ leer.

Nein

Der PPPoE-Intermediate-Agent übernimmt vorhandene PPPoE-Tags.

Default-Wert:

Nein

2.21 HTTP

Dieses Menü enthält die Einstellungen des HTTP.

SNMP-ID: 2.21

Pfad Telnet: /Setup

2.21.1 Dokumentenwurzel

Dieser Parameter definiert den Pfad zu einem Verzeichnis, in dem die Hilfe für WEBconfig lokal gespeichert ist.

SNMP-ID: 2.21.1

Pfad Telnet: /Setup/HTTP/Dokumentenwurzel

Mögliche Werte:

- maximal 99 alphanumerische Zeichen

Default: leer

Dieser Parameter ist für die zukünftige, lokale Nutzung der WEBconfig-Hilfe vorgesehen. In aktuellen Firmware-Versionen ist dieser Parameter ohne Funktion.

2.21.2 Seitenueberschriften

Mit dieser Einstellung wählen Sie aus, ob bei der Darstellung der HTTP-Seiten des Public Spot Überschriften als Texte oder als Bilder angezeigt werden.

SNMP-ID: 2.21.2

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- Bilder
- Texte

Default: Bilder

Die Einstellungen für die Seitenüberschriften werden nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.21.3 Schrift-Familie

Schrift-Familie zur Darstellung der Weboberfläche.

SNMP-ID: 2.21.3

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- max. 39 Zeichen

Default:

- helvetica
- sans-serif

2.21.5 Seitenueberschriften

Wählen Sie hier aus, ob der Public Spot die Überschriften in den Standard-Seiten als Text oder als Grafiken anzeigt.

Pfad Telnet: /Setup/HTTP/Seitenueberschriften

Mögliche Werte:

- Bilder
- Texte

Default: Bilder

2.21.6 Fehlerseiten-Stil

Normale Fehlerseite oder Bluescreen

SNMP-ID: 2.21.6

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- Standard
- Nifty

2.21.7 Port

Port für die HTTP-Server-Verbindung

SNMP-ID: 2.21.7

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- max. 5 Zeichen

Default: 80

2.21.9 Max.-Tunnel-Verbindungen

max. Anzahl der gleichzeitig aktiven HTTP-Tunnel.

SNMP-ID: 2.21.9

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- max. 255 Tunnel.

Default: 3

2.21.10 Tunnel-Idle-Timeout

Lebensdauer eines Tunnels ohne Aktivität. Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

SNMP-ID: 2.21.10

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- max. 4294967295 Sekunden.

Default: 300

2.21.11 Sitzungs-Timeout

Gültigkeitsdauer der Webconfig-Sitzung ohne Benutzeraktivität in Sekunden. Nach Ablauf dieser Zeit wird erneut das Kennwort abgefragt.

SNMP-ID: 2.21.11

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- max. 10 Zeichen

Default: 600

2.21.13 Standard-Design

Wählt das Design, das standardmäßig für die Anzeige von WEBconfig verwendet wird.

SNMP-ID: 2.21.13

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- Normales_Design
- Design_für_kleine_Auflösungen
- Design_mit_hohem_Kontrast

Default: Normales_Design

2.21.14 Geräteinformation-anzeigen

In dieser Tabelle wird definiert, welche Systeminformationen auf der Seite Systeminformation/Gerätestatus in Webconfig angezeigt werden.

SNMP-ID: 2.21.14

Pfad Telnet: /Setup/HTTP

2.21.14.1 Geräte-Information

Auswahl der Geräteinformationen, die im Webconfig angezeigt werden sollen.

Pfad Telnet:

Setup > **HTTP** > **Geräteinformation-anzeigen**

Mögliche Werte:

CPU
Speicher
UMTS/Modem-Schnittstelle
Ethernet-Ports
P2P-Verbindungen
Durchsatz(Ethernet)
Router
Firewall
DHCP
DNS
VPN
Verbindungen
Uhrzeit
IPv4-Adressen
IPv6-Adressen
IPv6-Praefixe
DHCPv6-Client
DHCPv6-Server
Betriebszeit
ADSL
ISDN
DSLoL

2.21.14.2 Position

Index für die Reihenfolge der Anzeige der Geräteinformationen.

Pfad Telnet: /Setup/HTTP/Geräteinformation-anzeigen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.21.15 HTTP-Kompression

Zur schnelleren Anzeige werden die Inhalte von WEBconfig komprimiert. Für Browser, welche die Kompression nicht unterstützen, kann die Kompression deaktiviert werden.

SNMP-ID: 2.21.15

Pfad Telnet: /Setup/HTTP

Mögliche Werte:

- Aktiviert
- Deaktiviert
- Nur_für_WAN

Default: Aktiviert

2.21.16 Server-Ports-offen-halten

In diesem Menü finden Sie die Parameter zum Einschränken des Zugriffs auf Web-Server-Dienste.

Pfad Telnet: /Setup/HTTP/Server-Ports-offen-halten

2.21.16.1 Ifc.

Wählen Sie hier den Zugangsweg aus, für den Sie den Zugang zu den Web-Server-Diensten einstellen möchten.

Pfad Telnet: /Setup/HTTP/Server-Ports-offen-halten/Ifc.

Mögliche Werte:

- Alle im Gerät verfügbaren Zugangswege (je nach Modell z. B. LAN, WAN, WLAN).

Default: Leer

2.21.16.2 Server-Ports-offen-halten

Der Zugriff auf ein Gerät über HTTP für die Konfiguration kann generell erlaubt, nicht erlaubt oder auf nur lesen eingeschränkt werden. Unabhängig davon kann der Zugriff auf die Web-Server-Dienste separat geregelt werden, z. B. um die Kommunikation von CAPWAP, SSL-VPN oder SCEP-CA über HTTP(S) zu ermöglichen, auch wenn der HTTP(S)-Zugang generell nicht erlaubt ist.

Für jeden Zugriffsweg (je nach Gerät LAN, WAN, WLAN) stellen Sie hier das Zugriffsrecht von Web-Server-Diensten des Gerätes auf den HTTP-Server-Port ein.

Pfad Telnet: /Setup/HTTP/Server-Ports-offen-halten/Server-Ports-offen-halten

Mögliche Werte:

- Automatisch: Der HTTP-Server-Port ist offen, solange ein Dienst angemeldet ist (z. B. CAPWAP). Ist kein Dienst mehr angemeldet, wird der Server-Port geschlossen.
- Aktiviert: Der HTTP-Server-Port ist immer offen, auch wenn der Zugriff auf die Konfiguration über HTTP nicht erlaubt ist. Hiermit kann der direkte Konfigurationszugriff unterbunden werden, jedoch die automatische Konfiguration von APs über einen WLAN-Controller weiterhin erlaubt werden.
- Deaktiviert: Der HTTP-Server-Port ist geschlossen, so dass kein Dienst den Web-Server benutzen kann. Wenn der Zugriff auf die Konfiguration über HTTP erlaubt ist, wird mit der entsprechenden Meldung quittiert, dass der Web-Server nicht erreichbar ist.

Default: Automatisch

2.21.20 Rollout-Wizard

Dieses Menü enthält die Einstellungen des Rollout-Wizards.

SNMP-ID: 2.21.20

Pfad Telnet: /Setup/HTTP

2.21.20.1 In-Betrieb

Schaltet den Rollout-Assistenten ein oder aus. Nach dem Einschalten wird der Assistent auf der Startseite von WEBconfig angeboten.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Mögliche Werte:

nein

ja

Default:

nein

2.21.20.2 Titel

Name für den Rollout-Assistenten, wie er im Navigationsbaum unter **Setup-Wizards** von WEBconfig angezeigt wird.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Mögliche Werte:

Beliebiger String, max. 50 Zeichen aus

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

Default:

Rollout

2.21.20.8 Benutze-Zusatzpruefungen

Diese Option aktiviert einige Konsistenz-Tests, die interne Aspekte des Assistenten püfen.

Die Ausführung der Zusatzprüfungen ist sehr zeitaufwändig. Aktivieren Sie diese Option nur während der Entwicklung des Assistenten und deaktivieren Sie diese Option für den normalen Betrieb.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Mögliche Werte:

nein

ja

Default:

nein

2.21.20.9 Vorbelegungen

Über diese Tabelle haben Sie die Möglichkeit, alle Parameter, die der Default-Rollout-Assistent standardmäßig abfragt, mit vorgegebenen Werten zu belegen. So konfigurierte Parameter werden beim Ausführen des Default-Rollout-Assistenten anschließend übergangen und nicht mehr abgefragt.

Eine 'leere' Vorbelegung bei den Werten **Port** und **Quell-Loopback-Adresse** wertet das Gerät als Eintrag 'Auto'. In diesem Fall benutzt der Default-Rollout-Assistent den entsprechenden HTTP(S)-Standard-Port sowie als Loopback-Adresse die zum Ziel passende Adresse Ihres Gerätes. Wenn Sie mit verschiedenen ARF-Netzen arbeiten, müssen Sie über die Loopback-Adresse das ARF angeben, in dem der LSR-Server erreichbar ist.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

2.21.20.9.1 Name

Dieser Eintrag zeigt den Namen des Parameters, der sich mit vorbelegten Werten füllen lässt.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

2.21.20.9.2 Vorbelegung

Dieser Eintrag zeigt den Wert, mit dem der betreffende Parameter im Rollout-Assistenten vorbelegt wird.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

Mögliche Werte:

Beliebiger String, max. 127 Zeichen aus

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

Default:

2.21.20.9.2 Benutze-Vorbelegung

Über diesen Eintrag legen Sie fest, ob das Gerät den vom Rollout-Wizard abgefragten Parameter automatisch mit dem hier konfigurierten Inhalt vorbelegt. Dieser Parameter wird dann nicht mehr im Rollout-Wizard abgefragt.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard** > **Vorbelegungen**

Mögliche Werte:

nein

ja

Default:

(zeilenabhängig)

2.21.20.10 Loesche-Assistent

Über diese Aktion löschen Sie einen benutzerdefinierten Rollout-Assistenten. Das Gerät verwendet dann den LCOS-internen Default-Assistenten, wenn Sie den Rollout-Assistenten aktivieren.

Pfad Telnet:

Setup > **HTTP** > **Rollout-Wizard**

Mögliche Parameter:

Keine Parameter vorhanden

2.21.21 Max-Anzahl-HTTP-Jobs

Über diese Einstellung legen Sie die maximale Anzahl der HTTP-Jobs fest. Ein HTTP-Job ist ein Job im LCOS, der eine HTTP-Verbindung von einem Client bedient, z. B. in Form einer Anfrage an die WEBconfig. Die Einstellung definiert somit die maximale Anzahl gleichzeitiger HTTP-Verbindungen.

Pfad Telnet:

Setup > **HTTP**

Mögliche Werte:

5 bis 512

Default:

Geräteabhängig

2.21.30 Datei-Server

Dieses Menü beinhaltet die Einstellungen zum Fileserver für externe USB-Medien.

SNMP-ID: 2.21.30

Pfad Telnet: /Setup/HTTP/Datei-Server

2.21.30.1 Oeffentliches-Unterverzeichnis

Dieses Verzeichnis ist das root-Verzeichnis auf einem USB-Medium. Das Gerät ignoriert alle anderen Dateien auf dem USB-Medium .

Pfad Telnet: /Setup/HTTP/Datei-Server/Oeffentliches-Unterverzeichnis

Mögliche Werte:

- maximal 64 alphanumerische Zeichen

Default: public_html

2.21.30.2 In-Betrieb

Aktivieren oder deaktivieren Sie mit diesem Parameter den File-Server für USB-Medien.

Pfad Telnet: /Setup/HTTP/Datei-Server/In-Betrieb

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.21.40 SSL

Hier werden die Parameter für HTTPS-Verbindungen festgelegt.

Pfad Telnet:

Setup > **HTTP**

2.21.40.3 Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

Pfad Telnet:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

2.21.40.4 Schluesselaustausch-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

2.21.40.5 Krypto-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.21.40.6 Hash-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

2.21.40.7 PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

Pfad Telnet:

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

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

2.21.40.8 Neuverhandlungen

Mit dieser Einstellung steuern Sie, ob der Client eine Neuverhandlung von SSL/TLS auslösen kann.

Pfad Telnet:

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

Mögliche Werte:

verboten
Das Gerät bricht die Verbindung zur Gegenstelle ab, falls diese eine Neuverhandlung anfordert.

erlaubt
Das Gerät lässt Neuverhandlungen mit der Gegenstelle zu.

ignoriert
Das Gerät ignoriert die Anforderung der Gegenseite zur Neuverhandlung.

Default-Wert:

erlaubt

2.21.40.10 Port

Port für die HTTPS-Server-Verbindung.

Pfad Telnet:

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

Mögliche Werte:

0 … 65535

Default-Wert:

443

2.21.40.11 Verwende-benutzer-geliefertes-Zertifikat

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

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.22 SYSLOG

Dieses Menü enthält die Einstellungen des SYSLOGs.

SNMP-ID: 2.22

Pfad Telnet: /Setup

2.22.1 Aktiv

Aktiviert den Versand von Informationen über Systemereignisse an die konfigurierten SYSLOG-Clients.

SNMP-ID: 2.22.1

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.22.2 Tabelle-SYSLOG

In dieser Tabelle werden die SYSLOG-Clients definiert.

SNMP-ID: 2.22.2

Pfad Telnet: /Setup/SYSLOG

2.22.2.1 Idx.

Position des Eintrags in der Tabelle.

SNMP-ID: 2.22.2.1

Pfad Telnet: /Setup/SYSLOG/Tabelle-SYSLOG

Mögliche Werte:

- max. 4 Zeichen

Default: Leer

2.22.2.2 IP-Adresse

IP-Adresse des SYSLOG-Clients.

SNMP-ID: 2.22.2.2

Pfad Telnet: /Setup/SYSLOG/Tabelle-SYSLOG

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.22.2.3 Quelle

Quelle, die zum Versenden einer Meldung führt. Jede Quelle wird durch einen bestimmten Code dargestellt.

SNMP-ID: 2.22.2.3

Pfad Telnet: /Setup/SYSLOG/Tabelle-SYSLOG

Mögliche Werte:

- Systemzeit: 01
- Konsolen-Logins: 02
- Systemzeit: 04
- Logins: 08
- Verbindungen: 10
- Accounting: 20
- Verwaltung: 40
- Router: 80

Default: 00

Besondere Werte: 00: Es wird keine Quelle spezifiziert.

2.22.2.4 Level

SYSLOG-Level, mit dem die Meldung verschickt wird. Jedes Level wird durch einen bestimmten Code dargestellt.

SNMP-ID: 2.22.2.4

Pfad Telnet: /Setup/SYSLOG/Tabelle-SYSLOG

Mögliche Werte:

- Alarm: 01
- Fehler: 02
- Warning: 04
- Information: 08
- Debug: 10

Default: 00

Besondere Werte: 00: Es wird kein Level spezifiziert.

2.22.2.6 Loopback-Addr.

Absenderadresse, die in den die SYSLOG-Meldung eingetragen wird. Auf SYSLOG-Meldungen werden keine Antworten erwartet.

SNMP-ID: 2.22.2.6

Pfad Telnet: /Setup/SYSLOG/Tabelle-SYSLOG

Mögliche 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

Default: Leer

2.22.3 Facility-Mapper

In dieser Tabelle werden die Zuordnungen von SYSLOG-Quellen zu Facilities definiert.

SNMP-ID: 2.22.3

Pfad Telnet: /Setup/SYSLOG

2.22.3.1 Quelle

Zuordnung der Quellen zu bestimmten Facilities.

SNMP-ID: 2.22.3.1

Pfad Telnet: /Setup/SYSLOG/Facility-Mapper

Mögliche Werte:

- System
- Logins
- Systemzeit
- Konsolen-Logins
- Verbindungen
- Accounting
- Verwaltung
- Router

2.22.3.2 Facility

Zuordnung der Quellen zu bestimmten Facilities.

SNMP-ID: 2.22.3.2

Pfad Telnet: /Setup/SYSLOG/Facility-Mapper

Mögliche Werte:

- KERNEL
- AUTH
- CRON
- AUTHPRIV
- LOCAL0
- LOCAL1
- LOCAL2
- LOCAL3

2.22.4 Port

Port, der für den Versand der SYSLOG-Nachichten verwendet wird.

SNMP-ID: 2.22.4

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- max. 10 Zeichen

Default: 514

2.22.5 Meldungs-Tabellen-Reihenfolge

Bestimmen Sie hier die Reihenfolge in der die Meldungs-Tabellen angezeigt werden.

SNMP-ID: 2.22.5

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- oldest on top

- newest-on-top

Default: newest-on-top

2.22.6 Backup-Intervall

Dieser Parameter definiert das Intervall für das persistente Speichern der SYSLOG-Nachrichten im Flash des Gerätes in Stunden.

SNMP-ID: 2.22.6

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- 1 bis 99

Default: 2

2.22.7 Backup-aktiv

Aktiviert das persistente Speichern der SYSLOG-Nachrichten im Flash des Gerätes.

SNMP-ID: 2.22.7

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.22.8 Log-CLI-Aenderungen

Dieser Parameter aktiviert das Protokollieren der Kommandozeilenbefehle. Aktivieren Sie diesen Parameter, um bei der Ausführung eines Befehls an der Kommandozeile des Gerätes einen Eintrag im internen SYSLOG-Speicher vorzunehmen.

Diese Protokollierung umfasst ausschließlich die an der Kommandozeile ausgeführten Befehle. Konfigurationsänderungen und Aktionen über LANconfig oder Webconfig sind davon nicht erfasst.

SNMP-ID: 2.22.8

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.22.9 Max-Nachrichtenalter-Stunden

Dieser Parameter definiert das maximale Alter der SYSLOG-Nachrichten im internen SYSLOG-Speicher des Gerät in Stunden. Nach Ablauf dieser Zeit löscht das Gerät die veralteten SYSLOG-Nachrichten automatisch, sofern das automatische Löschen unter *Alte-Nachrichten-Entfernen* aktiv ist.

Pfad Telnet:

Setup > **SYSLOG**

Mögliche Werte:

1 bis 99

Default:

24

2.22.10 Alte-Nachrichten-Entfernen

Dieser Parameter aktiviert das Löschen der SYSLOG-Nachrichten im Gerät nach der unter *Maximales-Nachrichtenalter* definierten Zeit.

Pfad Telnet:

Setup > **SYSLOG**

Mögliche Werte:

Ja

Nein

Default:

Nein

2.22.11 Nachrichtenalter-Einheit

Dieser Parameter bestimmt, ob das angegebene Nachrichtenalter in Stunden, Tagen oder Monaten gilt.

Ein Monat entspricht hierbei 30 Tagen.

Pfad Telnet:

Setup > **SYSLOG**

Mögliche Werte:

Stunde

Tag

Monat

Default:

Stunde

2.22.12 Kritische-Prio

Über diese Einstellung definieren Sie, ab welcher Syslog-Priorität das Gerät Syslog-Einträge als 'kritisch' betrachtet. Auf Basis dieses Prioritätslevels generiert das Gerät entsprechende Warnungen, die Sie z. B. innerhalb von WEBconfig erhalten.

Pfad Telnet:

Setup > **SYSLOG**

Mögliche Werte:

Notfall
Alarm
Kritisch
Fehler
Warnung
Hinweis
Info
Debug

Default-Wert:

Kritisch

2.23 Schnittstellen

Dieses Menü enthält die Einstellungen der Schnittstellen.

SNMP-ID: 2.23

Pfad Telnet: /Setup

2.23.1 S0

Hier können Sie für diese Schnittstelle Ihres Gerätes weitere Einstellungen vornehmen.

SNMP-ID: 2.23.1

Pfad Telnet: /Setup/Schnittstellen

2.23.1.1 Ifc

Auswahl der ISDN-Schnittstelle, auf die sich die Einstellungen beziehen.

SNMP-ID: 2.23.1.1

Pfad Telnet: /Setup/Schnittstellen/S0/Ifc

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren ISDN-Schnittstellen, z. B. S0-1 oder S0-2

2.23.1.2 Protokoll

Wählen Sie hier das D-Kanal-Protokoll für dieses Interface aus.

Pfad Telnet: /Setup/Schnittstellen/S0/Protokoll

Mögliche Werte:

- nein
- DSS1
- 1TR6
- P2P-DSS1
- GRP0
- Auto

Default: Auto

2.23.1.7 FV-B-Kanal

Stellen Sie den Festverbindungskanal ein, der bei einer Festverbindung des Typs **Gruppe 0** benutzt werden soll.

Pfad Telnet: /Setup/Schnittstellen/S0/FV-B-Kanal

Mögliche Werte:

- kein
- B1
- B2

Default: kein

2.23.1.9 Anwahl-Praefix

Geben Sie hier eine Nummer ein, die jeder Rufnummer bei abgehenden Rufen vorangestellt werden soll.

Wenn Ihr Gerät beispielsweise an einer Telefonanlage betrieben wird, welche die Vorwahl einer Amtskennzahl erfordert, dann sollten Sie diese hier eintragen.

Pfad Telnet: /Setup/Schnittstellen/S0/Anwahl-Praefix

Mögliche Werte:

- max. 8 Zeichen

Default: leer

2.23.1.13 Max-pass-Verb

Mit dieser Einstellung können Sie die Anzahl der Verbindungen beschränken, die über dieses Interface aufgebaut werden. So können Sie beispielsweise sicherstellen, dass für andere Geräte immer eine Leitung verfügbar bleibt.

Pfad Telnet: /Setup/Schnittstellen/S0/Max-pass-Verb

Mögliche Werte:

- keine
- eine
- zwei

Default: zwei

2.23.1.14 Max-akt-Verb

Mit dieser Einstellung können Sie die Anzahl der Verbindungen beschränken, die über dieses Interface aufgebaut werden. So können Sie beispielsweise sicherstellen, dass für andere Geräte immer eine Leitung verfügbar bleibt.

Pfad Telnet: /Setup/Schnittstellen/S0/Max-akt-Verb

Mögliche Werte:

- keine
- eine
- zwei

Default: zwei

2.23.4 DSL

Hier finden Sie die Einstellungen für das DSL-Interface.

SNMP-ID: 2.23.4

Pfad Telnet: /Setup/Schnittstellen

2.23.4.1 Ifc

Auswahl der Schnittstelle, auf die sich die Einstellungen beziehen.

SNMP-ID: 2.23.4.1

Pfad Telnet: /Setup/Schnittstellen/S0/Ifc

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren ISDN-Schnittstellen, z. B. S0-1 oder S0-2
- ADSL
- VDSL
- Auswahl aus den im Gerät verfügbaren DSL-Schnittstellen, z. B. DSL-1 oder DSL-2
- UMTS

Die Auswahlmöglichkeiten hängen von der jeweiligen Ausstattung Ihres Gerätes aus.

2.23.4.2 Aktiv

Hier können Sie einstellen, ob die Schnittstelle aktiv ist oder nicht.

SNMP-ID: 2.23.4.2

Pfad Telnet: /Setup/Schnittstellen/DSL/Aktiv

Mögliche Werte:

- nein
- ja

Default: nein

2.23.4.6 Mode

Wählen Sie hier den Modus, wie das WAN-Interface genutzt wird. Im Automatik-Modus werden alle PPPoE-Frames sowie alle Datenpakete, die zu einer über das DSLoL-Interface aufgebauten Verbindung gehören (konfiguriert in der IP-Parameter-Liste), über das DSLoL-Interface (WAN) weitergeleitet. Alle anderen Datenpakete werden als normale LAN-Pakete behandelt. Im Exclusiv-Modus wird das LAN-Interface ausschließlich als WAN-Interface benutzt.

Pfad Telnet:

Setup > **Schnittstellen** > **DSLoL-Interface**

Mögliche Werte:

Auto

Exclusiv

Default:

Exclusiv

2.23.4.16 Upstream-Rate

Hier können Sie die Brutto-Upstreamrate für diese Schnittstelle bestimmen. Die hier eingegebene Datenmenge (kbit/s) limitiert die vom Gerät abgehenden Datenströme.

Pfad Telnet: /Setup/Schnittstellen/DSL/Upstream-Rate

Mögliche Werte:

- maximal 6 numerische Zeichen

Default: leer

Besondere Werte: 0: keine Limitierung der übertragenen Datenmenge

2.23.4.17 Ext.-Overhead

Der externe Overhead ergibt sich aus den Daten, die das Modem selbst noch vor jedes Paket setzt. Bei PPPoE-Verbindungen sind das 4 Byte für den LLC-Header und 8 Byte für den AAL-5-Trailer. Da das Modem zudem keine "angebrochenen" ATM-Zellen verschicken kann, muss im Schnitt noch eine halbe ATM-Zelle (= 24 Bytes) aufgeschlagen werden. Somit ergibt sich ein Gesamt-Overhead von 36 Bytes pro übertragenem Paket.

Pfad Telnet: /Setup/Schnittstellen/S0/Ext.-Overhead

Mögliche Werte:

- maximal 3 numerische Zeichen

Default: leer

2.23.4.18 Downstream-Rate

Die Downstreamrate wird in Kilobit angegeben und enthält alles, was den Router über das WAN-Ethernet erreicht. So beträgt z. B. auf einem T-DSL Anschluss mit garantierten 768 kbit Downstream die vom Modem ausgehandelte Upstreamrate 864 kbit. Diese beinhalten allerdings noch einen für diese Verbindung typischen Overhead, welcher sich aus der Verwendung von ATM als Transportprotokoll des Modems ergibt. Bereinigt man die 864 kbit um den Overhead, der sich aus dem Aufbau einer ATM-Zelle ergibt (48 Byte Nutzdaten bei 53 Byte Zellenlänge), so erhält man 864 *48 /53 = 792 kbit Brutto-Downstreamrate, welche auf dem Ethernet vom Modem zum Router übertragen werden. Sind die vom Modem ausgehandelten Datenraten nicht bekannt, so kann man aus den garantierten Datenraten durch Multiplikation mit 56/55 die Brutto-Datenraten annähern.

Pfad Telnet: /Setup/Schnittstellen/DSL/Downstream-Rate

Mögliche Werte:

- maximal 6 numerische Zeichen

Default: leer

Besondere Werte: 0: keine Beschränkung des empfangenen Datenverkehrs

2.23.4.23 LAN-Ifc

Wählen Sie an welches LAN-Interface das DSLoL-Interface gebunden ist.

Pfad Telnet: /Setup/Schnittstellen/DSLoL-Schnittstellen/LAN-Ifc

Mögliche Werte:

- LAN-1
- WLAN-1
- P2P-1-1
- P2P-1-2
- P2P-1-3
- P2P-1-4
- P2P-1-5
- P2P-1-6
- WLAN-1-2
- WLAN-1-3
- WLAN-1-4
- WLAN-1-5
- WLAN-1-6
- WLAN-1-7

- WLAN-1-8
- BRG-1
- BRG-2
- BRG-3
- BRG-4
- BRG-5
- BRG-6
- BRG-7
- BRG-8
- beliebig

Default: LAN-1

2.23.6 ADSL-Interface

Hier finden Sie die Einstellungen für das ADSL-Interface.

Pfad Telnet: /Setup/Schnittstellen/ADSL-Interface

2.23.6.1 Ifc

Wählen Sie hier die betreffende Schnittstelle aus.

Pfad Telnet: /Setup/Schnittstellen/ADSL-Interface/Ifc

Mögliche Werte:

- ADSL
- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS

Die Auswahlmöglichkeiten hängen von der jeweiligen Austattung Ihres Gerätes ab.

2.23.6.2 Protokoll

Wählen Sie hier das Protokoll aus, das Sie für diese Schnittstelle verwenden möchten.

Beim ADSL-Multimode werden reihum die Protokolle G.DMT, T1.413 und G.Lite versucht. Beim Auto-Modus wird zuerst versucht mit dem ADSL2+-Protokoll eine Verbindung aufzubauen. Kann damit keine Verbindung aufgebaut werden findet ein Fallback über ADSL2 nach G.Dmt statt.

Pfad Telnet: /Setup/Schnittstellen/ADSL-Interface/Protokoll

Mögliche Werte:

- nein
- Auto
- ADSL2+
- ADSL2
- ADSL-Multimode
- Annex-M-Auto
- G.Dmt
- T1.413

Default: nein

2.23.7 Modem-Mobilfunk

Hier finden Sie die Einstellungen für das Mobilfunk-Modem.

SNMP-ID: 2.23.7

Pfad Telnet: /Setup/Schnittstellen

2.23.7.1 Ifc

Wählen Sie hier das Interface aus, das Sie konfigurieren möchten.

Pfad Telnet: /Setup/Schnittstellen/Modem-Mobilfunk/Ifc

Mögliche Werte:

- DSL-1
- EXT
- ADSL
- S0-1
- DSL-1
- DSL-2
- DSL-3
- UMTS

Die Auswahlmöglichkeiten hängen von der Ausstattung Ihres Gerätes ab.

2.23.7.2 Aktiv

Wählen Sie hier, auf welche Weise die Schnittstelle aktiv ist.

Pfad Telnet:

Setup > **Schnittstellen** > **Modem-Mobilfunk**

Mögliche Werte:

Nein

Modem

WWAN

UMTS-GPRS

Default:

Nein

2.23.7.21 Datenrate

Wählen Sie hier die Datenrate, mit der Datenströme in Kilobyte pro Sekunde übertragen werden.

Pfad Telnet: /Setup/Schnittstellen/Modem-Mobilfunk/Datenrate

Mögliche Werte Telnet:

- 19200
- 38400
- 57600
- 115200

Default: 115200

2.23.7.22 Profil

Wählen Sie hier das Profil, das für die UMTS-Schnittstelle verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/Modem-Mobilfunk/Profil

Mögliche Werte:

- maximal 16 alphanumerische Zeichen

Default: leer

2.23.8 VDSL

Dieses Menü enthält die Einstellungen für die VDSL-Schnittstelle.

Pfad Telnet:

Setup > **Schnittstellen**

2.23.8.1 Ifc

Bezeichnung der Schnittstelle (Interface).

Pfad Telnet:

Setup > **Schnittstellen** > **VDSL**

2.23.8.2 Protokoll

Über diesen Parameter definieren Sie das Protokoll bzw. den Standard, den die Schnittstelle für die Datenüberträgung verwendet.

Pfad Telnet:

Setup > **Schnittstellen** > **VDSL**

Mögliche Werte:

Off
Diese Einstellung deaktiviert die VDSL-Schnittstelle.

Auto
Das Gerät wählt das beste Übertragungsprotokoll selbstständig aus.

VDSL
Das Gerät verwendet VDSL2 nach ITU-T G.993.2.

ADSL

ADSL2+
Das Gerät verwendet ADSL2+ nach ITU-T G.992.5.

ADSL2
Das Gerät verwendet ADSL2 nach ITU-T G.992.3.

ADSL1
Das Gerät verwendet ADSL1 nach ITU-T G.992.1 oder G.DMT.

ADSL2+J
Das Gerät verwendet ADSL2+ nach ITU-T G.992.5 Annex J.

ADSL2J

Das Gerät verwendet ADSL2 nach ITU-T G.992.3 Annex J.

Default-Wert:

Auto

2.23.18 Permanente-L1-Aktivierung

Die Permanente L1-Aktivierung verhindert ein Deaktivieren des S0-Busses oder eine erneute Aktivierung nach erfolgter Deaktivierung.

Diese Einstellung ist von besonderer Relevanz, wenn Sie einen Bus als PCM-Sync-Source verwenden. Im Falle einer Deaktivierung des Busses verlieren Sie dann auch den PCM-Takt.

Pfad Telnet:

Setup > **Schnittstellen**

Mögliche Werte:

deaktiviert
nur Sync-Quelle
Alle TE-Schnittstellen

2.23.19 PCM-SYNC-SOURCE

PCM-Sync-Source legt den S0-Bus fest, von dem der Voice Call Manager den Takt bezieht.

Diese Einstellung ist relevant, wenn Sie einen Bus intern verwenden und der zweite Bus extern angeschlossen ist (z. B. an einem Anschluss des ISDN-Anbieters). In dem Fall sollten Sie den Takt vom externen Anschluss beziehen. Mit der Einstellung **Auto** wählt das Gerät den Bus selber aus.

Pfad Telnet:

Setup > **Schnittstellen**

Mögliche Werte:

Auto
S0-1

2.23.20 WLAN

Dieses Menü enthält die Einstellungen für kabellose Netzwerke (WLAN)

SNMP-ID: 2.23.20

Pfad Telnet: /Setup/Schnittstellen

2.23.20.1 Netzwerk

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes weitere Netzwerk-Einstellungen vornehmen.

SNMP-ID: 2.23.20.1

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.1.1 Ifc

Auswahl aus den logischen WLAN-Schnittstellen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

2.23.20.1.2 Netzwerkname

Stellen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche WLAN-Clients, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- max. 64 Zeichen

Default: BLANK

2.23.20.1.4 Closed-Network

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der Access Point veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der Access Point mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der Access Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der Access Point ebenfalls mit einer leeren SSID.
- **Verschärft**: Der Access Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der Access Point überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der Access Point diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Nein

Ja

Verschärft

Default:

Nein

2.23.20.1.8 Aktiv

Schaltet das logische WLAN separat ein- oder aus.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.23.20.1.9 MAC-Filter

In der MAC-Filterliste werden die MAC-Adressen der Clients hinterlegt, die sich bei einem Access Point einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Ein
- Aus

Default: Ein

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

2.23.20.1.10 Maximum-Stationen

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point in dieses Netzwerk einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- 0 bis 65535

Default: 0

Besondere Werte: 0 = Limitierung ausgeschaltet

2.23.20.1.11 Cl.-Brg.-Support

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

Dazu werden in dieser Betriebsart nicht die beim Client-Modus üblichen drei MAC-Adressen verwendet (in diesem Beispiel für Server, Access Point und Clientstation), sondern wie bei Punkt-zu-Punkt-Verbindungen vier Adressen (zusätzlich die MAC-Adresse der Station im LAN der Clientstation). Die volltransparente Anbindung eines LANs an der Clientstation

ermöglicht die gezielte Übertragung der Datenpakete im WLAN und damit Funktionen wie TFTP-Downloads, die über einen Broadcast angestoßen werden.

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

Pfad Telnet:

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

Mögliche Werte:

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

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

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

Default-Wert:

Nein

2.23.20.1.12 RADIUS-Accounting

Schaltet Accounting über einen RADIUS-Server auf diesem Netz ein oder aus

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.23.20.1.13 Inter-Stations-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Für jedes logische WLAN kann separat eingestellt werden, ob die Clients in dieser SSID untereinander Daten austauschen können.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.23.20.1.14 APSD

Aktiviert den Stromsparmodus APSD für dieses logische WLAN-Netzwerk.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk

Mögliche Werte:

- Ein
- Aus

Default: Aus

Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

2.23.20.1.15 Aironet-Erweiterungen

Aktiviert Aironet-Erweiterungen für dieses logische Wireless LAN.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk/Aironet-Erweiterungen

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.23.20.1.16 Minimal-Stations-Staerke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der Access Point keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den Access Point somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren Access Points, da keine Access Points aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

0-100

Default:

0

2.23.20.1.17 UUID-Einschliessen

Hier bestimmen Sie, ob das entsprechende Funkmodul seine UUID übertragen soll.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja

2.23.20.1.19 Nur-Unicasts-senden

Multi- und Broadcast-Sendungen innerhalb einer WLAN-Funkzelle bedeuten eine Belastung für die Bandbreite dieser Funkzelle, zumal die WLAN-Clients mit diesen Sendungen oft nichts anfangen können. Der Access-Point fängt durch

ARP-Spoofing bereits einen Großteil der Multi- und Broadcast-Sendungen in die Funkzelle ab. Mit der Beschränkung auf Unicast-Sendungen filtert er z. B. überflüssige IPv4-Broadcasts wie Bonjour oder NetBIOS aus den Anfragen heraus.

Die Unterdrückung von Multi- und Broadcast-Sendungen ist zudem eine Forderung der HotSpot-2.0-Spezifikation.

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Ja

Nein

Default:

Nein

2.23.20.1.20 Tx-Limit

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

2.23.20.1.21 Rx-Limit

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

2.23.20.1.22 Accounting-Server

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

Pfad Telnet:

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

Mögliche Werte:

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

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

Default-Wert:

leer

2.23.20.1.23 Pro-Client-Tx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

Pfad Telnet:

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

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert die Begrenzung.

2.23.20.1.24 Pro-Client-Rx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

Pfad Telnet:

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

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert die Begrenzung.

2.23.20.1.25 LBS-Tracking

Dieser Eintrag aktiviert oder deaktiviert das LBS-Tracking für diese SSID.

Pfad Telnet:

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

Mögliche Werte:

nein
LBS-Tracking ist deaktiviert.

ja
LBS-Tracking ist aktiviert.

2.23.20.1.26 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 Client den angegebenen Listennamen, die MAC-Adresse des Access Points und die eigene MAC-Adresse an den LBS-Server.

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

2.23.20.2 Uebertragung

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes weitere Übertragungs-Einstellungen vornehmen.

Pfad Telnet:

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

2.23.20.2.1 Ifc

Öffnet die Einstellungen für die logischen WLAN-Netzwerke

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

2.23.20.2.2 Paketgroesse

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

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 500 bis 1600 (nur gerade Werte)

Default: 1600

2.23.20.2.3 Min-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die minimale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- Automatisch
- Auswahl aus den angebotenen Geschwindigkeiten

Default: Automatisch

2.23.20.2.4 Basis-Rate

Die Basis-Rate ist die Übertragungsrate, mit der das Gerät alle Multicast- und Broadcast-Pakete versendet.

Die hier eingestellte Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch mit dieser Geschwindigkeit zu erreichen sind.

Wenn Sie hier "Auto" auswählen, richtet sich das Gerät automatisch nach der Übertragungsrate des langsamsten WLAN-Clients im Netzwerk.

Pfad Telnet:

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

Mögliche Werte:

Auto

Auswahl aus den angebotenen Geschwindigkeiten von 1Mbit/s - 54Mbit/s

Default:

2Mbit/s

2.23.20.2.6 RTS-Schwelle

Mit dem RTS-Schwellwert wird das Phänomen der „Hidden-Station" durch Verwendung des RTS/CTS-Protokolls vermieden.

Eine Kollision bei den recht kurzen RTS-Paketen ist sehr unwahrscheinlich, die Verwendung von RTS/CTS erhöht aber dennoch den Overhead. Der Einsatz dieses Verfahrens lohnt sich daher nur für längere Datenpakete, bei denen Kollisionen wahrscheinlich sind. Mit dem RTS-Schwellwert wird eingestellt, ab welcher Paketlänge das RTS/CTS eingesetzt werden soll. Der passende Werte ist in der jeweiligen Umgebung im Versuch zu ermitteln.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 512 bis 2347

Default: 2347

2.23.20.2.7 11b-Praeambel

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem Access Point selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.23.20.2.9 Max-Tx-Rate

Der Access Point handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der Access Point die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die maximale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- Automatisch
- Auswahl aus den angebotenen Geschwindigkeiten

Default: Automatisch

2.23.20.2.10 Min.-Frag.-Laenge

Paket-Fragmentlänge, unterhalb der Fragmente verworfen werden

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 0 bis 2347

Default: 16

2.23.20.2.11 Soft-Retries

Wenn ein Paket von der Hardware nicht verschickt werden konnte, wird mit der Anzahl der Soft-Retries festgelegt, wie oft der gesamte Sendeversuch wiederholt werden soll.

Die Gesamtzahl der Versuche ist also (Soft-Retries + 1) * Hard-Retries.

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

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 0 bis 999

Default: 0

2.23.20.2.12 Hard-Retries

Dieser Wert gibt an, wie oft die Hardware versuchen soll, Pakete zu verschicken, bevor sie als Tx-Fehler gemeldet werden. Kleinere Werte ermöglichen es so, dass ein nicht zu versendendes Paket den Sender weniger lange blockiert.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 0 bis 15

Default: 10

2.23.20.2.13 Kurzes-Guard-Intervall

In der Standardeinstellung wird das Guard-Intervall automatisch optimal eingestellt. Wenn die momentanen Betriebsbedingungen es zulassen wird ein kurzes Intervall zugelassen.

Weiterhin haben Sie die Möglichkeit diese Automatik abzuschalten, um das kurze Guard-Intervall bewusst zu verhindern.

Das Guard-Intervall dient grob gesagt dazu die Störanfälligkeit bei Mehrträgerverfahren (OFDM) durch Intersymbolinterferenz (ISI) zu minimieren.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Kurzes-Guard-Intervall

Mögliche Werte:

- aktiviert
- deaktiviert

Default: aktiviert

2.23.20.2.14 Max.-Spatiale-Stroeme

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

In der Standardeinstellung werden die Spatial-Streams automatisch eingestellt, um das Funksystem optimal zu nutzen.

Weiterhin haben Sie die Möglichkeit die Spatial-Streams auf einen oder zwei einzustellen um das Funksystem beispielsweise bewusst geringer zu belasten.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Max.-Spatiale-Stroeme

Mögliche Werte:

- automatisch
- einer
- zwei

Default: automatisch

2.23.20.2.15 Sende-Aggregate

Hier finden Sie die Einstellungen für die Frame-Aggregation. Frame-Aggregation ist als offizieller Standard und herstellerunabhängig im 802.11n Standard vorgesehen. Er gleicht dem seit längerem bekannten Burst-Modus.

Bei Frame-Aggregation wird das WLAN-Frame soweit verlängert, dass mehrere Ethernet-Pakete hinein passen. Mit diesem Verfahren wird die Wartezeit zwischen den Datenpaketen verkürzt und der Durchsatz gesteigert. Der Overhead wird reduziert und kann für die Übertragung der Daten genutzt werden.

Mit der zunehmenden Länge der Frames steigt aber auch die Wahrscheinlichkeit, dass durch Funkstörung die Pakete nochmal gesendet werden müssen. Außerdem müssen andere Stationen länger auf einen freien Kanal warten und sie müssen die Datenpakete sammeln bis mehrere auf einmal gesendet werden können. In der Standardeinstellung ist die Frame-Aggregation eingeschaltet. Wenn Sie den Datendurchsatz dieser Station erhöhen möchten und andere auf diesem Medium nicht von Bedeutung sind, ist dies sinnvoll. .

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Sende-Aggregate

Mögliche Werte:

- ja
- nein

Default: ja

2.23.20.2.16 Min.-HT-MCS

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

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

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

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Min.-HT-MCS

Mögliche Werte:

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

Default: automatisch

2.23.20.2.17 Max.-HT-MCS

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

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

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

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Max.-HT-MCS

Mögliche Werte:

- automatisch
- MCS 0/8
- MCS 1/9
- MCS 2/10

- MCS 3/11
- MCS 4/12
- MCS 5/13
- MCS 6/14
- MCS 7/15

Default: automatisch

2.23.20.2.18 Min.-Spatiale-Stroeme

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

In der Standardeinstellung werden die Spatial-Streams automatisch eingestellt, um das Funksystem optimal zu nutzen.

Weiterhin haben Sie die Möglichkeit die Spatial-Streams auf einen oder zwei einzustellen um das Funksystem beispielsweise bewusst geringer zu belasten.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Min.-Spatiale-Stroeme

Mögliche Werte:

- automatisch
- einer
- zwei

Default: automatisch

2.23.20.2.19 EAPOL-Rate

Legen Sie hier die Datenrate für die Übertragung der EAPOL-Pakete fest.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- Wie-Daten

Auswahl aus den angebotenen Geschwindigkeiten:

- 1M
- 2M
- 5.5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-12M
- T-18M
- T-24M
- T-36M

- T-48M
- T-72M
- T-96M
- T-108M

Default: Wie-Daten

Besondere Werte: Wie-Daten überträgt die EAPOL-Daten mit der gleichen Datenrate wie die Nutzdaten.

2.23.20.2.20 Max.-Aggr.-Paket-Anzahl

Dieser Parameter definiert, wie viele Pakete maximal zu einem Aggregat zusammengepackt werden dürfen. Die Aggregierung bei WLAN-Übertragungen nach IEEE 802.11n fasst mehrere Datenpakete zu einem großen Paket zusammen, reduziert so den Overhead und beschleunigt die Übertragung.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung/Max.-Aggr.-Paket-Anzahl

Mögliche Werte:

- maximal 2 numerische Zeichen

Default: 16

2.23.20.2.21 ProbeRsp-Retries

Dies ist die Anzahl der Hard-Retries für Probe-Responses, also Antworten, die ein Access Point als Antwort auf einen Probe-Request von einem Client schickt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Uebertragung

Mögliche Werte:

- 0 bis 15

Default: 3

Werte größer als 15 werden wie 15 behandelt.

2.23.20.2.22 Empfange-Aggregate

Mit dieser Einstellung erlauben bzw. verbieten Sie den Empfang von aggregierten (zusammengefassten) Datenpaketen über dieses Interface.

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Durch dieses Verfahren kann der Overhead der Pakete reduziert werden, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

Pfad Telnet:

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

Mögliche Werte:

nein

ja

Default:

ja

2.23.20.2.23 Nutze-STBC

Hier aktivieren Sie die Verwendung von STBC zur Datenübertragung pro logischem Netzwerk (SSID).

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

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja (wenn der WLAN-Chipsatz STBC unterstützt)

Nein (wenn der WLAN-Chipsatz STBC nicht unterstützt)

2.23.20.2.24 Nutze-LDPC

Hier aktivieren Sie die Verwendung von LDPC zur Datenübertragung pro logischem Netzwerk (SSID).

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

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja (wenn der WLAN-Chipsatz STBC unterstützt)

Nein (wenn der WLAN-Chipsatz STBC nicht unterstützt)

2.23.20.2.25 in-Unicast-wandeln

Über diesen Parameter legen Sie fest, welche Art von als Broadcast gesendeten Datenpaketen das Gerät innerhalb eines WLAN-Netzwerks automatisch in Unicast umwandelt.

Pfad Telnet:

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

Mögliche Werte:

- Keine Auswahl
- **DHCP**: Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

Default:

DHCP

2.23.20.3 Verschluesselung

Hier können Sie für jedes logische Wireless-LAN-Netzwerk (MultiSSID) Ihres Gerätes spezifische Verschlüsselungs-Einstellungen vornehmen.

SNMP-ID: 2.23.20.3

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.3.1 Ifc

Öffnet die WPA- / Einzel-WEP-Einstellungen für die logischen WLAN-Netzwerke

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- Auswahl aus den verfügbaren logischen WLAN-Netzwerken.

2.23.20.3.2 Verschluesselung

Aktiviert die Verschlüsselung für dieses logische WLAN

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.23.20.3.3 Vorgabeschluessel

Wählt den WEP-Schlüssel aus, mit dem die von diesem logischen WLAN gesendeten Pakete verschlüsselt werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- Schlüssel 1
- Schlüssel 2
- Schlüssel 3
- Schlüssel 4

Default: Schlüssel 1

Schlüssel 1 gilt nur für das aktuelle logische WLAN, Schlüssel 2 bis 4 sind als Gruppenschlüssel für alle logischen WLANs der gleichen physikalischen Schnittstelle gültig.

2.23.20.3.4 Methode

Wählt das Verschlüsselungs-Verfahren bzw. bei WEP die Schlüssellange aus, die bei der Verschlüsselung von Datenpaketen auf dem Wireless-LAN verwendet wird.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- 802-11i-(WPA)-PSK
- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)
- 802-11i-(WPA)-802.1x

- WEP-156 (128 Bit)-802.1x
- WEP-128 (104 Bit)-802.1x
- WEP-64 (40 Bit)-802.1x

Default: WEP-128 (104 Bit)

Beachten Sie, dass nicht jedes Verschlüsselungs-Verfahren von jeder Wireless-Karte unterstützt wird.

2.23.20.3.5 Authentifizierung

Für die Nutzung von WEP kann das Verschlüsselungsverfahren ausgewählt werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- Open-System: Beim Open-System-Authentifizierungsverfahren werden grundsätzlich alle Clients angenommen. Es findet keine Authentifizierung statt. Die Daten müssen von den WLAN-Clients immer korrekt verschlüsselt übertragen werden, um von der Basisstation weitergeleitet zu werden.
- Shared-Key: Beim Shared-Key-Authentifizierungsverfahren muss der WLAN-Client zunächst ein vom Server geliefertes Datenpaket korrekt verschlüsselt zurücksenden, um authentifiziert zu werden. Erst danach werden von ihm verschlüsselte Daten akzeptiert und weitergeleitet. Dadurch steht einem Angreifer allerdings ein Datenpaket in seiner unverschlüsselten und in seiner verschlüsselten Form zur Verfügung, wodurch der Schlüssel selbst angreifbar wird.

Default: Open-System

Aufgrund der Sicherheitsaspekte wird grundsätzlich das Open-System-Authentifizierungsverfahren empfohlen.

2.23.20.3.6 Schluessel

Sie können die Schlüssel oder Passphrases als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes 'Ox' möglich.

Folgende Langen ergeben sich für die verwendeten Formate:

Verfahren Länge

WPA-PSK 8 bis 63 ASCII-Zeichen

WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen

WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen

WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- ASCII-Zeichenkette oder Hexadezimalzahl

Default: Leer

Bei Verwendung von 802.1x im AP-Modus verweist der hier eingetragene Name auf den zu verwendenden RADIUS-Server.

Bei Verwendung von 802.1x im Client-Modus und PEAP oder TTLS als Client-EAP-Methode werden hier die Zugangsdaten (user:password) hinterlegt.

2.23.20.3.9 WPA-Version

Mit dieser WPA-Version werden die Daten in diesem logischen WLAN verschlüsselt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- WPA1
- WPA2
- WPA1/2

Default: WPA1/2

2.23.20.3.10 Client-EAP-Methode

LANCOM Wireless Router und Access Points in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen Access Point authentifizieren. Zur Aktivierung der EAP/802.1X-Authentifizierung im Client-Modus wird bei den Verschlüsselungsmethoden für das erste logische WLAN-Netzwerk die Client-EAP-Methode ausgewählt.

Beachten Sie, dass die gewählte Client-EAP-Methodezu den Einstellungen des Access Points passen muss, bei dem sich der Access Point einbuchen will.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- TLS
- TTLS/PAP
- TTLS/CHAP
- TTLS/MSCHAP
- TTLS/MSCHAPv2
- TTLS/MD5
- PEAP/MSCHAPv2

Default: TLS

Beachten Sie neben der Einstellung der Client-EAP-Methode auch die entsprechende Einstellung der Betriebsart als WLAN-Client.

2.23.20.3.11 WPA-Rekeying-Zyklus

Angabe, wie oft der WPA-Key-Handshake während einer bestehenden Verbindung wiederholt werden soll (Rekeying)

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- 0 bis 4294967295 s

Default: 0

Besondere Werte: 0 = Rekeying deaktiviert

2.23.20.3.12 WPA1-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- TKIP
- AES
- TKIP/AES

Default: TKIP

2.23.20.3.13 WPA2-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Verschluesselung

Mögliche Werte:

- TKIP
- AES
- TKIP/AES

Default: AES

2.23.20.3.14 Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

Pfad Telnet:

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

Mögliche Werte:

Nein

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

Zwingend

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

Optional

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

Default-Wert:

Nein

2.23.20.3.15 PMK-Caching

Aktiviert das PMK-Caching im WLAN-Client-Modus

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

2.23.20.3.16 Prae-Authentisierung

Aktiviert die Prä-Authentifizierung für das entsprechende WLAN.

Um Prä-Authentifizierung nutzen zu können, muss das PMK-Caching aktiviert sein.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

2.23.20.3.17 OKC

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

Diesen Wert übernimmt das Gerät ausschließlich, wenn die Schnittstelle im Client-Modus arbeitet. Befindet sich die Schnittstelle im AP-Modus, ist die Aktivierung oder Deaktivierung von OKC nur über die Profilverwaltung eines WLCs möglich.

Im PMK-Caching-Status unter **Status** > **WLAN** > **PMK-Caching** > **Inhalt** sind OKC-PMKs an der Authenticator-Adresse `ff:ff:ff:ff:ff:`n zu erkennen, wobei n die zugeordnete Profilnummer ist (z. B. `0` für „WLAN-1“, `1` für „WLAN1-2“ etc.).

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.23.20.3.19 WPA2-Schluessel-Management

Mit diesen Optionen konfigurieren Sie die WPA2-Schlüsselverwaltung.

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

Pfad Telnet:

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

Mögliche Werte:

Schnelles-Roaming

Aktiviert Fast Roaming über 802.11r

SHA256

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

Standard

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

Default-Wert:

Standard

2.23.20.4 Gruppen-Schluessel

Hier definieren Sie für jedes physikalische Wireless-LAN-Interface Ihres Gerätes die WEP-Gruppen-Schlüssel 2 bis 4, die von allen darauf aufgespannten logischen Wireless-LAN-Netzen gemeinsam genutzt werden.

SNMP-ID: 2.23.20.4

Pfad Telnet: /Setup/Schnittstellen/WLAN

Wenn 802.1x/EAP aktiviert ist werden die Gruppenschlüssel von 802.1x/EAP verwendet und stehen damit nicht mehr für die WEP-Verschlüsselung zur Verfügung.

2.23.20.4.1 Ifc

Öffnet die WEP-Gruppen-Schlüssel für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.4.3 Schluessel-2

WEP-Gruppenschlüssel 2

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge

- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

Default: Leer

2.23.20.4.4 Schluessel-3

WEP-Gruppenschlüssel 3

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge
- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

Default: Leer

2.23.20.4.5 Schluessel-4

WEP-Gruppenschlüssel 4

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- Sie können den Schlüssel als ASCII-Zeichenkette oder Hexadezimalzahl (mit vorangestelltem 'Ox') eintragen
- Folgende Langen ergeben sich für die verwendeten Formate:
- Verfahren Länge
- WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen
- WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen
- WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

Default: Leer

2.23.20.4.7 Schluessel-Typ-2

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 2 verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

Default: WEP-64 (40 Bit)

2.23.20.4.8 Schluessel-Typ-3

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 3 verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- WEP-156 (128 Bit)

- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

Default: WEP-64 (40 Bit)

2.23.20.4.9 Schluessel-Typ-4

Wählt die Schlüssellänge, die für den WEP-Gruppenschlüssel 4 verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Gruppen-Schluessel

Mögliche Werte:

- WEP-156 (128 Bit)
- WEP-128 (104 Bit)
- WEP-64 (40 Bit)

Default: WEP-64 (40 Bit)

2.23.20.5 Interpoint-Einstellungen

Hier können Sie wichtige Parameter für die Kommunikation zwischen Basisstationen vornehmen, bzw. das Verhalten für diese festlegen.

SNMP-ID: 2.23.20.5

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.5.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.5.2 Freigeben

Das Verhalten eines Access Points beim Datenaustausch mit anderen Access Points wird in der „Punkt-zu-Punkt-Betriebsart" festgelegt.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- Aus: Der Access Point kann nur mit mobilen Clients kommunizieren
- An: Der Access Point kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- Exklusiv: Der Access Point kann nur mit anderen Basis-Stationen kommunizieren

Default: Aus

2.23.20.5.9 Isolierter-Modus

Erlaubt oder verbietet die Übertragung von Paketen zwischen P2P-Links auf der gleichen WLAN-Schnittstelle (Kompatibilitätseinstellung für LCOS-Versionen vor 2.70)

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.23.20.5.10 Kanalwahlverfahren

Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer Access Points kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituationen kann mit dem geeigneten „Kanalwahlverfahren“ verhindert werden.

Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen Access Point als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4 GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- Master: Dieser Access Point übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- Slave: Alle anderen Access Points suchen solange, bis sie einen sendenden Master gefunden haben.

Default: Master

Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i/WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich.

2.23.20.5.11 Link-Verlust-Timeout

Zeit in Sekunden, nach der ein (DFS-)Slave eine Verbindung zum Master als verloren betrachtet, wenn keine Beacons empfangen werden,

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- 0 bis 4294967295 Sekunden

Default: 4

2.23.20.5.12 Key-Handshake-Rolle

Legt fest, ob bei Verwendung von WPA diese Seite als Authenticator oder Supplicant arbeiten soll. Im Default-Modus ist der Master einer Strecke Authenticator, im Auto-Modus ist die Seite mit der niedrigeren MAC-Adresse Authenticator

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Einstellungen

Mögliche Werte:

- Default
- Auto

Default: Default

2.23.20.5.13 Lokaler-Name

Geben Sie hier einen im WLAN eindeutigen Namen für diese physikalische WLAN-Schnittstelle ein. Dieser Name kann auf anderen WLAN-Geraten genutzt werden, um diese Basisstation über Punkt-zu-Punkt anzubinden.

Sie können dieses Feld frei lassen, wenn das Gerat nur eine WLAN-Schnittstelle hat und bereits ein im WLAN eindeutiger Geräte-Name konfiguriert ist oder die übrigen Basisstation diese Schnittstelle aber die MAC-Adresse des WLAN-Adapters identifizieren.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Einstellungen**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.23.20.5.14 Fern-Status-Reporting

Über diesen Parameter bewirken Sie, dass das Gerät seinem P2P-Partner meldet, ob er ihn mit der erforderliche Signalstärke empfängt. Dieser Parameter ist ausschließlich dann relevant, wenn Sie für eine P2P-Verbindung Signalschwellwerte definiert haben.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Einstellungen**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.23.20.5.15 Netzwerk-Name

Geben Sie hier einen eindeutigen Namen für das Netzwerk ein, in dem sich diese WLAN-Schnittstelle befindet.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Einstellungen**

Mögliche Werte:

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

Default-Wert:

leer

2.23.20.6 Client-Einstellungen

Wenn Sie ihr Gerät im Client-Modus betreiben, können Sie detaillierte Einstellung an dessen Verhalten vornehmen.

SNMP-ID: 2.23.20.6

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.6.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.6.3 Verbindung-halten

Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.23.20.6.4 Netzwerk-Typen

Mit der Auswahl der 'Netzwerktypen' wird festgelegt, ob sich die Station nur an Infrastruktur- oder auch in Adhoc-Netzwerken anmelden darf.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- Infrastruktur
- Adhoc

Default: Infrastruktur

2.23.20.6.5 Scanne-Baender

Legen Sie hier fest, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- 2,4/5 GHz
- 2,4 GHz
- 5 GHz

Default: 2,4/5 GHz

2.23.20.6.6 Bevorzugtes-BSS

Wenn sich die Clientstation nur bei einem bestimmten Access Point einbuchen soll, können Sie hier die MAC-Adresse der WLAN-Karte aus diesem Access Point eintragen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- Gültige MAC-Adresse

Default: Leer

2.23.20.6.7 Adress-Anpassung

Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der Access-Point auf der anderen Seite der Verbindung „sieht" also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners.

In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den Access Point übertragen wird. Mit der Option 'Adress-Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der originalen MAC-Adresse übertragen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen

Mögliche Werte:

- Ein
- Aus

Default: Aus

Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur ein einzelner Rechner angeschlossen ist!

2.23.20.6.12 Auswahl-Vorrang

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Client-Einstellungen/WLAN-1

Mögliche Werte:

- Signalstärke: Wählt das Profil, dessen WLAN aktuell das stärkste Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald diese ein stärkeres Signal bietet.
- Profil: Wählt aus den verfügbaren WLANs das zu verwendende Profil in der Reihenfolge der definierten Einträge (WLAN-Index, z. B. WLAN-1, WLAN-1-2 etc.), auch wenn ein anderes WLAN ein stärkeres Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald ein WLAN mit einem niedrigeren WLAN-Index erkannt wird (unabhängig von der Signalstärke dieses WLANs).

Default: Signalstärke

2.23.20.6.13 Deauthentisierung-senden-bei

Über diesen Parameter legen Sie fest, in welchen Fällen sich ein als WLAN-Client agierendes Gerät beim AP explizit abmeldet.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Client-Einstellungen**

Mögliche Werte:

Deaktivierung

Abmeldung bei Abschaltung des WLAN

Default-Wert:

Deaktivierung

2.23.20.7 Betriebs-Einstellungen

In den Betriebseinstellungen können Sie grundsätzliche Parameter für den Betrieb ihrer WLAN-Schnittstelle vornehmen.

SNMP-ID: 2.23.20.7

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.7.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

Mögliche Werte:

- WLAN-1
- WLAN-2

2.23.20.7.2 Aktiv

Schaltet die physikalische WLAN-Schnittstelle separat ein- oder aus.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.23.20.7.3 Betriebsart

LANCOM-Geräte können grundsätzlich in verschiedenen Betriebsarten arbeiten.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Betriebs-Einstellungen**

Mögliche Werte:

Access Point: Als Basisstation (Access Point) stellt das Gerät für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.

Station: Als Station (Client) sucht das Gerät selbst die Verbindung zu einem anderen Access Point und versucht, sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.

Managed-AP: Als managed Access Point sucht das Gerät einen zentralen WLAN Controller, von dem es eine Konfiguration beziehen kann.

Sonde: In der Betriebsart 'Sonde' nutzt der Spectral Scan das Funkmodul des Access Points. In diesem Betriebsmodus kann das Gerät Daten weder senden noch empfangen. Das Gerät schaltet beim Start des Spectral Scans automatisch in die Betriebsart 'Sonde', so dass Sie diese Einstellung nicht manuell konfigurieren sollten.

Default:

Router: Access Point

Access Points: Managed-AP

2.23.20.7.4 Link-LED-Funktion

Bei der Einrichtung von Point-to-Point-Verbindungen oder in der Betriebsart als WLAN-Client ist es für eine möglichst gute Positionierung der Antennen wichtig, die Empfangsstärke in verschiedenen Positionen zu erkennen. Die WLAN-Link-LED kann z. B. für die Phase der Einrichtung zur Anzeige der Empfangsqualität genutzt werden. In der entsprechenden Betriebsart blinkt die WLAN-Link-LED umso schneller, je besser die Empfangsqualität in der jeweiligen Antennenposition ist.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen

Mögliche Werte:

- Verbindungsanzahl: In dieser Betriebsart zeigt die LED mit einem „inversen Blitzen" die Anzahl der WLAN-Clients an, die bei dem Access Point als Client eingebucht sind. Nach der Anzahl der Blitzer für jeden Client erfolgt eine kurze Pause. Wählen Sie diese Betriebsart dann, wenn Sie das Gerät im Access-Point-Modus betreiben.
- Client-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des Access Points an, bei dem ein Gerät selbst als Client eingebucht ist. Je schneller die LED blinkt, umso besser ist das Signal. Wählen Sie diese Betriebsart nur, wenn Sie das Gerät im Client-Modus betreiben.
- P2P1- bis P2P6-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des jeweiligen P2P-Partners, mit dem ein Gerät eine P2P-Strecke bildet. Je schneller die LED blinkt, umso besser ist das Signal.

Default: Verbindungsanzahl

2.23.20.7.5 Link-Fehler-Erkennung

Wenn ein Access Point keine Verbindung zum kabelgebundenen LAN hat, kann er in den meisten Fällen seine wesentliche Aufgabe – den eingebuchten WLAN-Clients einen Zugang zum LAN zu ermöglichen – nicht mehr erfüllen. Mit der Funktion der Broken-Link-Detection (Link-Fehler-Erkennung) können die WLAN-Module eines Geräts deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim Access Point eingebuchten Clients einen anderen Access Point (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden.

Bis zur LCOS-Version 7.80 bezog sich die Aktivierung der Link-Fehler-Erkennung immer auf LAN-1, auch wenn das Gerät über mehrere LAN-Interfaces verfügte. Außerdem wirkte sich die Deaktivierung auf alle verfügbaren WLAN-Module des Gerätes aus. Ab LCOS-Version 8.00 kann die Link-Fehler-Erkennung gezielt an ein bestimmtes LAN-Interface gebunden werden.

Mit dieser Funktion werden die WLAN-Module des Geräts deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Betriebs-Einstellungen/Link-Fehler-Erkennung

Mögliche Werte:

- Nein: Link-Fehler-Erkennung wird nicht genutzt.
- LAN-1 bis LAN-n (je nach verfügbaren LAN-Interfaces im Gerät): Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

Default:

- Nein

Die Interface-Bezeichnungen LAN-1 bis LAN-n repräsentieren die logischen LAN-Schnittstellen. Die verfügbaren physikalischen Ethernet-Ports des Geräts müssen zur Nutzung dieser Funktion ggf. auf die entsprechenden Werte LAN-1 bis LAN-n eingestellt werden.

Die Link-Fehler-Erkennung kann auch für WLAN-Geräte in der Betriebsart als WLAN-Client genutzt werden. Bei eingeschalteter Link-Fehler-Erkennung werden die WLAN-Module eines WLAN-Clients nur dann aktiviert, wenn die entsprechenden LAN-Schnittstellen eine Verbindung zum kabelgebunden LAN haben.

2.23.20.8 Radio-Einstellungen

Hier können Sie Einstellungen am physikalischen Sende- und Empfangsverhalten ihrer WLAN-Schnittstelle vornehmen.

SNMP-ID: 2.23.20.8

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.8.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.8.2 Sende-Leistungs-Reduktion

Im Gegensatz zum Antennen-Gewinn reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- 0 bis 999 dB

Default: 0

Durch die Sendeleistungsreduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

2.23.20.8.3 5GHz-Modus

Wenn Sie gleichzeitig zwei benachbarte, freie Kanäle für die Funkübertragung nutzen, können Sie die Übertragungsgeschwindigkeit mit dem Turbo-Modus auf bis zu 108 MBit/s steigern.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Normal (54 Mbit/s-Modus)
- 108 Mbit/s (Turbo-Modus)

Default: Normal (802.11a) oder 802.11a/n gemischt (bei 11n-Geräten)

Diese Einstellung ist nur verfügbar für Geräte, die DFS2 bzw. DFS3 beherrschen.

2.23.20.8.4 Maximalentfernung

Bei sehr großen Entfernungen zwischen Sender und Empfänger im Funknetz steigt die Laufzeit der Datenpakete. Ab einer bestimmten Grenze erreichen die Antworten auf die ausgesandten Pakete den Sender nicht mehr innerhalb der erlaubten Zeit. Mit der Angabe des maximalen Abstands kann die Wartezeit auf die Antworten erhöht werden. Diese Distanz wird umgerechnet in eine Laufzeit, die den Datenpakete bei der drahtlosen Kommunikation zugestanden werden soll.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- 0 bis 65535 km

Default: 0

2.23.20.8.6 Band

Mit der Auswahl des Frequenzbandes legen Sie fest, ob die WLAN-Karte im 2,4 GHz- oder im 5 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- 2,4 GHz

- 5 GHz

Default: 2.4 Ghz

2.23.20.8.7 Unterbaender

Im 5 GHz-Band kann neben dem Frequenzband ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Je nach gewähltem Frequenzband

Default: Band-1

2.23.20.8.8 Funk-Kanal

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Je nach gewähltem Frequenzband und nach gewähltem Land.

Default: 11

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

2.23.20.8.9 2.4GHz-Modus

Im 2,4 GHz-Band gibt es zwei verschiedene Funk-Standards: den IEEE 802.11b-Standard mit einer Übertragungsgeschwindigkeit von bis zu 11 MBit/s und den IEEE 802.11g-Standard mit bis zu 54 MBit/s. Wenn als Frequenzband das 2,4 GHz-Band ausgewählt ist, kann zusätzlich die Übertagungsgeschwindigkeit eingestellt werden.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere Clients nicht auszuschließen, bietet sich der 802.11g/b-Kompatibilitätsmodus an. In diesem Modus arbeitet die WLAN-Karte im Access Point grundsätzlich nach dem schnelleren Standard, fällt aber auf den langsameren Modus zurück, wenn sich entsprechende Clients im WLAN anmelden. Im '2-MBit-Kompatibilitätsmodus' unterstützt der Access Point auch die älteren 802.11b-Karten mit einer maximalen Übertragungsgeschwindigkeit von 2 MBit/s.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- 802.11g/b gemischt
- 802.11g/b 2 Mbit-kompatibel
- 802.11b (11 Mbit)
- 802.11g (54 Mbit)
- 802.11g (108 Mbit)

Default: 802.11b/g gemischt oder 802.11b/g/n gemischt (bei 11n-Geräten)

Bitte beachten Sie, dass sich Clients, die nur einen langsameren Standard unterstützen, sich ggf. nicht mehr in Ihrem WLAN anmelden können, wenn Sie die Übertragungsgeschwindigkeit auf einen hohen Wert einstellen.

2.23.20.8.10 AP-Dichte

Mit zunehmender Dichte von Access Points überlagern sich die Empfangsbereich der Antennen. Mit der Einstellung der 'Basisstations-Dichte' kann die Empfangs-Empfindlichkeit der Antennen reduziert werden.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Niedrig
- Mittel
- Hoch
- Mini-Zelle
- Mikro-Zelle

Default: Niedrig

2.23.20.8.12 Antennengewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und (evtl.) Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Die Sendeleistung kann minimal auf 0,5 dBm im 2,4-GHz-Band bzw. 6,5 dBm im 5-GHz-Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4-GHz-Band auf 17,5 dBi, im 5-GHz-Band auf 11,5 dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel: AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte: max. 4 Zeichen

Default: 3

Das Minimum von 6,5 dBm gilt nur bei alten abg-Funkmodulen mit WLAN im G-Modus.

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

2.23.20.8.13 Kanalliste

Bei automatischer Kanalwahl oder im Client-Modus legt dieses Feld die Untermenge der zu benutzenden Kanäle fest.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Kommaseparierte Liste von einzelnen Zahlen oder Bereichen.

Default: leer

2.23.20.8.14 Hintergrund-Scan

Zur Erkennung anderer Access Points in der eigenen Funkreichweite können die Geräte die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der Access Points abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Wird hier ein Wert angegeben, so sucht das Gerät innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

Für Geräte im Access-Point-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte Access Points erkannt werden sollen, z. B. 1 Stunde.

Für Geräte im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- 0 bis 4294967295

Default: 0

Besondere Werte: 0: Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

2.23.20.8.15 DFS-Rescan-Stunden

Über diesen Parameter legen Sie fest, zu welchen Stunden (0-24) das Gerät die DFS-Datenbank löscht und einen DFS-Rescan durchführt. Für die Definition der Stunde lassen sich die Möglichkeiten der cron-Befehle nutzen: Z. B. `1,6,13` für einen DFS-Rescan immer um 1 Uhr, 6 Uhr und 13 Uhr oder `0-23/4` für einen DFS-Scan in der Zeit von 0 bis 23 Uhr alle vier Stunden.

Beim DFS-Rescan scannt der AP solange nach freien Kanälen, bis er das konfigurierte Minimum an freien Kanälen gefunden hat. Die minimale Anzahl der freien Kanäle definieren Sie über den Parameter *2.23.20.8.27 DFS-Rescan-Kanalzahl* auf Seite 488. Ist noch kein erzwungener Kanalwechsel erfolgt und wurden beim letzten DFS-Scan genug freie Kanäle gefunden, um das Minimum an freien Kanälen zu erfüllen, führt das Gerät keinen DFS-Rescan durch.

Voraussetzung für das Terminieren eines DFS-Scans ist eine korrekte Systemzeit im Gerät.

Das DFS-Verfahren selbst ist in einigen Ländern zur automatischen Kanalsuche vorgeschrieben. Beim DFS-Verfahren (Dynamic Frequency Selection) wählt ein AP automatisch eine freie Frequenz, z. B. um das Stören von Radaranlagen zu verhindern und um WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Beim Booten wählt das Gerät aus den (z. B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus. Anschließend prüft das Gerät, ob auf diesem Kanal ein Radarsignal vorhanden ist und ob auf diesem Kanal schon ein anderes WLAN arbeitet. Dieser Scan-Vorgang wird solange wiederholt, bis hinreichend radarfreie Kanäle mit möglichst wenig anderen Netzwerken gefunden sind. Anschließend wählt das Gerät einen der freien Kanäle aus und beobachtet diesen Kanal für 60 Sekunden, um evtl. auftretende Radarsignale sicher auszuschließen. Die Datenübertragung kann daher durch diesen Scan-Vorgang und die erneute Suche eines freien Kanals für 60 Sekunden unterbrochen werden.

Indem Sie bestimmte Zeiten für einen DFS-Rescan angeben, reduzieren Sie die Wahrscheinlichkeit, dass der 60-Sekunden-Scanvorgang im späteren Betrieb zu einer unpassenden Zeit auslöst.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

Kommasepartierte Liste. Max. 19 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Besondere Werte:

leer

Das Gerät führt einen DFS-Rescan erst dann durch, wenn kein freier Kanal mehr verfügbar ist. Dies ist dann der Fall, wenn die beim initialen DFS-Scan ermittelten Kanäle die minimale Anzahl der freien Kanäle unterschreiten.

Default-Wert:

leer

2.23.20.8.17 Antennen-Maske

Um den Gewinn durch Spatial-Multiplexing zu optimieren ist es notwendig die Antennengruppierung optimal zu konfigurieren. In der Standardeinstellung wird die Gruppierung automatisch anhand der gegenwärtigen Bedingungen optimal gewählt. Weiterhin haben Sie die Möglichkeit eine Antennengruppe mit beliebiger Antennenkombination manuell einzustellen. Die Einstellung hat sowohl Einfluss auf das Abstrahl-, als auch auf das Empfangsverhalten des Funksystems.

SNMP-ID: 2.23.20.8.17

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Antennen-Maske

Mögliche Werte:

- Auto
- Antenne-1
- Antenne-1+2
- Antenne-1+3
- Antenne-1+2+3

Default: Auto

2.23.20.8.18 Hintergrund-Scan-Einheit

Einheit für die Angabe des Background-Scan-Intervalls

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen

Mögliche Werte:

- Millisekunden
- Sekunden
- Minuten
- Stunden
- Tage

Default: Sekunden

2.23.20.8.19 Kanal-Paarung

Dieser Wert bestimmt bei 11n-Geräten im 40-MHz-Modus, welche Kanalpaare das Gerät verwendet.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Radio-Einstellungen/Kanal-Paarung

Mögliche Werte:

- 11n-konform: das Gerät die Kanäle nach Vorschrift der 802.11n. Dabei verschieben sich die 40-MHz-Kanäle gegenüber den alten, proprietären Kanälen im Turbo-Modus um 20 MHz.
- legacy-turbo-freundlich: nur sinnvoll im Outdoor-Bereich, um Überlappungen mit anderen 11a-Strecken im Turbo-Modus zu vermeiden.

Default: 11n-konform

2.23.20.8.20 Bevorzugtes-DFS-Schema

Um das WLAN-Gerät gemäß aktueller ETSI-Funkstandards zu betreiben, wählen Sie hier den entsprechenden Standard aus.

Beim Upgrade einer LCOS-Version auf einen aktuellen Funk-Standard wird die vorherige Einstellung beibehalten.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Bevorzugtes-DFS-Schema**

Mögliche Werte:

EN 301 893-V1.3
EN 301 893-V1.5
EN 301 893-V1.6
EN 301 893-V1.7

Default-Wert:

EN 301 893-V1.7

2.23.20.8.21 CAC-Dauer

Dauer des Channel-Availibility-Checks. Mit dieser Einstellung bestimmen Sie die Zeit (in Sekunden), wie lange das WLAN-Modul bei der Benutzung von DFS zuerst die Kanäle überprüft, bevor es den eigentlichen Funkkanal wählt und mit der Datenübertragung beginnt.

Die Dauer Channel-Availibility-Checks ist durch entsprechende Normen geregelt (in Europa z. B. durch ETSI EN 301 893). Beachten Sie daher die für Ihr Land gültigen Vorschriften!

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **CAC-Dauer**

Mögliche Werte:

0 bis 4294967295

Default:

60

2.23.20.8.22 Erzwinge-40MHz

Option, mit der das Gerät zwingend die 40-MHz-Bandbreite nutzt.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Erzwinge-40MHz**

Mögliche Werte:

Ja

Nein

Default:

Nein

2.23.20.8.23 Adaptive-Rausch-Immunitaet

Innerhalb eines WLANs kann es aus unterschiedlichen Gründen zu Störungen durch Interferenzen kommen. Einerseits stören Geräte wie Mikrowellenherde oder Funktelefone die Datenübertragung, andererseits können die Netzgeräte selber durch Aussendung von Störfrequenzen die Kommunikation behindern. Die Art dieser Störungen ist jeweils charakteristisch. Bei der adaptiven Rausch-Immunität (Adaptive Noise Immunity, ANI) ermittelt der Access Point anhand verschiedener Fehlerzustände die für die aktuelle Situation beste Kompensation der Störungen. Durch die automatische Erhöhung der Rausch-Immunität wird die Funkzelle gezielt verkleinert, sodass sich die Auswirkungen der Interferenzen auf die Datenübertragung verringern.

Die aktuellen Werte sowie die Aufzeichnung der vergangenen Aktionen finden Sie unter **Status** > **WLAN** > **Rausch-Immunität**.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

nein

ja

Default:

ja

2.23.20.8.24 Max.-Kanal-Bandbreite

Geben Sie den maximalen Frequenzbereich an, in dem die physikalische WLAN-Schnittstelle die zu übertragenen Daten auf die Trägersignale aufmoduliert (Kanal-Bandbreite).

In der Einstellung **Auto** stellt der AP die Kanal-Bandbreite optimal ein. Sie haben aber auch die Möglichkeit, die Automatik abzuschalten, um die Kanal-Bandbreite bewusst zu begrenzen. Die verfügbaren möglichen Werte sind abhängig von den unterstützten WLAN-Standards des Geräts.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

Auto
Der AP stellt die Kanal-Bandbreite automatisch optimal ein. Dabei lässt der AP die maximal verfügbare Bandbreite zu, sofern die momentanen Betriebsbedingungen dies erlauben. Andernfalls begrenzt der AP die Kanal-Bandbreite auf 20MHz.

20MHz
Der AP benutzt auf 20MHz gebündelte Kanäle.

40MHz
Der AP benutzt auf 40MHz gebündelte Kanäle.

80MHz
Der AP benutzt auf 80MHz gebündelte Kanäle.

Default-Wert:

Auto

2.23.20.8.25 Allow-PHY-Restarts

Über diesen Parameter legen Sie fest, ob das Gerät PHY-Restarts erlaubt, um bei Signalüberlagerungen trotzdem auswertbare Informationen zu erhalten.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

nein

Diese Einstellung verbietet PHY-Restarts. Das WLAN-Modul verwirft die überlagerten Datenpakete und fordert sie neu an.

ja

Diese Einstellung erlaubt PHY-Restarts. Das WLAN-Modul wertet bei einer Überlagerung von zwei zeitgleich empfangenen WLAN-Paketen das jeweils stärkere aus.

Default-Wert:

ja

2.23.20.8.26 DFS-Rescan-Kanaele-loeschen

Über diesen Parameter legen Sie fest, ob die physikalische WLAN-Schnittstelle nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle löscht oder für weitere DFS-Rescans zwischenspeichert.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

ja

Die physikalische WLAN-Schnittstelle löscht nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, damit diese bei einem erneuten DFS-Rescan wieder zur Verfügung stehen.

nein

Das Gerät speichert nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, sodass das Gerät diese Kanäle bei einem erneuten DFS-Rescan sofort überspringt.

Default-Wert:

nein

2.23.20.8.27 DFS-Rescan-Kanalzahl

Über diesen Parameter definieren Sie das Minimum an freien Kanälen, welches ein DFS-Scanvorgang erreichen muss.

Bei dem Standardwert von 2 führt der AP so lange einen DFS-Scan durch, bis 2 freie Kanäle vorhanden sind. Erkennt der AP im späteren Betrieb ein aktives Radarmuster, ist immer noch ein weiterer freier Kanal verfügbar, auf den der AP direkt wechseln kann.

Eine hohe Kanalzahl sorgt dafür, dass das Gerät beim initialen DFS-Scan sehr viele Kanäle scannen muss. Ein Scan-Vorgang pro Kanal dauert 60 Sekunden. Bitte beachten Sie in diesem Zusammenhang auch die unter *2.23.20.8.15 DFS-Rescan-Stunden* auf Seite 484 gegebenen Informationen.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

0 … 4294967295

Besondere Werte:

0

Dieser Wert deaktiviert die Beschränkung. Die physikalische WLAN-Schnittstelle führt einen DFS-Scan auf sämtlichen zur Verfügung stehenden Kanälen aus.

Default-Wert:

2

2.23.20.8.28 Bevorzugtes-2.4-Schema

Über diesen Parameter legen Sie fest, nach welcher Version der EN 300 328 das Gerät im 2,4-GHz-Band operiert.

Bei einem Firmware-Update wird die aktuelle Version beibehalten. Neue Geräte und Geräte, bei denen ein Konfigurations-Reset durchgeführt wurde, verwenden standardmäßig Version 1.8.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

EN300328-V1.7
EN300328-V1.8

Default-Wert:

EN300328-V1.8

2.23.20.9 Leistung

Hier können Sie Parameter definieren, die Einfluss auf die Leistung ihrer WLAN-Schnittstelle haben.

SNMP-ID: 2.23.20.9

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.9.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Leistung

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.9.2 Tx-Bursting

Erlaubt/Verbietet das Paket-Bursting, was den Durchsatz erhöht, jedoch die Fairness auf dem Medium verschlechtert.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Leistung

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.23.20.9.5 QoS

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienst-güten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voiceoder WLAN – VoWLAN).Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM(Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video,Best Effort und Hintergrund) die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

Pfad Telnet: /Setup/Schnittstellen/WLAN/Leistung

Mögliche Werte:

- Ein
- Aus

Default: Aus

Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der Access Point den802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechen-den Prioritäten kennzeichnen.

2.23.20.10 Beaconing

Die Beaconing-Einstellungen sind nur in der Basisstations-Betriebsart von Bedeutung. Die Wireless-LAN-Basisstation (WLAN-AP) sendet regelmäßig ein Funksignal (Beacon), damit die Clients ihn bzw. die durch ihn aufgespannten logischen WLAN-Netze (SSIDs) finden können.

SNMP-ID: 2.23.20.10

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.10.1 Ifc

Öffnet die Experten-Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Beaconing

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.10.2 Beacon-Periode

Dieser Wert gibt den zeitlichen Abstand in Kµs an, in dem Beacons verschickt werden (1 Kµs entspricht 1024 Mikrosekunden und stellt eine Recheneinheit des 802.11-Standard dar – 1 Kµs wird auch als Timer Unit TU bezeichnet). Niedrigere Werte ergebenen kleinere Beacon-Timeout-Zeiten auf dem Client und erlauben damit ein schnelleres Roaming beim Access Point-Ausfall, erhöhen aber den Overhead auf dem WLAN.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Beaconing

Mögliche Werte:

- 20 bis 65535 TU

Default: 100

2.23.20.10.3 DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Beaconing

Mögliche Werte:

- 1 bis 255

Default: 1

2.23.20.10.4 Beacon-Abfolge

Die Beacon-Abfolge bezeichnet die Reihenfolge, in der die Beacon zu den verschiedenen WLAN-Netzen versendet werden. Wenn z. B. drei logische WLAN-Netze aktiv sind und die Beacon-Periode 100 Kµs beträgt, so werden alle 100 Kµs die Beacons für die drei WLANs verschickt. Je nach Beacon-Abfolge werden die Beacons zu folgenden Zeitpunkten versendet

Pfad Telnet: /Setup/Schnittstellen/WLAN/Beaconing

Mögliche Werte:

- Zyklisch: In diesem Modus beginnt der Access Point beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, gefolgt von WLAN-2 und WLAN-3. Beim zweiten Beacon-Versand (100 Kµs) wird zuerst WLAN-2 versendet, das WLAN-3 und erst dann kommt wieder WLAN-1 an die Reihe. Beim dritten Beacon-Versand (200 Kµs) entsprechend WLAN-3, WLAN-1, WLAN-2 – dann beginnt die Reihe wieder von vorne.
- Gestaffelt: In diesem Modus werden die Beacons nicht gemeinsam zu einem Zeitpunkt verschickt, sondern auf die verfügbare Beacon-Periode aufgeteilt. Zum Start bei 0 Kµs wird nur WLAN-1 verschickt, nach 33,3 Kµs kommt WLAN-2, nach 66,6 Kµs WLAN-3 – mit Beginn einer neuen Beacon-Periode startet der Versand wieder mit WLAN-1.
- Einfach-Burst: In diesem Modus verschickt der Access Point die Beacons für die definierten WLAN-Netze immer in der gleichen Abfolge. Beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, WLAN-2 und WLAN-3, beim zweiten Versand nach dem gleichen Muster und so weiter.

Default: zyklisch

Ältere WLAN-Clients sind manchmal nicht in der Lage, die schnell aufeinander folgenden Beacons richtig zu verarbeiten, wie sie bei einem einfachen Burst auftreten. In der Folge erkennen diese Clients oft nur die ersten Beacons und können sich daher auch nur bei diesem einem Netz einbuchen. Die gestaffelte Aussendung der Beacons führt zum besten Ergebnis, erhöht aber die Prozessorlast für den Access Point. Die zyklische Aussendung stellt sich als guter Kompromiss dar, weil hier jedes Netz einmal als erstes ausgesendet wird.

2.23.20.11 Roaming

Die Roaming-Einstellungen sind nur in der Client-Betriebsart von Bedeutung. Sie regeln ob und wann der Client seine Basis-Station wechselt, wenn er mehr als eine Basisstation erreichen kann.

SNMP-ID: 2.23.20.11

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.11.1 Ifc

Öffnet die Experten-Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.11.2 Beacon-Verlust-Schwellwert

Der Beacon-Verlust-Schwellwert gibt an, wie viele Beacons der Access Points empfangsgestört sein dürfen, bevor ein eingebuchter Client eine erneute Suche beginnt.

Je höher der eingestellte Wert ist, desto eher kann es unbemerkt zu einer Unterbrechung der Verbindung kommen, gefolgt von einem zeitverzögerten Wiederaufbau der Verbindung.

Je kleiner der eingestellte Wert ist, desto eher kann eine möglicherweise folgende Unterbrechung erkannt werden, der Client kann frühzeitig mit dem Suchen nach einem alternativen Access Point beginnen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 4

Zu kleine Werte können dazu führen, dass der Client unnötig oft einen Verbindungsverlust erkennt.

2.23.20.11.3 Roaming-Schwellwert

Dieser Schwellwert gibt an, um wieviel Prozent die Signalstärke eines anderen Access Points besser sein muss, damit der Client auf den anderen Access Point wechselt.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 15

In anderem Zusammenhang wird die Signalstärke teilweise in dB angegeben. In diesen Fällen gilt für die Umrechnung:

64dB - 100%

32dB - 50%

0dB - 0%

2.23.20.11.4 Kein-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle Access Point als so gut betrachtet wird, dass auf keinen Fall auf einen anderen Access Point gewechselt wird.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 45

2.23.20.11.5 Zwangs-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle Access Point als so schlecht betrachtet wird, dass auf jeden Fall auf einen anderen, besseren Access Point gewechselt wird.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 12

2.23.20.11.6 Soft-Roaming

Diese Option ermöglicht dem Client, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren Access Point durchzuführen (Soft-Roaming). Roaming aufgrund eines Verbindungsverlustes (Hard-Roaming) bleibt davon natürlich unbeeinflusst. Die eingestellten Roaming-Schwellwerte haben nur eine Funktion, wenn Soft-Roaming aktiviert ist.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.23.20.11.7 Verbindungs-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die ein Access Point mindestens aufweisen muss, damit ein Client einen Versuch zum Einbuchen bei diesem Access Point startet.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 0

2.23.20.11.8 Verbindung-Halten-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, die der aktuelle Access Point mindestens aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 99%

Default: 0

2.23.20.11.9 Min.-Verbindungs-Signalpegel

Analog zum Verbindungs-Schwellwert, Angabe jedoch als absolute Signalstärke

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis -128 dBm

Default: 0

2.23.20.11.10 Min.-Verbindung-Halten-Signalpegel

Analog zum Verbindung-Halten-Schwellwert, Angabe jedoch als absolute Signalstärke

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis -128 dBm

Default: 0

2.23.20.11.11 Sperrzeit

In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkte (gleiche SSID auf mehreren Access Points) können Sie hier einen Zeitraum zu definieren, in dem sich der WLAN-Client nicht mehr mit einem Access Point verbindet, nachdem die Anmeldung an diesem Access Point abgelehnt wurde (Association-Reject).

Pfad Telnet: /Setup/Schnittstellen/WLAN/Roaming

Mögliche Werte:

- 0 bis 4294967295 in Sekunden
- maximal 10 Zeichen

Default:

- 0

2.23.20.12 Interpoint-Gegenstellen

Tragen Sie hier die WLAN-Basisstation ein, die über Punkt-zu-Punkt-Verbindung vernetzt werden sollen.

SNMP-ID: 2.23.20.12

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.12.1 Ifc

Öffnet die Einstellungen für die Punkt-zu-Punkt-Partner.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

Mögliche Werte:

- Auswahl aus den verfügbaren Punkt-zu-Punkt-Verbindungen.

2.23.20.12.2 Erkenne-An

Wählen Sie hier aus, anhand welchen Merkmals die P2P-Gegenstelle identifiziert werden soll.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

Mögliche Werte:

- MAC-Adresse: Wählen Sie diese Einstellung, wenn die Geräte den P2P-Partner anhand der MAC-Adresse erkennen können. Tragen Sie in diesem Fall als 'MAC-Adresse' die WLAN-MAC-Adresse der physikalischen WLAN-Schnittstelle des P2P-Partners ein.
- Stations-Name: Wählen Sie diese Einstellung, wenn die Geräte den P2P-Partner anhand des Stations-Namens erkennen können. Tragen Sie in diesem Fall als 'Gegenstellen-Name' den Geräte-Names des P2P-Partners ein oder alternativ den als 'Stations-Name' in den physikalischen Einstellungen definierten Namen.
- Serial-Autoconfig: Wählen Sie diese Einstellung, wenn die P2P-Partner beim Start der Geräte die MAC-Adresse über eine serielle Verbindung austauschen.

Default: MAC-Adresse

2.23.20.12.3 MAC-Adresse

MAC-Adresse der P2P-Gegenstelle

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

Mögliche Werte:

- Gültige MAC-Adresse

Default: Leer

Wenn Sie die Erkennung durch MAC-Addresse verwenden, dann tragen Sie hier die MAC-Addresse des WLAN-Adapters und nicht die des Gerätes selbst ein.

2.23.20.12.4 Gegenstellen-Name

Stations-Name der P2P-Gegenstelle

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

max. 24 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.23.20.12.5 Aktiv

Aktiviert bzw. deaktiviert diesen Punkt-zu-Punkt-Kanal.

Pfad Telnet: Setup/Schnittstellen/WLAN/Interpoint-Gegenstellen

Mögliche Werte:

- Ein
- Aus

Default: Aus

2.23.20.12.6 Tx-Limit

Mit dieser Einstellung begrenzen Sie die Bandbreite des Uplinks (in Kbit/s) für die konfigurierte Punkt-zu-Punkt-Verbindung. Der Wert `0` deaktiviert die Begrenzung (= unlimitierte Bandbreite).

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.23.20.12.7 Rx-Limit

Mit dieser Einstellung begrenzen Sie die Bandbreite des Downlinks (in Kbit/s) für die konfigurierte Punkt-zu-Punkt-Verbindung. Der Wert `0` deaktiviert die Begrenzung (= unlimitierte Bandbreite).

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.23.20.12.8 Schluessel

Geben Sie die WPA2-Passphrase für die P2P-Verbindung an. Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

min. 8 Zeichen; max. 63 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.` `

2.23.20.12.9 Verbindungs-Schwellwert

Ein WLAN-Interface kann zu mehr als einer Gegenstelle Punkt-zu-Punkt-Verbindungen betreiben, und jede dieser Verbindungen kann eine andere 'nominale' Signal-Stärke haben.

- Der **Verbindungs-Schwellwert** definiert die Beacon-Signal-Stärke, mit der die Gegenseite gesehen werden muss, um die Punkt-zu-Punkt-Verbindung aufzubauen.
- Der **Verbindung-halten-Schwellwert** definiert die Beacon-Signal-Stärke, mit der die Gegenseite gesehen werden muss, um eine bestehende Punkt-zu-Punkt-Verbindung zu halten.

Beide Werte repräsentieren den erforderlichen Signal-Rausch-Abstand (SNR) in Prozent. Der Zweck zweier unterschiedlicher Werte ist, eine Hysterese aufzuspannen, welche Verbindungs-Zustands-Flattern vermeidet. Schnelle Verbindungs-Zustands-Wechsel würden andernfalls zu Instabilitäten – z. B. in den Topologie-Entscheidungen des Spanning-Tree-Algorithmusses – führen.

Der **Verbindung-halten-Schwellwert** muss kleiner zu sein als der **Verbindungs-Schwellwert**. Der Wert `0` deaktiviert die betreffenden Grenzen.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

0 bis 255

Default:

0

2.23.20.12.10 Verbindung-halten-Schwellwert

Ein WLAN-Interface kann zu mehr als einer Gegenstelle Punkt-zu-Punkt-Verbindungen betreiben, und jede dieser Verbindungen kann eine andere 'nominale' Signal-Stärke haben.

- Der **Verbindungs-Schwellwert** definiert die Beacon-Signal-Stärke, mit der die Gegenseite gesehen werden muss, um die Punkt-zu-Punkt-Verbindung aufzubauen.
- Der **Verbindung-halten-Schwellwert** definiert die Beacon-Signal-Stärke, mit der die Gegenseite gesehen werden muss, um eine bestehende Punkt-zu-Punkt-Verbindung zu halten.

Beide Werte repräsentieren den erforderlichen Signal-Rausch-Abstand (SNR) in Prozent. Der Zweck zweier unterschiedlicher Werte ist, eine Hysterese aufzuspannen, welche Verbindungs-Zustands-Flattern vermeidet. Schnelle Verbindungs-Zustands-Wechsel würden andernfalls zu Instabilitäten – z. B. in den Topologie-Entscheidungen des Spanning-Tree-Algorithmusses – führen.

Der **Verbindung-halten-Schwellwert** muss kleiner zu sein als der **Verbindungs-Schwellwert**. Der Wert `0` deaktiviert die betreffenden Grenzen.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Gegenstellen**

Mögliche Werte:

0 bis 255

Default:

0

2.23.20.13 Netzwerk-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Netzwerk-Alarm-Grenzen für die logischen WLAN-Netzwerke des Gerätes (SSIDs).

SNMP-ID: 2.23.20.13

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.13.1 Ifc

Wählen Sie hier das logische WLAN_Netzwerk (SSID), für welches Sie die Netzwerk-Alarm-Grenzen bearbeiten möchten.

SNMP-ID: 2.23.20.13.1

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren SSIDs, z. B. WLAN-1, WLAN-1-2 etc.

2.23.20.13.2 Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden SSID. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.2

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 3 numerische Zeichen

Default: 0

2.23.20.13.3 Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.3

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

2.23.20.13.4 Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende SSID. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.13.4

Pfad Telnet: /Setup/Schnittstellen/WLAN/Netzwerk-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

2.23.20.14 Interpoint-Alarm-Grenzen

In dieser Tabelle finden Sie die Einstellungen der Interpoint-Alarm-Grenzen für P2P-Verbindungen des Gerätes (SSIDs).

SNMP-ID: 2.23.20.14

Pfad Telnet: /Setup/Schnittstellen/WLAN

2.23.20.14.1 Ifc

Wählen Sie hier die P2P-Verbindung, für welche Sie die Interpoint-Alarm-Grenzen bearbeiten möchten.

SNMP-ID: 2.23.20.14.1

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren P2P-Verbindungen, z. B. P2P-1-1, P2P-1-2 etc.

2.23.20.14.2 Phy-Signal

Der negative Grenzwert für den Signalpegel der entsprechenden P2P-Verbindung. Wird dieser Grenzwert unterschritten, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.2

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 3 numerische Zeichen

Default: 0

2.23.20.14.3 Total-Wiederholungen

Der Grenzwert für die Gesamtanzahl an Sendewiederholungen für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.3

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

2.23.20.14.4 Tx-Fehler

Die Gesamtanzahl der verlorenen Pakete für die entsprechende P2P-Verbindung. Sobald der Wert erreicht ist, wird ein Alarm abgesetzt. Der Wert 0 entspricht einer Deaktivierung der Prüfung.

SNMP-ID: 2.23.20.14.4

Pfad Telnet: /Setup/Schnittstellen/WLAN/Interpoint-Alarm-Grenzen

Mögliche Werte:

- 4 numerische Zeichen zur Angabe der Wiederholungen in Promille

Default: 0 Promille

2.23.20.15 Probe-Einstellungen

In dieser Tabelle befinden sich die Einstellungen für den Spectral Scan.

In diesem Betriebsmodus kann das Gerät weder Daten senden noch empfangen.

Pfad Telnet:

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

2.23.20.15.1 Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

2.23.20.15.2 Radio-Baender

Hier können Sie auswählen, welche Frequenzbänder der Spectral Scan untersuchen soll.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

2,4GHz

5GHz

2,4GHz/5GHz

Default:

2,4GHz

2.23.20.15.3 Unterbaender-2.4GHz

Bestimmen Sie hier die zu untersuchenden Unterbänder der 2,4GHz-Frequenz.

Der Spectral Scan beachtet dieses Feld nur, wenn unter **Radio-Baender** entweder '2,4GHz' oder '2,4GHz/5GHz' eingestellt ist.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Band-1

Band-2

Band-1+2

Default:

Band-1

2.23.20.15.4 Kanalliste-2.4GHz

In diesem Feld bestimmen Sie die Kanalliste für den Spectral Scan im 2,4GHz-Frequenzband. Trennen Sie die einzelnen Kanäle durch Kommas.

Für den Betrieb müssen Sie die Default-Werte des Spectral Scans nicht verändern. Der Spectral Scan fragt jeweils 20MHz breite Frequenzbereiche ab. Aufgrund der 5MHz-Abstände zwischen den einzelnen 20MHz breiten Kanälen des 2,4GHz-Radiobandes ergibt sich mit den vorgegebenen Kanälen ein durchgängiger Scan des gesamten 2,4GHz-Radiobandes. Im 5GHz-Band beträgt die Kanalbandbreite ebenfalls 20MHz, und die einzelnen Kanäle liegen überlappungsfrei nebeneinander. Keine Kanalvorgabe bedeutet, dass alle Kanäle gescannt werden, was im 5GHz-Band zu einem vollständigen Scan führt.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max. 48 Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

1,5,9,13

2.23.20.15.5 Unterbaender-5GHz

Bestimmen Sie hier die zu untersuchenden Unterbänder der 5GHz-Frequenz.

Der Spectral Scan beachtet dieses Feld nur, wenn unter **Radio-Baender** entweder '5GHz' oder '2,4GHz/5GHz' eingestellt ist.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Band-1

Band-2

Band-1+2

Default:

Band-1

2.23.20.15.6 Kanalliste-5GHz

In diesem Feld bestimmen Sie die Kanalliste für den Spectral Scan im 5GHz-Frequenzband. Trennen Sie die einzelnen Kanäle durch Kommas.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max. 48 Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.23.20.15.7 Kanal-Verweil-Zeit

Bestimmen Sie hier, wie viele Millisekunden der Spectral Scan auf einem Kanal verweilen soll.

Die Web-Applikation kann über den Time-Slider bis zu 300 Messwerte im Wasserfall-Diagramm zur Anzeige bringen, wobei sie insgesamt die Messwerte von maximal 24 Stunden zwischenspeichern kann. In der Regel ist der Default-Wert ausreichend. Sie sollten den Wert nur heruntersetzen, wenn Sie eine genauere zeitliche Auflösung benötigen und Ihr Browser bzw. Ihr PC genügend Performance besitzt, die schnellere Darstellung der Messwerte zu verarbeiten.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max 10 Zeichen

von 0 bis 9

Default:

250

2.23.20.16 IEEE802.11u

Die Tabelle **IEEE802.11u** ist die höchste Verwaltungsebene für 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jede Schnittstelle ein- oder auszuschalten, Ihnen unterschiedliche Profile zuzuweisen oder allgemeine Einstellungen vorzunehmen.

Pfad Telnet:

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

2.23.20.16.1 Ifc

Name der logischen WLAN-Schnittstelle, die Sie gerade bearbeiten.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

2.23.20.16.2 Operating

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – respektiv für die dazugehörige SSID – das Interworking-Element in den Beacons/Probes. Dieses Element dient als Erkennungsmerkmal für IEEE 802.11u-fähige

Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

2.23.20.16.3 Hotspot2.0

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinformationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

Diese Funktion setzt die aktivierte Unterstützung für Verbindungen nach IEEE 802.11u voraus!

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

2.23.20.16.4 Internet

Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

2.23.20.16.5 Network-Typ

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

- `Private`: Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.
- `Private-GuestAcc`: Wie `Private`, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B. für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.
- `Public-Charge`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.
- `Public-Free`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.
- `Personal-Dev`: Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.
- `Emergency`: Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.
- `Experimental`: Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.
- `Wildcard`: Platzhalter für bislang undefinierte Netzwerk-Typen.

Default:

Private

2.23.20.16.6 Asra

Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und/oder **WISPr** für das Public-Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

ja

nein

Default:

nein

2.23.20.16.7 HESSID

Geben Sie an, woher das Gerät seine HESSID für das homogene ESS bezieht. Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von Access Points, die alle dem selben Netzwerk angehören. Als weltweit eindeutige

Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen Access Points (seine BSSID). Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie "HOTSPOT".

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

BSSID

user

none

Default:

BSSID

2.23.20.16.8 HESSID-MAC

Sofern Sie als **HESSID** die Einstellung `user` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen Access Apoints in Ihrem homogenen ESS in Großbuchstaben und ohne Trennzeichen, z. B. `008041AEFD7E` für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern Ihr Gerät nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle Schnittstellen identisch!

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

MAC-Adresse, in Großbuchstaben und ohne Trennzeichen

Default:

000000000000

2.23.20.16.10 ANQP-Profil

Über diesen Parameter spezifizieren Sie ein gültiges ANQP-Profil.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **ANQP-Profile**, max. 32 Zeichen

Default:

2.23.20.16.13 HS20-Profil

Über diesen Parameter spezifizieren Sie ein gültiges Hotspot-2.0- bzw. HS20-Profil.

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **IEEE802.11u**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profile**, max. 32 Zeichen

Default:

2.23.20.19 Interpoint-Uebertragung

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

Pfad Telnet:

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

2.23.20.19.1 Ifc

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

Pfad Telnet:

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

Mögliche Werte:

Auswahl aus den verfügbaren P2P-Strecken.

2.23.20.19.2 Paketgroesse

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

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

Pfad Telnet:

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

Mögliche Werte:

600 … 2347

Default-Wert:

1600

2.23.20.19.3 Min-Tx-Rate

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

Auto

2.23.20.19.6 RTS-Schwelle

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

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

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

Pfad Telnet:

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

Mögliche Werte:

60 … 2347

Default-Wert:

2347

2.23.20.19.7 11b-Praeambel

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

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

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

Pfad Telnet:

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

Mögliche Werte:

Auto

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

Lang

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

Default-Wert:

Auto

2.23.20.19.9 Max-Tx-Rate

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

Auto

2.23.20.19.10 Min.-Frag.-Laenge

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

Pfad Telnet:

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

Mögliche Werte:

0 … 65535

Besondere Werte:

0, 1

Das Gerät lässt Paket-Fragmente mit beliebiger Länge zu.

Default-Wert:

16

2.23.20.19.11 Soft-Retries

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

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

Pfad Telnet:

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

Mögliche Werte:

0 … 255

Default-Wert:

10

2.23.20.19.12 Hard-Retries

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

Pfad Telnet:

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

Mögliche Werte:

0 … 255

Default-Wert:

10

2.23.20.19.13 Kurzes-Guard-Intervall

Aktivieren oder deaktivieren Sie das kurze Guard-Intervall.

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

Pfad Telnet:

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

Mögliche Werte:

Auto

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

Nein

Deaktiviert das kurze Guard-Intervall.

Default-Wert:

Auto

2.23.20.19.14 Max.-Spatiale-Stroeme

Geben Sie die Maximalanzahl der erlaubten Spatial-Streams an.

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

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

Pfad Telnet:

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

Mögliche Werte:

Auto
Einer
Zwei
Drei

Default-Wert:

Auto

2.23.20.19.15 Sende-Aggregate

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

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

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

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.23.20.19.16 Min.-HT-MCS

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

Auto

2.23.20.19.17 Max.-HT-MCS

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

Auto

2.23.20.19.18 Min.-Spatiale-Stroeme

Geben Sie die Mindestanzahl der erlaubten Spatial-Streams an.

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

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

Pfad Telnet:

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

Mögliche Werte:

Auto
Einer
Zwei
Drei

Default-Wert:

Auto

2.23.20.19.19 EAPOL-Rate

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

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

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

Pfad Telnet:

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

Mögliche Werte:

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

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

Default-Wert:

wie-Daten

2.23.20.19.20 Max.-Aggr.-Paket-Anzahl

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

Pfad Telnet:

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

Mögliche Werte:

0 … 11/16/24 (geräteabhängig)

Besondere Werte:

0

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

Default-Wert:

0

2.23.20.19.22 Empfange-Aggregate

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

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

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

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.23.20.19.23 Nutze-STBC

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

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

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.23.20.19.24 Nutze-LDPC

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

LDPC ist eine Methode zur Fehlerkorrektur. Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

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

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.23.20.20 Interpoint-Verschluesselung

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

Pfad Telnet:

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

2.23.20.20.1 Ifc

Name des physikalischen WLAN-Interfaces

Pfad Telnet:

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

2.23.20.20.2 Verschluesselung

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.23.20.20.3 Vorgabeschluessel

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

Pfad Telnet:

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

Mögliche Werte:

0 … 9

Default-Wert:

1

2.23.20.20.4 Methode

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

802.11i-WPA-PSK

2.23.20.20.9 WPA-Version

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

Pfad Telnet:

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

Mögliche Werte:

WPA1
WPA2
WPA1/2

Default-Wert:

WPA1/2

2.23.20.20.11 WPA-Rekeying-Zyklus

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

Bei WPA1/2 erfolgt die Authentifizierung an einem Netz mit einem Pre-Shared-Key (PSK), welcher Teil eines 128 Bit langen individuellen Schlüssels ist. Das Gerät (als Authenticator) generiert diesen Schlüssel mit einem 48 Bit langen Initialization Vector (IV), welcher die Berechnung des WPA-Schlüssels für Angreifer erschwert. Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels erfolgt so erst nach 2^{48} Datenpaketen, die in absehbarer Zeit kein WLAN erreicht.

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

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

Default-Wert:

0

2.23.20.20.12 WPA1-Sitzungsschluessel

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

Pfad Telnet:

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

Mögliche Werte:

TKIP
AES
TKIP/AES

Default-Wert:

TKIP

2.23.20.20.13 WPA2-Sitzungsschluessel

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

Pfad Telnet:

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

Mögliche Werte:

TKIP
AES
TKIP/AES

Default-Wert:

AES

2.23.20.20.14 Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

Pfad Telnet:

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

Mögliche Werte:

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

Zwingend

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

Optional

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

Default-Wert:

Nein

2.23.20.20.19 WPA2-Schluessel-Management

Mit diesen Optionen können Sie die WPA2-Schlüsselverwaltung konfigurieren.

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

Pfad Telnet:

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

Mögliche Werte:

SHA256

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

Standard

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

Default-Wert:

Standard

2.23.21 LAN-Schnittstellen

Dieses Menü enthält die Einstellungen für die LAN-Schnittstellen.

SNMP-ID: 2.23.21

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

2.23.21.1 Ifc

Wählen Sie hier die LAN-Schnittstelle, für welche die folgenden Einstellungen gelten.

SNMP-ID: 2.23.21.1

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen/Ifc

Mögliche Werte:

- Auswahl aus den verfügbaren LAN-Schnittstellen.

2.23.21.2 Anschluss

Wählen Sie hier aus, welchen Netzwerkanschluss Sie für die Verbindung zu Ihrem lokalen Netz verwenden. Wenn Sie die Einstellung **Auto** wählen, wird der benutzte Anschluss vom Gerät automatisch erkannt.

SNMP-ID: 2.23.21.2

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen/Anschluss

Mögliche Werte:

- Auto
- Auto-10
- Auto-100
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX
- FD1000B-TX
- Power-Down

Default: Auto

Die LAN-Schnittstellen des Geräts sind je nach Modell mit unterschiedlicher Hardware ausgestattet. Die erste LAN-Schnittstelle unterstützt bis zu 1000 MBit im Full-Duplex-Modus. Die zweite LAN-Schnittstelle unterstützt maximal 100 MBit im Full-Duplex-Modus.

2.23.21.3 MDI-Modus

Dieser Schalter aktiviert oder deaktiviert das automatische Kreuzen der Sende- und Empfangsleitungspaare (Auto-MIDIX), was den Einsatz von Node/Hub-Schaltern bzw. Crossover-Kabeln überflüssig macht. In Einzelfällen (z. B. bestimmte Glasfaser- Medienkonverter) kann es erforderlich sein, diese Automatik auszuschalten und die Leitungen fix zu kreuzen (MDIX) oder nicht zu kreuzen (MDI).

SNMP-ID: 2.23.21.3

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen/MDI-Modus

Mögliche Werte:

- Auto
- MDI
- MDIX

Default: Auto

2.23.21.5 Takt-Rolle

Ein Ethernet-Port, der im 1000BASE-Tx-Modus arbeitet, erfordert einen kontinuierlichen Datenstrom zwischen beiden verbundenen Partnern, um synchronisiert zu bleiben. Naturgemäß brauchen beide Seiten eine synchronisierte Uhr (Takt), um Daten zu übertragen. IEEE 802.3 führte das Konzept eines Masters und eines Slaves für solche Verbindungen ein. Der Master gibt den Takt zur Datenübertragung in beide Richtungen vor, und der Slave synchronisiert sich auf diesen Takt. Die Rollen als Takt-Master und -Slave werden in der automatischen Aushandlungs-Phase der Verbindung verteilt. Normalerweise braucht diesem Detail keine Beachtung geschenkt zu werden, da die automatische Aushandlung durchaus gut funktioniert. In bestimmten Fällen kann es erforderlich werden, die Master-/Slave-Aushandlung zu beeinflussen. Hierzu dient die Einstellung des Takt-Gebers mit folgenden möglichen Werten:

SNMP-ID: 2.23.21.5

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen/Takt-Rolle

Mögliche Werte:

- Bevorzugt Slave: Dies ist die empfohlene Standard-Einstellung für Geräte, die nicht als Switch eingesetzt werden. Während der Aushandlungs-Phase versucht der Port die Rolle des Slave auszuhandeln. Falls erforderlich, akzeptiert er auch die Rolle des Masters.
- Bevorzugt Master: Während der Aushandlungs-Phase versucht der Port die Rolle des Masters auszuhandeln. Falls erforderlich, akzeptiert er auch die Rolle des Slave.
- Slave: Der Port ist ausschließlich auf die Rolle des Slaves eingestellt. Eine Verbindung wird abgelehnt, wenn beide Verbindungs-Partner die Rolle des Slaves verwenden.
- Master: Der Port ist ausschließlich auf die Rolle des Masters eingestellt. Eine Verbindung wird abgelehnt , wenn beide Verbindungs-Partner die Rolle des Masters verwenden.

Default: Bevorzugt Slave

Die LAN-Schnittstellen des Geräts sind je nach Modell mit unterschiedlicher Hardware ausgestattet. Die Einstellung für den Takt-Geber hat für die zweite LAN-Schnittstelle keine Auswirkung.

2.23.21.7 Aktiv

Aktivieren oder deaktivieren Sie hier die ausgewählte LAN-Schnittstelle.

SNMP-ID: 2.23.21.7

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.23.21.8 Tx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Senderichtung an. Der Wert 0 entspricht keinem Limit.

SNMP-ID: 2.23.21.8

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Mögliche Werte:

- Maximal 10 numerische Zeichen

Default: 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

2.23.21.9 Rx-Limit

Geben Sie hier das Bandbreitenlimit (kbit/s) in Empfangsrichtung an. Der Wert 0 entspricht keinem Limit.

SNMP-ID: 2.23.21.9

Pfad Telnet: /Setup/Schnittstellen/LAN-Schnittstellen

Mögliche Werte:

- Maximal 10 numerische Zeichen

Default: 0

Diese Einstellung ist nur bei Geräten verfügbar, die über ein WLAN-Modul verfügen.

2.23.21.10 Energie-sparend

Über diese Einstellung aktivieren bzw. deaktivieren Sie die 'Green-Ethernet'-Erweiterungen gemäß IEEE 802.3az.

Damit Ihr Gerät die betreffenden Erweiterungen für Ethernet-Verbindungen auch verwendet, muss die Gegenstelle IEEE 802.3az ebenfalls unterstützen! Ob dies der Fall ist, können Sie im Status-Menü unter **LAN** > **Schnittstellen** > **Energie-sparend** nachprüfen.

Pfad Telnet:

Setup > **Schnittstellen** > **LAN-Schnittstellen**

Mögliche Werte:

nein

ja

Default:

ja

2.23.21.11 Flusssteuerung

Mit der Flusssteuerung können Sie dem Verlust von Datenpaketen vorbeugen, wenn ein Netzpartner zeitweise z. B. aufgrund eines Speicherüberlaufs die ankommenden Datenpakete nicht verarbeiten kann. In diesem Fall signalisiert der Empfänger dem Sender, mit der Datenübertragung für einen bestimmten Zeitraum zu pausieren.

Pfad Telnet:

Setup > **Schnittstellen** > **Ethernet-Ports**

Mögliche Werte:

Auto

Ist die automatische Verbindungsverhandlung aktiviert, erfolgt auch die Flusssteuerung automatisch, je nach Fähigkeit der Partner (symmetrisch, asymmetrisch).

Ist die automatische Verbindungsverhandlung deaktiviert, findet auch keine Flusssteuerung statt.

an

Aktiviert die symmetrische Flusssteuerung, wenn die automatische Verbindungsverhandlung deaktiviert ist.

aus

Deaktiviert die Flusssteuerung, wenn die automatische Verbindungsverhandlung aktiviert ist.

2.23.30 Ethernet-Ports

Die Ethernet-Schnittstellen von öffentlich zugänglichen Geräten können ggf. von unbefugten Anwendern genutzt werden, um physikalischen Zugang zu einem Netzwerk zu erhalten. Um diesen Versuch zu verhindern, können die Ethernet-Schnittstellen der Geräte ausgeschaltet werden.

SNMP-ID: 2.23.30

Pfad Telnet: /Setup/Schnittstellen

2.23.30.1 Port

Der Name des gewählten Ports.

Pfad Telnet: /Setup/Schnittstellen/Ethernet-Ports

2.23.30.2 Anschluss

Wählen Sie hier aus, welchen Netzwerkanschluss Sie für die Verbindung zu Ihrem lokalen Netz verwenden. Wenn Sie die Einstellung Auto wählen, wird der benutzte Anschluss vom Gerät automatisch erkannt.

Pfad Telnet: /Setup/Schnittstellen/Ethernet-Ports

Mögliche Werte:

- Auto
- Auto-100
- 10B-T
- FD10B-TX
- 100B-TX
- FD100B-TX
- FD1000B-TX

Default: Auto

2.23.30.3 Privat-Modus

Wird der Privat-Modus aktiviert, kann dieser Switch-Port keine Daten unmittelbar mit den anderen Switch- Ports austauschen.

Pfad Telnet: /Setup/Schnittstellen/Ethernet-Ports

Mögliche Werte:

- ja
- nein

Default: nein

2.23.30.4 Zuordnung

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Pfad Telnet: /Setup/Schnittstellen/Ethernet-Ports

Mögliche Werte:

- LAN-1 bis LAN-n: Die Schnittstelle ist einem logischen LAN zugeordnet.
- DSL-1 bis DSL-n: Die Schnittstelle ist einem DSL-Interface zugeordnet.
- Idle: Die Schnittstelle ist keiner Verwendung zugeordnet, sie ist allerdings physikalisch aktiv.
- Monitor: Der Port ist ein Monitor-Port, d.h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z. B. ein Paket-Sniffer (wie Ethereal) angeschlossen werden.
- Power down: Die Schnittstelle ist deaktiviert.

Default: Abhängig von der jeweiligen Schnittstelle bzw. dem spezifischen Hardware-Modell.

2.23.30.5 MDI-Modus

Hier kann die Verbindungsart des Switch-Ports eingestellt werden. Die Verbindungsart wird entweder automatisch gewählt oder sie kann fest eingestellt werden, auf gekreuzte (MDIX) oder nicht gekreuzte (MDI) Verbindung.

Pfad Telnet: /Setup/Schnittstellen/Ethernet-Ports

Mögliche Werte: Auto, MDI, MDIX

Default: Auto

2.23.30.6 Takt-Rolle

Ein Ethernet-Port, der im 1000BASE-Tx-Modus arbeitet, erfordert einen kontinuierlichen Datenstrom zwischen beiden verbundenen Partnern, um synchronisiert zu bleiben. Naturgemäß brauchen beide Seiten eine synchronisierte Uhr (Takt), um Daten zu übertragen. IEEE 802.3 führte das Konzept eines Masters und eines Slaves für solche Verbindungen ein. Der Master gibt den Takt zur Datenübertragung in beide Richtungen vor, und der Slave synchronisiert sich auf diesen Takt. Die Rollen als Takt-Master und -Slave werden in der automatischen Aushandlungsphase der Verbindung verteilt. Normalerweise braucht diesem Detail keine Beachtung geschenkt zu werden, da die automatische Aushandlung durchaus gut funktioniert. In bestimmten Fällen kann es erforderlich werden, die Master-/Slave-Aushandlung zu beeinflussen.

Pfad Telnet: /Setup/Schnittstellen/WLAN/Ethernet-Ports/Takt-Rolle

Mögliche Werte:

- Bevorzugt Slave: Dies ist die empfohlene Standard-Einstellung für Nicht-Switch-Geräte. Während der Aushandlungphase versucht der Port die Rolle des Slave auszuhandeln. Falls erforderlich, akzeptiert er allerdings auch die Rolle des Masters.
- Bevorzugt Master: Während der Aushandlungsphase versucht der Port die Rolle des Masters auszuhandeln. Falls erforderlich, akzeptiert er allerdings auch die Rolle des Slave.
- Slave: Der Port wird gezwungen, die Rolle des Slave auszuhandeln. Eine Verbindung wird **nicht** zustande kommen, wenn beide Verbindungs-Partner dazu gezwungen werden, die Rolle des Slave auszuhandeln.
- Master: Der Port wird gezwungen, die Rolle des Masters auszuhandeln. Eine Verbindung wird **nicht** zustande kommen, wenn beide Verbindungs-Partner dazu gezwungen werden, die Rolle des Masters auszuhandeln.

Default: Bevorzugt Slave

2.23.30.7 Downshift

Mit dieser Einstellung aktivieren bzw. deaktivieren Sie für den betreffenden Ethernet-Port die automatische Anpassung der Verbindungsgeschwindigkeit an die verwendete Infrastruktur. Indem Sie Downshift aktivieren, erlauben Sie dem Gerät, einen Ethernet-Link mit niedriger Übertragungsrate zu betreiben, falls die prinzipiell mögliche Geschwindigkeit aufgrund der Verkabelung nicht möglich ist.

Werden beispielsweise zwei Gigabit-fähige Geräte mit einem Kabel verbunden, das nicht voll belegt ist, versuchen beide Geräte zunächst, einen Gigabit-Link aufzubauen. Da Gigabit-Ethernet im Gegensatz zu Fast Ethernet (10 oder 100 Mbit) alle vier Adernpaare benötigt, schlägt der Verbindungsaufbau fehl. Die Downshift-Funktion erlaubt in diesem Fall den automatischen Rückfall auf die maximal mögliche Übertragungsrate des Kabels.

Ob für einen Ethernet-Link ein Downshift vorliegt, können Sie im Status-Menü unter **Ethernet-Ports** > **Ports** nachprüfen.

Pfad Telnet:

Setup > **Schnittstellen** > **Ethernet-Ports**

Mögliche Werte:

nein

ja

Default:

nein

2.23.30.8 Energie-sparend

Über diese Einstellung aktivieren bzw. deaktivieren Sie die 'Green-Ethernet'-Erweiterungen gemäß IEEE 802.3az.

Damit Ihr Gerät die betreffenden Erweiterungen für Ethernet-Verbindungen auch verwendet, muss die Gegenstelle IEEE 802.3az ebenfalls unterstützen! Ob dies der Fall ist, können Sie im Status-Menü unter **LAN** > **Schnittstellen** > **Energie-sparend** nachprüfen.

Pfad Telnet:

Setup > **Schnittstellen** > **Ethernet-Ports**

Mögliche Werte:

nein

ja

Default:

nein

2.23.30.9 Flusssteuerung

Mit der Flusssteuerung können Sie dem Verlust von Datenpaketen vorbeugen, wenn ein Netzpartner zeitweise z. B. aufgrund eines Speicherüberlaufs die ankommenden Datenpakete nicht verarbeiten kann. In diesem Fall signalisiert der Empfänger dem Sender, mit der Datenübertragung für einen bestimmten Zeitraum zu pausieren.

Pfad Telnet:

Setup > **Schnittstellen** > **LAN-Schnittstellen**

Mögliche Werte:

Auto

Ist die automatische Verbindungsverhandlung aktiviert, erfolgt auch die Flusssteuerung automatisch, je nach Fähigkeit der Partner (symmetrisch, asymmetrisch).

Ist die automatische Verbindungsverhandlung deaktiviert, findet auch keine Flusssteuerung statt.

an

Aktiviert die symmetrische Flusssteuerung, wenn die automatische Verbindungsverhandlung deaktiviert ist.

aus

Deaktiviert die Flusssteuerung, wenn die automatische Verbindungsverhandlung aktiviert ist.

2.23.40 Modem

Fortsetzung der Befehle und Optionen für ein optional am seriellen Interface angeschlossenes externes Modem.

SNMP-ID: 2.23.40

Pfad Telnet: /Setup/Schnittstellen

2.23.40.1 Ring-Count

Anzahl Klingeltöne bis zur Rufannahme.

Pfad Telnet: /Setup/Schnittstellen/Modem/Ring-Count

Mögliche Werte:

- Numerische Zeichen von 0 bis 99

Default: 1

2.23.40.2 Echo-Deaktivieren

Wenn das Modem-Echo aktiviert ist, sendet das extern angeschlossene Modem jedes empfangene Zeichen zurück. Für die korrekte Funktion des externen Modems am hier beschriebenden Gerät ist es erforderlich, das Modem-Echo zu deaktivieren. Das Gerät verwendet diesen Befehl zum Deaktivieren des "Modem-Echo".

Pfad Telnet: /Setup/Schnittstellen/Modem/Echo-Deaktivieren

Mögliche Werte:

- maximal 9 alphanumerische Zeichen

Default: E0

2.23.40.3 Reset

Das Gerät verwendet diesen Befehl, um einen Hardware-Reset auf dem extern angeschlossenen Modem auszuführen.

SNMP-ID: 2.23.40.3

Pfad Telnet: /Setup/Schnittstellen/Modem/Reset

Mögliche Werte:

- maximal 9 alphanumerische Zeichen

Default: &F

2.23.40.4 Initialisierung

Das Gerät verwendet diesen Befehl zur Initialisierung des extern angeschlossenen Modems.

Das Gerät sendet diese Sequenz nach einem Hardware-Reset des extern angeschlossenen Modems an eben dieses extern angeschlossene Modem.

Pfad Telnet: /Setup/Schnittstellen/Modem/Initialisierung

Mögliche Werte:

- maximal 63 alphanumerische Zeichen

Default: L0X1M1S0=0

2.23.40.5 Anwahl

Das Gerät verwendet diesen Befehl zum Wählen über das extern angeschlossene Modem. Dabei hängt das Gerät die Rufnummer aus der Gegenstellentabelle an die hier eingetragene Zeichenkette an.

Pfad Telnet: /Setup/Schnittstellen/Modem/Anwahl

Mögliche Werte:

- maximal 31 alphanumerische Zeichen

Default: DT

2.23.40.6 Modemkennung_abfragen

Das Gerät verwendet diesen Befehl zur Abfrage der Modemkennung. Das Ergebnis wird im Modem-Status ausgegeben.

Pfad Telnet: /Setup/Schnittstellen/Modem/Modemkennung_abfragen

Mögliche Werte:

- maximal 9 alphanumerische Werte

Default: I6

2.23.40.7 Rufannahme

Das Gerät verwendet diesen Befehl zur Annahme eines Rufes am extern angeschlossenen Modem.

Pfad Telnet: /Setup/Schnittstellen/Modem/Rufannahme

Mögliche Werte:

- Max. 9 Alphanumerische Zeichen

Default: A

2.23.40.8 Verbindung_trennen

Das Gerät verwendet diesen Befehl zum Trennen eines Rufes am extern angeschlossenen Modem (Auflegen).

Pfad Telnet: /Setup/Schnittstellen/Modem/Verbindung_trennen

Mögliche Werte:

- Max. 9 Alphanumerische Zeichen

Default: H

2.23.40.9 Escapsesquenz-(Data-CMD)

Das Gerät verwendet diese Befehlssequenz, um in der Datenphase einzelne Kommandos an das Modem zu übertragen.

Pfad Telnet: /Setup/Schnittstellen/Modem/Escapsesquenz-(Data-CMD)

Mögliche Werte:

- Max. 9 Alphanumerische Zeichen

Default: +++

2.23.40.10 Wartezeit-nach-Escapesequenz-(ms)

Nach der Escapesequenz wartet das Gerät für die hier eingestellte Zeit, bevor das Kommando zum Auflegen ausgegeben wird.

Pfad Telnet: /Setup/Schnittstellen/Modem/Wartezeit-nach-Escapesequenz-(ms)

Mögliche Werte:

- Numerische Werte von 0 bis 9999 Millisekunden

Default: 1000

2.23.40.11 Init.-Anwahl

Das Gerät sendet die Initialisierungssequenz zur Anwahl vor der Ausgabe des Wählbefehls an das extern angeschlossene Modem.

Pfad Telnet: /Setup/Schnittstellen/Modem/Init.-Anwahl

Mögliche Werte:

- maximal 63 alphanumerische Zeichen

Default: leer

2.23.40.12 Init.-Rufannahme

Das Gerät sendet die Initialisierungssequenz zur Rufannahme vor der Ausgabe des Rufannahmebefehls an das extern angeschlossene Modem.

Pfad Telnet: /Setup/Schnittstellen/Modem/Init.-Rufannahme

Mögliche Werte:

- maximal 63 alphanumerische Zeichen

Default: leer

2.23.40.13 Zykluszeit-AT-Poll-(s)

Wenn keine Verbindung besteht, prüft das Gerät die Existenz und korrekte Funktion des extern angeschlossenen Modems durch Ausgabe der Zeichenfolge "AT" an das Modem. Wenn das Modem korrekt angeschlossen ist und funktioniert, antwortet es mit "OK". Die Zykluszeit für den "AT-Poll" definiert den Abstand zwischen zwei Prüfungen.

Pfad Telnet: /Setup/Schnittstellen/Modem/Zykluszeit-AT-Poll-(s)

Mögliche Werte:

- Numerische Zeichen von 0 bis 9 Sekunden

Default: 1 Sekunde

2.23.40.14 AT-Poll_Anzahl

Wenn das extern angeschlossene Modem auf die AT-Polls des Gerätes für die hier eingestellte Anzahl nacheinander nicht antwortet, führt das Gerät einen Hardware-Reset für das extern angeschlossene Modem aus.

Pfad Telnet: /Setup/Schnittstellen/Modem/AT-Poll_Anzahl

Mögliche Werte

- Numerische Zeichen von 0 bis 9

Default: 5

2.23.41 Mobilfunk

Hier finden Sie die Einstellungen für den Mobilfunk.

SNMP-ID: 2.23.41

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk

2.23.41.1 Profile

In dieser Tabelle finden Sie die Einstellungen für die GPRS/UMTS-Profile.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile

2.23.41.1.1 Profil

Geben Sie hier einen eindeutigen Namen für dieses UMTS/GPRS-Profil ein. Dieses Profil kann dann in den UMTS/GPRS-WAN-Einstellungen ausgewählt werden.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/Profil

Mögliche Werte:

- maximal 16 alphanumerische Zeichen

Default: leer

2.23.41.1.2 PIN

Geben Sie hier die 4-stellige PIN der im UMTS/GPRS-Interface verwendeten Mobilfunk-SIM-Karte ein. Das Gerät benötigt diese Information, um das UMTS/GPRS-Interface in Betrieb zu nehmen.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/PIN

Mögliche Werte:

- maximal 6 numerische Zeichen

Default: leer

Die SIM-Karte protokolliert jeden Fehlversuch mit einer ungeeigneten PIN. Die Anzahl dieser Fehlversuche bleibt auch dann erhalten, wenn das Gerät zwischenzeitlich vom Stromnetz getrennt ist. Nach 3 Fehlversuchen sperrt sich die SIM-Karte gegen weitere Zugangsversuche. In diesem Zustand benötigen Sie die in der Regel 8-stelligen PUK oder SuperPIN, um die Sperre aufzuheben.

2.23.41.1.3 APN

Geben Sie hier den Namen des Zugangs-Servers für Mobilfunk-Datendienste ein, kurz APN (AP Name). Er ist spezifisch für Ihren Mobilfunk-Dienstanbieter und Sie finden diese Information in den Unterlagen Ihres Mobilfunk-Vertrages.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/APN

Mögliche Werte:

- maximal 48 alphanumerische Zeichen

Default: leer

2.23.41.1.4 Netz

Wenn Sie die manuelle Mobilfunk-Netzwahl selektiert haben, dann bucht sich das UMTS/GPRS-Interface ausschließlich in dem hier unter seinem vollen Namen angegebenen Mobilfunk-Netz ein.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/Netz

Mögliche Werte:

- maximal 16 alphanumerische Zeichen

Default: leer

2.23.41.1.5 Auswahl

Wenn Sie die automatische Mobilfunk-Netzwahl selektieren, dann bucht sich das UMTS/GPRS-Interface selbstständig in einem der verfügbaren und erlaubten Mobilfunk-Netze ein. Selektieren Sie hingegen die manuelle Mobilfunk- Netzwahl, dann bucht sich das UMTS/GPRS-Interface ausschließlich in dem darunter angegebenen Mobilfunk-Netz ein.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/Auswahl

Mögliche Werte:

- Auto.
- Manuell

Default: Auto.

Die manuelle Mobilfunk-Netzwahl eignet sich insbesondere dann, wenn das Gerät stationär betrieben wird und es häufiger vorkommen kann, dass sich das UMTS/GPRS-Interface in ein benachbartes oder funktechnisch stärkeres, mitunter aber unerwünschtes oder teureres Mobilfunk-Netz einbucht.

2.23.41.1.6 Modus

Wählen Sie hier die Mobilfunk-Übertragungs-Betriebsart.

Pfad Telnet:

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

Mögliche Werte:

Auto.
Automatische Wahl der Übertragungs-Betriebsart

UMTS
Ausschließlicher UMTS-Betrieb

GPRS
Ausschließlicher GPRS-Betrieb

UMTS-GPRS
Kombinierter UMTS-GPRS-Betrieb

LTE
Ausschließlicher LTE-Betrieb

Default-Wert:

Auto.

2.23.41.1.7 QoS-Downstream-Datenrate

Damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren, geben Sie hier die Übertragungsraten des verwendeten UMTS-Anschlusses an.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/QoS-Downstream-Datenrate

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 0

Besondere Werte: 0: das Interface ist unbeschränkt und QoS-Mechanismen können nicht greifen.

2.23.41.1.8 QoS-Upstream-Datenrate

Damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren, geben Sie hier die Übertragungsraten des verwendeten UMTS-Anschlusses an.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Profile/QoS-Upstream-Datenrate

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 0

Besondere Werte: 0: das Interface ist unbeschränkt und QoS-Mechanismen können nicht greifen

2.23.41.1.9 PDP-Typ

Mit dieser Einstellung geben Sie den Typ des PDP-Kontextes für das Mobilfunk-Profil an. Der PDP-Kontext beschreibt die Unterstützung der Adressräume, welche das Backbone des betreffenden Mobilfunkanbieters für Verbindungen aus dem Mobilfunknetz ins Internet anbietet. Dies kann entweder IPv4 oder IPv6 allein, oder die Unterstützung für beide Adressräume umfassen (Dual-Stack). Clients, die den betreffenden Mobilfunkanbieter nutzen wollen, müssen mindestens einen der angegebenen Adressräume unterstützen.

Pfad Telnet:

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

Mögliche Werte:

IPv4

IPv6

IPv4v6

Default:

IPv4

2.23.41.1.10 LTE-Baender

Wenn aufgrund ungünstiger Umgebungsbedingungen das Gerät ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen. Mit dieser Auswahl geben Sie dem Mobilfunk-Gerät vor, welche Frequenzbänder es verwenden darf bzw. soll. Zur Auswahl stehen die folgenden Frequenzbänder:

- **B1_2100**: 2,1GHz-Band ist aktiviert.
- **B3_1800**: 1,8GHz-Band ist aktiviert.
- **B7_2600**: 2,6GHz-Band ist aktiviert.
- **B8_900**: 900MHz-Band ist aktiviert.
- **B20_800**: 800MHz-Band ist aktiviert.
- **Alle**: Alle Frequenzbänder sind aktiviert.

Diese Auswahl schränkt nur die Frequenzbänder bei der Übertragung im LTE-Standard ein. Für UMTS und GPRS bleiben grundsätzlich alle Bänder erlaubt.

Pfad Telnet:

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

Mögliche Werte:

Alle

B1_2100

B3_1800

B7_2600

B8_900

B20_800

Default:

Alle

2.23.41.1.11 LTE-Anmeldung

Legen Sie fest, ob die Anmeldung an einem LTE-Netz unmittelbar oder mit zeitlicher Verzögerung erfolgt.

Pfad Telnet:

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

Mögliche Werte:

Sofort
Verzoegert

Default-Wert:

Sofort

2.23.41.2 Netzsuche

Dieser Befehl startet eine Suche nach den verfügbaren Netzen. Die Liste der gefundenen Netze finden Sie im Modem-Status als Netzwerkliste.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Netzsuche

2.23.41.3 PUK-Eingeben

Wenn die PIN der im Gerät verwendeten SIM-Karte nach mehrfacher Fehleingabe gesperrt ist (z. B. aufgrund fehlerhafter Profile), ist die Freischaltung der SIM-Karte durch die Eingabe der PUK erforderlich. Dieser Befehl startet die Abfrage der PUK.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/PUK-Eingeben

2.23.41.6 Protokollierungsintervall(Sec)

Protokollierungsintervall in Sekunden für die Werte, die der Modem-Status unter History anzeigt.

PfadTelnet: /Setup/Schnittstellen/Mobilfunk/Protokollierungsintervall(Sec)

Mögliche Werte:

- 0 bis 999999 Sekunden

Default: 0

Besondere Werte: '0' deaktivierte die Protokollierung der History-Werte.

2.23.41.7 Syslog-senden

Aktivieren Sie diese Option, damit das Gerät die Werte aus der History im Modem-Status (siehe auch '2.23.41.6 Protokollierungsintervall(Sec)') auch per SYSLOG protokolliert.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Syslog-senden

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.23.41.8 HSUPA-erlauben

Aktivieren oder deaktivieren Sie hier die Nutzung von HSUPA.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/HSUPA-erlauben

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.23.41.9 Signal-Pruefintervall(Min)

Dieser Wert gibt die Zeit in Minuten an, nach der das Gerät wieder eine 3G-Verbindung (sofern verfügbar) wechseln darf.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Signal-Pruefintervall(Min)

Mögliche Werte:

- 0 bis 9999 Minuten

Default: 0 Minuten

Besondere Werte: '0' deaktiviert den Rückfall von 3G- auf 2G-Verbindungen.

2.23.41.10 Schwellwert-3G-nach-2G(dB)

Dieser Wert gibt den Schwellwert für den Rückfall von 3G- nach 2G-Verbindungen an. Wird im 3G-Betrieb dieser Schwellwert unterschritten, wechselt das Gerät auf eine 2G-Verbindung (sofern verfügbar). Positive Werte werden automatisch in negative Werte umgewandelt.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Schwellwert-3G-nach-2G(dB)

Mögliche Werte:

- -51 bis -111 bzw. von 51 bis 111 dB

Default: -89 dB

Besondere Werte: '0' deaktiviert den Rückfall von 3G- auf 2G-Verbindungen.

2.23.41.11 Rueckfallpruefung-wenn-verbunden

Aktivieren Sie diese Option, wenn das Gerät auch bei bestehenden WAN-Verbindungen auf 2G-Verbindungen zurückfallen darf.

Pfad Telnet: /Setup/Schnittstellen/Mobilfunk/Rueckfallpruefung-wenn-verbunden

Mögliche Werte:

- Ja
- Nein

Default: Ja

Diese Einstellung wirkt sich nur aus, wenn der Rückfall von 3G- auf 2G-Verbindungen generell konfiguriert ist.

2.23.41.12 PIN-Aendern

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

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

Pfad Telnet:

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

Mögliche Werte:

4 Zeichen aus `[0-9]`

2.24 Public-Spot-Modul

In diesem Menü finden sie die Einstellungen für den Public-Spot.

SNMP-ID: 2.24

Pfad Telnet: /Setup

2.24.1 Authentifizierungs-Modus

Ihr Gerät unterstützt unterschiedliche Arten der Authentifizierung für den Netzwerk-Zugriff im Public Spot. Sie können zunächst festlegen, ob sich ein Benutzer überhaupt anmelden muss. Der Public Spot speichert die Zugangsdaten in der Benutzer-Tabelle. Falls Sie sich für ein Anmeldeverfahren entscheiden, haben Sie drei Möglichkeiten:

- Die Anmeldung erfolgt mit Benutzername und Passwort oder zusätzlich mit der physikalischen bzw. MAC-Adresse. In diesem Fall teilt der Adminstrator den Benutzern die Zugangsdaten z. B. über einen Ausdruck mit.
- Die Anmeldung erfolgt mit Benutzername und Passwort, welche sich der Benutzer selber generiert. Der Versand der Zugangsdaten bei erstmaliger Anmeldung automatisch entweder per E-Mail oder per SMS.
- Die Anmeldung erfolgt automatisiert über einen RADIUS-Server, nachdem der Benutzer die Nutzungsbedingungen auf der vom Administrator eingerichteten Willkommensseite akzeptiert hat. Die Zugangsdaten selbst bleiben dem Benutzer verborgen; sie werden von ihm auch nicht benötigt. Die Anlage eines Benutzerkontos über den RADIUS-Server erfolgt lediglich zur internen Verwaltung der betreffenden Nutzer.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Modus**

Mögliche Werte:

keine

Benutzer+Passwort

MAC+Benutzer+Passwort

E-Mail

E-Mail2SMS

Login-nach-Einverstaendniserklaerung

Default:

keine

2.24.2 Benutzer-Tabelle

Die Benutzer, welche Zugang zu Ihrem Netz erhalten sollen, werden in der Benutzer-Tabelle angelegt.

SNMP-ID: 2.24.2

Pfad Telnet: /Setup/Public-Spot-Modul

2.24.2.1 Name

Tragen Sie den Namen des Benutzers ein.

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/Name

Mögliche Werte:

- max. 64 Zeichen

2.24.2.2 Passwort

Geben Sie ein Passwort ein.

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/Passwort

Mögliche Werte:

- max. 16 Zeichen

2.24.2.3 MAC-Adresse

Geben sie die MAC-adresse an.

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/MAC-Adresse

Mögliche Werte:

- max. 12 Zeichen

2.24.2.4 Kommentar

Hier können Sie einen Kommentar eingeben.

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/Kommentar

Mögliche Werte:

- max. 80 Zeichen

2.24.2.5 Anbieter

Geben Sie den Namen des Anbieters ein.

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/Anbieter

Mögliche Werte:

- max. 16 Zeichen

2.24.2.6 Ende

Geben Sie den Gültigkeitsbereich für die Einstellung an (Datum).

Pfad Telnet: /Setup/Public-Spot-Modul/Benutzer-Tabelle/Ende

Mögliche Werte:

- max. 20 Zeichen

2.24.3 Anbieter-Tabelle

Bei der Konfiguration eines Public-Spot können die Benutzer-Anmeldedaten zur Authentifizierung und für das Accounting an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese werden in der Anbieter-Liste konfiguriert.

SNMP-ID: 2.24.3

Pfad Telnet: /Setup/Public-Spot-Modul

Konfigurieren Sie neben den dedizierten Parametern für die RADIUS-Anbieter auch die allgemeinen RADIUS-Werte wie Wiederholung und Timeout in den entsprechenden Konfigurationsbereichen.

2.24.3.1 Name

Name des Anbieters, der den RADIUS-Server für die Authentifizierung und/oder das Accounting bereitstellt.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Name

Mögliche Werte:

- max. 16 alphanumerische Zeichen

Default: leer

2.24.3.3 Auth.-Server-Port

Geben Sie hier den Port des Servers an, über den der Public-Spot die Authentifizierung der Zugänge bei diesem Anbieter anfragt.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Port

Mögliche Werte:

- gültige Port-Bezeichnung

Default: l0

2.24.3.4 Auth.-Server-Schluessel

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

SNMP-ID: 2.24.3.4

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Schluessel

Mögliche Werte:

- max. 32 alphanumerische Zeichen

Default: leer

2.24.3.6 Acc.-Server-Port

Geben Sie hier den Port des Servers an, über den der Public-Spot das Accounting der Zugänge bei diesem Anbieter durchführt.

SNMP-ID: 2.24.3.6

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Port

Mögliche Werte:

- gültige Port-Bezeichnung

Default: l0

2.24.3.7 Acc.-Server-Schluessel

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

SNMP-ID: 2.24.3.7

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Schluessel

Mögliche Werte:

- max. 32 alphanumerische Zeichen

Default: leer

2.24.3.8 Backup

Wählen Sie einen anderen Eintrag der Anbieter-Tabelle als Backup aus. Der Public Spot kontaktiert den Backup-Anbieter zur Authentifizierung und/oder Accounting der Zugänge, wenn der Server des primären Anbieters nicht erreichbar ist.

SNMP-ID: 2.24.3.8

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Backup

Mögliche Werte:

- Auswahl aus der Liste der definierten RADIUS-Anbieter, max. 16 Zeichen

Default: leer

2.24.3.9 Auth.-Server-Loopback-Adr.

Geben Sie hier die Loopback-Adresse des Servers an, den der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter kontaktiert.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Loopback-Adr.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Default: leer

2.24.3.10 Acc.-Server-Loopback-Adr.

Geben Sie hier die Loopback-Adresse des Servers an, den der Public-Spot für das Accounting der Zugänge bei diesem Anbieter kontaktiert.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Loopback-Adr.

Mögliche Werte:

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LBO ... LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Default: leer

2.24.3.11 Auth.-Server-Protokoll

Wählen Sie hier das Protokoll, das der Public-Spot für die Authentifizierung der Zugänge bei diesem Anbieter verwendet.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Auth.-Server-Protokoll

Mögliche Werte:

- RADIUS
- RADSEC

Default: RADIUS

2.24.3.12 Acc.-Server-Protokoll

Wählen Sie hier das Protokoll, das der Public-Spot für das Accounting der Zugänge bei diesem Anbieter verwendet.

Pfad Telnet: /Setup/Public-Spot-Modul/Anbieter-Tabelle/Acc.-Server-Protokoll

Mögliche Werte:

- RADIUS
- RADSEC

Default: RADIUS

2.24.3.13 Auth.-Server-Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.3.14 Acc.-Server-Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.3.15 Auth.-Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.3.16 Acc.-Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.5 Traffic-Limit-Bytes

Bereits vor der Anmeldung sind unabhängig von den oben angegebenen Servern, Netzen und Seiten einige DHCP-, DNS- und ARP-Anfragen notwendig. Diese sind daher grundsätzlich erlaubt. Sie können allerdings dazu missbraucht werden, unberechtigterweise andere Daten zu tunneln.

Hier können Sie daher ein maximales Transfervolumen definieren. Es umfasst ausschließlich Daten, welche vor der Anmeldung und nicht vom bzw. zum oben angegebenen freien Web-Server übertragen werden. Dieser bleibt zu jeder Zeit unlimitiert.

SNMP-ID: 2.24.5

Pfad Telnet: /Setup/Public-Spot-Modul

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.24.6 Server-Verzeichnis

Geben Sie hier das Verzeichnis der öffentlichen Seite Ihres Public-Spot Dienstes an. Auf dieser Seite sollten Sie Informationen anbieten, die den neuen Benutzer in die Lage versetzen, Sie zu kontaktieren, um sich bei Ihnen anzumelden.

SNMP-ID: 2.24.6

Pfad Telnet: /Setup/Public-Spot-Modul/Server-Verzeichnis

Mögliche Werte:

- max. 127 Zeichen

Default: leer

2.24.7 Accounting-Meldezyklus

Geben Sie hier die Zeit in Sekunden für den Accounting-Meldezyklus ein.

SNMP-ID: 2.24.7

Pfad Telnet: /Setup/Public-Spot-Modul

2.24.8 Seitentabelle

Zusätzlich zum frei erreichbaren Web-Server können Sie Spezial-Seiten definieren, die Ihre Kunden ohne Anmeldung nutzen dürfen.

In der Seitentabelle können Sie bestimmten vordefinierten Ereignissen bestimmte Seiten auf Ihren Servern zuordnen, um die für diese Ereignisse im Gerät vorhandenen Standard-Seiten zu ersetzen.

SNMP-ID: 2.24.8

Pfad Telnet: /Setup/Public-Spot-Modul

2.24.8.1 Seite

Name der Seite, die Ihre Kunden ohne Anmeldung nutzen dürfen.

SNMP-ID: 2.24.8.1

Pfad Telnet: /Setup/Public-Spot-Modul/Seitentabelle/Seite

2.24.8.2 URL

URL der Seite, die Ihre Kunden ohne Anmeldung nutzen dürfen.

SNMP-ID: 2.24.8.2

Pfad Telnet: /Setup/Public-Spot-Modul/Seitentabelle/URL

Mögliche Werte:

- max. 100 Zeichen

Default: Standardmäßig sind je nach gewählter Seite verschiedene HTML-Seiten aus dem Dateisystem des Geräts voreingestellt.

2.24.8.3 Rueckfall

Aktivieren oder deaktivieren Sie den Rückfall auf die eingebaute Seite für den Fall, dass der Public Spot die benutzerdefinierte URL nicht anzeigen kann.

SNMP-ID: 2.24.8.3

Pfad Telnet: /Setup/Public-Spot-Modul/Seitentabelle/Rueckfall

Mögliche Werte:

- ja
- nein

Default: nein

2.24.8.4 Typ

Wählen Sie den Typ der Seite.

SNMP-ID: 2.24.8.4

Pfad Telnet: /Setup/Public-Spot-Modul/Seitentabelle/Typ

Mögliche Werte:

- Template
- Redirect

Default: Template

2.24.8.5 Loopback-Addr.

Geben Sie eine Loopback-Adresse ein.

SNMP-ID: 2.24.8.5

Pfad Telnet: /Setup/Public-Spot-Modul/Seitentabelle/Loopback-Addr.

Mögliche 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

Default: Leer

2.24.8.6 Template-Cache

Über diesen Parameter aktivieren Sie das Caching von Public Spot-Templates.

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways) die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Seitentabelle**

Mögliche Werte:

nein

ja

Default:

nein

2.24.9 Roaming-Schluessel

Beim Wechsel in den Funkbereich einer anderen Basis-Station (Roaming) wird die erneute Anmeldung erforderlich. Wenn Sie sich im Überschneidungsbereich zweier Basis-Stationen befinden, kann es sogar zu einem regelmäßigen Verbindungswechsel zwischen beiden Basis-Stationen kommen. Die Angabe des Roaming Secret ermöglicht die Übergabe einer Public-Spot-Sitzung an anderen Access Point ohne Neuanmeldung.

SNMP-ID: 2.24.9

Pfad Telnet: /Setup/Public-Spot-Modul/Roaming-Schluessel

Mögliche Werte:

- max. 32 Zeichen

Default: leer

2.24.12 Kommunikations-Port

Stellen Sie hier den Port ein, über den der Public Spot mit den angemeldeten Clients kommuniziert.

SNMP-ID: 2.24.12

Pfad Telnet: /Setup/Public-Spot-Modul/Kommunikations-Port

Mögliche Werte:

- Gültige Port-Bezeichnung, max. 5 Zeichen

Default: leer

2.24.14 Idle-Timeout

Wenn eine Leerlaufzeitüberschreitung definiert wird (entweder hier oder über RADIUS), beendet der Public-Spot die Verbindung, wenn innerhalb des angegebenen Intervalls keine Daten vom Client empfangen wurden.

SNMP-ID: 2.24.14

Pfad Telnet: /Setup/Public-Spot-Modul

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.24.15 Port-Tabelle

In dieser Tabelle aktivieren oder deaktivieren Sie die Authentifizierung über den Public Spot für die im Gerät vorhandenen Ports.

SNMP-ID: 2.24.15

Pfad Telnet: /Setup/Public-Spot-Modul/Port-Tabelle

2.24.15.2 Port

Wählen Sie hier den Port, für den Sie die Authentifizierung über den Public Spot aktivieren oder deaktivieren möchten.

SNMP-ID: 2.24.15.2

Pfad Telnet: /Setup/Public-Spot-Modul/Port-Tabelle/Port

Mögliche Werte:

- Auswahl aus den im Gerät verfügbaren Ports, z. B. LAN-1

2.24.15.3 Authentifizierung-erforderlich

Aktivieren oder deaktivieren Sie die Authentifizierung über den Public Spot für den gewählten Port.

SNMP-ID: 2.24.15.3

Pfad Telnet: /Setup/Public-Spot-Modul/Port-Tabelle/Authentifizierung-erforderlich

Mögliche Werte:

- ja
- nein

Default: nein

2.24.16 Auto-Löschen-Benutzer-Tabelle

Bestimmen Sie, ob die automatische Bereinigung der Benutzer-Liste aktiviert ist. Da die Größe der Benutzer-Tabelle beschränkt ist, sollten verwaiste Konten so bald wie möglich gelöscht werden.

SNMP-ID: 2.24.16

Pfad Telnet: /Setup/Public-Spot-Modul

Mögliche Werte:

- ja
- nein

Default: nein

2.24.17 Server-Datenbank-liefern

Wählen Sie hier aus, ob der Public Spot die MAC-Adressliste über RADIUS zur Verfügung stellt.

SNMP-ID: 2.24.17

Pfad Telnet: /Setup/Public-Spot-Modul/Server-Datenbank-liefern

Mögliche Werte:

- ja
- nein

Default: nein

2.24.18 Verbiete-Mehrfach-Logins

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

SNMP-ID: 2.24.18

Pfad Telnet: /Setup/Public-Spot-Modul

Mögliche Werte:

- nein
- ja

Default: nein

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

2.24.19 Neuer-Benutzer-Assistent

Mit Hilfe des Assistenten in WEBconfig können Sie Public-Spot-Benutzerkonten auf einfache Weise angelegen. Der Assistent generiert automatisch Benutzername und Passwort und präsentiert eine Seite zum Ausdrucken aller notwendigen Zugangsdaten. In diesem Menü finden Sie die Einstellungen für diesen Assistenten.

SNMP-ID: 2.24.19

Pfad Telnet: /Setup/Public-Spot-Modul

2.24.19.2 Benutzer-Name-Muster

Geben Sie hier das Format für den Namen des neuen Benutzerkontos an.

SNMP-ID: 2.24.19.2

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

Mögliche Werte:

- max. 19 Zeichen. Für die Zeichenfolge '%n' setzt der Public Spot eine automatisch generierte, eindeutige Nummer für das Konto ein.

Default: user%n

2.24.19.3 Passwort-Länge

Definieren Sie hier die Länge des Passworts, welches der Public-Spot-Benutzer-Assistent für ein neues Konto generiert.

SNMP-ID: 2.24.19.3

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

Mögliche Werte:

- 0 bis 255

Default: 6

2.24.19.4 SSID

Geben Sie hier die SSID an, die der Public-Spot-Benutzer-Assistent auf dem Formular für den Benutzer ausgibt.

SNMP-ID: 2.24.19.4

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

Englische Bezeichnung: SSID

Mögliche Werte:

- max. 32 alphanumerische Zeichen

Default: leer

Wenn Sie dieses Feld frei lassen, gibt der Public-Spot-Benutzer-Assistent auf dem Formular die SSID des ersten logischen WLAN mit aktivem Public-Spot aus.

2.24.19.5 Default-Laufzeit

In dieser Tabelle definieren Sie die möglichen Standard-Laufzeiten für den Public-Spot-Benutzer-Assistenten. Der Assistent bietet diese Laufzeiten beim Erstellen eines Benutzerkontos an.

SNMP-ID: 2.24.19.5

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent

2.24.19.5.1 Laufzeit

Wählen Sie hier die Laufzeit eines Benutzerkontos für den Public Spot.

SNMP-ID: 2.24.19.5.1

Pfad Telnet: /Setup/Public-Spot-Modul/Default-Laufzeit

Mögliche Werte: max. 5 Zeichen

Default: leer

2.24.19.5.2 Einheit

Wählen Sie hier die Einheit für die Laufzeit eines Benutzerkontos für den Public Spot.

SNMP-ID: 2.24.19.5.2

Pfad Telnet: /Setup/Public-Spot-Modul/Default-Laufzeit

Mögliche Werte:

- Minuten(n)
- Stunde(n)
- Tage(e)

Default: Stunden(n)

2.24.19.6 Kommentarfelder

In dieser Tabelle definieren Sie die Kommentarfelder für den Public-Spot-Benutzer-Assistenten.

SNMP-ID: 2.24.19.6

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Kommentarfelder

2.24.19.6.1 Feldname

Der Public-Spot-Benutzer-Assistent kann auf dem Ausdruck bis zu 5 Kommentare ausgeben. Wählen Sie hier die Namen dieser Kommentarfelder, die der Assistent im Formular beim Erstellen der Benutzerkonten anzeigt.

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Kommentarfelder/Feldname

Mögliche Werte:

- max. 31 Zeichen

Default: leer

Aktivieren Sie den Ausdruck der Kommentare mit der Option *2.24.19.8 Drucke-Kommentare-auf-Voucher*.

2.24.19.7 Standard-Startzeitpunkt

Wählen Sie hier aus, zu welchem Zeitpunkt die Laufzeit des Vouchers startet. Mit der Option, die Laufzeit erst ab dem ersten Login beginnen zu lassen, können Sie mehrere Voucher auf Vorrat drucken. Der Benutzer kann dennoch die komplette Laufzeit nutzen.

SNMP-ID: 2.24.19.7

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Standard-Startzeitpunkt

Wählen Sie den Standard-Startzeitpunkt.

Mögliche Werte:

- sofort
- erster-Login

Default: erster-Login

2.24.19.8 Drucke-Kommentare-auf-Voucher

Aktivieren oder deaktivieren Sie hier den Ausdruck der Kommentarfelder auf dem Voucher für den Public-Spot-Benutzer.

SNMP-ID: 2.24.19.8

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Drucke-Kommentare-auf-Voucher

Mögliche Werte:

- ja
- nein

Default: nein

2.24.19.9 Maximale-Voucher-Gueltigkeitsdauer

Mit diesem Wert definieren Sie die maximale Gültigkeitsdauer des Vouchers in Tagen.

SNMP-ID: 2.24.19.9

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Maximale-Voucher-Gueltigkeitsdauer

Mögliche Werte:

- max. 10 Zeichen

Default: 365 Tage

Wenn Sie den Startzeitpunkt für die Laufzeit eines Vouchers auf 'erster-Login' einstellen (*2.24.19.7 Standard-Startzeitpunkt*), beginnt die Laufzeit des Vouchers erst zu einem Zeitpunkt in der Zukunft. Die maximale Gültigkeit hat Vorrang vor der Laufzeit des einzelnen Vouchers. Wenn der Benutzer das Voucher aktiviert, kann die Laufzeit ggf. schon abgelaufen sein oder noch während der eigentlich vorgesehenen Laufzeit ablaufen.

2.24.19.10 Verfuegbare-Ablauf-Methoden

Mit dieser Einstellung legen Sie fest, welche Ablauf-Methoden der Public-Spot-Benutzer-Assistent bei der Erstellung von neuen Benutzerkonten anbietet.

SNMP-ID: 2.24.19.10

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/Verfuegbare-Ablauf-Methoden

Mögliche Werte:

- Alle-Methoden: Der Assistent bietet alle verfügbaren Ablauf-Methoden an.
- Aktuelle-Zeit-Methode: Der Assistent bietet nur die Ablauf-Methode der aktuellen Zeit an. Die Laufzeit der so erstellen Benutzerkonten beginnt sofort zu dem Zeitpunkt, an dem das Benutzerkonto erstellt wird.
- Login-Zeit-Methode: Der Assistent bietet nur die Ablauf-Methode der Login-Zeit an. Die Laufzeit der so erstellen Benutzerkonten beginnt erst zu dem Zeitpunkt, zu dem sich der Benutzer zum ersten Mal am Public Spot anmeldet.

Default: Alle-Methoden

Wenn Sie die Login-Zeit-Methode auswählen, kann die Laufzeit eines Benutzerkontos je nach Einstellung der maximalen Voucher-Gültigkeitsdauer (*2.24.19.9 Maximale-Voucher-Gueltigkeitsdauer*) schon vor dem ersten Login überschritten werden.

2.24.19.11 SSID-Tabelle

Diese Tabelle enthält die Liste der für Public-Spot-Benutzer freigegebene Netzwerknamen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

2.24.19.11.1 Netzwerkname

Geben Sie hier den Namen eines im Gerät gespeicherten logischen WLAN-Netzes an, wenn Sie für dessen Zugang Public-Spot-Benutzern abrechenbare Vouchers erstellen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

Mögliche Werte:

maximal 32 alphanumerische Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default

leer

2.24.19.11.2 Default

Bestimmen Sie den Namen des WLAN-Netzes als Standardwert. Der Assistent zum Anlegen neuer Public-Spot-Benutzer schlägt in der Liste verfügbarer WLAN-Netze diesen Wert automatisch vor. Diesen Vorschlag ändern Sie bei Bedarf noch in der Eingabemaske des Assistenten.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **SSID-Tabelle**

Mögliche Werte:

nein

ja

Default

nein

2.24.19.12 Groß-Kleinschreibung

Mit dieser Einstellung bestimmen Sie, ob der Assistent für das Anlegen eines neuen Public-Spot-Benutzers die Groß-/Kleinschreibung des Benutzernamens beachtet.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Ja

Nein

Default:

Ja

2.24.19.13 Groß-Kleinschreibung-Schalter-verstecken

Bestimmen Sie hier, ob der Assistent für das Anlegen eines neuen Public-Spot-Benutzers den Schalter für die Beachtung der Groß-/Kleinschreibung des Benutzernamens ein- oder ausblendet.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Ja

Nein

Default:

Ja

2.24.19.14 Max-gleichzeitige-Logins-Tabelle

In dieser Tabelle legen Sie durch Eingabe einzelner oder mehrerer Werte die Anzahl der Geräte fest, die gleichzeitig auf einen einzelnen Account zugreifen können. Die Eingabe unterschiedlicher Werte (z. B. 1, 3, 4, 5) bietet Ihnen die Möglichkeit, variabel auf die Bedürfnisse von unterschiedlichen Benutzern bzw. Benutzergruppen zu reagieren.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**

Mögliche Werte:

Max. 5 Ziffern

Default:

0, 3, 10

Besondere Werte:

0 ermöglicht eine unbegrenzte Anzahl von Logins mit einem Account.

2.24.19.14.1 Wert

Über diesen Eintrag definieren Sie einen Vorgabewert für das Auswahlmenü **Max-gleichzeitige-Logins**, welches Sie innerhalb des Setup-Wizards **Public-Spot-Benutzer einrichten** vorfinden. Der betreffende Wert beschreibt die maximale Anzahl der Geräte, die über ein einzelnes Benutzerkonto gleichzeitig angemeldet sein können. Der Wert `0` steht dabei für "Unbegrenzt".

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**

Mögliche Werte:

0 bis 99999

Default:

2.24.19.15 Mehrfach-Login

Über diese Einstellung geben Sie an, ob die mehrfache Anmeldung für Benutzer, die Sie mit dem Setup-Wizard **Public-Spot-Benutzer einrichten** oder via Web-API (ohne Variablen-/Werteangabe) erstellen, standardmäßig erlaubt ist. Im Setup-Wizard z. B. ist dann das Optionsfeld **Mehrfach-Logins** standardmäßig vormarkiert.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

nein

ja

Default:

nein

2.24.19.16 Mehrfach-Login-verstecken

Über diese Einstellung verstecken Sie das Optionsfeld **Mehrfach-Logins** im Setup-Wizard **Public-Spot-Benutzer einrichten**.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

nein

ja

Default:

nein

2.24.19.17 Bandbreitenprofile

In dieser Tabelle verwalten Sie die einzelnen Bandbreitenprofile. Über ein Bandbreitenprofil haben Sie die Möglichkeit, die Public-Spot-Benutzern zur Verfügung gestellte Bandbreite (Uplink und Downlink) bei der Kontoerstellung selektiv zu beschränken.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

2.24.19.17.1 Profilename

Geben Sie hier den Namen für das Bandbreitenprofil ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

String, max. 255 Zeichen

Default:

2.24.19.17.2 TX-Bandbreite

Geben Sie hier die maximale Bandbreite (in Bit/s) ein, die einem Public-Spot-Benutzer im Uplink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.24.19.17.3 RX-Bandbreite

Geben Sie hier die maximale Bandbreite (in Bit/s) ein, die einem Public-Spot-Benutzer im Downlink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.24.19.18 Passworteingabe-Einstellung

In dieser Einstellung legen Sie fest, welchen Zeichensatz der Assistent **Public Spot-Benutzer einrichten** verwendet, um Passwörter für neue Benutzer zu erstellen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Buchstaben+Ziffern
Buchstaben
Ziffern

2.24.19.19 CSV-Export-verstecken

Dieser Parameter legt fest, ob der Schalter zum Export der Informationen in eine CSV-Datei im Assistenten zum Anlegen neuer Public Spot-Benutzer erscheint oder nicht.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.24.19.20 Benutzerverwaltung-Taste-verstecken

Dieser Parameter gibt Ihnen die Möglichkeit, die Schaltfläche **Benutzerverwaltung aufrufen** im Setup-Wizard auszublenden.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

ja
Der Setup-Wizard **Public-Spot-Benutzer einrichten** blendet die Schaltfläche **Benutzerverwaltung aufrufen** aus.

nein
Der Setup-Wizard zeigt die Schaltfläche **Benutzerverwaltung aufrufen** an.

Default-Wert:

nein

2.24.20 VLAN-Tabelle

Standardmäßig werden alle Daten über das relevante Interface geroutet. Bei Angabe von VLAN-ID-Tags werden jedoch nur Daten über die relevanten Interfaces geroutet, die mit der angegebenen VLAN-ID getaggt sind. Wählen Sie hier nur VLAN-IDs aus, wenn nicht alle Datenpakete über das entsprechende Interface geroutet werden sollen.

SNMP-ID: 2.24.20

Pfad Telnet: /Setup/Public-Spot-Modul

2.24.20.1 VLAN-ID

Geben Sie die VLAN-ID ein.

Pfad Telnet: /Setup/Public-Spot-Modul/Neuer-Benutzer-Assistent/VLAN-Tabelle/VLAN-ID

Mögliche Werte:

- 0 bis 4096

Default: leer

2.24.21 Login-Seiten-Typ

Wählen Sie aus, über welches Protokoll der Public Spot die Login-Seiten anzeigt.

SNMP-ID: 2.24.21

Pfad Telnet: /Setup/Public-Spot-Modul/Login-Seiten-Typ

Mögliche Werte:

- HTTP
- HTTPS

Default: HTTP

2.24.22 Geräte-Hostname

Zertifikate werden üblicherweise auf DNS-Namen ausgestellt, deswegen muss der PublicSpot hier anstelle einer internen IPAdresse den DNS-Namen des Zertifikats als Ziel angeben. Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des PublicSpots aufgelöst werden.

SNMP-ID: 2.24.22

Pfad Telnet: /Setup/Public-Spot-Modul

Mögliche Werte:

- max. 31 Zeichen

Default: leer

2.24.23 MAC-Adress-Tabelle

In dieser Tabelle finden Sie die erlaubten WLAN-Clients für die automatische Authentifizierung am Public Spot mit Hilfe der MAC-Adresse.

Pfad Telnet:

Setup > **Public-Spot**

2.24.23.1 MAC-Adresse

MAC-Adresse des WLAN-Clients, der die automatische Authentifizierung nutzen kann.

Pfad Telnet:

Setup > **Public-Spot** > **MAC-Adress-Tabelle**

Mögliche Werte:

Gültige MAC-Adresse, 12 Zeichen

Default:

2.24.23.2 Benutzer

Benutzername des WLAN-Clients, der die automatische Authentifizierung nutzen kann. Der Public Spot verwendet diesen Namen für das optionale Accounting der Sitzung über einen RADIUS-Server.

Pfad Telnet:

Setup > **Public-Spot** > **MAC-Adress-Tabelle**

Mögliche Werte:

Innerhalb dieser Tabelle eindeutiger Name, maximal 32 alphanumerische Zeichen

Default:

2.24.23.3 Provider

Der Public Spot verwendet diesen Provider für das optionale Accounting der Sitzung über einen RADIUS-Server.

Pfad Telnet:

Setup > **Public-Spot** > **MAC-Adress-Tabelle**

Mögliche Werte:

Auswahl eines in der Anbieter-Liste definierten RADIUS-Servers

Default:

2.24.24 MAC-Address-Prüfungs-Anbieter

Der Public Spot verwendet diesen Provider für die Authentifizierung der MAC-Adresse über einen RADIUS-Server.

Wenn kein Provider ausgewählt ist, findet keine Authentifizierung der MAC-Adresse über einen RADIUS-Server statt. In diesem Fall werden nur die in der MAC-Adress-Tabelle aufgeführten WLAN-Clients ohne Anmeldung am Public Spot authentifiziert.

Pfad Telnet:

Setup > **Public-Spot** >

Mögliche Werte:

Auswahl eines in der Anbieter-Liste definierten RADIUS-Servers

Default:

2.24.25 MAC-Address-Prüfungs-Cache-Zeit

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die hier definierte Lebensdauer (in Sekunden). Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot während der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

Pfad Telnet:

Setup > **Public-Spot**

Mögliche Werte:

0 bis 4294967295

Default:

60

2.24.26 Stations-Tabellen-Limit

Sie können die maximale Anzahl der Clients auf bis zu 65536 Teilnehmer vergrößern.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Stations-Tabellen-Limit**

Mögliche Werte:

16 bis 65536

Default:

8192

Während des Betriebs wird ausschließlich eine Erweiterung der Stationstabelle sofort übernommen. Starten Sie den Access-Point neu, damit eine Reduzierung der Stationstabelle wirksam wird.

2.24.30 Freier-Server

Geben Sie hier die IP-Adresse der öffentlichen Seite Ihres Public-Spot Dienstes an. Auf dieser Seite sollten Sie Informationen anbieten, die den neuen Benutzer in die Lage versetzen, Sie zu kontaktieren, um sich bei Ihnen anzumelden.

SNMP-ID: 2.24.30

Pfad Telnet: /Setup/Public-Spot-Modul/Freier-Server

Mögliche Werte:

- max. 64 Zeichen

Default: leer

2.24.31 Freie Netze

Zusätzlich zum frei erreichbaren Web-Server können Sie weitere Netze oder bestimmte Web-Seiten definieren, die Ihre Kunden ohne Anmeldung nutzen dürfen. Ab LCOS-Version 8.80 haben Sie die Möglichkeit, bei der Eingabe des Host-Namens auch Wildcards zu verwenden.

Pfad Telnet:

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

2.24.31.1 Host-Name

Mit diesem Eingabefeld der Tabelle **Freie-Netze** definieren Sie einen Server, ein Netz oder einzelne Web-Seiten, welche die Kunden ohne Anmeldung nutzen dürfen. Sie können hier entweder eine IP-Adresse oder einen Host-Namen eingeben, wobei in beiden Fällen die Verwendung von Wildcards zulässig ist. Sie können also Werte wie z. B. "203.000.113.*", "google.??*" oder "*. wikipedia.org" eingeben. Die Tabelle ist dynamisch und passt sich bei Eingabe mehrerer Host-Namen bzw. IP-Adressen entsprechend an.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Freie-Netze** > **Host-Name**

Mögliche Werte:

Max. 64 Zeichen, wobei Sie Buchstaben, Zahlen, Bindestriche, Punkte und Wildcards (?, *) eingeben dürfen.

Default:

leer

2.24.31.2 Maske

Geben Sie hier die zugehörige Netzmaske ein. Wenn Sie nur eine einzelne Station mit der zuvor angegebenen Adresse freischalten wollen, geben Sie 255.255.255.255 ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie die zugehörige Netzmaske ein.

Pfad Telnet:

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

Mögliche Werte:

Max. 15 Zeichen

Default:

0.0.0.0

2.24.31.3 VLans

Über diesen Parameter definieren Sie für den angegebenen Host-Namen optional eine Liste von VLAN-IDs, an welche die Erreichbarkeit der freien Seite(n) gekoppelt ist. Auschließlich Benutzer, welche über die in der Stationstabelle hinterlegte VLAN-ID verfügen, sind in der Lage, diesen Host ohne Anmeldung aufzurufen. Nutzen Sie diesen Parameter, um z. B. in Anwendungsszenarien mit VLAN-getrennten Public Spot-Netzen/SSIDs den Zugriffsbereich für einzelne Nutzergruppen unterschiedlich stark einzuschränken.

Pfad Telnet:

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

Mögliche Werte:

Default-Wert:

leer

Kommaseparierte Liste, max. 16 Zeichen aus `[0-9],`

Besondere Werte:

leer, **0**

Der Zugriff auf den eingetragenen Host ist aus allen VLANs heraus möglich.

2.24.32 Freie-Hosts-Minimal-TTL

Die Konfiguration des Public Spots ermöglicht es Nutzern, unentgeltlich und ohne Anmeldung entsprechend freigeschaltete Webseiten, Webserver oder Netzwerke zu besuchen. Der Access Point leitet die Besucher gemäß der angegebenen Hostnamen an die entsprechenden IP-Adressen. In den Statustabellen **Status** > **Public-Spot** > **Freie-Hosts** und **Status** > **Public-Spot** > **Freie-Netze** speichert der Access Point die Hostnamen sowie die entsprechenden IP-Adressen.

Mit diesem Wert bestimmen Sie die Dauer in Sekunden, für die die Adress-Einträge in der Statustabelle **Freie-Hosts** gültig sein sollen (TTL: 'Time to live').

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Freie-Hosts-Minimal-TTL**

Mögliche Werte:

max. 10 Zeichen

Besondere Werte:

0: Die Gültigkeit richtet sich nach der in der DNS-Antwort übertragenen Dauer (TTL).

Default:

300

2.24.33 Login-Text

Die Einstellung bietet Ihnen die Möglichkeit, einen individuelle Text anzugeben, den das Gerät auf der Anmeldeseite des Public Spot-Moduls innerhalb der Box des Anmeldeformulars einblendet. Um Umlaute einzugeben, sollten Sie deren HTML-Äquivalente verwenden (z. B. `&uuml;` für ü), da der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das Formular aus.</i>)
```

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

Beliebiger String, max. 254 Zeichen aus

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

Default:

2.24.34 WAN-Verbindung

Über diesen Parameter benennen Sie die Gegenstelle, deren Verbindungsstatus das Public Spot-Modul überwacht, um bei Wegfall der WAN-Verbindung eine entsprechende Meldung auf der Fehlerseite gegenüber unauthentifizierten

Benutzern anzuzeigen. Dadurch werden mögliche Benutzer bereits vorab über die fehlende Verfügbarkeit des Netzwerks informiert.

Ohne Benennung einer zu überwachenden Gegenstelle deaktiviert das Public Spot-Modul die Ausgabe von Verbindungsfehlern auf der Fehlerseite. Ein Wegfall der WAN-Verbindung führt dann bei unauthentifizierten Benutzern stattdessen zu einem Verbindungs-Timeout in ihrem Browser.

Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

Gültiger Name einer Gegenstelle, max. 16 Zeichen

Default:

2.24.35 Drucke-Logo-Und-Kopfbild

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das Kopfbild "Hotspot" sowie das Logo "Powered by LANCOM". Sie haben die Möglichkeit, die Einbindung dieser Grafiken direkt im Gerät zu deaktivieren, ohne dafür einen individuell angepasstes Vouchers-Template hochladen zu müssen, welches diese Grafiken entfernt. Wenn Sie die Grafikausgabe deaktivieren, wird ein reiner Text-Voucher ausgegeben.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

Default:

ja

2.24.36 Benutzer-muss-AGBs-akzeptieren

Durch aktivieren dieses Parameters haben Sie in bestimmten Anmeldungsmodi die Möglichkeit, die Anmeldung an die Anerkennung von Nutzungsbedingungen zu koppeln. In diesem Fall zeigt der Public Spot auf der Anmeldeseite ein zusätzliches Optionsfeld an, welches die Benutzer vor Registrierung bzw. Anmeldung zum Akzeptieren der Nutzungsbedingungen auffordert. Stimmt ein Nutzer diesen Nutzungsbedingungen nicht explizit zu, bleibt ihm eine Anmeldung am Public Spot verwehrt.

Folgende Anmeldungsmodi lassen sich an die Anerkennung von Nutzungsbedingungen koppeln:

- Benutzer+Passwort
- MAC+Benutzer+Passwort
- E-Mail
- E-Mail2SMS

Denken Sie daran, eine individuelle Seitenvorlage in das Gerät zu laden, bevor Sie eine Bestätigung von Nutzungsbedingungen einfordern.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

Default:

nein

2.24.37 Drucke-Logout-Link

Über diesen Parameter legen Sie fest, ob das Gerät beim Erstellen eines Vouchers die URL für die Abmeldung vom Public Spot auf dem Voucher hinterlegt.

Damit die korrekte URL auf dem Voucher erscheint, muss für den Parameter **Geraete-Hostname** (SNMP-ID 2.24.22) der Wert `logout` eingetragen sein.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

ja

Default:

ja

2.24.38 LBS-Tracking

Bestimmen Sie hier, ob der LBS-Server die am Public Spot angemeldeten Benutzer nachverfolgen darf.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.24.39 LBS-Tracking-Liste

Name der LBS-Tracking-Liste

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

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

Default-Wert:

leer

2.24.40 XML-Interface

Hier konfigurieren Sie das XML-Interface.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

2.24.40.1 Aktiv

Hier aktivieren Sie das XML-Interface.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

Mögliche Werte:

Ja

Nein

Default:

Nein

2.24.40.2 Radius-Authentifizierung

Hier aktivieren bzw. deaktivieren Sie die Authentifizierung über einen RADIUS-Server bei der Verwendung der XML-Schnittstelle des Public Spots.

Die zusätzliche Authentifizierung über einen RADIUS-Server ist nur aktiv, wenn die XML-Schnittstelle des Public Spots aktiviert ist (siehe *XML-Schnittstelle)*.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

Mögliche Werte:

Ja: Anfrage wird vom Public Spot an den internen RADIUS Server weitergeleitet oder bei einer RADIUS-Weiterleitung über einen Realm an einen externen RADIUS Server übergeben.

Nein: Keine weitere Authentifizierung notwendig

Default:

Ja

2.24.41 Authentifizierungs-Module

In diesem Menüpunkt definieren Sie einzelne Parameter zur Benutzung des Netzwerk-Zugriffs und legen fest, wie und mit welchen Parametern die Authentifizierung und der Versand der Anmeldedaten erfolgt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

2.24.41.1 E-Mail-Authentifizierung

In diesem Menü nehmen Sie die Einstellungen für die Authentifizierung am Netzwerk und den Versand der Anmeldedaten vor. Letzterer erfolgt bei diesem Verfahren per E-Mail.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

2.24.41.1.1 E-Mail-pro-Stunde-Limit

Hier geben Sie die maximale Anzahl von E-Mails ein, die innerhalb einer Stunde verschickt werden, um Benutzern im Public Spot die Login-Daten mitzuteilen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **E-Mail-pro-Stunde-Limit**

Mögliche Werte:

Max. 5 Ziffern

Default:

100

2.24.41.1.3 Betreffzeile

Geben Sie hier den in der versendeten E-Mail angezeigten Betreff ein.

Die Betreffzeile darf auch die folgenden Steuerzeichen enthalten:

- `\n`: CRLF (Carriage Return, Line Feed)
- `\t`: Tabulator
- `\xy`: ASCII-Code des entsprechenden Zeichens

Sie können diese Steuerzeichen sowohl im Betreff, als auch im Textinhalt für E-Mail bzw. E-Mail2SMS nutzen. Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dieses unterbindet die Umwandung des "\" durch das LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Max. 250 Zeichen

Default:

Your Public Spot Account

2.24.41.1.4 Textinhalt

Mit diesem Parameter legen Sie den Inhalt der versendeten E-Mail fest, wobei "$PSpotPasswd" die Variable für das generierte Passwort ist.

Der Textinhalt darf auch die folgenden Steuerzeichen enthalten:

- `\n`: CRLF (Carriage Return, Line Feed)
- `\t`: Tabulator

- \xy: ASCII-Code des entsprechenden Zeichens

Sie können diese Steuerzeichen sowohl im Betreff, als auch im Textinhalt für E-Mail bzw. E-Mail2SMS nutzen. Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dieses unterbindet die Umwandung des "\" durch das LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Max. 500 Zeichen

Default:

Leer

2.24.41.1.5 Max-Request-Versuche

Mit diesem Parameter legen Sie fest, wie viele verschiedene Zugangsdaten Sie innerhalb eines Tages für eine MAC-Adresse bereitstellen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Max-Request-Versuche**

Mögliche Werte:

Max. 5 Ziffern

Default:

3

2.24.41.1.6 Lokale-E-Mail-Adresse

Geben Sie hier die in der versendeten E-Mail angezeigte Absenderadresse ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Lokale-E-Mail-Adresse**

Mögliche Werte:

Gültige E-Mail-Adresse mit maximale 150 Zeichen.

Default:

leer

2.24.41.1.7 Name

Geben Sie hier den in der versendeten E-Mail angezeigten Absendernamen ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Name**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

2.24.41.1.8 Black-White-Domain-List

Mit diesem Parameter legen Sie an, ob das Gerät die Tabelle **Domain-List** als Blacklist oder Whitelist verwendet. Diese Definition bestimmt, welche E-Mail-Adressen bzw. Domains Ihre Public Spot-Benutzer zur Registrierung angeben dürfen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

Mögliche Werte:

- **Blacklist**: Die Registrierung ist über alle E-Mail-Domains erlaubt bis auf diejenigen, die in dieser Tabelle stehen.
- **Whitelist**: Die Registrierung ist ausschließlich über die E-Mail-Domains möglich, die in dieser Tabelle stehen.

Default:

Blacklist

2.24.41.1.9 Domain-List

Mit dieser Liste können Sie festlegen, ob Sie E-Mails von bestimmten E-Mail-Anbietern grundsätzlich akzeptieren oder ablehnen wollen. Über die Schaltfläche "Hinzufügen" fügen Sie der Liste einzelne Anbieter hinzu. Die Entscheidung, ob Sie mit einer erstellten Liste Anbieter akzeptieren oder ablehnen, treffen Sie mit dem Parameter *Black-White-Domain-List*.

Bitte beachten Sie, dass der Public Spot bei einer leeren Domain-List als Whitelist alle Domains ablehnt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

Mögliche Werte:

Gültige E-Mail-Domänen (z. B. @web.de) mit maximal 150 Zeichen.

Default:

leer

2.24.41.1.9.1 Domain

Über diesen Eintrag definieren Sie die E-Mail-Domains, die Sie im Falle einer Anmeldung Ihrer Public Spot-Benutzer via E-Mail erlauben bzw. verbieten. Die Entscheidung, ob Sie mit einer erstellten Liste Anbieter akzeptieren oder ablehnen, treffen Sie mit dem Parameter *Black-White-Domain-List*.

Bitte beachten Sie, dass der Public Spot bei einer leeren Domain-List als Whitelist alle Domains ablehnt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Domain-List**

Mögliche Werte:

Gültige E-Mail-Domänen (z. B. @web.de) mit maximal 150 Zeichen.

Default:

leer

2.24.41.1.20 Name

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Absender-Namen, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

2.24.41.1.20.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Absender-Namen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Name**

2.24.41.1.20.2 Inhalt

Über diesen Parameter vergeben Sie den Absender-Namen für die ausgewählte Sprache.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Name**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.1.21 Textinhalt

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Nachrichtentext, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

2.24.41.1.21.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Nachrichtentext.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Textinhalt**

2.24.41.1.21.2 Inhalt

Über diesen Parameter vergeben Sie den Nachrichtentext für die ausgewählte Sprache. Dabei stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an den Benutzer automatisch mit Werten gefüllt.

Folgende **Variablen** stehen Ihnen zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

Platzhalter für die Abmelde-URL des Public Spots in der Form `http://<IP-Adresse des Public Spots>/authen/logout`. Über diese URL hat ein Public Spot-Benutzer die Möglichkeit, sich vom Public Spot abzumelden, falls nach einem erfolgreichen Login das Sitzungsfenster – welches diesen Link ebenfalls enthält – z. B. vom Browser geblockt oder vom Benutzer geschlossen wird.

Folgende **Steuerzeichen** stehen Ihnen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandung des "\" durch LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.1.22 Betreffzeile

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für die Betreffzeile, welche das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung**

2.24.41.1.22.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Betreffzeilen-Text.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Betreffzeile**

2.24.41.1.22.2 Inhalt

Über diesen Parameter vergeben Sie den Betreffzeilen-Text für die ausgewählte Sprache. Dabei stehen Ihnen folgende Steuerzeichen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandlung des "\" durch LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.2 E-Mail2SMS-Authentifizierung

In diesem Menü nehmen Sie die Einstellungen für die Authentifizierung am Netzwerk und den Versand der Anmeldedaten vor. Letzterer erfolgt bei diesem Verfahren per SMS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

2.24.41.2.1 E-Mail-pro-Stunde-Limit

Hier geben Sie die maximale Anzahl von E-Mails ein, die innerhalb einer Stunde verschickt werden, um Benutzern im Public Spot die Login-Daten mitzuteilen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **E-Mail-pro-Stunde-Limit**

Mögliche Werte:

Max. 5 Ziffern

Default:

100

2.24.41.2.3 Betreffzeile

Geben Sie hier den in der versendeten E-Mail angezeigten Betreff ein. Beachten Sie dabei etwaige Formatierungsvorgaben des verwendeten SMS-Gateways.

Die Betreffzeile darf auch die folgenden Steuerzeichen enthalten:

- `\n`: CRLF (Carriage Return, Line Feed)
- `\t`: Tabulator
- `\xy`: ASCII-Code des entsprechenden Zeichens

Sie können diese Steuerzeichen sowohl im Betreff, als auch im Textinhalt für E-Mail bzw. E-Mail2SMS nutzen. Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dieses unterbindet die Umwandung des "\" durch das LCOS.

Sofern die Vorgaben des verwendeten E-Mail2SMS-Gateways es erlauben oder erfordern, nutzen Sie die folgenden Variablen:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers
- `$PSpotPasswd` für das vom Public Spot generierte Password des Benutzers

Der Public Spot überträgt die Mobilfunknummer des Benutzers aus der Variable `$PSpotUserMobileNr` ohne evtl. vorhandende führende Nullen and das SMS-Gateway. Falls das SMS-Gateway eine bestimmte Zeichenfolge als Länderkennzeichen erwartet (z. B. "00" oder "+"), dann tragen Sie das entsprechende Prefix vor der Variablen ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Max. 250 Zeichen

Default:

Leer

2.24.41.2.4 Max-Request-Versuche

Mit diesem Parameter legen Sie fest, wie viele verschiedene Zugangsdaten Sie innerhalb eines Tages für eine MAC-Adresse bereitstellen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Max-Request-Versuche**

Mögliche Werte:

Max. 5 Ziffern

Default:

3

2.24.41.2.5 Lokale-E-Mail-Adresse

Geben Sie hier die in der versendeten E-Mail angezeigte Absenderadresse ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Lokale-E-Mail-Adresse**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

2.24.41.2.6 Name

Geben Sie hier den in der versendeten SMS angezeigten Absendernamen ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Name**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

2.24.41.2.12 Textinhalt

Mit diesem Parameter legen Sie den Inhalt der versendeten E-Mail fest. Beachten Sie dabei etwaige Formatierungsvorgaben des verwendeten SMS-Gateways.

Der Textinhalt darf auch die folgenden Steuerzeichen enthalten:

- `\n`: CRLF (Carriage Return, Line Feed)
- `\t`: Tabulator
- `\xy`: ASCII-Code des entsprechenden Zeichens

Sie können diese Steuerzeichen sowohl im Betreff, als auch im Textinhalt für E-Mail bzw. E-Mail2SMS nutzen. Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dieses unterbindet die Umwandung des "\" durch das LCOS.

Sofern die Vorgaben des verwendeten E-Mail2SMS-Gateways es erlauben oder erfordern, nutzen Sie die folgenden Variablen:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers
- `$PSpotPasswd` für das vom Public Spot generierte Password des Benutzers

Der Public Spot überträgt die Mobilfunknummer des Benutzers aus der Variable `$PSpotUserMobileNr` ohne evtl. vorhandende führende Nullen and das SMS-Gateway. Falls das SMS-Gateway eine bestimmte Zeichenfolge als Länderkennzeichen erwartet (z. B. "00" oder "+"), dann tragen Sie das entsprechende Prefix vor der Variablen ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Max. 512 Zeichen

Default:

#Key#Route#From#

2.24.41.2.13 Gateway-E-Mail-Adresse

Geben Sie hier die Adresse Ihres E-Mail2SMS-Gateways für den Versand der Zugangs-SMS ein. Beachten Sie dabei etwaige Formatierungsvorgaben des verwendeten SMS-Gateways.

Sofern die Vorgaben des verwendeten E-Mail2SMS-Gateways es erlauben oder erfordern, nutzen Sie die folgenden Variablen:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2SMS-Authentifizierung** > **Gateway-E-Mail-Adresse**

Mögliche Werte:

Gültige E-Mail-Adresse eines Gateways mit max. 150 Zeichen. .

Default:

leer

2.24.41.2.14 Erlaubte-Landesvorwahlen

In dieser Tabelle definieren Sie die Landesvorwahlen, die Sie im Falle einer Anmeldung Ihrer Public Spot-Benutzer via SMS erlauben Ein Benutzer kann sich seine Anmeldedaten nur an Rufnummern schicken lassen, deren Landesvorwahl in dieser Liste enthalten sind.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

2.24.41.2.14.1 Name

Über diesen Eintrag vergeben Sie eine Bezeichnung für die Landesvorwahl, z. B. `DE` oder `Deutschland`.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Erlaubte-Landesvorwahlen**

Mögliche Werte:

String, max. 150 Zeichen

Default:

2.24.41.2.14.2 Code

Über diesen Eintrag vergeben Sie die Landesvorwahl für das Land, das Sie hinzufügen möchten, z. B. `0049` für Deutschland.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Erlaubte-Landesvorwahlen**

Mögliche Werte:

Gültige Landesvorwahl, max. 5 Zeichen

Default:

0

2.24.41.2.15 SMS-Senden

Über diesen Parameter legen Sie fest, auf welche Art und Weise der SMS-Versand erfolgt. Dabei können Sie – je nach Gerätetyp – zwischen mehreren Varianten wählen.

Für den erfolgreichen Versand der Anmeldedaten als Kurznachricht durch ein 3G/4G WWAN-fähiges Gerät muss unter **Setup** > **SMS** dessen internes SMS-Modul eingerichtet sein.

Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Setup** > **Mail** ein gültiges SMTP-Konto eingerichtet sein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

Direkt-Senden

Versand der Anmeldedaten als SMS über das geräteeigene 3G/4G WWAN-Modul.

HTTP2SMS

Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes

Sie haben bei der Public Spot-Anmeldung via SMS die Möglichkeit, den Versand der Zugangsdaten über ein anderes Gerät mit 3G/4G WWAN-Modul abzuwickeln. Dazu hinterlegen Sie im Gerät, das den Public Spot bereitstellt, die Adresse und die Zugangsdaten des anderen Gerätes. Für den Versand der SMS meldet sich das Public Spot-Modul am anderen Gerät an und initiiert über die aufgerufene URL den Versand der Kurznachricht durch das fremde 3G/4G WWAN-Modul.

Stellen Sie sicher, dass das SMS-Modul auf dem anderen Gerät korrekt konfiguriert ist. Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.

SMS-Gateway

Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, welches die Umwandlung der E-Mail in eine SMS übernimmt.

Default-Wert:

SMS-Gateway

2.24.41.2.16 HTTP-Benutzername

Über diesen Parameter geben Sie den Benutzernamen an, mit dem sich Ihr Gerät an einem anderen Gerät anmeldet.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

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

Default-Wert:

leer

2.24.41.2.17 HTTP-Passwort

Über diesen Parameter geben Sie das Passwort für den Benutzernamen an, mit dem sich Ihr Gerät an einem anderen Gerät anmeldet.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

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

Default-Wert:

leer

2.24.41.2.18 HTTP-Gateway-Adresse

Über diesen Parameter geben Sie die IP-Adresse des anderen Gerätes an, welches Sie für den SMS-Versand verwenden wollen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Mögliche Werte:

Gültige IPv4-/IPv6-Adresse, max. 15 Zeichen aus `[0-9][A-F][a-f]:./`

Default-Wert:

leer

2.24.41.2.23 Name

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Absender-Namen, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

2.24.41.2.23.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Absender-Namen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Name**

2.24.41.2.23.2 Inhalt

Über diesen Parameter vergeben Sie den Absender-Namen für die ausgewählte Sprache.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Name**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.2.24 Textinhalt

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für den Nachrichtentext, welchen das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

2.24.41.2.24.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Nachrichtentext.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Textinhalt**

2.24.41.2.24.2 Inhalt

Über diesen Parameter vergeben Sie den Nachrichtentext für die ausgewählte Sprache. Dabei stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an das SMS-Gateway automatisch mit Werten gefüllt.

Folgende **Variablen** stehen Ihnen zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

Platzhalter für die Abmelde-URL des Public Spots in der Form `http://<IP-Adresse des Public Spots>/authen/logout`. Über diese URL hat ein Public Spot-Benutzer die Möglichkeit, sich vom Public Spot abzumelden, falls nach einem erfolgreichen Login das Sitzungsfenster – welches diesen Link ebenfalls enthält – z. B. vom Browser geblockt oder vom Benutzer geschlossen wird.

Folgende **Steuerzeichen** stehen Ihnen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandung des "\" durch LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.2.25 Betreffzeile

In dieser Tabelle verwalten Sie die unterschiedlichen Sprachvarianten für die Betreffzeile, welche das Public Spot-Modul für den Versand der Anmeldedaten via E-Mail2SMS verwendet. Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

2.24.41.2.25.1 Sprache

Dieser Parameter zeigt die Sprachvariante für den individuellen Betreffzeilen-Text.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Betreffzeile**

2.24.41.2.25.2 Inhalt

Über diesen Parameter vergeben Sie den Betreffzeilen-Text für die ausgewählte Sprache. Dabei stehen Ihnen folgende Steuerzeichen zur Verfügung:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandlung des "\" durch LCOS.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Beliebiger String, max. 251 Zeichen aus

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

Default:

2.24.41.3 Benutzer-Template

In diesem Menü verwalten Sie die Standardwerte, nach denen der Public Spot automatisch neue Benutzerkonten anlegt, wenn die Anmeldung via E-Mail, SMS oder nach Bestätigen einer Einverständniserklärung erfolgt. Die konfigurierbaren Parameter entsprechend weitgehend denen des Setup-Wizards **Public-Spot-Benutzer einrichten**.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

2.24.41.3.2 Kommentar

Über diesen Eintrag vergeben Sie einen Kommentar oder Infotext, mit dem der RADIUS-Server ein automatisch erstelltes Benutzerkonto versieht.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

String, max. 251 Zeichen

Default:

2.24.41.3.3 Volumen-Budget

Über diesen Eintrag definieren Sie das Volumen-Budget in MByte, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

schaltet die Überwachung des Datenvolumens aus.

2.24.41.3.4 Zeit-Budget

Über diesen Eintrag definieren Sie das Zeit-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.24.41.3.5 Rel.-Ablauf

Über diesen Eintrag definieren Sie die relative Ablaufzeit eines automatisch angelegten Benutzerkontos (in Sekunden). Der von Ihnen gewählte **Ablauf-Typ** muss ein `relativ` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

3600

2.24.41.3.6 Abs.-Ablauf

Über diesen Eintrag definieren Sie die absolute Ablaufzeit eines automatisch angelegten Benutzerkontos (in Tagen). Der von Ihnen gewählte **Ablauf-Typ** muss ein `absolut` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet zu dem in diesem Feld angegebenen Zeitpunkt, hochgerechnet vom Tag der Kontoerstellung.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

365

2.24.41.3.7 Ablauf-Typ

Über diesen Eintrag definieren Sie, auf welche Art ein automatisch angelegtes Public Spot-Benutzerkonto abläuft. Sie können festlegen, ob die Gültigkeitsdauer eines Benutzer-Accounts absolut (fester Zeitpunkt) und/oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) ist. Wenn Sie beide Werte auswählen, hängt der Ablaufzeitpunkt davon ab, welcher Fall als Erstes eintritt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

absolut

relativ

Default:

absolut, relativ

2.24.41.3.8 Max-gleichzeitige-Logins

Über diesen Eintrag legen Sie die maximale Anzahl der Geräte fest, die gleichzeitig unter einem automatisch erstellten Account angemeldet sein dürfen. Der Wert `0` steht dabei für 'unbegrenzt'.

Damit diese Einstellung greift, muss gleichzeitig der Parameter ***Mehrfach-Logins*** aktiviert sein.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

1

2.24.41.3.9 Mehrfach-Logins

Über diesen Eintrag erlauben bzw. verbieten Sie ganz allgemein, ob Nutzer eines automatisch erstellten Accounts mehrere Geräte gleichzeitig mit den selben Zugangsdaten am Public Spot anmelden dürfen. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über den Parameter ***Max-gleichzeitige-Logins*** fest.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

ja

nein

Default:

ja

2.24.41.3.10 Tx-Limit

Mit dieser Einstellung begrenzen Sie die maximale Sende-Bandbreite (in Kbit/s), die dem Benutzer zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung (= unlimitierte Bandbreite).

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.24.41.3.11 Rx-Limit

Mit dieser Einstellung begrenzen Sie die maximale Empfangs-Bandbreite (in Kbit/s), die dem Benutzer zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung (= unlimitierte Bandbreite).

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.24.41.4 Login-nach-Einverstaendniserklaerung

In diesem Menü nehmen Sie die Einstellungen für die automatische Anmeldung und Authentifizierung via RADIUS vor.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

2.24.41.4.1 Max-Request-Pro-Stunde

Dieser Eintrag zeigt die maximale Anzahl der Benutzer pro Stunde an, die sich am Gerät automatisch ein Konto erstellen können. Verringern Sie diesen Wert, um Leistungseinbußen durch übermäßig viele Nutzer zu reduzieren.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

0 bis 65535

Default:

100

2.24.41.4.2 Benutzer-Konto-Pro-Tag

Dieser Eintrag zeigt für den bezeichneten Anmeldungs-Modus die Anzahl der Konten, die ein Nutzer am Tag anlegen kann. Ist dieser Wert erreicht und die Nutzer-Session abgelaufen, kann sich ein Benutzer für den betreffenden Tag nicht mehr automatisch am Public Spot anmelden und authentifizieren lassen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

0 bis 65535

Default:

1

2.24.41.4.3 Benutzername-Prefix

Dieser Eintrag enthält den Prefix, der automatisch generierten Public-Spot-Benutzernamen vorangestellt wird, wenn Sie vom Gerät im Anmeldungs-Modus "Kein-Authentifizierung" (automatische Anmeldung und Authentifizierung) erstellt wurden.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Login-nach-Einverstaendniserklaerung**

Mögliche Werte:

String, max. 10 Zeichen

Default:

free

2.24.42 WISPr

Dieses Menü beinhaltet die Einstellungen für WISPr.

Pfad Telnet:

Setup > **Public-Spot-Modul**

2.24.42.1 In-Betrieb

Aktivieren oder deaktivieren Sie die WISPr-Funktion für Ihr Gerät.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

nein

ja

Default:

nein

2.24.42.2 Standort-Id

Vergeben Sie hierüber eine eindeutige Standort-Nummer oder -Kennung für Ihr Gerät, z. B. in der Form `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

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

Default:

2.24.42.3 Operator-Name

Geben Sie hier den Namen des Hotspot-Betreibers ein, z. B. `providerX`. Diese Angabe hilft dem Nutzer bei der manuellen Auswahl eines Internet-Service-Providers.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

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

Default:

2.24.42.4 Standort-Name

Beschreiben Sie den Standort Ihres Gerätes, z. B. `CafeX_Markt3`. Diese Angabe dient einem Nutzer zur besseren Identifizierung Ihres Hotspots.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

String, max. 255 Zeichen, mit folgenden Zeichenbeschränkungen:

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

Default:

2.24.42.5 Login-URL

Geben Sie die HTTPS-Adresse ein, an die die WISPr-Client die Zugangsdaten für Ihren Internet-Service-Provider übermittelt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

2.24.42.6 Logout-URL

Geben Sie die HTTPS-Adresse ein, über die sich ein WISPr-Client von Ihrem Internet-Service-Provider abmeldet.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

2.24.42.7 Abbruch-Login-URL

Geben Sie die HTTPS-Adresse ein, an die das Gerät einen WISPr-Client weiterleitet, wenn die Authentifizierung fehlschlägt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

HTTPS-URL, max. 255 Zeichen

Default:

2.24.42.8 Max-Authen-Fehler

Geben Sie hier die Anzahl der Fehlversuche ein, welche die Login-Seite Ihres Internet-Service-Providers maximal erlaubt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **WISPr**

Mögliche Werte:

0 bis 65535

Default:

5

2.24.43 Werbung

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

Pfad Telnet:

Setup > **Public-Spot-Modul**

2.24.43.1 Aktiv

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.24.43.2 Intervall

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

Pfad Telnet:

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

Mögliche Werte:

0 … 65535 Minuten

Default-Wert:

10

Besondere Werte:

0

Die Umleitung erfolgt direkt nach der Anmeldung.

2.24.43.3 URL

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.43.3.1 Inhalt

Über diesen Parameter definieren Sie die jeweilige Werbe-URL.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.43.4 User-Agent-White-List

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.43.4.1 User-Agent

Name des User-Agents, den Sie in die White-List aufnehmen.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.43.5 WISPr-Redirect-URL-Verarbeiten

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

Pfad Telnet:

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

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.24.43.6 Freie-Netze

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

Pfad Telnet:

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

2.24.43.6.1 Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.24.43.6.2 Maske

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

0.0.0.0

2.24.44 Verwalte-Benutzer-Assistent

In diesem Eintrag finden Sie die erweiterten Einstellungen für den Assistenten **Public Spot-Benutzer verwalten**.

Pfad Telnet:

Setup > **Public-Spot-Modul**

2.24.44.10 Zeige-Statusinformationen

Dieser Eintrag bietet Ihnen die Möglichkeit, Statusinformationen im Setup-Wizard zu verbergen.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

nein

Der Setup-Wizard blendet folgende Spalten aus: **Online-Zeit**, **Traffic**, **Status**, **MAC-Adresse**, **IP-Adresse**.

ja

Der Setup-Wizard zeigt alle Statusinformationen an.

2.24.44.11 Zeige-Alle-Benutzer-Admin-unabhaengig

Dieser Eintrag bietet Ihnen die Möglichkeit, im Setup-Wizard nur Benutzerkonten anzuzeigen, die der aktuell angemeldete Administrator angelegt hat.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

ja

Der Setup-Wizard zeigt alle Public Spot Accounts an.

nein

Der Setup-Wizard zeigt nur die vom aktuell angemeldeten Administrator generierten Public Spot Accounts an.

Default-Wert:

ja

2.24.47 Herkunft-VLAN-verifizieren

Über diesen Parameter legen Sie fest, ob das XML-Interface die VLAN-ID des Netzes, aus dem sich ein Benutzer authentisiert hat, bei der Verifikation von Benutzer-Requests berücksichtigt. Dies ist z. B. in Szenarien relevant, in denen Sie mehrere Public Spot-SSIDs via VLAN trennen und eine einmalige Authentifizierung an einer dieser SSIDs den Benutzer nicht automatisch für den Zugriff auf die übrigen SSIDs berechtigen soll.

Der Parameter setzt voraus, dass Sie die Setup-Parameter 2.24.40.1 (das XML-Interface selbst) und 2.24.40.2 (die Authentifizierung für das XML-Interface über einen internen oder einen externen RADIUS-Server) ebenfalls aktiviert haben.

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

Der Public Spot berücksichtigt die VLAN-ID nicht bei der Verifikation von Benutzern. Eine einmalige Authentifizierung eines Benutzers berechtigt zum Zugriff auf sämtliche vom Public Spot verwaltete SSIDs. Solange das Benutzerkonto gültig ist, erfolgt die Anmeldung automatisch.

ja

Der Public Spot berücksichtigt die VLAN-ID bei der Verifikation von Benutzern. Hierzu hinterlegt der Public Spot die VLAN-ID in der gleichnamigen Spalte der Stationstabelle, sofern die Authentifizierung durch den RADIUS-Server erfolgreich war. Diese VLAN-ID entspricht dem Wert für SOURCE_VLAN im Login-Request des externen Gateways. Wechselt der Public Spot-Benutzer in ein Netz mit abweichender VLAN-ID, ändert der Public Spot dessen Stationstabelleneintrag zu „nicht authentifiziert“ und fordert den Benutzer zur erneuten Authentifizierung am RADIUS-Server auf. Der Benutzer erhält in diesem Fall bei erneuter Anmeldung die Anmeldeseite.

Weitere Informationen zu den Request- und Response-Typen sowie dem SOURCE_VLAN-Element finden Sie im Referenzhandbuch.

Default-Wert:

nein

2.24.48 Circuit-IDs

In dieser Tabelle konfigurieren Sie die Circuit-ID, die der AP bei einer Anmeldung eines Public Spot-Benutzers zusätzlich zu Username und Passwort als Kennung an den WLC sendet.

Der Public Spot-Setup-Assistent prüft beim Anlegen eines neuen Public Spot-Nutzers, ob für den angemeldeten Administrator ein Eintrag in dieser Tabelle hinterlegt ist. Ist das der Fall, übernimmt der Setup-Assistent die entsprechende Circuit-ID als „gerufene Station" in die RADIUS-User-Tabelle.

Pfad Telnet:

Setup > **Public Spot**

2.24.48.1 Administrator

Enthält den Namen des Administrators, der berechtigt ist, diese Circuit-ID zu vergeben.

Pfad Telnet:

Setup > **Public-Spot** > **Circuit-IDs**

Mögliche Werte:

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

Default-Wert:

leer

2.24.48.2 Circuit-Id

Enthält die Circuit-ID, die der AP bei einer Anmeldung eines Public Spot-Benutzers zusätzlich zu Username und Passwort als Kennung an den WLC sendet.

Pfad Telnet:

Setup > **Public-Spot** > **Circuit-IDs**

Mögliche Werte:

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

Default-Wert:

leer

2.24.50 Auto-Re-Login

Mobile WLAN-Clients (z. B. Smartphones und Tablett-PCs) buchen sich automatisch in bekannte WLAN-Netze (SSID) ein, wenn sie erneut deren Funkzelle erreichen. Viele Apps greifen in diesem Fall automatisch ohne Umweg über den Webbrowser auf Webinhalte zu, um aktuelle Daten abzufragen (z. B. Emails, soziale Netzwerke, Wetterbericht etc.). In diesen Fällen ist es unpraktisch, wenn der Benutzer sich zunächst erneut im Browser manuell an einem Public Spot authentifizieren muss.

Mit dem automatischen Re-Login genügt es, wenn der Benutzer sich beim erstmaligen Aufenthalt in der Funkzelle am Public Spot identifiziert. Nach einer zwischenzeitlichen Abwesenheit kann der Benutzer anschließend nahtlos weiter den Public Spot nutzen.

Der Public Spot protokolliert sowohl die manuelle An- und Abmeldung sowie einen Re-Login im SYSLOG. Dabei speichert er für einen Re-Login dieselben Anmeldedaten, die der Benutzer für die erstmalige Authentifizierung verwendet hat.

Bitte beachten Sie, dass die Authentifizierung ausschließlich anhand der MAC-Adresse stattfindet, wenn Auto-Re-Login aktiviert ist.

In diesem Menüpunkt konfigurieren Sie die Parameter für das automatische Re-Login.

Pfad Telnet:

Setup > **Public-Spot-Modul**

2.24.50.1 Aktiv

Mit dieser Aktion aktivieren bzw. deaktivieren sie das automatische Re-Login.

Die Authentifizierung erfolgt ausschließlich über die MAC-Adresse des WLAN-Clients, wenn Re-Login aktiviert ist. Da das zu Sicherheitsproblemen führen kann, ist Re-Login standardmäßig deaktiviert.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

ja

nein

Default:

nein

2.24.50.2 Stations-Tabellen-Limit

Sie können die maximale Anzahl der Clients, die die Funktion Re-Login nutzen dürfen, auf bis zu 65536 Teilnehmer vergrößern.

Während des Betriebs wird ausschließlich eine Vergrößerung der Stationstabelle sofort übernommen. Starten Sie den Access-Point neu, damit eine Reduzierung der Stationstabelle wirksam wird.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

16 bis 65536

Default:

8192

2.24.50.3 Exist-Timeout

Dieser Wert gibt an, wie lange der Public Spot die Anmeldedaten eines WLAN-Clients für ein Re-Login in der Tabelle speichert. Nach Ablauf dieser Frist (in Sekunden) muss sich der Public-Spot-Benutzer erneut über den Browser auf der Anmeldeseite des Public Spots anmelden.

Sofern ein Public-Spot-Nutzer über ein Zeitkontingent verfügt, welches kleiner ist als der hier eingestellte Timeout-Wert, ist dieser Parameter für ihn wirkungslos. Ein automatisches Re-Login findet nicht statt, sobald ein Benutzer den Status "Unauthentifiziert" trägt.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Auto-Re-Login**

Mögliche Werte:

max. 10 Zeichen

Default:

259200

2.24.60 Login-Text

Über diese Tabelle verwalten Sie die Login-Texte.

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen Text anzugeben, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Dieser **Login-Text** ist in mehreren Sprachen hinterlegbar; welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).

Pfad Telnet:

Setup > **Public-Spot-Modul**

2.24.60.1 Sprache

Dieser Parameter zeigt die Sprache, für die Sie einen Login-Text vergeben.

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Login-Text**

2.24.60.2 Inhalt

Über diesen Parameter vergeben Sie einen Login-Text für die ausgewählte Sprache. Um Umlaute einzugeben, sollten Sie deren HTML-Äquivalente verwenden (z. B. `&uuml;` für ü), da der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das Formular aus.</i>
```

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Login-Text**

Mögliche Werte:

Beliebiger String, max. 254 Zeichen aus

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

Default:

2.25 RADIUS

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

SNMP-ID: 2.25

Pfad Telnet: /Setup

2.25.4 Auth.-Timeout

Dieser Wert gibt an, nach wie vielen Millisekunden eine erneute RADIUS-Authentifizierung versucht werden soll.

SNMP-ID: 2.25.4

Pfad Telnet: /Setup/RADIUS

Mögliche Werte:

- max. 10 Zeichen

Default: 5000

2.25.5 Auth.-Wiederholung

Dieser Wert gibt an, wie viele Authentifizierungs-Versuche insgesamt durchgeführt werden, bevor eine Ablehnung erfolgt.

SNMP-ID: 2.25.5

Pfad Telnet: /Setup/RADIUS

Mögliche Werte:

- max. 10 Zeichen

Default: 3

2.25.9 Backup-Abfrage-Strategie

Dieser Wert gibt an, wie das Gerät mit unbeantworteten Anfragen mehrerer RADIUS-Server umgehen soll.

SNMP-ID: 2.25.9

Pfad Telnet: /Setup/RADIUS/Backup-Abfrage-Strategie

Mögliche Werte:

- Block: das Gerät schickt zunächst die maximale Anzahl an Wiederholungsanfragen an den ersten Server zurück, bevor es diese an den Backup-Server weiterleitet.
- Zyklisch: das Gerät schickt unbeantwortete Anfragen abwechselnd an die konfigurierten Server.

Default: Block

2.25.10 Server

Dieses Menü enthält die Einstellungen für den RADIUS-Server.

SNMP-ID: 2.25.10

Pfad Telnet: /Setup/RADIUS

2.25.10.1 Authentifizierungs-Port

Geben Sie hier den Port an, über den die Authenticator mit dem RADIUS-Server im Access Point kommunizieren.

SNMP-ID: 2.25.10.1

Pfad Telnet: /Setup/RADIUS/Server

Mögliche Werte:

- max. 5 Ziffern

Default: 0

Besondere Werte: 0: schaltet den RADIUS-Server aus.

2.25.10.2 Clients

Hier tragen Sie die Clients ein, die mit dem RADIUS-Server kommunizieren.

Pfad Telnet:

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

2.25.10.2.1 IP-Netz

IP-Netz (Bereich von IP-Adressen) der RADIUS-Clients, für die das in diesem Eintrag definierte Kennwort gilt.

SNMP-ID: 2.25.10.2.1

Pfad Telnet: /Setup/RADIUS/Server/Clients

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.25.10.2.2 Secret

Kennwort, das der Client für den Zugang zum RADIUS-Server im Access Point benötigt.

SNMP-ID: 2.25.10.2.2

Pfad Telnet: /Setup/RADIUS/Server/Clients

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.25.10.2.3 IP-Netzmaske

IP-Netzmaske des RADIUS-Clients.

SNMP-ID: 2.25.10.2.3

Pfad Telnet: /Setup/RADIUS/Server/Clients

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.25.10.2.4 Protokoll

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

SNMP-ID: 2.25.10.2.4

Pfad Telnet: /Setup/RADIUS/Server/Clients

Mögliche Werte:

- RADSEC
- RADIUS
- alle

Default: RADIUS

2.25.10.2.5 Kommentar

Kommentar zu diesem Eintrag.

Pfad Telnet:

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

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.25.10.3 Weiterleit-Server

Wenn Sie RADIUS-Weiterleitung nutzen möchten, müssen Sie hier weitere Angaben machen.

SNMP-ID: 2.25.10.3

Pfad Telnet: /Setup/RADIUS/Server

2.25.10.3.1 Realm

Zeichenkette, mit der der RADIUS-Server das Weiterleitungs-Ziel identifiziert.

Pfad Telnet:

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

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

2.25.10.3.3 Port

Offener Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.

SNMP-ID: 2.25.10.3.3

Pfad Telnet: /Setup/RADIUS/Server/Weiterleit-Server

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.25.10.3.4 Secret

Kennwort, das für den Zugang zum Weiterleitungs-Server benötigt wird.

SNMP-ID: 2.25.10.3.4

Pfad Telnet: /Setup/RADIUS/Server/Weiterleit-Server

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.25.10.3.5 Backup

Alternativer Weiterleitungs-Server, an den der RADIUS-Server Anfragen weiterleitet, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

Pfad Telnet:

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

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

2.25.10.3.6 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

SNMP-ID: 2.25.10.3.6

Pfad Telnet: /Setup/RADIUS/Server/Weiterleit-Server

Mögliche 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

Default: Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

2.25.10.3.7 Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

SNMP-ID: 2.25.10.3.7

Pfad Telnet: /Setup/RADIUS/Server/Weiterleit-Server

Mögliche Werte:

- RADSEC
- RADIUS

Default: RADIUS

2.25.10.3.9 Accnt.-Port

Geben Sie hier den Port des Servers an, an den der geräteinterne RADIUS-Server Datenpakete für das Accounting weiterleitet.

Pfad Telnet:

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

Mögliche Werte:

0 bis 65535

Default:

0

2.25.10.3.10 Accnt.-Secret

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

Pfad Telnet:

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

Mögliche Werte:

Gültiger Schlüssel, max. 64 Zeichen

Default:

2.25.10.3.11 Accnt.-Loopback-Adresse

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

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

Pfad Telnet:

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

Mögliche Werte:

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

  Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!
- `LB0...LBF` für eine der 16 Loopback-Adressen oder deren Name
- Beliebige IPv4-Adresse

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

Default:

2.25.10.3.12 Accnt.-Protocol

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

Pfad Telnet:

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

Mögliche Werte:

RADIUS

RADSEC

Default:

RADIUS

2.25.10.3.13 Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.3.14 Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.3.15 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.3.16 Accnt.-Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.5 Default-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername einen unbekannten Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

Pfad Telnet:

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

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

2.25.10.6 Empty-Realm

Dieser Realm gilt alternativ, wenn der übermittelte Benutzername keinen Realm enthält.

Pfad Telnet:

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

Mögliche Werte:

max. 64 Zeichen

Default:

Leer

2.25.10.7 Benutzer

Tragen Sie in die folgende Tabelle die Daten der Benutzer ein, die von diesem Server authentifiziert werden.

SNMP-ID: 2.25.10.7

Pfad Telnet: /Setup/RADIUS/Server/Benutzer

Mehrfach-Logins

Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

Mögliche Werte: Ja, Nein

Default: Ja

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

Ablauf-Art

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Mögliche Werte:

- Absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.
- Relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Default: Leer: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

Abs.-Ablauf

Wenn der Ablauf-Typ “Absolut” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

Mögliche Werte: Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus 0123456789/:.Pp

Default: Leer

Besondere Werte: 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

Rel.-Ablauf

Wenn der Ablauf-Typ “Relativ” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Mögliche Werte: Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der relativen Ablaufzeit aus.

Zeit-Budget

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte: Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der Nutzungsdauer aus.

Volumen-Budget

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

Mögliche Werte: Volumen-Budget in Bytes. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung des Datenvolumens aus.

Kommentar

Kommentar zu diesem Eintrag.

Service-Typ

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt.

Mögliche Werte:

- Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
- Login: Für Public-Spot-Anmeldungen.
- Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.
- Beliebig

Default: Beliebig

Die Anzahl der Einträge mit dem Service-Typ "Beliebig" oder "Login" ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service-Typ "Beliebig" verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

2.25.10.7.1 Benutzername

Name des Benutzers.

SNMP-ID: 2.25.10.7.1

Pfad Telnet: /Setup/RADIUS/Server/Benutzer

Mögliche Werte:

- max. 48 Zeichen

Default: Leer

2.25.10.7.2 Passwort

Passwort des Benutzers.

SNMP-ID: 2.25.10.7.2

Pfad Telnet: /Setup/RADIUS/Server/Benutzer

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.25.10.7.3 Limitiere-Auth-Methoden

Mit dieser Option können die für den Benutzer erlaubten Authentifizierungsverfahren eingeschränkt werden.

SNMP-ID: 2.25.10.7.3

Pfad Telnet: /Setup/RADIUS/Server/Benutzer

Mögliche Werte:

- Beliebige Kombination aus folgenden Werten:
- PAP
- CHAP
- MSCHAP
- MSCHAPv2
- EAP
- Alle

Default: Alle

2.25.10.7.4 VLAN-Id

Über dieses Eingabefeld weisen Sie dem Benutzer eine individuelle VLAN-ID zu. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das Interface erhalten würde. Der Wert `0` deaktiviert die Zuweisung einer individuellen VLAN-ID.

Die Vergabe einer VLAN-ID erfordert technisch bedingt die erneute Adresszuweisung durch den DHCP-Server. Solange ein Client nach der erfolgreichen Authentifizierung noch keine neue Adresse zugewiesen bekommen hat, befindet sich er sich nachwievor in seinem bisherigen (z. B. ungetaggten) Netz. Damit der Client möglichst rasch in das neue Netz überführt wird, ist es notwendig, die Lease-Time des DHCP-Servers – im Setup-Menü unter **Setup** > **DHCP** – möglichst gering einzustellen. Mögliche Werte (in Minuten) sind z. B.:

- **Max.-Gueltigkeit-Minuten**: `2`
- **Default-Gueltigkeit-Minuten**: `1`

Berücksichtigen Sie dabei, dass eine derart starke Verkürzung der globalen Lease-Time Ihr Netz bedingt mit DHCP-Nachrichten flutet und bei größeren Nutzerzahlen zu einer gesteigerten Netzlast führt! Alternativ haben Sie die Möglichkeit, einen anderen DHCP-Server einzusetzen oder Ihre Nutzer manuell – über ihren Client – eine neue Adresse anfordern zu lassen. In der Windows-Kommandozeile erfolgt dies z. B. über die Befehle `ipconfig /release` und `ipconfig /renew`.

Durch die Zuweisung einer VLAN-ID verliert ein Nutzer nach Ablauf des initialen DHCP-Leases seine Verbindung! Erst ab dem zweiten Lease – also nach erfolgter Zuweisung der VLAN-ID – bleibt die Verbindung konstant.

Pfad Telnet:

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

Mögliche Werte:

0 bis 4094

Default:

4

2.25.10.7.5 Rufende-Station-Id-Maske

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

Pfad Telnet:

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

Mögliche Werte:

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

Besondere Werte:

*****

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

Default-Wert:

leer

2.25.10.7.6 Gerufene-Station-Id-Maske

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

Pfad Telnet:

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

Mögliche Werte:

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

Besondere Werte:

*****

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

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

Default-Wert:

leer

2.25.10.7.7 Tx-Limit

Begrenzung der Bandbreite für RADIUS-Clients.

Pfad Telnet: /Setup/RADIUS/Server/Benutzer/Tx-Limit

Mögliche Werte:

- 0 bis 4294967295 (2^32-1)

Default: 0

2.25.10.7.8 Rx-Limit

Begrenzung der Bandbreite für RADIUS-Clients.

Pfad Telnet: /Setup/RADIUS/Server/Benutzer/Rx-Limit

Mögliche Werte:

- 0 bis 4294967295 (2^32-1)

Default: 0

2.25.10.7.9 Mehrfach-Logins

Erlaubt oder verbietet mehr als eine parallele Session mit der gleichen Benutzer-ID. Wenn parallele Sessions verboten sind, wird das Gerät Authentifizierungs-Anfragen für die aktuelle Benutzer-ID zurückweisen, wenn bereits eine Session für diesen Benutzer in der aktiven Session-Abrechnungs-Tabelle läuft. Dies ist eine Voraussetzung für eine sinnvolle Durchsetzung von Zeit- oder Volumen-Budgets.

Pfad Telnet: /Setup/RADIUS/Server/Mehrfach-Logins

Mögliche Werte:

- ja
- nein

Default: ja

Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

2.25.10.7.10 Abs.-Ablauf

Wenn der Ablauf-Typ “Absolut” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

SNMP-ID: 2.25.10.7.10

Pfad Telnet: /Setup/RADIUS/Server/Abs.-Ablauf

Mögliche Werte:

- Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus 0123456789/:.

Default: 0

Besondere Werte: 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

2.25.10.7.11 Zeit-Budget

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

SNMP-ID: 2.25.10.7.11

Pfad Telnet: /Setup/RADIUS/Server/Zeit-Budget

Mögliche Werte:

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der Nutzungsdauer aus.

2.25.10.7.13 Ablauf-Typ

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Pfad Telnet: /Setup/RADIUS/Server/Weiterleit-Server/Ablauf-Typ

Mögliche Werte:

- absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.
- relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
- keiner: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

Default: absolut

Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

2.25.10.7.14 Rel.-Ablauf

Wenn der Ablauf-Typ “Relativ” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

SNMP-ID: 2.25.10.7.14

Pfad Telnet: /Setup/RADIUS/Server/Rel.-Ablauf

Mögliche Werte:

- Zeitspanne in Sekunden. Maximal 10 Zeichen aus 0123456789

Default: 0

Besondere Werte: 0 schaltet die Überwachung der relativen Ablaufzeit aus.

2.25.10.7.15 Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID: 2.25.10.7.15

Pfad Telnet: /Setup/RADIUS/Server/Kommentar

Mögliche Werte:

- Max. 64 Zeichen

Default: leer

2.25.10.7.16 Service-Typ

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt. Der Service-Typ für Public-Spot ist z. B. 'Login', für 802.1x 'Umrahmt'.

SNMP-ID: 2.25.10.7.16

Pfad Telnet: /Setup/RADIUS/Server/Service-Typ

Mögliche Werte:

- Beliebig

- Umrahmt: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
- Login: Für Public-Spot-Anmeldungen.
- Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.

Default: Beliebig

Die Anzahl der Einträge mit dem Service-Typ "Beliebig" oder "Login" ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service- Typ "Beliebig" verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

2.25.10.7.17 Case-Sensitiv

Mit dieser Einstellung bestimmen Sie, ob der RADIUS-Server die Groß-/Kleinschreibung des Benutzernamens beachtet.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja

2.25.10.7.18 WPA-Passphrase

Vergeben Sie hier die WPA-Passphrase, mit der sich der Benutzer am WLAN anmelden kann.

Der RADIUS-Server speichert diese Passphrase in der Benutzertabelle. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS (LANCOM Enhanced Passphrase Security) nutzen.

Pfad Telnet:

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

Mögliche Werte:

8 bis 63 Zeichen aus dem ASCII-Zeichensatz

Default:

2.25.10.7.19 Max-gleichzeitige-Logins

Mit diesem Parameter legen Sie fest, wie viele Clients gleichzeitig über dieses Benutzerkonto angemeldet sein dürfen, wenn Sie Mehrfach-Logins aktiviert haben.

Pfad Telnet:

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

Mögliche Werte:

0 bis 4294967295

Default:

0

2.25.10.7.20 aktiv

Über diesen Parameter aktivieren bzw. deaktivieren Sie gezielt einzelne RADIUS-Benutzerkonten. Auf diese Weise lassen sich z. B. einzelne Benutzerkonten temporär abschalten, ohne dafür das komplette Konto zu löschen.

Pfad Telnet:

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

Mögliche Werte:

Nein

Ja

Default:

Ja

2.25.10.7.21 Shell-Priv.-Level

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

2.25.10.7.22 Volumen-Budget-MByte

Mit diesem Eintrag haben Sie die Möglichkeit, das Volumenbudget des RADIUS-Benutzers in Megabyte festzulegen.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

0

Besondere Werte:

0

Das Volumenbudget ist deaktiviert.

2.25.10.10 EAP

Dieses Menü enthält die Einstellungen für EAP.

SNMP-ID: 2.25.10.10

Pfad Telnet: /Setup/RADIUS/Server

2.25.10.10.1 Tunnel-Server

Realm als Verweis auf den Eintrag in der Tabelle der Weiterleitungs-Server, der für getunnelte TTLS bzw. PEAP-Anfragen verwendet werden soll.

SNMP-ID: 2.25.10.10.1

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- max. 24 Zeichen

Default: Leer

2.25.10.10.3 Reauth-Periode

Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem CHALLENGE antwortet (Verhandlung des Authentifizierungsverfahrens ist noch nicht abgeschlossen), kann der RADIUS-Server dem Authenticator mitteilen, wie lange (in Sekunden) er auf eine Antwort des Clients warten soll, bevor der CHALLENGE erneut zugestellt wird.

SNMP-ID: 2.25.10.10.3

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- max. 10 Ziffern

Default: 0

Besondere Werte: 0: Es wird kein Timeout an den Authenticator übermittelt.

Diese Funktion wird nicht von jedem Authenticator unterstützt.

2.25.10.10.4 Retransmit-Timeout

Wenn der interne RADIUS-Server auf die Anfrage eines Clients mit einem ACCEPT antwortet (Verhandlung des Authentifizierungsverfahrens ist erfolgreich abgeschlossen), kann der RADIUS-Server dem Authenticator mitteilen, nach welcher Zeit (in Sekunden) er eine erneute Authentifizierung des Clients auslösen soll.

SNMP-ID: 2.25.10.10.4

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- max. 10 Ziffern

Default: 0

Besondere Werte: 0: Es wird kein Timeout an den Authenticator übermittelt.

Diese Funktion wird nicht von jedem Authenticator unterstützt.

2.25.10.10.5 TTLS-Vorgabe-Tunnel-Methode

Bei der Verwendung von TTLS werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer (TLS-Tunnel) ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder anlehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem verfahren, welches er gerne nutzen

würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

SNMP-ID: 2.25.10.10.5

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- Keine
- MD5
- GTC
- MSCHAPv2

Default: MD5

2.25.10.10.6 PEAP-Vorgabe-Tunnel-Methode

Bei der Verwendung von PEAP werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer (TLS-Tunnel) ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder anlehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem verfahren, welches er gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

SNMP-ID: 2.25.10.10.6

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- Keine
- MD5
- GTC
- MSCHAPv2

Default: MSCHAPv2

2.25.10.10.7 Default-Methode

Gibt, welche Methode der RADIUS-Server dem Client außerhalb eines eventuellen TTLS/PEAP-Tunnels anbieten soll.

SNMP-ID: 2.25.10.10.7

Pfad Telnet: /Setup/RADIUS/Server/EAP

Mögliche Werte:

- Keine
- MD5
- GTC
- MSCHAPv2
- TLS
- TTLS
- PEAP

Default: MD5

2.25.10.10.8 Vorgabe-MTU

Definieren Sie hier die Maximum Transmission Unit, die das Gerät als Default für EAP-Verbindungen benutzt.

SNMP-ID: 2.25.10.10.8

Pfad Telnet: /Setup/RADIUS/Server/EAP/Vorgabe-MTU

Mögliche Werte:

- 100 bis 1496 Bytes

Default: 1036 Bytes

2.25.10.10.9 Erlaubte-Methoden

Hier wählen Sie den Server und das Verfahren zur EAP-Autentifizierung aus.

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **Erlaubte-Methoden**

2.25.10.10.9.1 Methode

Wählen Sie die Standard-EAP-Authentifizierungsmethode.

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **Erlaubte-Methoden**

Mögliche Werte:

MD5

GTC

MSCHAPv2

TLS

TTLS

PEAP

Default:

MD5

2.25.10.10.9.2 Allow EAP-TLS

Hier aktivieren Sie das EAP-TLS-Verfahren zur Authentifizierung.

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **Erlaubte-Methoden**

Mögliche Werte:

An

Aus

nur-intern

Default:

an

2.25.10.10.10 MSCHAPv2-Backend-Server

Mit dieser Einstellung definieren Sie optional einen externen RADIUS-Server, an den der interne RADIUS-Server bei EAP-MSCHAPv2 (wie es z. B. in einem PEAP-Tunnel gängig ist) die Prüfung des MS-CHAP v2 Response auslagert. Dadurch können Sie die Benutzerdatenbank auf einen externen RADIUS-Server auslagern, welcher EAP nicht untersützt.

Beachten Sie hierbei, dass der externe RADIUS-Server zumindest MSCHAPv2 unterstützen muss, da bei CHAP das eigentliche Passwort beim Server verbleibt.

Pfad Telnet:

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

Mögliche Werte:

Gültige(r) DNS-Name oder IP-Adresse des Servers. Wertebereich:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
```

Default:

Leer

2.25.10.10.18 EAP-SIM

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

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

Pfad Telnet:

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

2.25.10.10.18.1 Card-Keys

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

Pfad Telnet:

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

2.25.10.10.18.1.1 Benutzername

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

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

zusammen. Dadurch ergibt sich die folgende Syntax:

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.10.18.1.5 Rufende-Station-Id-Maske

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

Pfad Telnet:

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

Mögliche Werte:

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

Besondere Werte:

*****

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

Default-Wert:

leer

2.25.10.10.18.1.6 Gerufene-Station-Id-Maske

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

Pfad Telnet:

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

Mögliche Werte:

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

Besondere Werte:

*****

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

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

Default-Wert:

leer

2.25.10.10.18.1.7 Rand1

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

Pfad Telnet:

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

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

2.25.10.10.18.1.8 SRES1

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

Pfad Telnet:

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

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

2.25.10.10.18.1.9 Kc1

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

Pfad Telnet:

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

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

2.25.10.10.18.1.10 Rand2

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

Pfad Telnet:

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

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

2.25.10.10.18.1.11 SRES2

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

Pfad Telnet:

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

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

2.25.10.10.18.1.12 Kc2

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

Pfad Telnet:

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

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

2.25.10.10.18.1.13 Rand3

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

Pfad Telnet:

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

Mögliche Werte:

max. 32 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000000000000000000000000000

2.25.10.10.18.1.11 SRES3

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

Pfad Telnet:

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

Mögliche Werte:

max. 8 Zeichen aus `0123456789abcdef`

Default-Wert:

00000000

2.25.10.10.18.1.15 Kc3

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

Pfad Telnet:

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

Mögliche Werte:

max. 16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

2.25.10.10.19 EAP-TLS

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

Pfad Telnet:

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

2.25.10.10.19.3 Schluesselaustausch-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

2.25.10.10.19.4 Krypto-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.25.10.10.19.5 Hash-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

2.25.10.10.19.6 PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

Pfad Telnet:

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

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

2.25.10.10.19.10 Pruefe-Benutzernamen

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

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.25.10.11 Accounting-Port

Geben Sie hier den Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise wird der Port 1813 verwendet.

SNMP-ID: 2.25.10.11

Pfad Telnet: /Setup/RADIUS/Server

Mögliche Werte:

- max. 4 Ziffern

Default: 0

Besondere Werte: 0: schaltet die Verwendung dieser Funktion aus.

2.25.10.12 Accounting-Interim-Intervall

Geben Sie hier an, welchen Wert der RADIUS-Server bei erfolgreicher Authentifizierung als "Accounting-Interim-Interval" ausgeben soll. Sofern das anfragende Gerät dieses Attribut unterstützt, wird damit gesteuert, in welchem Intervall (in Sekunden) ein Update der Accounting-Daten an den Accounting-RADIUS-Server geschickt wird.

SNMP-ID: 2.25.10.12

Pfad Telnet: /Setup/RADIUS/Server

Mögliche Werte:

- 60 - 4294967295

Default: 0

Besondere Werte: 0: schaltet die Verwendung dieser Funktion aus.

2.25.10.13 RADSEC-Port

Geben Sie hier an, über welchen (TCP-)Port der Server über RADSEC verschlüsselte Accounting- oder Authentifizierungs-Anfragen annimmt. Üblicherweise wird Port 2083 verwendet.

SNMP-ID: 2.25.10.13

Pfad Telnet: /Setup/RADIUS/Server

Mögliche Werte:

- max. 5 Ziffern

Default: 0

Besondere Werte: 0: deaktiviert RADSEC im RADIUS-Server.

2.25.10.14 Auto-Loeschen-Benutzer-Tabelle

Wenn diese Funktion aktiviert ist, dann löscht der RADIUS-Server automatisch Accounts aus der Benutzertabelle, deren Ablaufdatum überschritten ist.

Pfad Telnet: /Setup/RADIUS/Server/Auto-Loeschen-Benutzer-Tabelle

Mögliche Werte:

- ja
- nein

Default: nein

2.25.10.15 Allow-Status-Requests

Legen Sie hier fest, ob Sie Status-Anfragen erlauben.

SNMP-ID: 2.25.10.15

Pfad Telnet: /Setup/RADIUS-Server

Mögliche Werte:

- Nein
- Ja

Default: Nein

2.25.10.16 IPv6-Clients

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

Pfad Telnet:

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

2.25.10.16.1 Adress-Praefix-Laenge

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.16.2 Adress-Praefix-Laenge

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.25.10.16.4 Protocols

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

Pfad Telnet:

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

Mögliche Werte:

RADIUS
RADSEC
Alle

Default-Wert:

RADIUS

2.25.10.16.5 Kommentar

Kommentar zu diesem Eintrag.

Pfad Telnet:

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

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.``

Default-Wert:

leer

2.25.10.17 Realm-Typen

Bestimmen Sie, wie der RADIUS-Server den Realm eines RADIUS-Requests ermittelt.

Pfad Telnet:

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

Mögliche Werte:

Mail-Domaene

`user@company.com`: `company.com` bildet den Realm und ist durch ein @-Zeichen vom Benutzernamen getrennt.

MS-Domaene

`company\user`: `company` bildet den Realm und ist durch einen Backslash („\") vom Benutzernamen getrennt. Diese Authentifizierung ist z. B. bei einem Windows-Login gebräuchlich.

MS-CompAuth

`host/user.company.com`: Beginnt der Benutzername mit dem String `host/` und enthält der restliche Name mindestens einen Punkt, dann betrachtet das Gerät alles hinter dem ersten Punkt als Realm (in diesem Fall also `company.com`).

Default-Wert:

Mail-Domaene

MS-Domaene

2.25.10.18 Auto-Loeschen-Accounting-Total

Mit diesem Eintrag haben Sie die Möglichkeit, alle Zugriffsinformationen auf den RADIUS-Server löschen zu lassen.

Pfad Telnet:

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

Mögliche Werte:

nein

Accouting-Informationen werden nicht automatisch gelöscht.

ja

Accounting Informationen werden automatisch gelöscht.

Default-Wert:

nein

2.25.20 RADSEC

Hier werden die Parameter für RADSEC-Verbindungen festgelegt.

Pfad Telnet:

Setup > **RADIUS**

2.25.20.1 Versionen

Diese Bitmaske definiert die erlaubten Protokoll-Versionen.

Pfad Telnet:

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

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

2.25.20.2 Schluesselaustausch-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

2.25.20.3 Krypto-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

2.25.20.4 Hash-Algorithmen

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

Pfad Telnet:

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

Mögliche Werte:

MD5
SHA1
SHA2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA2-256

SHA2-384

2.25.20.5 PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

Pfad Telnet:

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

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

2.25.20.6 Neuverhandlungen

Mit dieser Einstellung steuern Sie, ob der Client eine Neuverhandlung von SSL/TLS auslösen kann.

Pfad Telnet:

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

Mögliche Werte:

verboten
Das Gerät bricht die Verbindung zur Gegenstelle ab, falls diese eine Neuverhandlung anfordert.

erlaubt
Das Gerät lässt Neuverhandlungen mit der Gegenstelle zu.

ignoriert
Das Gerät ignoriert die Anforderung der Gegenseite zur Neuverhandlung.

Default-Wert:

erlaubt

2.26 NTP

Dieses Menü enthält die Einstellungen für NTP.

SNMP-ID: 2.26

Pfad Telnet: /Setup

2.26.2 Aktiv

Schalten Sie hier den Zeit-Server Ihres Gerätes für das lokale Netz ein. Andere Geräte im gleichen Netz können sich dann mit diesem Server über das Netzwerk-Zeit-Protokoll (NTP) synchronisieren.

SNMP-ID: 2.26.2

Pfad Telnet: /Setup/NTP

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.26.3 BC-Modus

Schalten Sie hier den Zeit-Server Ihres Gerätes in den Sende-Modus. In diesem Modus sendet er in regelmäßigen Abständen die jeweils aktuelle Zeit an alle erreichbaren Geräte oder Stationen des lokalen Netzes.

SNMP-ID: 2.26.3

Pfad Telnet: /Setup/NTP

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.26.4 BC-Intervall

Stellen Sie hier den zeitlichen Abstand ein, in welchem der Zeit-Server Ihres Gerätes jeweils die aktuelle Zeit an alle erreichbaren Geräte oder Stationen des lokalen Netzes senden soll.

SNMP-ID: 2.26.4

Pfad Telnet: /Setup/NTP

Mögliche Werte:

- max. 10 Zeichen

Default: 64

2.26.7 RQ-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.

SNMP-ID: 2.26.7

Pfad Telnet: /Setup/NTP

Mögliche Werte:

- max. 10 Zeichen

Default: 86400

Zum Erreichen der Zeit-Server wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

2.26.11 RQ-Addresse

Tragen Sie hier Zeit-Server ein, von denen sich das Gerät mit der aktuellen Uhrzeit versorgen kann.

SNMP-ID: 2.26.11

Pfad Telnet: /Setup/NTP

2.26.11.1 RQ-Addresse

Geben Sie hier die Zeit-Server (NTP) in der Reihenfolge an, in der Sie diese abfragen möchten. Die Server sollten über eines der vorhandenen Interfaces erreichbar sein. Vorsicht: Zum Erreichen der Zeit-Server wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

SNMP-ID: 2.26.11.1

Pfad Telnet: /Setup/NTP/RQ-Adresse

Mögliche Werte:

- max. 31 Zeichen

Default: leer

2.26.11.2 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

• Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.

• "INT" fiir die Adresse des ersten Intranets.

• "DMZ" fiir die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).

• LBO... LBF für die 16 Loopback-Adressen.

• Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

SNMP-ID: 2.26.11.2

Pfad Telnet: /Setup/NTP/RQ-Adresse

Mögliche 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

Default: leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wir diese Adresse genommen.

2.26.12 RQ-Versuche

Geben Sie hier an, wie oft eine Synchronisation mit dem Zeit-Server versucht werden soll. Bei Angabe einer Null wird so lange versucht, bis eine gültige Synchronisation durchgeführt wurde.

SNMP-ID: 2.26.12

Pfad Telnet: /Setup/NTP

Mögliche Werte:

- max. 10 Zeichen

Default: 4

2.27 Mail

Dieses Menü enthält die Einstellungen für E-Mail.

SNMP-ID: 2.27

Pfad Telnet: /Setup

2.27.1 SMTP-Server

Geben sie hier den Namen oder die IP-Adresse eines für Sie erreichbaren SMTP-Servers an. Diese Angabe ist erforderlich, wenn Ihr Gerät Sie über bestimmte auswählbare Ereignisse per E-Mail benachrichtigen soll.

SNMP-ID: 2.27.1

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 31 Zeichen

Default: leer

Zum Versenden von E-Mail-Benachrichtigungen wird bei Bedarf eine Verbindung aufgebaut. Bitte bedenken Sie, dass hierdurch zusätzliche Kosten entstehen können.

2.27.2 Serverport

Geben sie hier die Nummer des SMTP-Ports des o. a. Servers für unverschlüsselt übertragene E-Mails an. Standardmäßig hat dieser die Nummer 587.

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

max. 10 Zeichen

Default:

587

2.27.3 POP3-Server

Bei vielen P0P3-Servern, die eine SMTP-nach-POP-Anmeldung erfordern, unterscheidet sich der POP3-Servername lediglich im gleichnamigen Präfix vom SMTP-Servernamen. Sie brauchen dann hier nur den Namen Ihres SMTP-Servers anzugeben und das darin befindliche 'SMTP' durch 'POP' oder "POP3" zu ersetzen.

SNMP-ID: 2.27.3

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 31 Zeichen

Default: leer

2.27.4 POP3-Port

Geben sie hier die Nummer des POP3-Ports des o. a. Servers fiir unverschlüsselte Mail an. Standardmäßig hat dieser die Nummer 110.

SNMP-ID: 2.27.4

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 10 Zeichen

Default: 110

2.27.5 Benutzername

Geben Sie hier den Benutzername an, welcher benutzt wird um E-Mail-Benachrichtigungen an den o.a. SMTP-Server zu verschicken.

SNMP-ID: 2.27.5

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 63 Zeichen

Default: leer

2.27.6 Passwort

Geben Sie hier das Passwort an, welches benutzt wird, um E-Mail-Benachrichtigungen an den angegebenen SMTP-Server zu verschicken.

SNMP-ID: 2.27.6

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 31 Zeichen

Default: leer

2.27.7 E-Mail-Absender

Geben sie hier eine gültige Absender-E-Mail-Adresse an, welche Ihr Gerät als Absender-Adresse benutzt, um E-Mail-Benachrichtigungen zu verschicken. An diese Adresse werden von den beteiligten SMTP-Servern Zustellprobleme gemeldet, wenn die Empfänger- E-Mail- Adresse vorübergehend nicht erreichbar sein sollte. Außerdem wird die Absender-E-Mail-Adresse von einigen Servern auf Gültigkeit überprüft und eine Zustellung verweigert, falls sie fehlt, eine ungültige Domain enthält oder eine ungültige E-Mail-Adresse ist.

SNMP-ID: 2.27.7

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 63 Zeichen

Default: leer

2.27.8 Sendewiederholung-(Min)

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die Zeit ein, nach der erneut versucht wird, alle gepufferten Nachrichten zuzustellen - Außerdem wird eine Zustellung aller gepufferten Nachrichten bei jedem Eintreffen einer neuen Nachricht versucht.

SNMP-ID: 2.27.8

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 10 Zeichen

Default: 30

2.27.9 Vorhaltezeit-(Std)

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die maximale Haltezeit einer Nachricht ein. Nach Ablauf der angegebenen Zeit wird nicht mehr versucht eine bestimmte Nachricht zuzustellen.

SNMP-ID: 2.27.9

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 10 Zeichen

Default: 72

2.27.10 Pufferanzahl

Bei Verbindungsproblemen zum SMTP-Server werden die Nachrichten gepuffert und es wird wiederholt versucht, diese zuzustellen. Das gilt auch für Nachrichten, die aufgrund von fehlenden Einstellungen (z. B. SMTP-Daten hier oder Empfänger-E-Mail in den Mail erzeugenden Modulen) nicht zustellbar sind. Stellen Sie die maximale Anzahl gepufferter Nachrichten ein. Ist der eingestellte Puffer voll und es trifft eine weitere Nachricht ein, so wird die jeweils älteste Nachricht verworfen.

SNMP-ID: 2.27.10

Pfad Telnet: /Setup/Mail

Mögliche Werte:

- max. 10 Zeichen

Default: 100

2.27.11 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.27.11

Pfad Telnet: /Setup/Mail

Mögliche 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

Default: leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wird deren Name genommen.

2.27.12 SMTP-benutze-TLS

Bestimmen Sie hier, ob und wie das Gerät die Verbindung verschlüsseln soll. Die möglichen Werte haben folgende Bedeutung:

- **Nein**: Keine Verschlüsselung. Das Gerät beachtet eine ggf. vom Server gesendete STARTTLS-Antwort nicht.
- **Ja**: Das Gerät verwendet SMTPS, verschlüsselt also ab Verbindungsaufbau.
- **Bevorzugt**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server STARTTLS an, verschlüsselt das Gerät. Diese Einstellung ist der Defaultwert.
- **Erforderlich**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server kein STARTTLS an, überträgt das Gerät keine Daten.

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

Nein

Ja

Bevorzugt

Erforderlich

Default:

Bevorzugt

2.27.13 SMTP-Authentifizierung

Bestimmen Sie hier, ob und wie sich das Gerät beim SMTP-Server authentifiziert. Das Verhalten das Gerätes ist abhängig von der Server-Einstellung: Wenn der Server keine Authentifizierung erfordert, erfolgt in jedem Fall eine Anmeldung. Andernfalls verhält sich das Gerät den nachfolgend beschriebenen Einstellungen entsprechend.

Pfad Telnet:

Setup > **Mail**

Mögliche Werte:

Keine

Grundsätzlich keine Authentifizierung.

Klartext-bevorzugt

Die Authentifizierung erfolgt bevorzugt im Klartext (PLAIN, LOGIN), wenn der Server eine Authentifizierung verlangt. Akzeptiert dieser keine Klartext-Authentifizierung, verwendet das Gerät die sichere Authentifizierung.

Verschluesselt

Die Authentifizierung erfolgt ohne Übertragung des Passwortes im Klartext (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Eine Klartext-Authentifizierung findet nicht statt.

Bevorzugt-Verschluesselt

Die Authentifizierung erfolgt bevorzugt verschlüsselt (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Akzeptiert dieser keine sichere Authentifizierung, verwendet das Gerät die Klartext-Authentifizierung.

Default-Wert:

Bevorzugt-Verschluesselt

2.30 IEEE802.1x

Dieses Menü enthält die Einstellungen des IEEE802.1x-Protokolls.

SNMP-ID: 2.30

Pfad Telnet: /Setup

2.30.3 Radius-Server

Sie können die Authentifizierung aller Wireless-LAN-Netze in einem zentralen RADIUS-Server verwalten (Name ist DEFAULT). Sie können darüber hinaus für bestimmte Wireless-LAN-Netze eigene RADIUS-Server definieren (anstelle der Passphrase für das logische Wireless-LAN-Netz anzugeben). Für jeden RADIUS-Server kann hier außerdem ein Backup-Server spezifiziert werden.

SNMP-ID: 2.30.3

Pfad Telnet: /Setup/IEEE802.1x

2.30.3.1 Name

Name des Servers.

SNMP-ID: 2.30.3.1

Pfad Telnet: /Setup/IEEE802.1x /RADIUS-Server

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.30.3.3 Port

Port des RADIUS-Servers.

SNMP-ID: 2.30.3.3

Pfad Telnet: /Setup/IEEE802.1x /RADIUS-Server

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.30.3.4 Schlüssel

Schlüssel des RADIUS-Servers.

SNMP-ID: 2.30.3.4

Pfad Telnet: /Setup/IEEE802.1x /RADIUS-Server

Mögliche Werte:

- max. 32 Zeichen

Default: leer

2.30.3.5 Backup

Es besteht die Möglichkeit für jeden RADIUS-Server den Namen eines Backup-Servers anzugeben, welcher nur kontaktiert wird, wenn der hiesige Server nicht mehr erreicht werden kann. Den Namen des Backup-Servers können Sie aus derselben Tabelle wählen.

SNMP-ID: 2.30.3.5

Pfad Telnet: /Setup/IEEE802.1x /RADIUS-Server

Mögliche Werte:

- max. 24 Zeichen

Default: leer

2.30.3.6 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch fiir die Zieladresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.30.3.6

Pfad Telnet: /Setup/IEEE802.1x /RADIUS-Server

Mögliche Werte:

- Als Adresse werden verschiedene Eingabeformen akzeptiert:
- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen.

- LBO... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Default: leer

2.30.3.7 Protokoll

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

SNMP-ID: 2.30.3.7

Pfad Telnet: /Setup/IEEE802.1x/RADIUS-Server/Protokoll

Mögliche Werte:

- RADSEC
- RADIUS

Default: RADIUS

2.30.3.8 Host-Name

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

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

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

Besondere Werte:

DEFAULT

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

2.30.3.9 Attribut-Werte

Mit diesem Eintrag konfigurieren Sie die RADIUS-Attribute des RADIUS-Servers.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>,<Attribut_2>=<Wert_2>`.

Als Werte sind auch Variablen (z. B. `%n` für den Gerätenamen) erlaubt. Beispiel: `NAS-Identifier=%n`.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.30.4 Ports

Geben Sie für jedes lokale Netzwerk-Interface gesondert die Anmeldungseinstellungen an.

SNMP-ID: 2.30.4

Pfad Telnet: /Setup/IEEE802.1x

2.30.4.2 Port

Schnittstelle des Gerätes, auf die sich dieser Eintrag bezieht.

SNMP-ID: 2.30.4.2

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- Alle im Gerät verfügbaren Schnittstellen.

Default: leer

2.30.4.4 Re-Auth-Max

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.4

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 3

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.5 Max-Req

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.5

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 3

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.6 Tx-Period

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.6

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.7 Supp-Timeout

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.7

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.8 Server-Timeout

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.8

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 30

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.9 Quiet-Period

Bei diesem Parameter handelt es sich um einen Timer der Authentication State Machine für IEEE 802.1x.

SNMP-ID: 2.30.4.9

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 60

Die Änderungen dieser Parameter erfordert eine tiefgehende Kenntnis des Standards IEEE 802.1x. Nehmen Sie hier nur dann Änderungen vor, wenn die Systemkonfiguration das unbedingt erfordert.

2.30.4.10 Re-Authentication

Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet. Ein typischer Standardwert fiir das Neuanmelde-Intervall ist 3.600 Sekunden.

SNMP-ID: 2.30.4.10

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.30.4.11 Re-Auth-Interval

Ein typischer Standardwert für das Neuanmelde-Intervall ist 3.600 Sekunden.

SNMP-ID: 2.30.4.11

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 3600

2.30.4.12 Key-Transmission

Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

SNMP-ID: 2.30.4.12

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.30.4.13 Key-Tx-Interval

Ein typischer Standardwert für das Schlüssel-Intervall ist 900 Sekunden.

SNMP-ID: 2.30.4.13

Pfad Telnet: /Setup/IEEE802.1x /Ports

Mögliche Werte:

- max. 10 Zeichen

Default: 900

2.31 PPPoE-Server

Dieses Menü enthält die Einstellungen für den PPPoE-Server.

Pfad Telnet:

Setup

2.31.1 Aktiv

Mit diesem Schalter wird der PPPoE-Server ein- bzw. ausgeschaltet.

SNMP-ID: 2.31.1

Pfad Telnet: /Setup/PPPoE-Server

Mögliche Werte:

- Ja
- Nein

2.31.2 Namenliste

Definieren Sie in der Gegenstellen-Liste diejenigen Clients, welchen vom PPPoE-Server Zugang erlaubt und in der PPP-Liste oder der Firewall weitere Eigenschaften und Rechte zugeteilt werden sollen.

SNMP-ID: 2.31.2

Pfad Telnet: /Setup/PPPoE-Server

2.31.2.1 Gegenstelle

Definieren Sie hier einen Gegenstellen-Namen für jeden Client. Der Gegenstellen-Name muss beim Client als PPP-Benutzername verwendet werden.

SNMP-ID: 2.31.2.1

Pfad Telnet: /Setup/PPPoE-Server/Namenliste

Mögliche Werte:

- Auswahl aus der Liste der definierten Gegenstellen

Default: Leer

2.31.2.2 SH-Zeit

Definieren Sie hier die Haltezeit für die PPPoE-Verbindung an.

SNMP-ID: 2.31.2.2

Pfad Telnet: /Setup/PPPoE-Server/Namenliste

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.31.2.3 MAC-Adresse

Ist eine MAC-Adresse eingetragen, so wird die PPP-Verhandlung abgebrochen, wenn sich der Client von einer anderen MAC-Adresse anmeldet.

SNMP-ID: 2.31.2.3

Pfad Telnet: /Setup/PPPoE-Server/Namenliste

Mögliche Werte:

- max. 12 Zeichen

Default: 000000000000

2.31.3 Service

Unter 'Service' wird der Name des angebotenen Dienstes eingetragen. Das ermöglicht einem PPPoEClient die Auswahl eines bestimmten PPPoE-Servers, der dazu beim Client eingetragen wird.

SNMP-ID: 2.31.3

Pfad Telnet: /Setup/PPPoE-Server

Mögliche Werte:

- max. 32 Zeichen

Default: Leer

2.31.4 Session-Limit

Das 'Session-Limit' gibt an, wie oft ein Client mit der gleichen MAC-Adresse gleichzeitig angemeldet sein kann. Ist das Limit erreicht, dann antwortet der Server nicht mehr auf empfangene Anfragen des Clients. Defaultwert ist '1', max.wert '99'. Ein Session-Limit von '0' steht für eine unbegrenzte Session-Anzahl.

SNMP-ID: 2.31.4

Pfad Telnet: /Setup/PPPoE-Server

Mögliche Werte:

- 0 bis 99

Default: 1

Besondere Werte: 0: schaltet die Begrenzung der Sessions aus.

2.31.5 Ports

Hier können Sie für einzelne Ports festlegen, ob der PPPoE Server Aktiviert ist.

SNMP-ID: 2.31.5

Pfad Telnet: /Setup/PPPoE-Server

2.31.5.2 Port

Port, für den der PPPoE-Server aktiviert oder deaktiviert werden soll.

SNMP-ID: 2.31.5.2

Pfad Telnet: /Setup/PPPoE-Server/Ports

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

2.31.5.3 PPPoE-Aktiv

Aktiviert oder deaktiviert den PPPoE-Server für den gewählten Port.

SNMP-ID: 2.31.5.3

Pfad Telnet: /Setup/PPPoE-Server/Ports

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.31.6 AC-Name

Über dieses Eingabefeld haben Sie optional die Möglichkeit, dem PPPoE-Server einen eigenen Namen unabhängig vom Gerätenamen zuzuweisen (AC-Name = Access Concentrator Name).

Pfad Telnet:

Setup > **PPPoE-Server**

Mögliche Werte:

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

Besondere Werte:

leer

Sofern Sie dieses Feld leer lassen, verwendet der PPPoE-Server den Gerätenamen als Server-Namen.

Default-Wert:

leer

2.32 VLAN

Die Konfiguration im VLAN-Bereich der Geräte hat zwei wichtige Aufgaben:

- Virtuelle LANs definieren und ihnen dabei einen Namen, eine VLAN-ID und die zugehörigen Interfaces zuordnen
- Für die Interfaces definieren, wie mit Datenpaketen mit bzw. ohne VLAN-Tags verfahren werden soll

SNMP-ID: 2.32

Pfad Telnet: /Setup

2.32.1 Netzwerke

Die Netzwerkliste beinhaltet den Namen des VLANs, die VLAN-ID und die Ports. Zur Bearbeitung können Sie auf einen Eintrag klicken.

SNMP-ID: 2.32.1

Pfad Telnet: /Setup/VLAN

2.32.1.1 Name

Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.

SNMP-ID: 2.32.1.1

Pfad Telnet: /Setup/VLAN/Netzwerke

2.32.1.2 VLAN-ID

Diese Nummer kennzeichnet das VLAN eindeutig.

SNMP-ID: 2.32.1.2

Pfad Telnet: /Setup/VLAN/Netzwerke

Mögliche Werte:

- 0 bis 4096

Default: 0

2.32.1.4 Ports

Tragen Sie hier Interfaces des Geräts ein, die zu dem VLAN gehören. Für ein Gerät mit einem LAN-Interface und einem WLAN-Port können z. B. die Ports “LAN-1” und “WLAN-1” eingetragen werden. Bei Portbereichen werden die einzelnen Ports durch eine Tilde getrennt: “P2P-1~P2P-4”.

SNMP-ID: 2.32.1.4

Pfad Telnet: /Setup/VLAN/Netzwerke

Mögliche Werte:

- max. 251 Zeichen

Default: leer

Die erste SSID des ersten WLAN-Moduls heißt WLAN-1, die weiteren SSID WLAN-1-2 bis WLAN-1-8. Falls das Gerät über zwei WLAN-Module verfügt, heißen die SSIDs hier WLAN-2, WLAN-2-2 bis WLAN-2-8.

2.32.1.5 LLDP-Tx-TLV-PPID

Über diese Einstellung legen Sie fest, an welchen Ports, die Mitglieder dieses VLANs sind, das Gerät die Mitgliedschaft per LLDP propagiert.

Pfad Telnet:

Setup > **VLAN** > **Netzwerke**

Mögliche Werte:

Kommaseparierte Liste von Interface-Namen (analog zu den Namen in der Spalte **Ports**), max. 251 Zeichen

Default:

2.32.1.6 LLDP-Tx-TLV-Name

Über diese Einstellung legen Sie fest, an welchen Ports, die Mitglieder dieses VLANs sind, das Gerät den Namen des VLANs per LLDP propagiert.

Pfad Telnet:

Setup > **VLAN** > **Netzwerke**

Mögliche Werte:

Kommaseparierte Liste von Interface-Namen (analog zu den Namen in der Spalte **Ports**), max. 251 Zeichen

Default:

2.32.2 Port-Tabelle

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.

SNMP-ID: 2.32.2

Pfad Telnet: /Setup/VLAN

2.32.2.1 Port

Der Name des Ports; nicht editierbar.

SNMP-ID: 2.32.2.1

Pfad Telnet: /Setup/VLAN/Port-Tabelle

2.32.2.4 Alle-VLANs-zulassen

Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port nicht Mitglied dieses VLANs ist.

SNMP-ID: 2.32.2.4

Pfad Telnet: /Setup/VLAN/Port-Tabelle

Mögliche Werte:

- ja
- nein

Default: ja

2.32.2.5 Port-VLAN-Id

Diese Port-ID hat zwei Funktionen:

- Ungetaggte Pakete, die auf diesem Port im Modus 'Gemischt' oder 'ankommend gemischt' empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus 'Niemals'.
- Im Modus '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.

SNMP-ID: 2.32.2.5

Pfad Telnet: /Setup/VLAN/Port-Tabelle

Mögliche Werte:

- max. 4 Zeichen

Default: 1

2.32.2.6 Tagging-Modus

Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

SNMP-ID: 2.32.2.6

Pfad Telnet: /Setup/VLAN/Port-Tabelle

Mögliche Werte:

- **Nie**: Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werde 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.
- **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.
- **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 VLANTag, außer sie gehören dem für diesen Port definierten VLAN an.
- **Ingress-Gemischt:** Ankommende Pakete können ein VLAN-Tag haben oder nicht, ausgehende Pakete bekommen nie ein VLAN-Tag.

Default: Ingress-Gemischt

Tx-LLDP-TLV-Port-VLAN

Aktiviert oder deaktiviert den Port als LLDP-TLV-Port in diesem VLAN.

Path WEBconfig: LCOS-Menübaum/Setup/VLAN/Port-Tabelle/Tx-LLDP-TLV-Port-VLAN

Possible values:

- Ja
- Nein

Default: Ja

2.32.4 Aktiv

Schalten Sie das VLAN-Modul nur ein, wenn Sie mit den Auswirkungen der VLAN-Nutzung vertraut sind.

SNMP-ID: 2.32.4

Pfad Telnet: /Setup/VLAN

Mögliche Werte:

- ja
- nein

Default: nein

Mit fehlerhaften VLAN-Einstellungen können Sie den Konfigurationszugang zum Gerät verhindern.

2.32.5 Tag-Wert

Beim Übertragen von VLAN-getaggten Netzen über Netze der Provider, die ihrerseits VLAN verwenden, setzen die Provider teilweise spezielle VLAN-Tagging-IDs ein. Um die VLAN-Übertragung darauf einzustellen, kann der Ethernet2-Typ des VLAN-Tags als 'Tag-Value' als 16 Bit-Hexadezimalwert eingestellt werden. Default ist '8100' (VLAN-Tagging nach 802.1p/q), andere gängige Werte für VLAN-Tagging wären z. B. '9100' oder '9901'.

SNMP-ID: 2.32.5

Pfad Telnet: /Setup/VLAN

Mögliche Werte:

- max. 4 Zeichen

Default: 8100

2.33 Voice-Call-Manager

In diesem Menü finden sie die Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33

Pfad Telnet: /Setup

2.33.1 Operating

Schaltet den Voice-Call-Manager ein/aus.

Pfad Telnet:/Setup/Voice-Call-Manager

Mögliche Werte Telnet:

- ja
- nein

Default: nein

2.33.2 General

Dieses Menü enthält die allgemeinen Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.2

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.2.1 Domain

Name der Domain, in der die angeschlossenen Telefone und der VoIP Router betrieben werden.

Endgeräte, die mit der gleichen Domain arbeiten, melden sich als lokale Teilnehmer am VoIP Router an und nutzen so den SIP-Proxy.

Endgeräte, die mit der anderen Domain einer aktiven SIP-PBX-Leitung arbeiten, melden sich als Teilnehmer an einer übergeordneten TK-Anlage an.

SNMP-ID: 2.33.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: intern

2.33.2.2 Overlap-Timeout

Für diese Zeit in Sekunden wird bei der Wahl von einem ISDN-Telefon gewartet, bis die Rufnummer als vollständig angesehen wird und an den Call-Router übergeben wird.

SNMP-ID: 2.33.2.2

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- 0 bis 99

Default: 6

Besondere Werte: 0: Bei einer Wählverzögerung von '0' muss die Eingabe der Rufnummer mit einem '#' abgeschlossen werden. Die Eingabe des Zeichens '#' nach der Rufnummer verkürzt die Wählverzögeung manuell.

2.33.2.3 Local-authentication

Normalerweise akzeptiert der SIP-Proxy Anmeldung von allen SIP-Benutzern, die sich mit einer gültigen Domain anmelden. Wird die lokale Authentifizierung erzwungen, können sich nur solche Teilnehmer beim SIP-Proxy anmelden, die in einer der Benutzertabellen mit den entsprechenden Zugangsdaten hinterlegt sind.

SNMP-ID: 2.33.2.3

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- nein
- ja

Default: nein/Aus

Die automatische Anmeldung ohne Eintrag eines Passworts ist auf die SIP-Benutzer im LAN beschränkt. SIP-Benutzer aus dem WAN und ISDN-Benutzer müssen immer über einen entsprechenden Benutzer-Eintrag mit Passwort authentifiziert werden.

2.33.2.4 Echo_Canceler

Aktiviert die Echounterdrückung des fernen Echos. Bei einem zu starkem Echo hört der Teilnehmer sich selber mit kurzer Verzögerung wieder. Mit der Aktivierung dieser Option wird das Echo am SIP-Gateway reduziert.

SNMP-ID: 2.33.2.4

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- Ein

- Aus

Default: Ein

2.33.2.5 Outgoing-packet-reduction

Für alle SIP-Gespräche wird abhängig vom verwendeten Audio-Codec eine ausreichende Bandbreite über die Firewall reserviert (soweit die verfügbare Bandbreite ausreicht). Stellen Sie hier zur Steuerung der Firewall die Behandlung der restlichen Datenpakete ein, die nicht zu den SIP-Datenströmen gehören.

SNMP-ID: 2.33.2.5

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- PMTU: Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).
- Fragmentation: Der VoIP Router reduziert selbst die Datenpakete durch Fragmentierung auf die gewünschte Länge.
- NONE: Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.
- PMTU + Fragmentation

Default: NONE/Reduktion der PMTU

2.33.2.6 Incoming-packet-reduction

Analog zu den abgehenden Datenpaketen wird hier die Behandlung der Nicht-VoIP-Datenpakete bei Bandbreitenreservierung für SIP-Daten eingestellt.

SNMP-ID: 2.33.2.6

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- Reduktion der PMTU: Die Teilnehmer der Datenverbindung werden informiert, dass sie nur Datenpakete bis zu einer bestimmen Länge versenden sollen (Path Maximum Transmission Unit, PMTU).
- Keine Veränderung: Die Länge der Datenpakete wird durch den VoIP-Betrieb nicht verändert.

Default: keine Veränderung

2.33.2.7 Reduced-packet-size

Dieser Parameter gibt die Paketgröße in Byte an, die für die PMTU-Anpassung bzw. die Fragmentierung bei Bevorzugung der SIP-Daten verwendet werden soll.

SNMP-ID: 2.33.2.7

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- 0 bis 9999

Default: 576

2.33.2.9 Country

Das Land definiert die im Gerät erzeugten Inband-Töne.

SNMP-ID: 2.33.2.9

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- Unbekannt

- Österreich
- Belgien
- Schweiz
- Deutschland
- Frankreich
- Italien
- Niederlande
- Spanien
- Groß-Britannien

Default: Unbekannt

2.33.2.11 ClnPartyNumType

Hiermit wird der Typ der abgehenden Rufnummer (CallingPartyNumber) auf einem ISDN-Interface für rausgehende Rufe eingestellt. Dies ist für TK-Anlagen und manche Vermittlungsstellen im Ausland nötig, da diese einem bestimmten Typ benötigen.

SNMP-ID: 2.33.2.11

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

- subscriber
- unknown
- national

Default: subscriber(0)

2.33.2.12 Register-Time

Dieser Wert gibt die Re-Registrierungszeit in Sekunden an, die einem SIP-Benutzer auf der lokalen Seite signalisiert wird.

Mit dieser Funktion erreicht der Registrar eine Registrierung durch den VoIP-Client in kürzeren Zeitabständen, um so z. B. das Ausschalten des VoIP-Clients schneller zu erkennen.

SNMP-ID: 2.33.2.12

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte:

- 60 bis 3600

Default: 120

2.33.2.13 Convert-Canonicals

Aktivieren Sie hier die Konvertierung der kanonischen VoIP-Namen.

SNMP-ID: 2.33.2.13

Pfad Telnet: /Setup/Voice-Call-Manager/General/Convert-Canonicals

Mögliche Werte Telnet:

- ja
- nein

Default: ja

2.33.2.14 Symmetrisch-RTP

Dieser Parameter schaltet die strenge Prüfung des RTP-Absenders ab. In der Regel findet eine bidirektionale RTP-Kommunikationen zwischen zwei Socket-Adressen (IP:Port) statt; d.h. die Media-Datenquellen (ausgehend) sind gleichzeitig auch Media-Datensenken (eingehend). Der Datenfluss ist symmetrisch.

Es gibt allerdings auch Media-Server, deren Implementierungen hiervon abweichen und die RTP-Quelle und das RTP-Ziel nicht die gleiche Socket-Adresse aufweisen. Deaktivieren Sie in solchen Fällen die Option "Symmetrisch-RTP".

Pfad Telnet: /Setup/Voice-Call-Manager/General/Symmetrisch-RTP

Mögliche Werte:

- ja
- nein

Default: ja

2.33.2.15 SIP-DSCP

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die SIP-Pakete (Anruf-Signalisierung) markiert werden.

SNMP-ID: 2.33.2.15

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

BE/CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default: CS-1

Die Verwendung von CS-1 ist heute überholt und zur Erhaltung der Abwärts-Kompatibilität als Default gesetzt. Typische Werte für aktuellen VoIP-Installationen sind CS-3, AF-31 oder AF-41. Wegen großer Verbreitung im Markt empfehlen wir den Einsatz von CS-3.

2.33.2.16 RTP-DSCP

Legen Sie hier fest, mit welchen DiffServ-CodePoints (DSCP) die RTP-Pakete (Voice-Datenstrom) markiert werden.

SNMP-ID: 2.33.2.16

Pfad Telnet: /Setup/Voice-Call-Manager/General

Mögliche Werte Telnet:

BE, CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

BE/CS-0, CS-1, CS-2, CS-3, CS-4, CS-5, CS-6, CS-7, AF-11, AF-12, AF-13, AF-21, AF-22, AF-23, AF-31, AF-32, AF-33, AF-41, AF-42, AF-43, EF

Default: EF

Bei der Einstellung DSCP BE bzw. CS-0 werden die Pakete ohne Markierung versendet. Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

2.33.2.17 Sperr-Minuten

Bestimmen Sie, für wieviele Minuten ein SIP-Benutzer gesperrt wird, nachdem die Anmeldung aufgrund falscher Login-Daten fehlgeschlagen ist.

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Allgemein** > **Sperr-Minuten**

Mögliche Werte:

0 bis 255 Minuten

Besondere Werte:

0: Sperre deaktiviert

Default:

5 Minuten

2.33.2.18 Login-Fehler

Dieser Wert gibt an, nach welcher Anzahl von Fehlversuchen ein SIP-Benutzer für eine bestimmte Zeit gesperrt wird.

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Allgemein** > **Login-Fehler**

Mögliche Werte:

0 bis 255

Besondere Werte:

0: Die erste Falschanmeldung löst die Sperre aus.

Default:

5

2.33.3 User

Dieses Menü enthält die Benutzer-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.3

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.3.1 SIP-User

Dieses Menü enthält die SIP-Benutzer-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.3.1

Pfad Telnet: /Setup/Voice-Call-Manager/User

2.33.3.1.1 Users

Je nach Modell können unterschiedlich viele SIP-Benutzer angelegt werden. Mehr als die erlaubte Anzahl Benutzer können nicht angelegt werden, ebenso werden gleiche Namen oder gleiche Rufnummern nicht zugelassen.

SNMP-ID: 2.33.3.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User

Die vom SIP-Teilnehmer verwendete Domäne wird üblicherweise im Endgerät selbst eingestellt.

2.33.3.1.1.1 Number/Name

Telefonnummer des SIP-Telefons oder Name des Benutzers (SIP-URI).

SNMP-ID: 2.33.3.1.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/User

Mögliche Werte Telnet:

- max. 20 Zeichen

Default: Leer

2.33.3.1.1.2 Auth-Name

Name zur Authentifizierung am SIP-Proxy, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Der Name wird benötigt, wenn eine Anmeldung erforderlich ist (z. B. bei übergeordneter Anmeldung an einer SIP-TK-Anlage oder Setzen von "Lokale Authentifizierung erzwingen" für die SIP-Benutzer).

SNMP-ID: 2.33.3.1.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

Besondere Werte: Leer: Wenn hier nichts eingetragen ist, wird die Authentifizierung über den SIP-Namen (interne Rufnummer) versucht.

2.33.3.1.1.3 Secret

Passwort zum Anmelden des SIP-Benutzers, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich Benutzer lokal am SIP-Proxy ohne Authentifizierung anmelden ("Lokale Authentifizierung erzwingen" für SIP-Benutzer ist deaktiviert) und ggf. an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

SNMP-ID: 2.33.3.1.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- max. 32 Zeichen

Default: Leer

2.33.3.1.1.4 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.3.1.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- ja
- nein

Default: Ein

2.33.3.1.1.5 Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID: 2.33.3.1.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

2.33.3.1.1.6 Device-Type

Typ des angeschlossenen Geräts.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

SNMP-ID: 2.33.3.1.1.6

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- Phone
- Fax
- Auto

Default: Phone/Telefon

2.33.3.1.1.7 CLIR

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

SNMP-ID: 2.33.3.1.1.7

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User/Users

Mögliche Werte Telnet:

- ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

Default: nein/Aus

2.33.3.1.1.8 Zugriff von WAN

Bestimmen Sie hier, ob und wie sich SIP-Clients über eine WAN-Verbindung mit dem entsprechenden Benutzerdaten anmelden können.

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **SIP-User** > **User**

Mögliche Werte:

ja

nein

VPN

Default:

Nein

2.33.3.1.2 Intern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, internen Anruf der vorhandenen Calling Party ID vorangestellt, wenn wenn der Anruf an einen SIP-Benutzer gerichtet ist.

SNMP-ID: 2.33.3.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User

Mögliche Werte Telnet:

- max. 15 Ziffern oder *

Default: *

Ein Ruf gilt dann als extern, wenn er von einer „Leitung" kommt. Wenn diese Leitung eine SIP-PBX Leitung ist, dann ist der Ruf nur dann extern, wenn die kommende Calling Party ID eine führende „0" hat. Alle anderen Anruf gelten als intern.

2.33.3.1.3 Extern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, externen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen SIP-Benutzer gerichtet ist

SNMP-ID: 2.33.3.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/SIP-User

Mögliche Werte Telnet:

- max. 15 Ziffern oder *

Default: Leer

2.33.3.2 ISDN-User

Dieses Menü enthält die ISDN-Benutzer-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.3.2

Pfad Telnet: /Setup/Voice-Call-Manager/User

2.33.3.2.1 Interfaces

Hier wählen Sie die Schnittstelle aus, an der ISDN-Benutzer angeschlossen werden.

SNMP-ID: 2.33.3.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User

2.33.3.2.1.1 Name

Name der Schnittstelle

SNMP-ID: 2.33.3.2.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

Mögliche Werte Telnet:

- ISDN

Default: ISDN

2.33.3.2.1.2 Ifc

Schnittstelle, an welche die ISDN-Teilnehmer angeschlossen sind.

SNMP-ID: 2.33.3.2.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

Mögliche Werte Telnet:

- Auswahl aus verfügbaren ISDN-Schnittstellen, z. B. S0-1 und S0-2

Default: Je nach Modell verschieden.

2.33.3.2.1.3 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.3.2.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

Mögliche Werte Telnet:

- ja
- nein

Default: ja/Ein

2.33.3.2.1.4 Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID: 2.33.3.2.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Interfaces

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

2.33.3.2.1.5 Ortsvorwahl

Geben Sie die Ortsvorwahl für die Schnittstelle des ISDN-Benutzers an.

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **ISDN-User** > **Interfaces**

2.33.3.2.2 Users

Hier können Sie alle lokalen ISDN-Benutzer (Endgeräte) definieren. Darüber hinaus können Sie Authentizifierungs-Daten zur SIP-Anmeldung angeben.

SNMP-ID: 2.33.3.2.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User

2.33.3.2.2.1 Number/Name

Interne Rufnummer des ISDN-Telefons oder Name des Benutzers (SIP-URI).

SNMP-ID: 2.33.3.2.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/User

Mögliche Werte Telnet:

- max. 20 Zeichen

Default: Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag erfaßt werden. Mit der Rufnummer '#' und der DDI '#' werden z. B. die Durchwahlnummern ohne Veränderung in interne Rufnummern umgesetzt. Mit der Rufnummer '3#' und der DDI '#' wird z. B. ein ankommender Ruf für die Durchwahl '55' an die interne Rufnummer '355' weitergeleitet, bei ausgehenden Rufen von der internen Rufnummer '377' wird die '77' als Durchwahl verwendet.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

2.33.3.2.2.2 Ifc

ISDN-Interface, das für den Verbindungsaufbau verwendet werden soll.

SNMP-ID: 2.33.3.2.2.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- Kein, ein oder mehrere verfügbare S0-Busse.

Default: Abhängig vom Gerätetyp.

2.33.3.2.2.3 MSN/DDI

Interne MSN, die für diesen Benutzer auf dem internen ISDN-Bus verwendet wird.

MSN: Nummer des Telefonanschlusses, wenn es sich um einen Mehrgeräteanschluss handelt.

DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

SNMP-ID: 2.33.3.2.2.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- max. 19 Ziffern und #-Zeichen

Default: Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

2.33.3.2.2.4 Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

SNMP-ID: 2.33.3.2.2.4

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- max. 32 alphanumerische Zeichen

Default: Leer

2.33.3.2.2.5 Auth-Name

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

SNMP-ID: 2.33.3.2.2.5

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

Nur erforderlich bei Anmeldung des Benutzers an einer übergeordneten SIP-TK-Anlage.

2.33.3.2.2.6 Secret

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des ISDN-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

SNMP-ID: 2.33.3.2.2.6

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- max. 32 Zeichen

Default: Leer

2.33.3.2.2.7 Domain

Domäne einer übergeordneten SIP-TK-Anlage, wenn der ISDN-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

SNMP-ID: 2.33.3.2.2.7

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

Nur erforderlich bei Anmeldung des Benutzers an einer übergeordneten SIP-TK-Anlage.

2.33.3.2.2.8 DialCompl

Mit der Blockwahlerkennung kann die gewählt Nummer automatisch als vollständig markiert werden (z. B. bei Zielwahl oder Wahlwiederholung), der Ruf wird damit schneller aufgebaut. Eine Nachwahl ist nicht möglich.

SNMP-ID: 2.33.3.2.2.8

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- Auto: Blockwahl wird automatisch erkannt (z. B. bei Zielwahl oder Wahlwiederholung), und der Ruf damit schneller aufgebaut. Eine Nachwahl ist nicht möglich.
- Manual: Keine Blockwahl, mit Eingabe des "#" kann die Nummer als vollständig gekennzeichnet werden und somit der Rufaufbau initiiert werden.

Default: Auto/Automatisch

Mit Eingabe des "#" kann bei ausgeschalteter Blockwahlerkennung die Nummer manuell als vollständig gekennzeichnet und somit der Rufaufbau initiiert werden.

2.33.3.2.2.9 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.3.2.2.9

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- nein
- ja

Default: ja/Ein

2.33.3.2.2.10 Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID: 2.33.3.2.2.10

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/User

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: Leer

2.33.3.2.2.11 Device-Type

Typ des angeschlossenen Gerätes.

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

SNMP-ID: 2.33.3.2.2.11

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- Phone
- Fax
- Auto

Default: Phone/Telefon

2.33.3.2.2.12 CLIR

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

SNMP-ID: 2.33.3.2.2.12

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User/Users

Mögliche Werte Telnet:

- ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

Default: Nein/Aus

2.33.3.2.3 Intern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, internen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

SNMP-ID: 2.33.3.2.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User

Mögliche Werte Telnet:

- max. 15 Ziffern oder *.

Default: *

2.33.3.2.4 Extern-Cln-Prefix

Dieses Präfix wird bei einem eingehenden, externen Anruf der vorhandenen Calling Party ID vorangestellt, wenn der Anruf an einen ISDN-Benutzer gerichtet ist. Sofern ein Leitungspräfix definiert ist, wird dieses der gesamten Rufnummer vorangestellt.

SNMP-ID: 2.33.3.2.4

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User

Mögliche Werte Telnet:

- max. 15 Ziffern oder *.

Default: Leer

2.33.3.2.5 Intern-Dial-Tone

Der Wählton bestimmt, welchen Ton ein Benutzer nach dem Abheben des Hörers hört. Der „interne Wählton" gleicht dem Ton, den ein Benutzer an einer TK-Anlage ohne spontane Amtsholung hört (drei kurze Töne gefolgt von einer Pause). Der „externe Wählton" gleicht folglich dem Ton, dass nach dem Abheben ein Amt anzeigt (anhaltender Ton ohne Unterbrechungen). Passen Sie den Wählton nach Bedarf an die Verwendung der spontanen Amtsholung an, um ein ähnliches Verhalten wie an einem externen Anschluss zu simulieren.

SNMP-ID: 2.33.3.2.5

Pfad Telnet: /Setup/Voice-Call-Manager/User/ISDN-User

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein, es wird der externe Wählton verwendet

2.33.3.4 Extensions

Hier können Sie erweiterte Benutzer-Einstellungen wie Anklopfen oder Anrufweiterschaltung festlegen.

SNMP-ID: 2.33.3.4

Pfad Telnet: /Setup/Voice-Call-Manager/User

2.33.3.4.1 Name

Für diese Rufnummer bzw. diese SIP-ID gelten die Benutzer-Einstellungen.

SNMP-ID: 2.33.3.4.1

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Anrufweiterschaltungen können für alle lokalen Benutzer (SIP, ISDN oder Analog) eingerichtet werden.

2.33.3.4.2 User modifiable

Aktiviert oder deaktiviert die Möglichkeit, die Benutzer-Einstellungen auch über das Telefon zu konfigurieren.

SNMP-ID: 2.33.3.4.2

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ja
- Nein

Default: Ja

2.33.3.4.3 CFU-Active

Aktiviert oder deaktiviert die sofortige Rufweiterschaltung (CFU) ohne Bedingung.

SNMP-ID: 2.33.3.4.3

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.3.4.4 CFU-Target

Ziel für die sofortige Rufweiterschaltung ohne Bedingung.

SNMP-ID: 2.33.3.4.4

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

Default: Leer

2.33.3.4.5 CFNR-Active

Aktiviert oder deaktiviert die verzögerte Rufweiterschaltung (bei Abwesenheit; CFNR).

SNMP-ID: 2.33.3.4.5

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.3.4.6 CFNR-Target

Ziel für die verzögerte Rufweiterschaltung.

SNMP-ID: 2.33.3.4.6

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

Default: Leer

2.33.3.4.7 CFNR-Timeout

Wartezeit für die verzögerte Rufweiterschaltung. Nach Ablauf dieser Zeit wird der Anruf an das Rufziel weitergeleitet, wenn der Teilnehmer den Anruf nicht annimmt.

SNMP-ID: 2.33.3.4.7

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- max. 255 Sekunden

Default: 15 Sekunden

2.33.3.4.8 CFB-Active

Aktiviert oder deaktiviert die Weiterschaltung bei „besetzt".

SNMP-ID: 2.33.3.4.8

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.3.4.9 CFB-Target

Ziel für die Weiterschaltung bei „besetzt".

SNMP-ID: 2.33.3.4.9

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Maximal 64 Zeichen zur Bezeichnung lokaler Benutzer, von Rufgruppen oder externen Rufnummern

Default: Leer

2.33.3.4.10 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.3.4.10

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.3.4.11 Busy-on-Busy

Verhindert das Zustellen eines zweiten Anrufs zu einem Endgerät, unabhängig davon, ob „Anklopfen" (CW, Call Waiting Indication) auf dem Endgerät erlaubt oder unterbunden ist, d.h. auch das „Anklopfen" wird verhindert. Zudem erhält der zweite Anrufende einen Besetzt-Ton. Dies gilt auch, wenn sich bei der internen Rufnummer um eine Mehrfachanmeldung handelt und nur mit einem der möglichen Endgeräte telefoniert wird.

SNMP-ID: 2.33.3.4.11

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.3.4.12 CF-Set-Cln-Id

Stellen Sie hier ein, welche Rufnummer bei einer Weiterleitung (CF) signalisiert wird - zum Beispiel die aus CDIV - alternativ kann man auch eine eigene Rufnummer als Anrufernummer fest eintragen

SNMP-ID: 2.33.3.4.12

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- Extension-ID:
- Calling-ID: signalisiert die eingehende Rufnummer. Bei der Weiterleitung an ein Handy kann ein Teilnehmer so die Original-Rufnummer des anrufenden Teilnehmers erkennen.
- Custom-ID: signalisiert die unter /Setup/Voice-Call-Manager/User/Extensions/Custom-ID eingetragene Rufnummer

Default: Extension-ID

2.33.3.4.13 Custom-Id

Stellen Sie hier die Rufnummer ein, die bei einer Weiterleitung (CF) signalisiert wird.

SNMP-ID: 2.33.3.4.13

Pfad Telnet: /Setup/Voice-Call-Manager/User/Extensions

Mögliche Werte Telnet:

- maximal 64 Zeichen

Default: leer

Diese Rufnummer wird nur verwendet, wenn der Parameter /Setup/Voice-Call-Manager/User/Extensions/CF-Set-Cln-Id auf den Wetrt "Custom-ID" eingestellt ist.

2.33.4 Line

Dieses Menü enthält die Leitungs-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.4

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.4.1 SIP-Provider

Dieses Menü enthält die SIP-Provider-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.4.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line

2.33.4.1.1 Line

Über diese Leitungen meldet das Gerät sich bei anderen SIP-Gegenstellen (in der Regel SIP-Provider oder als Remote Gateway bei SIP-TK-Anlagen) an. Die Verbindung erfolgt entweder über das Internet oder einen VPN-Tunnel. Es können bis zu 16 SIP-Leitungen eingetragen werden.

SNMP-ID: 2.33.4.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider

2.33.4.1.1.1 Name

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

SNMP-ID: 2.33.4.1.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 16 Zeichen

Default: leer

2.33.4.1.1.2 Domain

SIP-Domäne/Realm der übergeordneten Gegenstelle. Sofern die Gegenstelle DNS-Service Records für SIP unterstützt, genügt diese Angabe, um Proxy, Outbound-Proxy, Port, Registrar automatisch zu ermitteln - das ist bei typischen SIP-Provider-Angeboten i.d.R. der Fall.

SNMP-ID: 2.33.4.1.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.1.3 Port

TCP/UDP-Port beim SIP-Provider, an den die SIP-Pakete gesendet werden.

SNMP-ID: 2.33.4.1.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Beliebieger freier TCP/IP-Port.

Default: 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

2.33.4.1.1.4 User-id

Telefonnummer des SIP-Accounts oder Name des Benutzers (SIP-URI).

SNMP-ID: 2.33.4.1.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

2.33.4.1.1.5 Auth-Name

Name zur Authentifizierung an der übergeordneten SIP-Gegenstelle (Provider/SIP-TK-Anlage).

SNMP-ID: 2.33.4.1.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

2.33.4.1.1.6 Secret

Das Passwort zur Authentifizierung beim SIP-Registrar und SIP-Proxy des Providers. Bei Leitungen ohne (Re-)Registrierung kann das Passwort unter Umständen entfallen.

SNMP-ID: 2.33.4.1.1.6

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.1.7 Outb-proxy

Der Outbound-Proxy des SIP-Providers nimmt alle vom Gerät ausgehenden SIP-Signalisierungen einer Verbindung zu diesem Provider für die Dauer der Verbindung entgegen.

SNMP-ID: 2.33.4.1.1.7

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Outbound-Proxy wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

2.33.4.1.1.8 Cln-Prefix

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

SNMP-ID: 2.33.4.1.1.8

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 9 Ziffern

Default: leer

2.33.4.1.1.9 Name

Die Wirkung dieses Feldes hängt von der Einstellung des Modus der Leitung ab:

Wenn der Modus der Leitung „Einzel-Account“ ist, werden alle über die Leitung eingehenden Rufe mit dieser Nummer als Ruf-Ziel (SIP: „To:“) an den Call-Router übergeben.

Wenn der Modus „Trunk“ ist, wird die Ziel-Nummer durch Entfernen der für den Trunk definierten Stammnummer ermittelt – falls dabei ein Fehler auftritt, wird der Ruf mit der in diesem Feld eingetragenen Nummer versehen (SIP: „To:“) an den Call-Router übergeben.

Wenn der Modus auf „Gateway“ oder „Link“ eingestellt ist, hat der Eintrag in diesem Feld keine Wirkung.

SNMP-ID: 2.33.4.1.1.9

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.1.10 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.4.1.1.10

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.4.1.1.11 Comment

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.4.1.1.11

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.1.14 Rtg-tag

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu diesem SIP-Provider.

SNMP-ID: 2.33.4.1.1.14

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Ziffern

Default: 0

2.33.4.1.1.15 Display-Name

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

SNMP-ID: 2.33.4.1.1.15

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: Leer

Dieser Wert sollte im Normalfall nicht gesetzt werden, da bei eingehenden Rufen der SIP-Provider den Display-Namen setzt und bei ausgehenden Rufen der lokale Client bzw. die Rufquelle (ggf. überschrieben mit den Einstellungen zum Display-Namen des jeweiligen Benutzers). Oftmals werden hier zusätzliche Informationen übermittelt (z. B. Originalrufnummer bei einer Umleitung etc.), die für den Angerufenen hilfreich sein können. Im Fall von SIP-Einzel-Accounts verlangen manche Provider allerdings auch den in den Anmeldedaten vorgegebenen Display-Namen bzw. einen zur SIP-ID identischen Eintrag (z. B. T-Online). Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

2.33.4.1.1.16 Registrar

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account beim SIP-Provider entgegen nimmt.

SNMP-ID: 2.33.4.1.1.16

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Registrar wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

2.33.4.1.1.17 Mode

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung.

SNMP-ID: 2.33.4.1.1.17

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- provider: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer. Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer ersetzt (maskiert). Eingehende Rufe werden der konfigurierten internen Ziel-Nummer zugestellt. Es kann nur maximal eine Verbindung zu einem Zeitpunkt bestehen.
- trunk: Verhält sich nach außen wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die SIP-ID wird als Stammnummer beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen fungiert die Stammnummer als Präfix, das jeder rufenden Nummer (Absender; SIP: "From:") vorangestellt wird. Bei eingehenden Rufen wird das Präfix aus der Ziel-Nummer entfernt (SIP: "To:"). Die verbleibende Nummer wird als interne Durchwahl verwendet. Im Fehlerfall (Präfix nicht auffindbar, Ziel gleich Präfix) wird der Ruf an die konfigurierte interne Ziel-Nummer geleitet. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.
- gateway: Sie verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer, der SIP-ID. Die Nummer (SIP-ID) wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer (SIP-ID in SIP: "From:") ersetzt (maskiert) und in einem separaten Feld (SIP: "Contact:") übertragen. Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.
- link: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer (SIP-ID). Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender; SIP: "From:") nicht modifiziert. Bei eingehenden Rufen wird die gerufene Nummer (Ziel; SIP: "To:") nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Default: provider

Der "Serviceprovider" kann ein Server im Internet, eine IP-Telefonanlage oder ein Voice-Gateway sein. Bitte beachten Sie auch die Hinweise zum 'SIP-Mapping'.

2.33.4.1.1.18 Refer-weiterleiten

Bei der Rufvermittlung (Verbindung) von zwei entfernten Gesprächsteilnehmern kann die Vermittlung im Gerät selbst gehalten (Media-Proxy) oder an die Vermittlungsstelle beim Provider übergeben werden, wenn beide zu verbindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden (andernfalls übernimmt der Media-Proxy im Gerät die Vermittlung der Medienströme, z. B. beim Verbinden zwischen zwei SIP-Provider-Leitungen).

SNMP-ID: 2.33.4.1.1.18

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Ja: Vermittlung wird an den Provider weitergeleitet.
- Nein: Die Verbindungen werden im Gerät selbst gehalten.

Default: Nein

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

2.33.4.1.1.19 Lokale-Portnummer

Dies ist der Port des Proxys zur Kommunikation mit dem Provider.

SNMP-ID: 2.33.4.1.1.19

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- 1 bis 65536

Default: 0

Besondere Werte: 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch auf der Providerseite eingetragen werden (z. B. bei Nutzung eines regsitrierungslosen Trunks im Firmen-VPN), damit sich beide Seiten SIP-Signalisierungen senden können.

2.33.4.1.1.20 (Re-)Registrierung

Hiermit wird die (wiederholte) Registrierung der SIP-Provider-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

SNMP-ID: 2.33.4.1.1.20

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Ja
- Nein

Default: Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar des Providers ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

2.33.4.1.1.21 Leitungsüberwachung

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-Provider-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

SNMP-ID: 2.33.4.1.1.21

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Auto: Die Methode wird automatisch ermittelt.
- Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.
- Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.
- Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Default: Auto

2.33.4.1.1.22 Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

SNMP-ID: 2.33.4.1.1.22

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- max. 5 Ziffern

Default: 60

Besondere Werte: Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

2.33.4.1.1.23 Vertrauenswürdig

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

SNMP-ID: 2.33.4.1.1.23

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Ja: Vertrauenswürdig
- Nein: Nicht vertrauenswürdig

Default: Ja

Diese Funktion wird nicht von allen Providern unterstützt.

2.33.4.1.1.24 Privacy-Methode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.

SNMP-ID: 2.33.4.1.1.24

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line

Mögliche Werte Telnet:

- Keine
- RFC3325: mittels P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

Default: Keine

2.33.4.1.1.25 FROM-Benutzertypen-entfernen

Aktivieren Sie diese Option, um die Information "user=phone" aus dem From-Feld eines Rufes zu entfernen, der über eine Provider-Leitung abgeht. Einzelne VoIP-Proxies verarbeiten diese Information nicht standard-konform und lehnen daraufhin den Verbindungsaufbau ab.

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Line/FROM-Benutzertypen-entfernen

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.33.4.1.1.26 Trunk-Inc-Cld-In-ToHeader

Über diese Einstellung aktivieren bzw. deaktivieren Sie den Workaround für den Fall, dass ein Provider die vollständige Zielnummer (Stammnummer+Durchwahl) nicht in der Request-Line, sondern in der TO-URI überträgt und dennoch die Nummer im To-Feld nicht unbedingt länger ist als die Nummer in der Request-Line. Um Kompatibilität mit den betreffenden Providern sicherzustellen, sollten Sie diese Einstellung daher aktiviert lassen.

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

nein

ja

Default:

ja

2.33.4.1.2 Mapping

Mit den Einträgen für das SIP-Mapping wird in Form von Regeln eine Rufnummernumsetzung auf SIP-Leitungen im Trunk- oder Gateway-Modus eingerichtet. Es können bis zu 40 SIP-Mapping-Regeln eingetragen werden.

Bei einer SIP-Leitung im Trunk-Modus wird eine Anpassung der intern verwendeten Rufnummern an den Rufnummernkreis des SIP-Accounts vorgenommen.

Bei ankommenden Rufen wird die Zielrufnummer (Called Party ID) verändert. Die interne Nummer wird eingesetzt, wenn die Called Party ID mit der externen Nummer übereinstimmt.

Bei abgehenden Rufen wird die Absenderrufnummer (Calling Party ID) verändert. Die externe Nummer wird eingesetzt, wenn die Calling Party ID mit der internen Nummer übereinstimmt.

SNMP-ID: 2.33.4.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider

2.33.4.1.2.1 SIP-Provider

Name der Leitung, für welche die Rufnummernumsetzung gilt.

SNMP-ID: 2.33.4.1.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- Alle definierten SIP-Leitungen.

Default: leer

2.33.4.1.2.2 Ext-Number/Name

Rufnummer im Bereich des SIP-Trunk-Accounts bzw. im Bereich der übergeordneten SIP-TK-Anlage.

SNMP-ID: 2.33.4.1.2.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.2.3 Number/Name

Rufnummer im Bereich des VoIP Router.

SNMP-ID: 2.33.4.1.2.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.2.4 Length

Dieser Wert gibt an, nach wie vielen Stellen eine gerufene Nummer als komplett angesehen wird. Er ist nur auf SIP-Gateway-Leitungen bei solchen Einträgen von Bedeutung, die mit einem #-Zeichen enden.

Bei einem abgehenden Ruf wird die von diesem Eintrag erzeugte externe Rufnummer automatisch nach der angegebenen Anzahl von Stellen als komplett betrachtet und weitergeleitet. Durch diesen Vorgang wird die Anwahl beschleunigt. Alternativ wird die Rufnummer als komplett betrachtet, wenn:

der Benutzer ein #-Zeichen als Abschluss der Rufnummer wählt oder

ein exakt passender Eintrag in der SIP-Mapping-Tabelle ohne #-Zeichen gefunden wurde oder

die eingestellte Wartezeit abgelaufen ist.

SNMP-ID: 2.33.4.1.2.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- max. 9 Ziffern

Default: 0

Besondere Werte: Eine Rufnummern-Länge von '0' deaktiviert die vorzeitige Anwahl über die Rufnummernlänge.

2.33.4.1.2.5 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.4.1.2.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.4.1.2.6 Kommentar

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.4.1.2.6

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.1.2.7 CLIR

Anzeige der eigenen Rufnummer wird beim angerufenen Teilnehmer unterdrückt.

SNMP-ID: 2.33.4.1.2.7

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-Provider/Mapping

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.4.2 SIP-PBX

Dieses Menü enthält die SIP-PBX-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.4.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line

2.33.4.2.1 SIP-PBX

Über diese Leitungen werden Verbindungen zu übergeordneten SIP-TK-Anlagen konfiguriert, die in der Regel über VPN angebunden sind. Es können bis zu 4 SIP-TK-Anlagen eingetragen werden.

SNMP-ID: 2.33.4.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX

2.33.4.2.1.1 Name

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

SNMP-ID: 2.33.4.2.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 16 Zeichen

Default: leer

2.33.4.2.1.2 Domain

SIP-Domäne/Realm der übergeordneten SIP-TK-Anlage.

SNMP-ID: 2.33.4.2.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.2.1.3 Port

TCP/UDP-Port der übergeordneten SIP-TK-Anlage, an den die SIP-Pakete vom Gerät aus gesendet werden.

SNMP-ID: 2.33.4.2.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Beliebieger freier TCP/IP-Port.

Default: 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

2.33.4.2.1.4 Secret

Gemeinsames Passwort zum Anmelden an der SIP-TK-Anlage. Dieses Passwort wird nur benötigt, wenn sich SIP-Teilnehmer an der TK-Anlage anmelden sollen, die nicht als SIP-Benutzer mit eigenen Zugangsdaten in der Liste der SIP-Benutzer angelegt sind, oder keine lokale Authentifizierung erzwungen wird, so dass sich SIP-Benutzer ohne Passwort am Gerät anmelden können, aber mit einem gemeinsamen Passwort bei der übergeordneten SIP-TK-Anlage angemeldet werden, wenn die Domäne der SIP-Benutzer mit der Domäne der SIP-PBX-Line übereinstimmt.

SNMP-ID: 2.33.4.2.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.2.1.5 Outb-proxy

Ein SIP-Proxy nimmt Anfragen von SIP-Clients entgegen und agiert für, die Dauer des Verbindungsaufbaus als Stellvertreter (Proxy).

SNMP-ID: 2.33.4.2.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Die Adresse des Proxies wird dann über den Realm aufgelöst.

2.33.4.2.1.6 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.4.2.1.6

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.4.2.1.7 Kommentar

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.4.2.1.7

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.2.1.8 Cln-Prefix

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser SIP-PBX-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

SNMP-ID: 2.33.4.2.1.8

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 9 Ziffern

Default: leer

2.33.4.2.1.9 Line-Prefix

Bei ausgehenden Anrufen über diese Leitung wird der angerufenen Rufnummer dieses Präfix vorangestellt, um eine vollständige für diese Leitung gültige Rufnummer zu erzeugen. Bei ankommenden Rufen wird dieses Präfix entfernt, falls vorhanden.

SNMP-ID: 2.33.4.2.1.9

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 9 Ziffern

Default: leer

2.33.4.2.1.12 Rtg-tag

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu dieser SIP-TK-Anlage.

SNMP-ID: 2.33.4.2.1.12

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 64 Ziffern.

Default: 0

2.33.4.2.1.13 Registrar

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account in der SIP-TK-Anlage entgegen nimmt.

SNMP-ID: 2.33.4.2.1.13

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 63 Zeichen

Default: leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Die Adresse des Registrars wird dann über den Realm aufgelöst.

2.33.4.2.1.14 Lokale-Portnummer

Dies ist der Port des Proxys zur Kommunikation mit der übergeordneten SIP-TK-Anlage.

SNMP-ID: 2.33.4.2.1.14

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- 1 bis 65536

Default: 0

Besondere Werte: 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch in der SIP-TK-Anlage eingetragen werden, damit sich beide Seiten SIP-Signalisierungen senden können.

2.33.4.2.1.15 (Re-)Registrierung

Hiermit wird die (wiederholte) Registrierung der SIP-PBX-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

SNMP-ID: 2.33.4.2.1.15

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Ja
- Nein

Default: Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar der SIP-TK-Anlage ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

2.33.4.2.1.16 Leitungsüberwachung

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-PBX-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

SNMP-ID: 2.33.4.2.1.16

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Auto: Die Methode wird automatisch ermittelt.
- Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.
- Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.
- Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Default: Auto

2.33.4.2.1.17 Überwachungsintervall

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

SNMP-ID: 2.33.4.2.1.17

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- max. 5 Ziffern

Default: 60

Besondere Werte: Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

2.33.4.2.1.18 Vertrauenswürdig

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

SNMP-ID: 2.33.4.2.1.18

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Ja: Vertrauenswürdig
- Nein: Nicht vertrauenswürdig

Default: Ja

Bitte beachten sie, dass diese Funktion nicht von allen Providern unterstützt wird.

2.33.4.2.1.19 Privacy-Methode

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.

SNMP-ID: 2.33.4.2.1.19

Pfad Telnet: /Setup/Voice-Call-Manager/Line/SIP-PBX/PBX

Mögliche Werte Telnet:

- Keine
- RFC3325: mittels P-Preferred-Id/P-Asserted-Id
- IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

Default: Keine

2.33.4.3 ISDN

Über diese Leitungen werden die ISDN-Anschlüsse konfiguriert. Dazu wird neben der zu verwendenden physikalische ISDN-Leitung auch eine Rufnummernumsetzung konfiguriert. Diese sorgt für eine Umsetzung der internen Rufnummer oder SIP-URL auf eine externe ISDN-Nummer.

SNMP-ID: 2.33.4.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line

2.33.4.3.1 Interfaces

Hier werden die Leitungen zu ISDN-Vermittlungsstellen oder TK-Anlagen konfiguriert (Router ist Endgerät).

SNMP-ID: 2.33.4.3.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN

2.33.4.3.1.1 Name

Dieser Name identifiziert die Leitung eindeutig. Er darf keiner weiteren Leitung zugeordnet werden.

SNMP-ID: 2.33.4.3.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Tragen Sie hier z. B. die Rufnummer einer Gruppe ein, die jeden eingehenden Anruf erhält und steuern Sie darüber flexibel, welche Telefone bei Rufen klingeln oder leiten Sie den Ruf nach einer Zeit auf eine Mobilnummer oder den Anrufbeantworter um.

2.33.4.3.1.2 Ifc

Interface, an das die ISDN-Teilnehmer angeschlossen sind.

SNMP-ID: 2.33.4.3.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- Alle verfügbaren ISDN-Schnittstellen.

Default: Modellabhängig.

2.33.4.3.1.3 Domain

Domäne, unter der die Anrufe von / zu der ISDN-Leitung in der SIP-Welt des Geräts verwaltet werden.

SNMP-ID: 2.33.4.3.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.3.1.4 Cln-Prefix

Das Anruf-Präfix wird den Anrufer-Nummern (CLI) aller ankommenden Anrufe vorangestellt, um eine eindeutige Rückrufnummer zu erzeugen.

SNMP-ID: 2.33.4.3.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- max. 9 Ziffern

Default: leer

2.33.4.3.1.5 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.4.3.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.4.3.1.6 Kommentar

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.4.3.1.6

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Interfaces

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.3.2 Mapping

Mit dem ISDN-Mapping wird eine Zuordnung von externen ISDN-Rufnummern (MSN oder DDI) zu den intern verwendeten Rufnummern vorgenommen. Es können bis zu 64 Rufnummernzuordnungen eingetragen werden.

SNMP-ID: 2.33.4.3.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN

2.33.4.3.2.1 MSN/DDI

Externe Telefonnummer des Anschlusses im ISDN-Netz.

Für ankommende Rufe, die an diese Nummer gerichtet sind, wird die zugehörige interne Rufnummer als Zielnummer eingetragen. Für ausgehende Rufe wird diese Nummer als eigene Nummer des Anrufenden eingetragen, wenn dies nicht unterdrückt ist.

MSN: Nummer des Telefonanschluss

DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

SNMP-ID: 2.33.4.3.2.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- max. 19 Ziffern

Default: leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

2.33.4.3.2.2 Ifc

ISDN-Schnittstelle(n), über die Endgeräte an den VoIP Router angeschlossen sind. Diese Leitungen müssen als ISDN-NT konfiguriert sein.

SNMP-ID: 2.33.4.3.2.2

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- Alle verfügbaren ISDN-Schnittstellen.

Default: Modellabhängig.

2.33.4.3.2.3 Number/Name

Interne Telefonnummer des ISDN-Telefons oder Name des Benutzers (SIP-URL).

Für ankommende Rufe ist das der SIP-Name oder interne Telefonnummer des Telefons, an das der Ruf von diesem Interface mit der zugehörigen MSN/DDI vermittelt wird. Für ausgehende Rufe wird der SIP-Name durch die MSN/DDI des zugehörigen Eintrages ersetzt.

SNMP-ID: 2.33.4.3.2.3

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z. B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfasst werden.

2.33.4.3.2.4 CLIR

Anzeige der eigenen Rufnummer wird beim angerufenen Teilnehmer unterdrückt.

SNMP-ID: 2.33.4.3.2.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- Ja
- Nein

Default: Nein

2.33.4.3.2.5 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.4.3.2.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.4.3.2.6 Comment

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.4.3.2.6

Pfad Telnet: /Setup/Voice-Call-Manager/Line/ISDN/Mapping

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.4.4 Predef-Dest.

Tabelle mit den vordefinierten Sonderfunktionen für die Ziel-Leitungen in den Call-Routing-Einträgen.

SNMP-ID: 2.33.4.4

Pfad Telnet: /Setup/Voice-Call-Manager/Line

2.33.4.4.1 Name

Vordefinierte Sonderfunktionen für die Ziel-Leitungen in den Call-Routing-Einträgen.

SNMP-ID: 2.33.4.4.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/Predef-Dest.

Mögliche Werte Telnet:

- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.

- RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

Default: REJECT

USER

RESTART

2.33.4.5 Source-Filters

Tabelle mit den vordefinierten Quell-Leitungen zum Filtern auf Anrufe von lokalen Benutzern.

SNMP-ID: 2.33.4.5

Pfad Telnet: /Setup/Voice-Call-Manager/Line

2.33.4.5.1 Name

Vordefinierte Quell-Leitungen zum Filtern auf Anrufe von lokalen Benutzern.

SNMP-ID: 2.33.4.5.1

Pfad Telnet: /Setup/Voice-Call-Manager/Line/Source-Filters

Mögliche Werte Telnet:

- USER.ANALOG für Rufe eines lokalen, analogen Teilnehmers
- USER.ISDN für Rufe eines lokalen ISDN-Teilnehmers
- USER.SIP für Rufe eines lokalen SIP-Teilnehmers
- USER# für Rufe eines lokalen Teilnehmers allgemein

Default: USER.ANALOG

USER.ISDN

USER.SIP

USER#

2.33.5 Call-Router

Dieses Menü enthält die Call-Router-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.5

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.5.1 Call-Routing

Hier können Sie Regeln definieren, um Rufe zu bestimmten Rufzielen oder Leitungen umzuleiten oder abzulehnen.

SNMP-ID: 2.33.5.1

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router

2.33.5.1.1 Called-Id

Der gewählte Called Party Name bzw. die Ziel-Rufnummer (ohne Domänen-Angabe).

SNMP-ID: 2.33.5.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Besondere Werte: Das #-Zeichen wird als Platzhalter für beliebige Zeichenfolgen verwendet. Alle Zeichen vor dem # werden entfernt, die restlichen Zeichen werden im Feld „Nummer/Name“ anstelle der #-Zeichens für den weiteren Verbindungsaufbau verwendet.

Beispiel: In der Call-Routing-Tabelle enthält ein Eintrag die '00049#' als gerufene Nummer/Name und die '00#' als Nummer/Name. Bei allen Rufen mit einer führenden Null für die Amtsholung und der kompletten Vorwahl für Deutschland wird als Nummer/Name nur die führende Null für die Amtsholung und die führende Null für die Ortsnetzvorwahl beibehalten, die Landeskennung wird entfernt. Aus '00049 2405 123456' wird also die '0 02405 123456'.

2.33.5.1.2 Cld-Domain

Dieser Eintrag filtert auf die gerufene Domäne, die „Called Party Domain“. Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Called Party Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede Zieldomäne akzeptiert.

SNMP-ID: 2.33.5.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Analog
- ISDN
- Die interne VoIP-Domäne des VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

Default: leer

2.33.5.1.3 Calling-Id

Dieser Eintrag filtert auf die rufende Nummer/Name, die „Calling Party ID“. Die Angabe erfolgt entweder als interne Nummer, nationale oder internationale Rufnummer. Die Domäne wird nicht mit angegeben. Es wird keine „0“ oder anderes Zeichen für eine Leitungskennung vorangestellt, die ID wird wie von der Leitung bzw. wie von internen Rufen kommend verwendet.

Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Party ID des anliegenden Rufes mit der hier eingetragenen Nummer übereinstimmt. Ab einem „#“ können beliebige Ziffern akzeptiert werden.

SNMP-ID: 2.33.5.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- interne Nummer
- nationale
- internationale Rufnummer.
- LOCAL schränkt auf interne Rufnummern ein (ohne führende „0“).
- EMPTY kann für nicht angegebene Calling Party IDs verwendet werden.

Default: leer

Wird hier nichts angegeben, wird jede Calling Party ID akzeptiert.

2.33.5.1.4 Cln-Domain

Dieser Eintrag filtert auf die rufende Domäne, die „Calling Domain". Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Calling Domain des anliegenden Rufes mit der hier eingetragenen Domain übereinstimmt. Wird hier nichts angegeben, wird jede rufende Domäne akzeptiert.

SNMP-ID: 2.33.5.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Analog
- ISDN
- Die interne VoIP-Domäne des VoIP Router.
- Alle bei den SIP- und SIP-PBX-Leitungen eingetragenen Domänen.

Default: leer

SIP-Telefone verfügen üblicherweise über mehrere Leitungstasten, für die verschiedene Domänen konfiguriert werden können. Mit diesem Filter kann der Auswahl entsprechend eine bestimmte Behandlung der Rufe über unterschiedliche Leitungstasten vorgenommen werden.

2.33.5.1.5 Src-Line

Dieser Eintrag filtert auf die Quell-Leitung. Der Call-Router-Eintrag wird nur dann als übereinstimmend gewertet, wenn die Quell-Leitung des anliegenden Rufes mit der hier eingetragenen Leitung übereinstimmt. Wird hier nichts angegeben, wird jede rufende Leitung akzeptiert.

SNMP-ID: 2.33.5.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- USER.ANALOG für Rufe eines lokalen, analogen Teilnehmers
- USER.ISDN für Rufe eines lokalen ISDN-Teilnehmers
- USER.SIP für Rufe eines lokalen SIP-Teilnehmers
- USER# für Rufe eines lokalen Teilnehmers allgemein
- Alle eingetragenen ISDN,- SIP- und SIP-PBX-Leitungen.

Default: leer

2.33.5.1.7 Dest-Id-1

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet. Kann über diese Rufnummer und die zugehörige Leitung keine Verbindung hergestellt werden, werden die Backup-Rufnummern mit den zugehörigen Leitungen verwendet.

SNMP-ID: 2.33.5.1.7

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Mindestens eines der „Nummer/Name", „1. Backup-Nr." oder „2.Backup-Nr." muss einen Inhalt haben. Die Auswertung erfolgt in dieser Reihenfolge. Ein leeres Feld wird übersprungen.

2.33.5.1.8 Dest-Line-1

Über die Zielleitung wird die Verbindung aufgebaut.

ISDN

Alle definierten SIP Leitungen.

Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:

REJECT markiert eine gesperrte Rufnummer.

USER leitet den Ruf an lokale SIP- bzw. ISDN-Teilnehmer weiter.

RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

SNMP-ID: 2.33.5.1.8

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:
- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

Default: leer

Dieses Feld muss ausgefüllt werden, sonst wird der Eintrag nicht verwendet!

2.33.5.1.9 Active

Der Routingeintrag kann aktiviert, deaktiviert oder aber als Default-Eintrag gekennzeichnet werden. Alle über die ersten Durchläufe nicht über die Call-Routing-Tabelle bzw. lokale Teilnehmertabelle auflösbaren Anrufe werden dann automatisch über diese Default-Einträge aufgelöst. Zielname und Zieldomain sind dann beliebig, nur die ggf. gesetzten Quellfilter werden berücksichtigt.

SNMP-ID: 2.33.5.1.9

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Aktiv
- Inaktiv
- Standard-Leitung

Default: Aktiv

2.33.5.1.10 Kommentar

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.5.1.10

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.5.1.11 Dest-Id-2

Diese Rufnummer wird für den weiteren Verbindungsaufbau verwendet, wenn unter „Nummer/Name“ nichts eingetragen ist oder die zugehörige „Leitung“ nicht erreichbar ist. Kann über diese 2. Rufnummer und die zugehörige 2. Leitung keine Verbindung hergestellt werden, werden die 3. Rufnummer und die 3. Leitung verwendet.

SNMP-ID: 2.33.5.1.11

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.5.1.12 Dest-Line-2

Über diese Leitung wird die Verbindung aufgebaut, wenn die 2. Rufnummer für den Verbindungsaufbau verwendet wird. Hier können die gleichen Leitungen ausgewählt werden wir bei „Leitung“.

SNMP-ID: 2.33.5.1.12

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:
- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name“ einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung“ gelöscht.

Default: leer

2.33.5.1.13 Dest-Id-3

Bedeutung analog zu 2. Nummer.

SNMP-ID: 2.33.5.1.13

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.5.1.14 Dest-Line-3

Bedeutung analog zu 2. Leitung.

SNMP-ID: 2.33.5.1.14

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- Analog
- ISDN
- Alle definierten SIP Leitungen.
- Folgende Sonderfunktionen können als Ziel-Leitung eingetragen werden:

- REJECT markiert eine gesperrte Rufnummer.
- USER leitet den Ruf an lokale SIP- bzw. Analog- oder ISDN-Teilnehmer weiter.
- RESTART beginnt mit der zuvor gebildeten „Nummer/Name" einen neuen Durchlauf in der Call-Routing-Tabelle. Dabei wird zuvor „Quell-Leitung" gelöscht.

Default: leer

2.33.5.1.15 Prio

Der Call-Manager sortiert alle Einträge mit gleicher Priorität automatisch so, dass die Tabelle sinnvoll von oben nach unten durchlaufen werden kann. Bei einigen Einträgen muss jedoch (z. B. zur Rufnummernumsetzung) die Reihenfolge der Einträge vorgegeben werden. Die Einträge mit der höchsten Priorität werden automatisch nach oben sortiert.

SNMP-ID: 2.33.5.1.15

Pfad Telnet: /Setup/Voice-Call-Manager/Call-Router/Call-Routing

Mögliche Werte Telnet:

- 0 bis 999

Default: 0

2.33.5.1.16 Dest-Calling-Id

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Call-Router** > **Call-Routing**

Mögliche Werte:

max. 38 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.33.7 Groups

Dieses Menü enthält die Benutzergruppen-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.7

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.7.1 Groups

Hier können Gruppen definiert werden, die eine automatische Verteilung eingehender Rufe zu zwei oder mehr Teilnehmern ermöglichen.

SNMP-ID: 2.33.7.1

Pfad Telnet: /Setup/Voice-Call-Manager/Groups

2.33.7.1.1 Name

Unter dieser Rufnummer bzw. dieser SIP-ID ist die Rufgruppe erreichbar.

SNMP-ID: 2.33.7.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

Namen für Rufgruppen dürfen nicht mit Namen von Benutzern (SIP, ISDN oder Analog) übereinstimmen.

2.33.7.1.2 Members

Kommaseparierte Liste der Mitglieder dieser Rufgruppe. Als Mitglieder können Benutzer, Rufgruppen oder auch externe Rufnummern eingetragen werden, so dass eine unbegrenzte Skalierung möglich ist.

SNMP-ID: 2.33.7.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- Benutzer
- Rufgruppen
- externe Rufnummern

Default: leer

Rufgruppen können sich nicht selbst oder einen Vorgänger in der hierarchischen Struktur enthalten – es sind also keine Rekursionen durch den Eintrag der Mitglieder möglich! Schleifen zu einem Vorgänger in der Struktur sind jedoch über das 'Weiterleitungs-Ziel' möglich.

2.33.7.1.3 Distribution-method

Bestimmt die Art der Ruf-Verteilung.

SNMP-ID: 2.33.7.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- Simultan: Der Anruf wird aufgeteilt und an alle Gruppenmitglieder gleichzeitig weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird die Anrufsignalisierung für die anderen Mitglieder beendet. Wenn kein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.
- Sequentiell: Der Anruf wird der Reihe nach an die Gruppenmitglieder weitergeleitet. Wenn ein Mitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf an das jeweils folgende Mitglied weitergeleitet. Wenn auch das letzte Gruppenmitglied den Anruf innerhalb der Weiterleitungs-Zeit nicht annimmt, wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

Default: Simultan

2.33.7.1.4 Forwarding-time

Wenn ein anliegender Ruf von einem Gruppenmitglied nicht innerhalb der Weiterleitungs-Zeit angenommen wird, wird der Ruf je nach Art der Ruf-Verteilung weitergeleitet:

Bei simultaner Ruf-Verteilung wird der Anruf zum Weiterleitungs-Ziel weitergeleitet.

Bei sequentieller Ruf-Verteilung wird der Anruf an das nächste Gruppenmitglied in der gültigen Reihenfolge weitergeleitet. Wenn das Gruppenmitglied das letzte Mitglied der Reihenfolge ist, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet.

SNMP-ID: 2.33.7.1.4

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- max. 255 Sekunden

Default: 15

Besondere Werte: 0 Sekunden. Der Ruf wird sofort zum Weiterleitungs-Ziel geleitet (temporäres Überspringen einer Rufgruppe in einer Hierarchie).

Sind alle Mitglieder der Gruppe besetzt oder aus anderen Gründen nicht erreichbar, wird der Anruf an das Weiterleitungs-Ziel weitergeleitet, ohne die Weiterleitungs-Zeit abzuwarten.

2.33.7.1.5 Forwarding-target

Wenn keines der Gruppenmitglieder den Anruf innerhalb der Weiterleitungs-Zeit annimmt, wird der Anruf an das hier eingetragene Weiterleitungs-Ziel weitergeleitet. Sowohl Benutzer, Rufgruppen als auch externe Rufnummern können als Weiterleitungs-Ziel eingetragen werden. Es kann dabei nur genau ein Weiterleitungs-Ziel angegeben werden.

SNMP-ID: 2.33.7.1.5

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- Benutzer
- Rufgruppen
- externe Rufnummern

Default: leer

Wenn kein Weiterleitungs-Ziel angegeben wird, wird der Anruf zurückgewiesen, sobald die Liste der Mitglieder abgearbeitet ist bzw. wenn alle Mitglieder besetzt oder nicht erreichbar sind.

Das Weiterleitungs-Ziel wird erst aktiv, wenn die Weiterleitungs-Zeit der Gruppe vollständig abgelaufen ist bzw. kein Mitglied erreichbar ist. Aus diesem Grund sind hier auch Verweise auf eine höhere Stelle einer Rufgruppenstruktur möglich, anders als beim Eintrag der 'Mitglieder'.

2.33.7.1.6 Active

Aktiviert oder deaktiviert den Eintrag.

SNMP-ID: 2.33.7.1.6

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- Ein
- Aus

Default: Ein

2.33.7.1.7 Kommentar

Kommentar zu diesem Eintrag

SNMP-ID: 2.33.7.1.7

Pfad Telnet: /Setup/Voice-Call-Manager/Groups/Groups

Mögliche Werte Telnet:

- max. 64 Zeichen

Default: leer

2.33.8 Protokollierung

Dieses Menü enthält die Protokollierung-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.8

Pfad Telnet: /Setup/Voice-Call-Manager

2.33.8.1 Call-Data-Records

Dieses Menü enthält die Protokollierung-Einstellungen für den Voice-Call-Manager.

SNMP-ID: 2.33.8.1

Pfad Telnet: /Setup/Voice-Call-Manager/Protokollierung

2.33.8.1.1 E-Mail-Benachrichtigung

Bei Bedarf können Sie sich per E-Mail über alle Anrufe informieren lassen, die über den VoIP Router geführt werden. Für jeden Anruf, der zu einem Verbindungsaufbau führt (intern oder extern, ankommende und abgehende Anrufe) wird dann eine entsprechende Nachricht mit Angabe verschiedener Informationen wie Quell- und Ziel-Rufnummern sowie Start- und Endzeit des Anrufs etc. verschickt.

SNMP-ID: 2.33.8.1.1

Pfad Telnet: /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

Mögliche Werte Telnet:

- Ein
- Aus

Default: Aus

Zur Nutzung dieser Benachrichtigungen muss ein SMTP-Konto eingerichtet sein.

2.33.8.1.2 E-Mail-Adresse

E-Mail-Adresse für den Versand der Nachrichten.

SNMP-ID: 2.33.8.1.2

Pfad Telnet: /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

Mögliche Werte Telnet:

- Gültige E-Mail-Adresse

Default: leer

2.33.8.1.3 Syslog

Bei Bedarf können Sie sich per SYSLOG (Facility: Accounting; Level: Info) über alle Anrufe informieren lassen, die über den VoIP Router geführt werden. Für jeden Anruf, der zu einem Verbindungsaufbau führt (intern oder extern, ankommende und abgehende Anrufe) wird dann eine entsprechende Nachricht mit Angabe verschiedener Informationen wie Quell- und Ziel-Rufnummern sowie Start- und Endzeit des Anrufs etc. verschickt.

SNMP-ID: 2.33.8.1.3

Pfad Telnet: /Setup/Voice-Call-Manager/Protokollierung/Call-Data-Records

Mögliche Werte Telnet:

- Ein
- Aus

Default: Aus

Zur Nutzung dieser Benachrichtigungen muss ein SYSLOG-Client eingerichtet sein.

2.34 Drucker

Dieses Menü enthält die Einstellungen für Drucker.

SNMP-ID: 2.34

Pfad Telnet: /Setup

2.34.1 Drucker

Hier können Sie Einstellungen am Netzwerk-Drucker vornehmen

SNMP-ID: 2.34.1

Pfad Telnet: /Setup/Drucker

2.34.1.1 Drucker

Der Name des Druckers.

SNMP-ID: 2.34.1.1

Pfad Telnet: /Setup/Drucker/Drucker

Mögliche Werte:

- max. 10 Zeichen

Default: *

2.34.1.2 RawIp-Port

Über diesen Port können Druckaufträge über RawIP angenommen werden.

SNMP-ID: 2.34.1.2

Pfad Telnet: /Setup/Drucker/Drucker

Mögliche Werte:

- max. 10 Zeichen

Default: 9100

2.34.1.3 LPD-Port

Über diesen Port können Druckaufträge über LDP angenommen werden.

SNMP-ID: 2.34.1.3

Pfad Telnet: /Setup/Drucker/Drucker

Mögliche Werte:

- max. 10 Zeichen

Default: 515

2.34.1.4 Aktiv

Aktiviert oder deaktiviert diesen Eintrag.

SNMP-ID: 2.34.1.4

Pfad Telnet: /Setup/Drucker/Drucker

Mögliche Werte:

- Ja: Der Printserver ist aktiv.
- Nein: Der Printserver ist nicht aktiv.

Default: Nein

2.34.1.5 Bidirektional

Dieser Parameter aktiviert oder deaktiviert den bidirektionalen Modus des Druckers.

SNMP-ID: 2.34.1.5

Pfad Telnet: /Setup/Drucker/Drucker

Der bidirektionale Modus des Druckers wird nur für interne Zwecke bei der Entwicklung oder im Support verwendet. Belassen Sie für diesen Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.34.1.6 Reset-beim-Oeffnen

Wenn diese Option aktiviert ist, sendet das Gerät von dem Öffnen einer Drucker-Session einen Reset-Befehl an den Drucker.

SNMP-ID: 2.34.1.6

Pfad Telnet: /Setup/Drucker/Drucker

Mögliche Werte:

- Ja
- Nein

Default: Nein

Aktivieren Sie diese Option, wenn der Verbindungsaufbau zum Drucker nicht wie erwartet funktioniert.

2.34.2 Zugangs-Liste

Legen Sie hier diejenigen Netzwerke fest, die Zugriff auf den Drucker haben.

SNMP-ID: 2.34.2

Pfad Telnet: /Setup/Drucker

2.34.2.1 IP-Adresse

IP-Adresse des Netzwerks, dessen Clients Zugriff auf den Drucker haben dürfen.

SNMP-ID: 2.34.2.1

Pfad Telnet: /Setup/Drucker/Zugangs-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.34.2.2 IP-Netzmaske

Netzmaske zu den erlaubten Netzwerken.

SNMP-ID: 2.34.2.2

Pfad Telnet: /Setup/Drucker/Zugangs-Liste

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.34.2.3 Rtg-Tag

Wenn sie ein Routing-Tag für diese Zugriffs-Regel angeben, so werden nur solche Pakete angenommen, die entweder in der Firewall mit dem gleichen Tag markiert oder über ein Netzwerk mit passendem Schnittstellen-Tag empfangen wurden. Wenn als Routing-Tag 0 angegeben ist, wird jeder Zugriff einer passenden IP-Adresse zugelassen.

SNMP-ID: 2.34.2.3

Pfad Telnet: /Setup/Drucker/Zugangs-Liste/Rtg-Tag

Mögliche Werte:

- max. 5 Zeichen

Default: leer

Die Verwendung von Routing-Tags macht folglich nur in Kombination mit entsprechend begleitenden Regeln in der Firewall oder getaggten Netzwerken Sinn.

2.35 ECHO-Server

Dieses Menü enthält die Konfiguration des ECHO-Servers.

SNMP-ID: 2.35

Pfad Telnet: /Setup

2.35.1 Aktiv

Der Echo-Server wird für die Überwachung der Leitungsqualität durch Messung von RTT und Jitter benötigt.

SNMP-ID: 2.35.1

Pfad Telnet: /Setup/ECHO-Server

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.35.2 Zugriffstabelle

Diese Tabelle legt die Zugriffsrechte für die Nutzung des ECHO-Servers fest.

SNMP-ID: 2.35.2

Pfad Telnet: /Setup/ECHO-Server

2.35.2.1 IP-Adresse

IP-Adresse der Gegenstelle.

SNMP-ID: 2.35.2.1

Pfad Telnet: /Setup/ECHO-Server/Zugriffstabelle

Mögliche Werte:

- Gültige IP-Adresse.

2.35.2.2 Netzmaske

IP-Adresse der Gegenstelle.

SNMP-ID: 2.35.2.2

Pfad Telnet: /Setup/ECHO-Server/Zugriffstabelle

Mögliche Werte:

- Gültige IP-Adresse.

2.35.2.3 Protokoll

Für die Messung verwendetes Protokoll.

SNMP-ID: 2.35.2.3

Pfad Telnet: /Setup/ECHO-Server/Zugriffstabelle

Mögliche Werte:

- Kein
- TCP
- UDP
- TCP+UDP

2.35.2.4 Aktiv

Aktiviert oder deaktiviert diesen Eintrag der Tabelle.

SNMP-ID: 2.35.2.4

Pfad Telnet: /Setup/ECHO-Server/Zugriffstabelle

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.35.2.5 Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID: 2.35.2.5

Pfad Telnet: /Setup/ECHO-Server/Zugriffstabelle

2.35.3 TCP-Timeout

Wenn eine zum ECHO-Server aufgebaute TCP-Sitzung 10 (Default) Sekunden inaktiv ist, baut der Server sie wieder ab. Normalerweise räumt TCP selbsttätig "liegengebliebene" Verbindungen ab, aber das dauert deutlich länger.

SNMP-ID: 2.35.3

Pfad Telnet: /Setup/ECHO-Server

Mögliche Werte:

- max. 10 Zeichen

Default: 10

2.36 Performance-Monitoring

Dieses Menü enthält die Konfiguration des Performance-Monitoring.

SNMP-ID: 2.36

Pfad Telnet: /Setup

2.36.2 RttMonAdmin

Diese Tabelle zeigt Informationen über die Art der Messvorgänge.

SNMP-ID: 2.36.2

Pfad Telnet: /Setup/Performance-Monitoring

2.36.2.1 Index

Gemeinsamer Index der Messung

SNMP-ID: 2.36.2.1

Pfad Telnet: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.4 Messungsart

Art der Messung.

SNMP-ID: 2.36.2.4

Pfad Telnet: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.6 Frequenz

Zeit bis zur Wiederholung der Messung in Millisekunden. Kann als einziger Parameter verändert werden, während der Status Actrive ist. Dann ist allerdings nur der Wert 0 erlaubt, mit dem eine weitere Wiederholung unterbunden wird.

SNMP-ID: 2.36.2.6

Pfad Telnet: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.7 Timeout

Timeout einer Messung in Millisekunden. Das Timeout muss kleiner sein, als die Zeit bis zur Messungswiederholung.

SNMP-ID: 2.36.2.7

Pfad Telnet: /Setup/Performance-Monitoring/RttMonAdmin

2.36.2.9 Status

Status der Messung.

SNMP-ID: 2.36.2.9

Pfad Telnet: /Setup/Performance-Monitoring/RttMonAdmin

Mögliche Werte:

- Active: Messung wird durchgeführt. Dieser Wert kenn nur gesetzt werden, wenn Status den Weret Not_In_Service hat. Solange der Status Active ist, können keine Messparameter geändert werden.
- Not_In_Service: Alle benötigten Parameter sind gesetzt, es wird aktuell keine Messung durchgeführt.
- Not_Ready: Nicht alle benötigten Parameter sind gesetzt.
- Create: Anlegen einer Tabellenzeile. Per SNMP-Set wird eine Tabellenzeile angelegt, indem mit dem gewünschten Index der Status auf Create gesetzt wird. Auch bei der Konfiguration per Menüsystem muß der Status zunächst auf Create gesetzt werden. Wird eine neue Tabellenzeile angelegt, werden automatisch auch die zugehörigen Zeilen in den anderen Tabellen erzeugt.
- Destroy: Löschen einer Tabellenzeile. Ist nur möglich, wenn der Status nicht Active ist. Die zugehörigen Zeilen in den anderen Tabellen werden automatisch mit gelöscht.

2.36.3 RttMonEchoAdmin

Diese Tabelle zeigt Informationen über die Messvorgänge.

SNMP-ID: 2.36.3

Pfad Telnet: /Setup/Performance-Monitoring

2.36.3.1 Protokoll

Zu verwendendes Protokoll

SNMP-ID: 2.36.3.1

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.2 Zieldresse

Adresse des Responders

SNMP-ID: 2.36.3.2

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

Mögliche Werte:

- Gültige IP-Adresse.

2.36.3.3 Paketgroese

Länge der Messpakete in Byte. Das Paket wird auf die zur Messung benötigte Mindestgröße vergrößert.

SNMP-ID: 2.36.3.3

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.5 Zielport

Zielport. Wird derzeit ignoriert.

SNMP-ID: 2.36.3.5

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.17 Intervall

Zeit zwischen zwei Messpaketen in Millisekunden

SNMP-ID: 2.36.3.17

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.18 Paketzahl

Anzahl Messpakete je Messung

SNMP-ID: 2.36.3.18

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.3.255 Index

Gemeinsamer Index der Messung

SNMP-ID: 2.36.3.255

Pfad Telnet: /Setup/Performance-Monitoring/RttMonEchoAdmin

2.36.4 RttMonStatistics

Diese Tabelle zeigt die Statistik über die beim Performance-Monitoring ermittelten Werte.

SNMP-ID: 2.36.4

Pfad Telnet: /Setup/Performance-Monitoring

2.36.4.2 Completions

Anzahl durchgeführter Messungen

SNMP-ID: 2.36.4.2

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.4 RTT-Count

Gesamtzahl ermittelter RTT-Werte

SNMP-ID: 2.36.4.4

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.5 RTT-Sum

Summe aller ermittelten RTT-Werte

SNMP-ID: 2.36.4.5

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.8 RTT-Min

Minimale Roundtrip-Zeit in uSec

SNMP-ID: 2.36.4.8

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.9 RTT-Max

maximale Roundtrip-Zeit in uSec

SNMP-ID: 2.36.4.9

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.10 Jitter-Min-Pos-SD

Minimaler positiver Jitterwert Sender zu Responder in uSec

SNMP-ID: 2.36.4.10

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.11 Jitter-Max-Pos-SD

maximaler positiver Jitterwert Sender zu Responder in uSec

SNMP-ID: 2.36.4.11

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.12 Jitter-Count-Pos-SD

Anzahl ermittelter positiver Jitterwerte Sender zu Responder

SNMP-ID: 2.36.4.12

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.13 Jitter-Sum-Pos-SD

Summe aller positiven Jitterwerte Sender zu Responder in uSec

SNMP-ID: 2.36.4.13

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.16 Jitter-Min-Pos-DS

Minimaler positiver Jitterwert Responder zu Sender in uSec

SNMP-ID: 2.36.4.16

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.17 Jitter-Max-Pos-DS

maximaler positiver Jitterwert Responder zu Sender in uSec

SNMP-ID: 2.36.4.17

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.18 Jitter-Count-Pos-DS

Anzahl ermittelter positiver Jitterwerte Responder zu Sender

SNMP-ID: 2.36.4.18

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.19 Jitter-Sum-Pos-DS

Summe aller positiven Jitterwerte Responder zu Sender in uSec

SNMP-ID: 2.36.4.19

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.22 Jitter-Min-Neg-SD

Minimaler negativer Jitterwert Sender zu Responder in uSec, Absolutwert

SNMP-ID: 2.36.4.22

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.23 Jitter-Max-Neg-SD

maximaler negativer Jitterwert Sender zu Responder in uSec, Absolutwert

SNMP-ID: 2.36.4.23

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.24 Jitter-Count-Neg-SD

Anzahl ermittelter negativer Jitterwerte Sender zu Responder

SNMP-ID: 2.36.4.24

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.25 Jitter-Sum-Neg-SD

Summe aller negativen Jitterwerte Sender zu Responder in uSec, Absolutwert

SNMP-ID: 2.36.4.25

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.28 Jitter-Min-Neg-DS

Minimaler negativer Jitterwert Responder zu Sender in uSec, Absolutwert

SNMP-ID: 2.36.4.28

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.29 Jitter-Max-Neg-DS

maximaler negativer Jitterwert Responder zu Sender in uSec, Absolutwert

SNMP-ID: 2.36.4.29

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.30 Jitter-Count-Neg-DS

Anzahl ermittelter negativer Jitterwerte Responder zu Sender

SNMP-ID: 2.36.4.30

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.31 Jitter-Sum-Neg-DS

Summe aller negativen Jitterwerte Responder zu Sender in uSec, Absolutwert

SNMP-ID: 2.36.4.31

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.34 Packet-Loss-SD

Anzahl verlorener Pakete Sender zu Responder

SNMP-ID: 2.36.4.34

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.35 Packet-Loss-DS

Anzahl verlorener Pakete Responder zu Sender

SNMP-ID: 2.36.4.35

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.62 Average-Jitter

Durchschnitt aller absoluten Jitterwerte

SNMP-ID: 2.36.4.62

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.63 Average-Jitter-SD

Durchschnitt aller absoluten Jitterwerte Sender zu Responder

SNMP-ID: 2.36.4.63

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.64 Average-Jitter-DS

Durchschnitt aller absoluten Jitterwerte Responder zu Sender

SNMP-ID: 2.36.4.64

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.36.4.255 Index

Gemeinsamer Index der Messung

SNMP-ID: 2.36.4.255

Pfad Telnet: /Setup/Performance-Monitoring/RttMonStatistics

2.37 WLAN-Management

Dieses Menü enthält die Konfiguration des WLAN-Managements für WLCs.

2.37.1 AP-Konfiguration

Dieses Menü enthält die Einstellungen der AP-Konfiguration.

SNMP-ID: 2.37.1

Pfad Telnet: /Setup/WLAN-Management

Default: Leer

2.37.1.1 Netzwerkprofile

Hier definieren Sie die logischen WLAN-Netzwerke, die auf den angemeldeten AP (APs) aktiviert und betrieben werden können.

SNMP-ID: 2.37.1.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

2.37.1.1.1 Name

Name des logischen WLAN-Netzwerks, unter dem die Einstellungen gespeichert werden. Dieser Name wird nur für die interne Verwaltung der logischen Netze verwendet.

SNMP-ID: 2.37.1.1.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.1.2 Abgeleitet-von

Mit einem WLC können sehr viele unterschiedliche AP an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten AP gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die logischen WLAN-Netzwerke ausgewählte Eigenschaften von anderen Einträgen „erben".

SNMP-ID: 2.37.1.1.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.1.3 Lokale-Werte

Legen Sie hier fest, welche logischen WLAN-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

SNMP-ID: 2.37.1.1.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Bitfeld als HEX-Zahl. Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der logischen WLAN-Netzwerke (GUI).

Default: Alle Werte werden vom Eltern-Element übernommen.

2.37.1.1.4 Aktiv

Schaltet das logische WLAN separat ein- oder aus.

SNMP-ID: 2.37.1.1.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ein
- Aus

Default: Ein

2.37.1.1.6 Verschluesselung

Wählt das Verschlüsselungs-Verfahren bzw. bei WEP die Schlüssellänge aus, die bei der Verschlüsselung von Datenpaketen auf dem Wireless-LAN verwendet wird.

SNMP-ID: 2.37.1.1.6

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 802.11i-WPA-PSK
- 802.11i-WPA-802.1x
- WEP-104-Bit
- WEP-40-Bit
- WEP-104-Bit-802.1x
- WEP-40-Bit-802.1x
- keine

Default: 802.11i-WPA-PSK (0)

Beachten Sie, dass nicht jedes Verschlüsselungs-Verfahren von jeder Wireless-Karte unterstützt wird.

2.37.1.1.7 WPA1-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

SNMP-ID: 2.37.1.1.7

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- TKIP/AES
- AES
- TKIP

Default: TKIP/AES

2.37.1.1.8 WPA-Version

Mit dieser WPA-Version werden die Daten in diesem logischen WLAN verschlüsselt.

SNMP-ID: 2.37.1.1.8

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- WPA1/2
- WPA1
- WPA2

Default: WPA1/2 (0)

2.37.1.1.9 Schluessel

Sie können die Schlüssel oder Passphrases als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes 'Ox' möglich. Folgende Langen ergeben sich für die verwendeten Formate: Verfahren Länge WPA-PSK 8 bis 63 ASCII-Zeichen WEP152 (128 bit) 16 ASCII-oder 32 HEX-Zeichen WEP128 (104 bit) 13 ASCII-oder 26 HEX-Zeichen WEP64 (40 bit) 5 ASCII-oder 10 HEX-Zeichen

SNMP-ID: 2.37.1.1.9

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- ASCII-Zeichenkette oder Hexadezimalzahl

Default: Leer

2.37.1.1.10 Band

Mit der Auswahl des Frequenzbandes legen Sie fest, ob die WLAN-Karte im 2,4 GHz- oder im 5 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

SNMP-ID: 2.37.1.1.10

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 2,4GHz/5GHz
- 2,4GHz
- 5GHz

Default: 2,4GHz/5GHz

2.37.1.1.11 Weiterbetrieb

Zeit in Minuten, für die der AP im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Die Konfiguration wird dem AP vom WLC zugewiesen und optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLC unterbrochen wird, arbeitet der AP für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der AP mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist und die Verbindung zum WLC noch nicht wiederhergestellt wurde, wird die Konfiguration im Flash gelöscht – der Access Point stellt seinen Betrieb ein. Sobald der WLC wieder erreichbar ist, wird die Konfiguration erneut vom WLC zum AP übertragen.

Durch diese Option kann der AP auch dann weiter arbeiten, wenn die Verbindung zum WLC kurzfristig unterbrochen wird. Außerdem stellt diese Maßnahme einen wirksamen Schutz gegen Diebstahl dar, da die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch gelöscht werden.

SNMP-ID: 2.37.1.1.11

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 0 bis 9999

Default: 0

Besondere Werte: 0: Schaltet das WLAN-Modul des Gerätes sofort aus, wenn die Verbindung zum Controller unterbrochen wird. Die vom WLC zugewiesene Konfiguration wird in diesem Fall nicht im Flash, sondern im RAM abgelegt und geht damit bei einer Trennung vom Stromnetz sofort verloren.

9999: Arbeitet unbegrenzt mit der aktuellen Konfiguration weiter, auch wenn der WLAN Controller dauerhaft unerreichbar ist. Erst mit einem Reset wird die WLAN-Konfiguration im Flash gelöscht.

Alle weiteren Parameter der WLAN-Netzwerke entsprechen denen der üblichen Konfiguration für AP.

Stellt der AP im Backupfall eine Verbindung zu einem sekundären WLC her, so wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der AP bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLAN Controller hat.

Bitte beachten Sie, dass die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb gelöscht werden, nicht jedoch durch die Trennung vom Stromnetz!

2.37.1.1.12 Min-Tx-Rate

Der AP handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der AP die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die minimale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

SNMP-ID: 2.37.1.1.12

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- 1M
- 2M
- 5,5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

Default: Auto

2.37.1.1.13 Max-Tx-Rate

Der AP handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der AP die Übertragungsgeschwindigkeit an die Empfangslage aus. Alternativ können Sie hier die maximale Übertragungsgeschwindigkeit fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

SNMP-ID: 2.37.1.1.13

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- 1M
- 2M
- 5,5M
- 11M
- 6M

- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

Default: Auto

2.37.1.1.14 Basis-Rate

Die eingestellte Broadcastgeschwindgkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch „schneller" zu erreichen sind.

SNMP-ID: 2.37.1.1.14

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 1M
- 2M
- 5,5M
- 11M
- 6M
- 9M
- 12M
- 18M
- 24M
- 36M
- 48M
- 54M
- T-72M
- T-96M
- T-108M

Default: 2M

2.37.1.1.15 11b-Praeambel

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

SNMP-ID: 2.37.1.1.15

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- Lang

Default: Auto

2.37.1.1.16 MAC-Filter

In der MAC-Filterliste werden die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter 'MAC-Filter aktiviert' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

SNMP-ID: 2.37.1.1.16

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ja
- Nein

Default: Nein

Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

2.37.1.1.17 Cl.-Brg.-Support

Während mit der Adress-Anpassung (’Adress-Anpassung’ Æ Seite 480) nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den AP sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den AP übertragen.

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

SNMP-ID: 2.37.1.1.17

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ja: Aktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Nein: Deaktiviert die Client-Bridge-Unterstützung für dieses logische WLAN.
- Exklusiv: Akzeptiert nur Clients, die ebenfalls den Client-Bridge-Modus unterstützen.

Default: Nein

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

2.37.1.1.18 Maximum-Stationen

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

SNMP-ID: 2.37.1.1.18

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 0 bis 65535

Default: 0

2.37.1.1.19 SSID-Broadcast

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" im AP ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast** ermöglicht folgende Einstellungen:

- **Ja**: Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentlich sichtbares WLAN).
- **Nein**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.
- **Verschärft**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.

Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

Die Funktion "Closed-Network" finden Sie im AP unter **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk**. Beachten Sie: Wenn Sie im WLC bei **SSID-Broadcast** die Option "Nein" auswählen (Gerät veröffentlicht die SSID nicht), setzt der AP bei **Closed-Network** die Einstellung auf "Ja" und umgekehrt. Nur die Logik bei der Einstellung "Verschärft" ist in beiden Geräten identisch.

Pfad Telnet:

Pfad Telnet: Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Nein

Ja

Verschärft

Default:

Ja

2.37.1.1.21 SSID

Stellen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen) ein. Nur solche WLAN-Clients, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

SNMP-ID: 2.37.1.1.21

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- max. 32 Zeichen

Default: BLANK

2.37.1.1.22 Min.-HT-MCS

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams.

802.11n verwendet diesen Begriff anstelle „Datenrate" bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

Die Auswahl des MCS gibt also an, welche Modulationsparameter minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert. Eine Liste mit den Werte der verschiedenen MCS finden Sie im Referenzhandbuch.

Die erste Ziffer gibt die Modulationsparameter für einen Spatial Stream an, die zweite Ziffer die Modulationsparameter für zwei Spatial Streams.

SNMP-ID: 2.37.1.1.22

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

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

Default: Auto

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

2.37.1.1.23 Max.-HT-MCS

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams. 802.11n verwendet diesen Begriff anstelle „Datenrate" bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

Die Auswahl des MCS gibt also an, welche Modulationsparameter minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert. Eine Liste mit den Werte der verschiedenen MCS finden Sie im Referenzhandbuch.

Die erste Ziffer gibt die Modulationsparameter für einen Spatial Stream an, die zweite Ziffer die Modulationsparameter für zwei Spatial Streams.

SNMP-ID: 2.37.1.1.23

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- MCS-0/8
- MCS-1/9
- MCS-2/10
- MCS-3/11
- MCS-4/12

- MCS-5/13
- MCS-6/14
- MCS-7/15

Default: Auto

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

2.37.1.1.24 Kurzes-Guard-Intervall

Mit dieser Option wird die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval) reduziert. Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite wird das WLAN-System anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die aktuellen Betriebsbedingungen das zulassen. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

SNMP-ID: 2.37.1.1.24

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- Nein

Default: Auto

2.37.1.1.25 Max.-Spatiale-Stroeme

Mit der Funktion des Spatial-Multiplexing können mehrere separate Datenströme über separate Antennen übertragen werden, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

SNMP-ID: 2.37.1.1.25

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Auto
- Einer
- Zwei

Default: Auto

Besondere Werte:

- **Auto:** Mit der Einstellung 'Auto' werden alle Spatial-Streams genutzt, die von dem jeweiligen WLAN-Modul unterstützt werden.

2.37.1.1.26 Sende-Aggregate

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Durch dieses Verfahren kann der Overhead der Pakete reduziert werden, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

SNMP-ID: 2.37.1.1.26

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.37.1.1.27 WPA2-Sitzungsschluessel

Wählen Sie hier die Verfahren aus, welche zur Generierung der WPA-Sitzungs- bzw -Gruppen-Schlüssel angeboten werden sollen. Es können das Temporal Key Integrity Protokoll (TKIP), der Advanced Encryption Standard (AES) oder beide angeboten werden.

SNMP-ID: 2.37.1.1.27

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- TKIP/AES
- AES
- TKIP

Default: TKIP/AES

2.37.1.1.28 RADIUS-Accounting aktiviert

Aktiviert oder deaktiviert das RADIUS-Accounting in diesem logischen WLAN-Netzwerk.

Die APs, die der WLC mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine Firmware der LCOS-Version 8.00 oder höher verwenden.

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.37.1.1.30 VLAN-Modus

Wählen Sie hier die VLAN-Modus für dieses WLAN-Netzwerks (SSID) aus.

SNMP-ID: 2.37.1.1.30

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- tagged: Der AP markiert die Pakete dieser SSID mit der unter *2.37.1.1.34 VLAN-Id* konfigurierten ID.
- untagged: Der AP leitet die Pakete dieser SSID ohne zusätzliche VLAN-ID weiter.

Default: untagged

Der AP verwendet die VLAN-Einstellungen für das logische WLAN nur dann, wenn Sie das VLAN-Modul des AP in den physikalischen WLAN-Parametern aktivieren. Mit der Einstellung 'untagged' für ein spezielles WLAN können Sie auch bei aktiviertem VLAN ein WLAN ohne VLAN betreiben.

2.37.1.1.32 Verbinde-SSID-mit

Stellen Sie hier ein, an welche logische Schnittstelle der AP die Nutzdaten aus diesem WLAN-Netzwerk (SSID) überträgt.

SNMP-ID: 2.37.1.1.32

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- LAN: Der AP leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an die eigene lokale LAN-Schnittstelle weiter. Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen direkt auf dem AP, z. B. durch einen separaten Internet-Zugang.
- WLC-Tunnel-1 bis WLC-Tunnel-x (modellabhängig): Der AP leitet die Nutzdaten aus diesem WLAN-Netzwerk über die Bridge an eine der virtuellen Schnittstellen für den WLC weiter (WLC-Tunnel). Konfigurieren Sie in diesem Fall die weitere Verarbeitung der Datenpakete durch entsprechende Routen zentral auf dem WLC, z. B. durch einen gemeinsam genutzten Internet-Zugang.

Default: LAN

Die Weiterleitung der Nutzdaten aus mehreren SSIDs an den WLC steigert die CPU-Last und die benötigte Bandbreite der zentralen Geräte. Berücksichtigen Sie die erforderlichen Leistungswerte beim zentralen WLAN-Management mit Layer-3-Tunneling.

Sie können für jeden AP bis zu 7 SSIDs mit einem WLC-Tunnel verbinden. Der WLC verbindet auf dem jeweiligen AP den WLC-Tunnel und damit die verbundene SSID mit einer freien Bridge-Gruppe. Da eine der verfügbaren 8 Bridge-Gruppen für andere Zwecke reserviert ist, verbleiben 7 Bridge-Gruppen für die Zuordnung der WC-Tunnel.

2.37.1.1.33 Inter-Stations-Verkehr

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Stellen Sie für jedes logische WLAN separat ein, ob die Clients in dieser SSID untereinander Daten austauschen können.

SNMP-ID: 2.37.1.1.33

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.37.1.1.34 VLAN-Id

Stellen Sie hier die VLAN-ID für dieses logische WLAN-Netzwerk ein. Der AP überträgt die Daten aus diesem WLAN-Netzwerk (SSID) mit der hier eingestellten VLAN-ID, wenn der VLAN-Modus auf 'tagged' eingestellt ist.

SNMP-ID: 2.37.1.1.34

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- 2 bis 4094

Default: 2

2.37.1.1.35 RADIUS-Profile

Tragen Sie hier den Namen des RADIUS-Profils ein, welches die Informationen der RADIUS-Server für die Authentifizierung der Benutzerdaten und das Accounting der Benutzeraktivitäten enthält.

SNMP-ID: 2.37.1.1.35

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Netzwerkprofile

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.37.1.1.36 Minimal-Stations-Staerke

Dieser Eintrag bestimmt den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren AP, da die Liste keine AP aufführt, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Pfad Telnet:

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

Mögliche Werte:

max. 3 Zeichen aus 0 bis 9

Default:

0

2.37.1.1.37 LDPC-aktiviert

Mit dieser Einstellung aktivieren Sie für das betreffende logische Netzwerk LDPC. LDPC (Low Density Parity Check) ist eine Methode zur Fehlerkorrektur bei der Datenübertragung. Wenn Sie LDPC nicht aktivieren, verwendet Ihr Gerät das im IEEE-802.11n-Standard definierte, aber weniger effektive Convolution Coding (CC) zur Fehlerkorrektur.

AP in Ihrem Netzwerkverbund, die kein LDPC unterstützen, ignorieren diese Einstellung.

Pfad Telnet:

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

Mögliche Werte:

nein

ja

Default:

ja

2.37.1.1.38 Minimal-Stations-Staerke

Eine WLAN-Installation an einem Standort mit einer wirklich großen möglichen Anzahl von Clients (z. B. ein Fußball-Stadion) hat erhebliche Durchsatz-Probleme. Ein möglicher Grund in einem solchen Szenario ist ein hoher Anteil an Overhead durch entfernte Stationen mit schwacher Verbindung. Wenn eine solche Station eingebucht ist (assoziiert), kann die Basisstation (AP) Daten nur mit einer vergleichsweise niedrigen physikalischen Bitrate zu dieser Station senden – unter

Umständen mit mehreren Wiederholungen pro Paket. Dies wird nicht nur vom Benutzer der Station mit schwacher Verbindung als unvorteilhaft wahrgenommen, es belastet auch zeitlich das Medium, sodass dieses den Clients mit einer stärkeren Verbindung genommen wird, welche einen deutlich effektiveren Gebrauch von der zur Verfügung stehenden Bandbreite machen könnten. Es bleibt zu erwähnen, dass selbst nicht eingebuchte entfernte Stationen, beim Versuch ein Netzwerk zu finden, den Durchsatz der Funkzelle negativ beeinflussen können. Die Probe Requests (Suchpakete) solcher Clients müssen vom AP nach dem Empfand direkt und gerichtet beantwortet werden, d. h. sie werden solange wiederholt, bis der Client den Empfang bestätigt hat oder die Maximalzahl der Wiederholungen erreicht worden ist. Die Sache ist umso störender, da diese Antwort-Pakete auch noch WLAN-Management-Pakete sind, welche daher mit einer festen, üblicherweise der niedrigsten vom AP unterstützten Bitrate gesendet werden.

Obwohl ein AP auf keine Weise verhindern kann, dass Clients Probe Requests verschicken, kann er diese jedoch einfach ignorieren bzw. nicht beantworten, wenn sie eine bestimmte Signalstärke unterschreiten.

Eine konfigurierte **Minimal-Stations-Staerke** wirkt folgendermaßen:

- Wenn ein Probe Request mit einer passenden oder einer Platzhalter-SSID empfangen wird, wird dieses nur dann beantwortet, wenn es mindestens die konfigurierte Signal-Stärke aufweist. Wenn nicht, so wird es stillschweigend verworfen.
- Wenn eine Authentifizierungs- oder Einbuch-Anfrage empfangen wird, die unterhalb der konfigurierten Signal-Stärke liegt, so wird diese zurückgewiesen. Beachten Sie, dass diese Situation eher selten vorkommen sollte, da meistens bereits die Probe Requests solcher Clients nicht beantwortet wurden und ein Client diesen AP nur durch ein passives Suchen seiner Funkbake (Beacon) gefunden haben kann.

Die Angabe dieses Wertes erfolgt in Prozent. Dieser gibt das Verhältnis von Signal- und Rauschpegel (SNR) an. Ein Prozentwert von 100 % bedeutet ein SNR von 64 dB, kleinere Prozentwerte entsprechend weniger. Der Standard-Wert ist 0, d. h. keine Clients werden ignoriert.

Pfad Telnet:

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

Mögliche Werte:

0 bis 255

Default:

0

2.37.1.1.39 IEEE802.11u-Netzwerk-Profil

Über diesen Parameter spezifizieren Sie den Namen eines 802.11u-Netzwerk-Pofils, welches Sie dem logischen WLAN-Netzwerk zuweisen möchten.

Pfad Telnet:

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

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**, max. 32 Zeichen

Default:

2.37.1.1.40 OKC

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

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

Mit dieser Einstellung aktivieren Sie OKC auf dem vom WLC zu verwaltenden AP.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

ja

2.37.1.1.41 WPA2-Schluessel-Management

Mit diesen Optionen konfigurieren Sie die WPA2-Schlüsselverwaltung.

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

Pfad Telnet:

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

Mögliche Werte:

Schnelles-Roaming

Aktiviert Fast Roaming über 802.11r

SHA256

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

Standard

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

Default-Wert:

Standard

2.37.1.1.42 APSD

Aktiviert den Stromsparmodus APSD für das betreffende logische WLAN-Netz.

Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

Pfad Telnet:

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

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.37.1.1.43 Gesch.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem AP angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

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

Konfigurieren Sie hier, ob das jeweilige WLAN-Interface Protected Management Frames (PMF) nach IEEE 802.11w unterstützen soll.

Pfad Telnet:

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

Mögliche Werte:

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

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

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

Default-Wert:

Nein

2.37.1.1.44 Tx-Limit

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

2.37.1.1.45 Rx-Limit

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

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Begrenzung.

Default-Wert:

0

2.37.1.1.46 LBS-Tracking

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.

Pfad Telnet:

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

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

2.37.1.1.47 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 Client den angegebenen Listennamen, die MAC-Adresse des AP und die eigene MAC-Adresse an den LBS-Server.

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

2.37.1.2 Radioprofile

Hier definieren Sie physikalische WLAN-Parameter, die auf allen logischen WLAN-Netzen eines gemanagten AP gemeinsam gelten.

SNMP-ID: 2.37.1.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

2.37.1.2.1 Name

Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

SNMP-ID: 2.37.1.2.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.2.2 Abgeleitet-von

Mit einem WLC können sehr viele unterschiedliche AP an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten AP gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die physikalischen WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen „erben“.

SNMP-ID: 2.37.1.2.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.2.3 Lokale-Werte

Legen Sie hier fest, welche physikalischen WLAN-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

SNMP-ID: 2.37.1.2.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- Bitfeld als HEX-Zahl . Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der logischen WLAN-Netzwerke (GUI).

Default: Alle Werte werden vom Elterne-Element übernommen.

2.37.1.2.4 Land

Damit ein WLAN mit den richtigen Parametern betrieben werden kann, muss das Gerat seinen nationalen Standort kennen.

SNMP-ID: 2.37.1.2.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- Albanien
- Argentinien
- Australien
- Oesterreich
- Bahrain
- Bangladesh
- Weissrussland
- Belgien
- Bosnien-Herzegovina
- Brasilien
- Brunei-Daressalam
- Bulgarien
- Kanada
- Chile
- China
- Kolumbien
- Costa-Rica
- Kroatien
- Zypern
- Tschechei
- Daenemark
- Ecuador
- Egalistan
- Aegypten
- Estland
- Finland
- Frankreich
- Deutschland
- Ghana
- Griechenland
- Guatemala
- Honduras
- Hong-Kong
- Ungarn

- Island
- Indien
- Indonesien
- Irland
- Israel
- Italien
- Japan
- Jordanien
- Sued-Korea
- Kuwait
- Lettland
- Libanon
- Liechentstein
- Litauen
- Luxemburg
- Macao
- Mazedonien
- Malaysia
- Malta
- Mexiko
- Moldavien
- Marokko
- Niederlande
- Neuseeland
- Nicaragua
- Norwegen
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippinen
- Polen
- Portugal
- Puerto-Rico
- Qatar
- Rumaenien
- Russland
- Saudi-Arabien
- Singapur
- Slowakei
- Slovenien
- Suedafrika
- Spanien
- Schweden
- Schweiz
- Taiwan
- Tansania
- Thailand

- Tunesien
- Tuerkei
- Uganda
- Ukraine
- Vereinigte-Arabische-Emirate
- Grossbritannien
- Vereinigte-Staaten-FCC
- Uruguay
- Venezuela

Default: Default

Besondere Werte: Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

2.37.1.2.5 Kanalliste

Standardmäßig können die AP alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z. B. '7-9') möglich.

SNMP-ID: 2.37.1.2.5

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- Kommaseparierte Liste mit max. 48 Zeichen

Default: Leer

2.37.1.2.6 2.4GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN.Client im 2,4-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

Pfad Telnet:

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

Mögliche Werte:

11bg-gemischt
802.11g/b (gemischt)

nur-11b
Nur 802.11b (11Mbit)

nur-11g
Nur 802.11g (54Mbit)

108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)

11bgn-gemischt
802.11g/b/n

11gn-gemischt
802.11g/n

Greenfield
Nur 802.11n (Greenfield-Modus)

Auto
Automatisch. Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **11bgn-gemischt** oder zu **11bg-gemischt**.

Default-Wert:

Auto

2.37.1.2.7 5GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN.Client im 5-GHz-Frequenzband unterstützt. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

Pfad Telnet:

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

Mögliche Werte:

normal
802.11g (54Mbit/s-Modus)

108Mbps
802.11g++ (108MBit/s-Modus / Turbo-Modus)

11an-gemischt
802.11a/n (gemischt)

Greenfield
Nur 802.11n (Greenfield-Modus)

11anac-gemischt
802.11a/n/ac (gemischt)

11nac-gemischt
802.11n/ac (gemischt)

nur-11ac
Nur 802.11ac

Auto
Automatisch. Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **11anac-gemischt**, **11an-gemischt** oder **normal**.

Default-Wert:

Auto

2.37.1.2.8 Unterbaender

Im 5 GHz-Band kann neben dem Frequenzband ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

SNMP-ID: 2.37.1.2.8

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- Band-1
- Band-2
- Band-3
- Band-1+2
- Band-1+3
- Band-2+3
- Band-1+2+3

Default: Band-1+2+3 (0)

2.37.1.2.9 QoS

Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienst-güten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voiceoder WLAN – VoWLAN).Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM(Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video,Best Effort und Hintergrund) die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

SNMP-ID: 2.37.1.2.9

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- Ja
- Nein

Default: Nein

Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der AP den802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechen-den Prioritäten kennzeichnen.

2.37.1.2.10 DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

SNMP-ID: 2.37.1.2.10

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- 0 bis 255

Default: 0

2.37.1.2.11 Hintergrund-Scan

Zur Erkennung anderer AP in der eigenen Funkreichweite können Geräte die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der „normalen" Funktätigkeit der AP abläuft, wird diese Funktion auch als „Background Scan" bezeichnet.

Wird hier ein Wert angegeben, so sucht das Gerät innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren AP ab.

Für Geräte im AP-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte AP erkannt werden sollen, z. B. 1 Stunde.

Für Geräte im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.

SNMP-ID: 2.37.1.2.11

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- 0 bis 4294967296

Default: 0

Besondere Werte: 0: Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

2.37.1.2.12 Antennengewinn

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist ein Dämpfung der Leistung auf den zulässigen Wert erforderlich.

In das Feld 'Antennen-Gewinn' wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.

Im Gegensatz dazu reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter. Siehe dazu auch ’Geometrische Auslegung von Outdoor-Funknetz-Strecken’ Æ Seite 512.

SNMP-ID: 2.37.1.2.12

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- minus 128 bis 127

Default: 0

2.37.1.2.13 Sende-Leistungs-Reduktion

Im Gegensatz zum Antennen-Gewinn reduziert der Eintrag im Feld 'Sendeleistungs-Reduktion' die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter.

SNMP-ID: 2.37.1.2.13

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- 0 bis 255

Default: 0

Durch die Sendeleistungsreduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

2.37.1.2.16 Nur-Indoor-Betrieb

Bestimmen Sie ob nur der Indoor-Betrieb zugelassen werden soll.

SNMP-ID: 2.37.1.2.16

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/WLAN-Modul-2-Default/Nur-Indoor-Betrieb

Mögliche Werte:

- ja
- nein

Default: nein

2.37.1.2.17 VLAN-Modul-der-verwalteten-APs-aktivieren

Aktivieren oder deaktivieren Sie hier das VLAN-Modul der verwalteten AP. Ist das VLAN aus, dann werden alle VLAN-Einstellungen in den logischen Netzen ignoriert.

SNMP-ID: 2.37.1.2.17

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- ja
- nein

Default: nein

2.37.1.2.18 Mgmt-VLAN-Modus

VLAN-Modus für das Management-Netzwerk. VLAN wird nur benutzt, wenn das VLAN-Modul des Access Points aktiviert ist. Das Mangement-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden.

SNMP-ID: 2.37.1.2.18

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- untagged: Die Management-Pakete des AP werden nicht mit einer VLAN-ID markiert.
- tagged: Die Management-Pakete des AP werden mit der als Management-VLAN-ID in diesem Radioprofil konfigurierten VLAN-ID markiert.

Default: untagged

2.37.1.2.19 Mgmt-VLAN-ID

VLAN-ID für das Management-Netzwerk. Mit der Management-VLAN-ID wird das Management-Netzwerk getaggt, auf dem der WLC mit den AP kommuniziert. VLAN wird nur benutzt, wenn das VLAN-Modul des APs aktiviert ist. Das

Mangement-Netzwerk kann trotz aktiviertem VLAN auch ungetaggt betrieben werden, indem die entsprechende Einstellung für den Managment-VLAN-Modus gewählt wird. Hierzu wird intern die VLAN-ID '1' reserviert.

SNMP-ID: 2.37.1.2.19

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Radioprofile

Mögliche Werte:

- 2 bis 4094

Default: 2

2.37.1.2.20 Melde-gesehene-Clients

Dieser Eintrag bestimmt, ob der AP im WLAN-Netz erkannte Clients melden soll.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja

2.37.1.2.21 Client-Steering

Dieser Eintrag bestimmt, ob der AP das Band-Steering aktivieren soll.

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

2.37.1.2.22 Bevorzugtes-Band

Dieser Eintrag bestimmt, in welches Frequenzband der AP den WLAN-Client bevorzugt leiten soll.

Pfad Telnet:

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

Mögliche Werte:

5GHz

2,4GHz

Default:

5GHz

2.37.1.2.23 Proberequest-Herausaltern-Sekunden

Dieser Eintrag bestimmt die Zeit in Sekunden, für die die Verbindung eines WLAN-Clients im AP gespeichert bleiben soll. Nach Ablauf dieser Zeit löscht der AP den Eintrag in der Tabelle.

Wenn Sie Clients im WLAN benutzen, die z. B. oft von Dual-Band- auf Single-Band-Modus umschalten, sollten Sie diesen Wert entsprechen niedrig ansetzen.

Pfad Telnet:

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

Mögliche Werte:

max. 10 Zeichen aus 0 bis 9

Besondere Werte:

0: Der AP betrachtet gesehene Probe-Requests sofort als ungültig.

Default:

120

2.37.1.3 Gesamtprofile

Hier definieren Sie ganze WLAN-Profile, die alle WLAN-Einstellungen zusammenfassen, welche auf die gemanagten APs angewendet werden können. Dazu gehören zum Beispiel bis zu 16 logische WLAN-Netze sowie ein Satz physikalische WLAN-Parameter.

SNMP-ID: 2.37.1.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

2.37.1.3.1 Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

SNMP-ID: 2.37.1.3.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.3.2 Netze

Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

SNMP-ID: 2.37.1.3.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

Mögliche Werte:

- max. 251 ASCII-Zeichen mehrere Werte durch Kommata getrennt.

Default: Leer

Die AP nutzen aus dieser Liste nur die ersten acht Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils acht WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und acht für reinen 5 GHz-Betrieb definiert werden. Für jeden AP – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen acht logischen WLAN-Netzwerke zur Verfügung.

2.37.1.3.3 AP-Parameter

Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der AP arbeiten sollen.

SNMP-ID: 2.37.1.3.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

Mögliche Werte:

- Auswahl aus der Liste der physikalischen WLAN-Parameter (GUI) oder maximal 31 ASCII-Zeichen

Default: Leer

2.37.1.3.4 Controller

Liste der WLCs, bei denen der AP eine Verbindung versuchen soll. Der AP leitet die Suche nach einem WLC über einen Broadcast ein. Wenn nicht alle WLCs über einen solchen Broadcast erreicht werden können (WLC steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLCs sinnvoll.

SNMP-ID: 2.37.1.3.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Gesamtprofile

Mögliche Werte:

- IP-Adressen, mehrere Werte getrennt durch Kommata. max. 159 Zeichen, also je nach Länge der IP-Adressen etwa 9 bis 10 Einträge.

Default: Leer

2.37.1.3.6 IEEE802.11u-General

Über diesen Parameter spezifizieren Sie den Namen des Standortprofils, das für das WLAN-Profil (also das hiesige Gesamtprofil) gelten sollen.

Pfad Telnet:

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

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**, max. 32 Zeichen

Default:

2.37.1.3.7 Konfigurationsverzoegerung

Über diesen Parameter definieren Sie die Verzögerungszeit, nach der ein AP ein vom WLC unmittelbar ausgerolltes Konfigurationsupdate ausführt.

Die Verzögerungszeit ist primär für APs relevant, die Sie ausschließlich über eine Funkstrecke (z. B. mittels AutoWDS) in Ihr gemanagtes WLAN integrieren. Dabei reduzieren Sie die Wahrscheinlichkeit, dass durch nicht zugestellte Konfigurationsupdates lediglich eine Teilkonfiguration Ihres Netzes erfolgt und die übrigen APs ggf. unerreichbar werden. Je höher Sie die Verzögerungszeit einstellen, desto wahrscheinlicher ist, dass sämtliche hinzukommenden APs das vom WLC ausgerollte Konfigurationsupdate auch tatsächlich erhalten.

Empfehlenswert ist ein Wert von mindestens 1 Sekunde pro (AutoWDS-)Hop.

Pfad Telnet:

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

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert das verzögerte Konfigurationsupdate.

Default-Wert:

0

2.37.1.3.8 LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll.

Pfad Telnet:

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

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

2.37.1.3.9 LBS-General-Profil

Wählen Sie aus der Liste der LBS-General-Profile das Profil aus, das im WLAN-Profil gelten soll.

Pfad Telnet:

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

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

2.37.1.3.10 Wireless-ePaper-Profile

Tragen Sie hier das auf dem Gerät konfigurierte Wireless-ePaper-Profil ein.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.4 Basisstationen

Hier definieren Sie alle gemanagten AP, die von diesem WLC verwaltet werden sollen. Dabei weisen Sie dem AP sein WLAN-Profil zu.

SNMP-ID: 2.37.1.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

2.37.1.4.1 MAC-Adresse

MAC-Adresse des AP.

SNMP-ID: 2.37.1.4.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Gültige MAC-Adresse

Default: Leer

Besondere Werte: FFFFFFFFFFFF: definiert die Default-Konfiguration

2.37.1.4.2 Name

Name des AP im Managed-Modus.

SNMP-ID: 2.37.1.4.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- max. 16 ASCII-Zeichen

Default: Leer

2.37.1.4.3 Standort

Standort des AP im Managed-Modus.

SNMP-ID: 2.37.1.4.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- max. 251 ASCII-Zeichen

Default: Leer

2.37.1.4.4 Profil

WLAN-Profil aus der Liste der definierten Profile, welches für diesen AP verwendet werden soll.

SNMP-ID: 2.37.1.4.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Auswahl aus der Liste der definierten WLAN-Profile, max. 31 ASCII-Zeichen.

Default: Leer

2.37.1.4.6 Kontrollkanalverschluesselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

SNMP-ID: 2.37.1.4.6

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- default
- DTLS
- Nein

Default: Default

Besondere Werte: Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

2.37.1.4.7 WLAN-Modul-1

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

SNMP-ID: 2.37.1.4.7

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- default
- 2,4 GHz
- 5 GHz
- Aus

Default: Default

Besondere Werte: Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

2.37.1.4.8 WLAN-Modul-2

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

SNMP-ID: 2.37.1.4.8

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- default
- 2,4 GHz
- 5 GHz
- Aus

Default: Default

Besondere Werte: Default: übernimmt die Verschlüsselung von der Definition im Bereich 'Optionen'.

2.37.1.4.9 Module-1-Kanalliste

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

SNMP-ID: 2.37.1.4.9

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Kommaseparierte Liste mit max. 48 Zeichen

Default: Leer

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

2.37.1.4.10 Module-2-Kanalliste

Mit dem Funkkanal wird ein Teil des theoretisch denkbaren Frequenzbandes für die Datenübertragung im Funknetz ausgewählt.

SNMP-ID: 2.37.1.4.10

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Kommaseparierte Liste mit max. 48 Zeichen

Default: Leer

Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

2.37.1.4.11 Aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

SNMP-ID: 2.37.1.4.11

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.37.1.4.12 IP-Adresse

Statische IP-Adresse für den AP, wenn kein DHCP genutzt werden kann/soll.

SNMP-ID: 2.37.1.4.12

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.37.1.4.13 Netz-Maske

Statisches Netzmaske, wenn kein DHCP genutzt werden kann/soll.

SNMP-ID: 2.37.1.4.13

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

nicht per LANconfig konfigurierbar

2.37.1.4.14 Gateway

Statisches IP-Adresse des Gateways, wenn kein DHCP genutzt werden kann/soll.

SNMP-ID: 2.37.1.4.14

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

Nicht per LANconfig konfigurierbar

2.37.1.4.16 Antennen-Maske

AP mit 802.11-Unterstützung können bis zu drei Antennen zum Senden und Empfangen der Daten einsetzen. Je nach Anwendung kann die Nutzung der Antennen eingestellt werden.

SNMP-ID: 2.37.1.4.16

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- 1+2+3: Beim Einsatz des Geräts im AP-Modus zur Anbindung von WLAN-Clients ist in der Regel die parallele Nutzung aller drei Antennen zu empfehlen
- um eine gute Netzabdeckung zu erzielen.
- 1+3: Für die Nutzung von zwei parallelen Datenströmen z. B. bei Point-to-Point-Verbindungen mit einer entsprechenden Dual-Slant-Antenne werden die Antennen-Anschlüsse 1 und 3 verwendet. Der dritte Antennen-Anschluss wird dabei deaktiviert.
- 1: Bei Anwendungen mit nur einer Antenne (z. B. Outdoor-Anwendung mit einer Antenne) wird die Antennen an den Anschluss 1 angeschlossen
- die Anschlüsse 2 und 3 werden deaktiviert.
- Auto: automatische Auswahl der Antennen

Default: Auto

Besondere Werte: Auto: Mit der Einstellung 'Auto' werden alle verfügbaren Antennen genutzt.

2.37.1.4.17 AP-Intranet

Hier wird auf eine Zeile in der AP-Intranets Tabelle verwiesen.

SNMP-ID: 2.37.1.4.17

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.4.18 Verwalte-Firmware

Hier kann der automatische Firmware Upload für diesen AP abgeschaltet werden. Bei bestimmten Fehlern wird dies auch automatisch durch den Kontroller abgeschaltet. Der Grund für die automatische Abschaltung wird in der Spalte "Verwalte-Firmware-Zusätzliche-Information" angezeigt.

SNMP-ID: 2.37.1.4.18

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Ja
- Nein

Default: Ja

nicht per LANconfig konfigurierbar

2.37.1.4.19 Verwalte-Firmware-Zusätzliche-Information

Hier kann der automatische Firmware Upload für diesen AP abgeschaltet werden. Bei bestimmten Fehlern wird dies auch automatisch durch den Kontroller abgeschaltet. Der Grund für die automatische Abschaltung wird in der Spalte "Verwalte-Firmware-Zusätzliche-Information" angezeigt.

SNMP-ID: 2.37.1.4.19

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte:

- Leer
- Ausgeschaltet_aufgrund_eines_Fehlers_während_des_Updates
- Ausgeschaltet_aufgrund_eines_manuellen_Updates

Default: Leer

nicht per LANconfig konfigurierbar

2.37.1.4.20 Module-1-Ant-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel: AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

SNMP-ID: 2.37.1.4.20

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen/Module-1-Ant-Gewinn

Mögliche Werte Telnet:

- 0 bis 999 dBi

Default: leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

2.37.1.4.21 Module-2-Ant-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet Ihre Basisstation die in Ihrem Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Beispiel: AirLancer O-18a: Antennengewinn: 18dBi, Kabeldämfung: 4dB --> Einzutragender Wert = 18dBi - 4dB = 14dBi.

SNMP-ID: 2.37.1.4.21

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen/Module-2-Ant-Gewinn

Mögliche Werte Telnet:

- 0 bis 999 dBi

Default: leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

2.37.1.4.22 Module-1-TX-Redukt.

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, dann können Sie mit diesem Eintrag die Sendeleistung Ihrer Basisstation auf die in Ihrem Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

SNMP-ID: 2.37.1.4.22

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte Telnet:

- 0 bis 999 dBi

Default: leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

2.37.1.4.23 Module-2-TX-Redukt.

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, dann können Sie mit diesem Eintrag die Sendeleistung Ihrer Basisstation auf die in Ihrem Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Lassen Sie das Feld leer, wird die Default-Einstellung verwendet, die bei der Konfigurationsgruppe des verwendeten WLAN-Profils eingestellt ist.

Die Sendeleistung kann auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz Band reduziert werden. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi. Bitte achten Sie darauf, dass Ihr Antennen/Kabel/Blitzschutz-Setup unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

SNMP-ID: 2.37.1.4.23

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Basisstationen

Mögliche Werte Telnet:

- 0 bis 999 dBi

Default: leer

Die aktuelle Sendeleistung können Sie mit Hilfe des Web-Interfaces des Gerätes oder per Telnet unter 'Status->WLAN-Statistik->WLAN-Parameter->Sendeleistung' oder per LANmonitor unter 'System-Informationen->WLAN-Karte->Sendeleistung' einsehen.

2.37.1.4.24 Gruppen

Über diesen Parameter ordnen Sie dem betreffenden AP-Profil optional eine oder mehrere Tag-Gruppen zu. Sofern Sie ein AP-Profil bearbeiten, kann dieser Parameter darüber hinaus auch jene Zuweisungs-Gruppen enthalten, die der WLC dem betreffenden AP im Rahmen der IP-abhängigen Autokonfiguration zugewiesen hat. Weiterführende Informationen hierzu erhalten Sie im Referenzhandbuch.

Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.

Pfad Telnet:

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

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**. Mehrere Einträge trennen Sie durch eine kommaseparierte Liste.

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Tag-Gruppen**. Mehrere Einträge trennen Sie durch eine kommaseparierte Liste.

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

Default-Wert:

leer

2.37.1.4.25 Modul-2-Max.-Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 2. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Pfad Telnet:

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

Mögliche Werte:

Automatisch
Der AP erkennt automatisch die maximale Kanal-Bandbreite.

20MHz
Der AP benutzt auf 20MHz gebündelte Kanäle.

40MHz
Der AP benutzt auf 40MHz gebündelte Kanäle.

80MHz
Der AP benutzt auf 80MHz gebündelte Kanäle.

Default-Wert:

Automatisch

2.37.1.4.26 Modul-1-Max.-Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die 1. physikalische WLAN-Schnittstelle festlegt.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Pfad Telnet:

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

Mögliche Werte:

Automatisch
Der AP erkennt automatisch die maximale Kanal-Bandbreite.

20MHz
Der AP benutzt auf 20MHz gebündelte Kanäle.

40MHz
Der AP benutzt auf 40MHz gebündelte Kanäle.

80MHz
Der AP benutzt auf 80MHz gebündelte Kanäle.

Default-Wert:

Automatisch

2.37.1.4.27 Client-Steering-Profil

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.4.28 LBS-Device-Location-Profil

Mit diesem Eintrag ordnen Sie dem AP ein unter **Setup** > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location** erstelltes Profil zu.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.4.29 Wireless-ePaper-Kanal

Wählen Sie aus dem Dropdown-Menü einen Kanal für das Wireless ePaper-Modul.

Pfad Telnet:

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

Mögliche Werte:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default-Wert:

Auto

2.37.1.4.30 iBeacon-Profile

Tragen Sie hier das auf dem Gerät konfigurierte iBeacon-Profil ein.

Pfad Telnet:

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

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.4.31 iBeacon-Kanal

Legen Sie hier den Sendekanal für das iBeacon-Modul fest.

Pfad Telnet:

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

Mögliche Werte:

2402MHz
2426MHz
2480MHz

Default-Wert:

2402MHz

2426MHz

2480MHz

2.37.2.4.32 Minor

Geben Sie hier die eindeutige Minor-ID des iBeacon-Moduls an.

Pfad Telnet:

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

Mögliche Werte:

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

1 … 65535 Integer-Wert

Default-Wert:

0

2.37.1.4.33 iBeacon-Sendeleistung

Legen Sie hier die Sendeleistung das iBeacon-Modul fest.

Pfad Telnet:

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

Mögliche Werte:

Gering
Das Modul sendet mit minimaler Leistung.

Mittel
Das Modul sendet mit durchschnittlicher Leistung.

Hoch
Das Modul sendet mit maximaler Leistung.

Default-Wert:

Hoch

2.37.1.5 WLAN-Modul-1-Default

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 1. physikalische WLAN-Schnittstelle betreibt.

Pfad Telnet:

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

Mögliche Werte:

Auto
Der AP wählt das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 2,4GHz-Band bevorzugt, sofern dieses verfügbar ist.

2,4GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 2,4Ghz-Band.

5GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 5Ghz-Band.

Aus
Der AP deaktiviert die physikalische WLAN-Schnittstelle.

Default-Wert:

Auto

2.37.1.6 WLAN-Modul-2-Default

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 2. physikalische WLAN-Schnittstelle betreibt.

Sofern ein verwalteter AP lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der AP die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

Pfad Telnet:

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

Mögliche Werte:

Auto
Der AP wählt das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 5GHz-Band bevorzugt, sofern dieses verfügbar ist.

2,4GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 2,4Ghz-Band.

5GHz
Der AP betreibt die physikalische WLAN-Schnittstelle im 5Ghz-Band.

Aus
Der AP deaktiviert die physikalische WLAN-Schnittstelle.

Default-Wert:

Auto

2.37.1.7 Kontrollkanalverschluesselungs-Default

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

SNMP-ID: 2.37.1.7

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- DTLS
- Nein

Default: DTLS (1)

2.37.1.8 Laendereinstellungs-Default

Land, in dem die AP betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wir die erlaubten Kanäle etc. festgelegt.

SNMP-ID: 2.37.1.8

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- Albanien
- Argentinien
- Australien
- Oesterreich
- Bahrain
- Bangladesh
- Weissrussland
- Belgien
- Bosnien-Herzegovina
- Brasilien
- Brunei-Daressalam
- Bulgarien
- Kanada
- Chile
- China
- Kolumbien
- Costa-Rica
- Kroatien
- Zypern
- Tschechei
- Daenemark
- Ecuador
- Egalistan
- Aegypten
- Estland
- Finland
- Frankreich
- Deutschland
- Ghana
- Griechenland
- Guatemala
- Honduras
- Hong-Kong
- Ungarn
- Island
- Indien

- Indonesien
- Irland
- Israel
- Italien
- Japan
- Jordanien
- Sued-Korea
- Kuwait
- Lettland
- Libanon
- Liechentstein
- Litauen
- Luxemburg
- Macao
- Mazedonien
- Malaysia
- Malta
- Mexiko
- Moldavien
- Marokko
- Niederlande
- Neuseeland
- Nicaragua
- Norwegen
- Oman
- Pakistan
- Panama
- Paraguay
- Peru
- Philippinen
- Polen
- Portugal
- Puerto-Rico
- Qatar
- Rumaenien
- Russland
- Saudi-Arabien
- Singapur
- Slowakei
- Slovenien
- Suedafrika
- Spanien
- Schweden
- Schweiz
- Taiwan
- Tansania
- Thailand
- Tunesien
- Tuerkei

- Uganda
- Ukraine
- Vereinigte-Arabische-Emirate
- Grossbritannien
- Vereinigte-Staaten-FCC
- Uruguay
- Venezuela

Default: Deutschland (276)

2.37.1.9 AP-Intranets

Definieren Sie hier bei Bedarf IP-Parameter-Profile zur Verwendung in der AP-Tabelle, wenn bestimmten AP ihre IP-Adressen nicht per DHCP zugewiesen werden.

SNMP-ID: 2.37.1.9

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

2.37.1.9.1 Name

Name des Intranetz, in dem AP betrieben werden. Dieser Name wird nur für die interne Verwaltung der Intranetze verwendet.

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.9.2 Abgeleitet-von

Mit einem WLC können sehr viele unterschiedliche AP an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten AP gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die Intranet-Parameter nicht in mehreren Profilen redundant gepflegt werden müssen, können die Intranetze ausgewählte Eigenschaften von anderen Einträgen „erben".

Mögliche Werte:

- max. 31 ASCII-Zeichen

Default: Leer

2.37.1.9.3 Lokale-Werte

Legen Sie hier fest, welche Intranet-Parameter bei der Vererbung vom Eltern-Element übernommen werden sollen. Alle nicht geerbten Parameter können lokal für diese Profil eingestellt werden.

Mögliche Werte:

- Bitfeld als HEX-Zahl . Gesetzte Bits spezifizieren zu vererbende Spalten. Auswahl aus der Liste der Intranetzwerke (GUI).

Default: 0

2.37.1.9.4 Domainname

Domain-Name welche vom AccessPoint bei der Auflösung von WLC-Adressen benutzt wird.

Mögliche Werte:

- max. 63 ASCII-Zeichen

Default: Leer

2.37.1.9.5 Netz-Maske

Statisches Netzmaske, wenn kein DHCP genutzt werden kann/soll.

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.37.1.9.6 Gateway

Statisches IP-Adresse des Gateways, wenn kein DHCP genutzt werden kann/soll.

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.37.1.9.7 Primärer-DNS-Srv

Statisches IP-Adresse des ersten DNS Servers, wenn kein DHCP genutzt werden kann/soll.

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.37.1.9.8 Sekundärer-DNS-Srv

Statisches IP-Adresse des zweiten DNS Servers, wenn kein DHCP genutzt werden kann/soll.

Mögliche Werte:

- Gültige IP-Adresse.

Default: Leer

2.37.1.9.9 IPv4-konfig-Pool-Start

Anfang des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Pfad Telnet:

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

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

2.37.1.9.10 IPv4-konfig-Pool-Ende

Ende des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Pfad Telnet:

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

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

2.37.1.10 Predef.-Intranets

Diese Tabelle enthält die Liste der vordefinierten AP-Intranets.

SNMP-ID: 2.37.1.10

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Predef.-Intranets

Die Einstellungen für vordefinierte Intranets werden nur für interne Zwecke bei der Kommunikation des Geräts mit LANconfig verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.37.1.10.1 Name

Hier sehen Sie den Namen des vordefinierten AP-Intranets.

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/WLAN-Modul-2-Default/Name

Die Einstellungen für vordefinierte Intranets werden nur für interne Zwecke bei der Kommunikation des Geräts mit LANconfig verwendet. Belassen Sie für diese Parameter die voreingestellten Werte. Eine abweichende Konfiguration kann zu unerwartetem Verhalten im Betrieb der Geräte führen.

2.37.1.12 DSCP-für-Kontrollpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Kontrollpakete über DiffServ (Differentiated Services) aus.

SNMP-ID: 2.37.1.12

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- Best-Effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41

- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

Default: Best-Effort

2.37.1.13 DSCP-für-Datenpakete

Wählen Sie hier die passende Einstellung für die Priorisierung der Datenpakete über DiffServ (Differentiated Services) aus.

SNMP-ID: 2.37.1.13

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

Mögliche Werte:

- Best-Effort
- Assured-Forwarding-11
- Assured-Forwarding-12
- Assured-Forwarding-13
- Assured-Forwarding-21
- Assured-Forwarding-22
- Assured-Forwarding-23
- Assured-Forwarding-31
- Assured-Forwarding-32
- Assured-Forwarding-33
- Assured-Forwarding-41
- Assured-Forwarding-42
- Assured-Forwarding-43
- Expedited-Forwarding

Default: Best-Effort

2.37.1.14 Multicast-Netzwerke

Diese Tabelle enthält die Einstellungen für die Übertragung von CAPWAP-Multicast-Paketen über die jeweiligen Bridge-Schnittstellen.

Wenn ein WLC ein Broadcast- oder Multicast-Paket für ein Netzwerk einer SSID empfängt, so muss er dieses Paket an alle AP weiterleiten, welche die betreffende SSID anbieten. Der WLC hat zwei Möglichkeiten, alle betroffenen AP zu erreichen:

- Der WLC kopiert das Paket und sendet es als Unicast an die jeweiligen AP. Die Vervielfältigung der Pakete steigert die CPU-Last auf dem Controller und die benötigte Bandbreite, was sich besonders auf WAN-Verbindungen negativ auf die Performance auswirkt.
- Der WLC sendet das Paket als Multicast. In diesem Falle reicht in den meisten Fällen ein einziges Paket. Allerdings erreicht der Controller mit diesen Multicast-Paketen nur die AP in der eigenen Broadcast-Domäne. AP, die über eine geroutete WAN-Strecke angebunden sind, können diese Multicast-Pakete des Controllers nicht empfangen.

> Die Weiterleitung der Multicast-Pakete ist abhängig von den verwendeten Geräten auf der WAN-Strecke.

Der WLC versendet regelmäßig Keep-Alive-Multicast-Pakete an die Multicast-Gruppe. Wenn ein AP diese Pakete beantwortet, kann der Controller diesen AP über Multicast-Pakete erreichen. Für alle anderen AP kopiert der Controller die bei ihm eingehenden Multicast-Pakete und versendet sie als Unicast an die entsprechenden AP.

Wenn die Übertragung von CAPWAP-Multicast-Paketen aktiviert ist und für die Bridge-Schnittstelle eine gültige Multicast-IP-Adresse mit Port definiert ist, sendet das Gerät die eingehenden Broadcast- und Multicast-Pakete als Multicast weiter an diese Adresse.

Um Informationen über die Mitgliedschaften in Multicastgruppen der eingebuchten WLAN-Clients auch beim Wechsel zu einem anderen AP aufrecht zu erhalten, schalten die Geräte bei der Aktivierung von Multicast auch gleichzeitig das IGMP Snooping ein, welches die Informationen über die Multicast-Struktur aktuell hält.

In Anwendungen mit mehreren WLCs führen Multicast-Pakete möglicherweise zu Schleifen. Um Schleifen durch Multicasts bei Verwendung der Bridge zu vermeiden nutzt der WLC die folgenden Maßnahmen:

- Der WLC beachtet die CAPWAP-Multicast-Pakete nicht. Wenn ein WLC-Datentunnel verwendet wird, sendet der Controller die Pakete als Unicast.
- Der WLC leitet keine Pakete weiter, die eine CAPWAP-Multicast-Adresse als Empfänger tragen.
- Der WLC aktiviert automatisch IGMP-Snooping auf allen verwalteten AP, wenn CAPWAP selbst Multicast verwendet.

2.37.1.14.1 Bridge-Schnittstelle

Wählen Sie hier eine Bridge-Schnittstelle für die Multicast-Einstellungen aus.

SNMP-ID: 2.37.1.14.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Auswahl aus einer der definierten Bridge-Schnittstellen

2.37.1.14.2 Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von CAPWAP-Multicast-Paketen für diese Bridge-Schnittstelle.

SNMP-ID: 2.37.1.14.2

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- ja
- nein

Default: nein

2.37.1.14.3 Multicast-Adresse

Wählen Sie hier eine IP-Adresse, an welche das Gerät für die gewählte Bridge-Schnittstelle die CAPWAP-Multicast-Pakete übermittelt.

SNMP-ID: 2.37.1.14.3

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Maximal 15 Zeichen zur Definition einer gültigen IP-Adresse

Default: 233.252.124.1 bis 233.252.124.32 (IP-Adressen aus dem nicht zugewiesenen Bereich)

2.37.1.14.4 Multicast-Port

Wählen Sie hier einen Port für die Übertragung von CAPWAP-Multicast-Paketen über die gewählte Bridge-Schnittstelle.

SNMP-ID: 2.37.1.14.4

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche Werte:

- Maximal 5 Ziffern zur Bezeichnung einer gültigen Port-Nummer

Default: 20000 bis 20031

2.37.1.14.5 Loopback-Addr.

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.37.1.14.5

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration/Multicast-Netzwerke

Mögliche 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

Default: 0.0.0.0

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet. Name einer Loopback- Adresse.

2.37.1.15 AutoWDS-Profile

Diese Tabelle enthält die Parameter für das AutoWDS-Profil, welches Sie über das WLAN-Profil den einzelnen AP zuweisen, um den Aufbau vermaschter Netze zu realisieren. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

Pfad Telnet:

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

2.37.1.15.0 Link-Calibrierung

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Profile** > **AutoWDS-Profile**

Mögliche Werte:

Aus
Kapazität
Robustheit

2.37.1.15.1 Name

Name des AutoWDS-Profils, auf das Sie aus anderen Tabellen referenzieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.15.2 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.

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

2.37.1.15.3 SSID

Geben Sie den Namen des logischen WLAN-Netzs (SSID) an, das ein gemanagter AP zum Aufspannen des AutoWDS-Basisnetzes heranzieht. Hinzukommende APs im Client-Modus nutzen die hier angegebene SSID außerdem, um eine Konfiguration vom WLC beziehen.

Die betreffende SSID ist exklusiv für AutoWDS reserviert. Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb Ihrer WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

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

Default-Wert:

AutoWDS-Rollout

2.37.1.15.4 Key

Geben Sie die WPA2-Passphrase für das AutoWDS-Basisnetz an, das ein gemanagter AP aufspannt. Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

min. 8 Zeichen; max. 63 Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.37.1.15.6 Aktiv

Legen Sie fest, ob AutoWDS für das gewählte Profil aktiv oder inaktiv ist. Inaktive Profile überträgt der WLC nicht zu einem AP.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.37.1.15.7 Erlaube-Express-Integration

Geben Sie an, ob die APs des betreffenden WLAN-Profils über das AutoWDS-Basisnetz die Express-Integration für hinzukommende APs erlauben. Wenn Sie diese Einstellung aktivieren, senden die betreffenden Master-APs in ihren Beacons (sofern Sie im AutoWDS-Profil 'SSID-Broadcast' aktiviert haben) und Probe-Responses eine zusätzliche herstellerspezifische Kennung aus, die hinzukommenden APs die Verfügbarkeit dieser Integrationsvariante signalisiert.

Sofern Sie AutoWDS aktivieren und die Express-Integration verbieten, erlaubt das AutoWDS-Basisnetz ausschließlich die vorkonfigurierte Integration hinzukommender oder eingebundener APs im Client-Modus.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

nein

Das AutoWDS-Basisnetz erlaubt ausschließlich die vorkonfigurierte Integration hinzukommender APs.

ja

Das AutoWDS-Basisnetz erlaubt sowohl die vorkonfigurierte als auch die Express-Integration hinzukommender APs .

Default-Wert:

nein

2.37.1.15.8 Topology-Management

Geben Sie an, welche Art des Topologie-Managements der WLC für das betreffende AutoWDS-Profil verfolgt.

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie die Topologie des vermaschten Netzes aufgebaut ist. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Die beiden betreffenden WLAN-Schnittstellen bilden dazu ein P2P-Paar: Die physikalische WLAN-Schnittstelle des hinzukommenden AP wird zum P2P-Slave; die des gewählten Zugangs-AP zum P2P-Master.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology** (SNMP-ID 1.73.2.13). Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest.

Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

Bei der manuellen Topologie-Konfiguration ist es wichtig, dass sich ein konfigurierter P2P-Master-AP innerhalb der Topologie näher am WLC befindet als ein entsprechender P2P-Slave-AP, da bei einer kurzzeitigen Unterbrechung der P2P-Verbindung der Slave-AP nach dem Master-AP scannt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

automatisch

Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.

semi-automatisch

Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.

manuell

Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Default-Wert:

automatisch

2.37.1.15.10 Slave-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

2.37.1.15.11 Master-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

2.37.1.15.12 Link-Verlust-Timeout

Definieren Sie die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die der WLC automatisch generiert hat. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

Der Link-Verlust-Timeout ist unabhängig von den übrigen Timeouts. Es ist empfehlenswert, den voreingestellten Wert nicht weiter zu verringern, um die Gesamtkonnektivität des AutoWDS-Basisnetzes stabil zu halten.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

4

2.37.1.15.14 Weiterbetrieb

Definieren Sie die Weiterbetriebszeit der automatisch generierten P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 9999 Minuten

Besondere Werte:

0

Der AP schaltet seine physikalische(n) WLAN-Schnittstelle(n) unverzüglich ab, sobald der Kontakt zum WLC verloren geht. Dabei löscht das Gerät umgehend seine Konfigurations-Parameter, sodass der WLC sie beim Wiederaufbau der Verbindung erneut übertragen muss.

Wählen Sie diese Einstellung, um die sicherheitsrelevanten Konfigurations-Parameter vor unbefugtem Zugriff und Missbrauch (z. B. im Fall eines Diebstahls des AP) zu schützen.

9999

Die Konfigurations-Parameter bleiben dauerhaft im Gerät gespeichert. Der AP arbeitet weiter; unabhängig davon, wie lange der Kontakt zum WLC verloren geht.

Default-Wert:

0

2.37.1.15.15 Zeit-bis-Preconf-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der im AutoWDS-Profil hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten abgelaufen sind. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die vorkonfigurierte Integration auf dem betreffenden AP.

Default-Wert:

60

2.37.1.15.16 Zeit-bis-Express-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, wenn sämtliche Weiterbetriebszeiten sowie die *Wartezeit für den Beginn der vorkonfigurierten Integration* abgelaufen sind (sofern gesetzt). Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Express-Integration auf dem betreffenden AP.

Default-Wert:

0

2.37.1.15.17 Schnittstellen-Paarung

Legen Sie fest, welche Art der Schnittstellen-Paarung ein Zugangs-AP anhand des ihm zugewiesenen AutoWDS-Profils erlaubt. Die Einstellung ist hauptsächlich für Geräte mit mehr als einer physikalischen WLAN-Schnittstelle relevant.

Die Schnittstellung-Paarung beeinflusst die Suche eines AP im Client-Modus nach geeigneten Zugangs-AP unter Beachtung der beteiligten WLAN-Schnittstellen. Sie legt fest, ob sich der hinzukommende AP für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden muss oder auch Paarungen mit anderen physikalischen WLAN-Schnittstellen eingehen darf. Die Definition der Schnittstellen-Paarung erlaubt, schon im Vorfeld ungültige Paarungen auszuschließen, die sich evtl. ansonsten durch die Zuweisung unterschiedlicher Frequenzbänder im Rahmen der WLC-Konfiguration ergeben würden.

Arbeiten die Zugangs-AP Ihres AutoWDS-Basisnetzes beispielsweise mit den physikalischen WLAN-Schnittstellen WLAN-1 fest im 2,4 GHz-Band und WLAN-2 fest im 5 GHz-Band, so vorhindert die Schnittstellen-Paarung **Strikt**, dass ein hinzukommender AP, der auf einer physikalischen WLAN-Schnittstelle beide Frequenzbänder durchsucht, für z. B. WLAN-1 das 5-GHz-Band wählt, um sich mit WLAN-2 des Zugangs-AP zu verbinden. Eine solche Verbindung wäre zwar für den Bezug der WLC-Konfiguration legitim. Der anschließende P2P-Verbindungsaufbau wäre aufgrund der unterschiedlichen Radio-Einstellungen jedoch nicht möglich. Der hinzukommende AP würde die Verbindung verlieren und müsste einen Rekonfigurationsprozess starten.

Funken hingegen beide physikalischen WLAN-Schnittstellen auf demselben Band, ist auch die Schnittstellen-Paarung **Gemischt** zulässig, da die oben beschriebene Problemkonfiguration so nicht auftreten kann.

Achten Sie nach Möglichkeit darauf, dass alle beteiligten APs je physikalischer WLAN-Schnittstelle durchgehend das gleiche Frequenzband (2,4GHz oder 5GHz) verwenden, um so eventuelle Probleme bei der automatischen Topologie-Konfiguration auszuschließen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Automatisch

Der WLC prüft, ob eine Problemkonfiguration auftreten kann. Tritt keine Problemkonfiguration auf, akzeptiert er die betreffende Schnittstellen-Paarung über den Zugangs-AP. Andernfalls lehnt der WLC diese ab und der hinzukommende AP muss sich neu verbinden.

Strikt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X ausschließlich mit der äquivalenten WLAN-Schnittstelle eines Zugangs-AP verbinden.

Gemischt

Ein hinzukommender AP darf seine physikalische WLAN-Schnittstelle X mit einer beliebigen WLAN-Schnittstelle eines Zugangs-AP verbinden.

Default-Wert:

Automatisch

2.37.1.15.18 Slave-Radio-Multi-Hop

Über diesen Parameter legen Sie fest, ob die Zugangs-APs Ihres AutoWDS-Basisnetzes Verbindungsanfragen hinzukommender APs auf jener physikalischen WLAN-Schnittstelle akzeptieren, mit der sie selber als Slave zum Master verbunden sind.

Ein Deaktivieren dieses Parameters kann die Stabilität und die Lastverteilung innerhalb Ihres AutoWDS-Basisnetzes verbessern. In Folge dessen sind Single-Radio-APs dann jedoch nicht mehr als Zugangs-APs für die Erweiterung Ihres AutoWDS-Basisnetzes verfügbar und stellen das Ende eines Hierarchie-Zweigs dar.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

Nein

Ein Zugangs-AP nimmt Verbindungsanfragen hinzukommender APs niemals auf der gleichen physikalischen WLAN-Schnittstelle an, mit der er bereits als Slave mit dem AutoWDS-Basisnetz verbunden ist. WLAN-Multihops sind ausschließlich auf Geräten mit zwei gemanagten physikalischen WLAN-Schnittstellen möglich.

Ja

Ein Zugangs-AP nimmt Verbindungsanfragen hinzukommender APs auch auf der gleichen physikalischen WLAN-Schnittstelle an, mit der er bereits als Slave mit dem AutoWDS-Basisnetz verbunden ist. WLAN-Multihops sind sowohl auf Geräten mit zwei als auch einer gemanagten physikalischen WLAN-Schnittstelle möglich.

Nur-Single-Radio-AP

Fallabhängige Einstellung:

Für Geräte mit einer physikalischen WLAN-Schnittstelle gilt die Einstellung **Ja**.

Für Geräte mit mehr als einer physikalischen WLAN-Schnittstelle gilt die Einstellung **Nein**.

Default-Wert:

Nein

2.37.1.15.19 Band

Geben Sie das Frequenzband an, in dem die APs das AutoWDS-Basisnetz ausstrahlen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

2,4GHz/5GHz
Für die Ausstrahlung des AutoWDS-Basisnetzes ist sowohl das 2,4-GHz-Band als auch das 5-GHz-Band zugelassen.

2,4GHz
Für die Ausstrahlung des AutoWDS-Basisnetzes ist ausschließlich das 2,4-GHz-Band zugelassen.

5GHz
Für die Ausstrahlung des AutoWDS-Basisnetzes ist ausschließlich das 5-GHz-Band zugelassen.

Default-Wert:

5GHz

2.37.1.15.20 Band

Über diesen Parameter legen Sie fest, ob die APs die SSID des AutoWDS-Basisnetzes in ihren Beacons aussenden oder nicht.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**

Mögliche Werte:

ja
Die APs senden die SSID des AutoWDS-Basisnetzes aus. Das Netz ist für andere WLAN-Clients sichtbar.

nein
Die APs verstecken die SSID des AutoWDS-Basisnetzes. Das Netz ist für andere WLAN-Clients nicht sichtbar.

Default-Wert:

nein

2.37.1.16 AutoWDS-Topology

In dieser Tabelle legen Sie die manuellen Bestandteile der AutoWDS-Topologie fest; genauer gesagt: die P2P-Strecken zwischen den einzelnen Slave-APs und Master-APs. Das Gerät wertet diese Tabelle nur dann aus, wenn sie das manuelle oder semi-automatische *Topologie-Management* aktiviert haben.

Pfad Telnet:

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

2.37.1.16.0 Link-Calibrierung

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Profile** > **AutoWDS-Topologie**

Mögliche Werte:

Standard
Aus
Kapazität
Robustheit

2.37.1.16.1 AutoWDS-Topology

Name des AutoWDS-Profils, für das diese manuelle P2P-Konfiguration gilt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profil**
max. 31 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.37.1.16.2 Priorität

Geben Sie die Priorität einer P2P-Verbindung aus Sicht der physikalischen WLAN-Schnittstelle des Slave-AP an.

Diese Einstellung ist zum gegenwärtigen Zeitpunkt lediglich ein Platzhalter; die Auswertung von Prioritäten ist noch nicht implementiert. Bitte tragen Sie für die Priorität stets den Wert `0` ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295

Default-Wert:

leer

2.37.1.16.3 Slave-AP-Name

Geben Sie den Namen des AP an, der die Rolle des Slaves einnimmt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

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

Default-Wert:

leer

2.37.1.16.4 Slave-AP-WLAN-Ifc.

Definieren Sie die physikalische WLAN-Schnittstelle, die der Slave-AP für die P2P-Strecke zum Master-AP verwendet.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen

Default-Wert:

WLAN-1

2.37.1.16.6 Master-AP-Name

Geben Sie den Namen des AP an, der die Rolle des Masters einnimmt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

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

Default-Wert:

leer

2.37.1.16.7 Master-AP-WLAN-Ifc.

Definieren Sie die physikalische WLAN-Schnittstelle, die der Master-AP für die P2P-Strecke zum Slave-AP verwendet.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen

Default-Wert:

WLAN-1

2.37.1.16.9 Schluessel

Geben Sie optional eine individuelle WPA2-Passphrase für die P2P-Verbindung an. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

min. 8 Zeichen; max. 63 Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Default-Wert:

leer

2.37.1.16.10 Aktiv

Legen Sie fest, ob die P2P-Konfiguration für das gewählte AutoWDS-Profil aktiv oder inaktiv ist.

Der WLC überträgt keine inaktiven P2P-Konfigurationen zum AP und ignoriert inaktive Einträge bei der Auswertung der manuellen AutoWDS-Topology-Tabelle im halbautomatischen Modus.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.37.1.16.12 Slave-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Slave-AP zum Master-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

2.37.1.16.13 Master-Tx-Limit

Begrenzen Sie optional die maximale Übertragungsbandbreite, welche für die P2P-Verbindung in Senderichtung vom Master-AP zum Slave-AP gilt. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 kBit/s

Besondere Werte:

0

Dieser Wert deaktiviert die Bandbreitenbegrenzung.

Default-Wert:

0

2.37.1.16.14 Link-Verlust-Timeout

Definieren Sie die Zeit, nach der ein AP die Verbindung zu seinem P2P-Partner als unterbrochen markiert. Die Einstellung betrifft ausschließlich P2P-Verbindungen, die Sie manuell anlegen. Hat das Gerät eine P2P-Strecke als unterbrochen markiert, beginnt seine physikalische WLAN-Schnittstelle damit, das WLAN nach dem verlorenen P2P-Partner zu scannen.

Der Link-Verlust-Timeout ist unabhängig von den übrigen Timeouts. Es ist empfehlenswert, den Timeout auf mindestens 4 Sekunden zu setzen, um die Gesamtkonnektivität des AutoWDS-Basisnetzes stabil zu halten.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Bei diesem Wert übernimmt der WLC den festgelegten Wert für **Link-Verlust-Timeout** aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.

Default-Wert:

0

2.37.1.16.16 Weiterbetrieb

Definieren Sie die Weiterbetriebszeit der manuellen P2P-Konfiguration.

Die besagte Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät diesen Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt sind, verwirft der AP den betreffenden Konfigurationsteil hingegen sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und die Express-Integration – die *eingestellte Zeit* bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology**

Mögliche Werte:

0 … 9999 Minuten

Besondere Werte:

0

Der AP schaltet seine physikalische(n) WLAN-Schnittstelle(n) unverzüglich ab, sobald der Kontakt zum WLC verloren geht. Dabei löscht das Gerät umgehend seine Konfigurations-Parameter, sodass der WLC sie beim Wiederaufbau der Verbindung erneut übertragen muss.

Wählen Sie diese Einstellung, um die sicherheitsrelevanten Konfigurations-Parameter vor unbefugtem Zugriff und Missbrauch (z. B. im Fall eines Diebstahls des AP) zu schützen.

9999

Die Konfigurations-Parameter bleiben dauerhaft im Gerät gespeichert. Der AP arbeitet weiter; unabhängig davon, wie lange der Kontakt zum WLC verloren geht.

Default-Wert:

0

2.37.1.17 IEEE802.11u

Über die Tabellen und Parameter in diesem Menü nehmen Sie sämtliche Einstellungen für Verbindungen nach IEEE 802.11u und Hotspot 2.0 vor. Über Profile lassen sich diese Einstellungen schließlich den an den WLC angeschlossenen AP zuweisen.

Pfad Telnet:

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

2.37.1.17.1 Netzwerk-Profile

Die Tabelle **Netzwerk-Profile** ist die höchste Verwaltungsebene für 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jedes angelegte Profil ein- oder auszuschalten, Ihnen nachgelagerte Profillisten (wie z. B. für ANQP oder HS20) zuzuweisen oder allgemeine Einstellungen vorzunehmen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.1.1 Name

Über diesen Parameter vergeben Sie einen Namen für das 802.11u-Profil. Dieses Profil weisen Sie anschließend in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile** unter **802.11u-Profil** einem logischen WLAN-Netzwerk zu.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.1.2 Operating

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – respektiv für die dazugehörige SSID – das Interworking-Element in den Beacons/Probes. Dieses Element dient als Erkennungsmerkmal für IEEE 802.11u-fähige Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

2.37.1.17.1.3 Hotspot2.0

Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinformationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

Diese Funktion setzt die aktivierte Unterstützung für Verbindungen nach IEEE 802.11u voraus!

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

2.37.1.17.1.4 Internet

Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

2.37.1.17.1.5 Network-Type

Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

- `Private`: Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.
- `Private-GuestAcc`: Wie `Private`, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B. für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.
- `Public-Charge`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.
- `Public-Free`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.
- `Personal-Dev`: Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.
- `Emergency`: Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.
- `Experimental`: Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.
- `Wildcard`: Platzhalter für bislang undefinierte Netzwerk-Typen.

Default:

Private

2.37.1.17.1.6 Asra

Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und/oder **WISPr** für das Public-Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

ja

nein

Default:

nein

2.37.1.17.1.7 HESSID-Type

Geben Sie an, welche HESSID das Gerät für das homogene ESS an die AP übermittelt.

Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von AP, die alle dem selben Netzwerk angehören. Als weltweit eindeutige Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen AP (seine BSSID) oder die MAC-Adresse des WLCs. Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie "HOTSPOT".

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

- **auto**: Das Gerät generiert für alle AP des betreffenden Netzwerkprofils eine gemeinsame HESSID, basierend auf seiner eigenen MAC-Adresse.
- **user**: Vergeben Sie manuell eine HESSID für alle AP des betreffenden Netzwerkprofils.
- **none**: Die angeschlossenen AP bekommen keine HESSID zugewiesen.

Default:

auto

2.37.1.17.1.8 HESSID-MAC

Sofern Sie als **HESSID-Type** die Einstellung `user` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen AP in Ihrem homogenen ESS oder die MAC-Adresse des WLCs in Großbuchstaben und ohne Trennzeichen, z. B. `008041AEFD7E` für die MAC-Adresse 00:80:41:ae:fd:7e.

Sofern ein AP nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle seine Schnittstellen identisch!

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

MAC-Adresse, in Großbuchstaben und ohne Trennzeichen

Default:

000000000000

2.37.1.17.1.10 ANQP-Profil

Über diesen Parameter spezifizieren Sie ein gültiges ANQP-Profil, das Sie für das 802.11u-Profil verwenden wollen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**, max. 32 Zeichen

Default:

2.37.1.17.1.12 HS20-Profil

Über diesen Parameter spezifizieren Sie ein gültiges Hotspot-2.0- bzw. HS20-Profil, das Sie für das 802.11u-Profil verwenden wollen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**, max. 32 Zeichen

Default:

2.37.1.17.2 ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für IEEE802.11u bzw. ANQP. IEEE802.11u-Profile bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Netzwerk-Profile** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.2.1 Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Diesen Namen geben Sie später in der Tabelle **Netzwerk-Profile** unter **ANQP-Profil** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.2.2 Include-in-Beacon-OUI

Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Additional-OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.2.3 Additional-OUI

Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.2.4 Domain-List

Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B. `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hostpot seines Heimat-Providers, um mögliche Roaming-Kosten über den AP eines Roaming-Partners zu vermeiden.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.2.5 NAI-Realm-List

Geben Sie in diesem Feld ein gültiges NAI-Realm-Profil an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.2.6 Cellular-List

Geben Sie in diesem Feld ein gültiges Mobilfunknetzwerk-Profil an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.2.7 Network-Auth-Type-List

Geben Sie in diesem Feld ein oder mehrere gültiges Authentifizierungs-Parameter an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Network-Authentication-Type**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.3 Hotspot2.0-Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. Hotspot-2.0-Profile bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Netzwerk-Profile** unter **HS20-Profil** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.3.1 Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Diesen Namen geben Sie später in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Netzwerk-Profile** unter **HS20-Profil** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.3.2 Operator-Name

Geben Sie in diesem Feld ein gültiges Profil für den Hotspot-Betreiber an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**, max. 65 Zeichen

Default:

2.37.1.17.3.3 Connection-Capabilities

Geben Sie in diesem Feld einen oder mehrere gültige Einträge aus den Verbindungs-Fähigkeiten an. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status "unbekannt" tragen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Connection-Capability**, max. 250 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.3.4 Operating-Class

Geben Sie hier den Code für die globale Betriebsklasse der verwalteten AP an. Über die Betriebsklasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen ein AP verfügbar ist. Beispiel:

- `81`: Betrieb bei 2,4 GHz mit Kanälen 1–13
- `116`: Betrieb bei 40 MHz mit Kanälen 36 und 44

Die für einen AP passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Hotspot2.0-Profile**

Mögliche Werte:

Betriebsklassen-Code, max. 32 Zeichen

Default:

2.37.1.17.4 Network-Authentication-Type

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Den Namen des Network-Authentication-Type-Profils geben Sie später in der Tabelle **ANQP-Profile** unter **Network-Auth-Type-List** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.4.1 Name

Vergeben Sie hierüber einen Namen für den Tabelleneintrag, z. B. `AGB akzeptieren`.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.4.2 Network-Auth-Type

Wählen Sie aus der Liste den Kontext, vor dem die Weiterleitung gilt.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

- `Accept-Terms-Cond`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.
- `Online-Enrollment`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer erst online registrieren muss.
- `Http-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.
- `DNS-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Default:

Accept-Terms-Cond

2.37.1.17.4.3 Redirect-URL

Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

URL, max. 65 Zeichen

Default:

2.37.1.17.5 Cellular-Network-Information-List

Über diese Tabelle verwalten Sie die Profillisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **ANQP-Profile** einem ANQP-Profil zu.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.5.1 Name

Vergeben Sie hierüber einen Namen für das Mobilfunknetz-Profil, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Diesen Namen geben Sie später in der Tabelle **ANQP-Profile** unter **Cellular-List** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.5.2 Country-Code

Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. 262 für Deutschland.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MCC, max. 3 Zeichen

Default:

2.37.1.17.5.3 Network-Code

Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MNC, max. 32 Zeichen

Default:

2.37.1.17.6 Venue-Name

In diese Tabelle geben Sie allgemeine Informationen zum Standort eines AP ein.

Mit Angaben zu den Standort-Informationen unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.6.1 Name

Tragen Sie einen Namen für den Listeneintrag in der Tabelle ein, über den Sie auf die angelegten Standortinformationen aus anderen Tabellen referenzieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 65 Zeichen

Default:

2.37.1.17.6.2 Language

Wählen Sie hier die Sprache aus, in der Sie die Informationen zum Standort hinterlegen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

Keine

Englisch

Deutsch

Chinesisch

Spanisch

Franzoesisch

Italienisch

Russisch

Niederlaendisch

Tuerkisch

Portugiesisch

Polnisch

Tschechisch

Arabisch

Default:

Keine

2.37.1.17.6.3 Venue-Name

Tragen Sie für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 65 Zeichen

Default:

2.37.1.17.7 NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt

der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **ANQP-Profile** einem ANQP-Profil zu.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.7.1 Name

Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Diesen Namen geben Sie später in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **ANQP-Profile** unter **NAI-Realm-List** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.7.2 NAI-Realm

Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in IETF RFC 2486 definiert und entspricht im einfachsten Fall `<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.7.3 EAP-Method

Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

- `Kein`: Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.
- `EAP-TLS`: Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installieren muss.
- `EAP-SIM`: Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.

- EAP-TTLS: Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.
- EAP-AKA: Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.

Default:

Kein

2.37.1.17.7.4 Auth-Parameter-List

Geben Sie in das Feld die zur EAP-Methode passenden Authentifizierungs-Parameter durch eine kommaseparierte Liste ein, z. B. für EAP-TTLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` oder für EAP-TLS `Credentials.Certificate`.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Auth-Parameter**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.37.1.17.8 Operator-List

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.8.1 Name

Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.8.2 Language

Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**

Mögliche Werte:

Keine
Englisch
Deutsch
Chinesisch
Spanisch
Franzoesisch
Italienisch
Russisch
Niederlaendisch
Tuerkisch
Portugiesisch
Polnisch
Tschechisch
Arabisch

Default:

Keine

2.37.1.17.8.3 Operator-Name

Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Operator-List**

Mögliche Werte:

String, max. 65 Zeichen

Default:

2.37.1.17.9 General

Über diese Tabelle verwalten Sie die allgemeinen Einstellungen für IEEE 802.11u/Hotspot 2.0.

Auf einem Standalone AP liegen diese Einstellungen in Form separater Parameter vor. Auf einem WLC sind diese Parameter in Tabellen zusammengefasst, die Sie den verwalteten AP anschließend über das WLAN-Profil (Tabelle **Gesamtprofile**) zuweisen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.9.1 Name

Vergeben Sie hierüber einen Namen für das Profil der allgemeinen Einstellungen. Diesen Namen geben Sie später in der Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile** unter **Hotspot2.0-General** an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.37.1.17.9.2 Link-Status

Über diesen Eintrag geben Sie den Konnektivitäts-Status Ihres Gerätes mit dem Internet an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

- `Auto`: Das Gerät ermittelt den Statuswert für diesen Parameter automatisch.
- `Link-Up`: Die Verbindung zum Internet ist herstellt.
- `Link-Down`: Die Verbindung zum Internet ist unterbrochen.
- `Link-Test`: Die Verbindung zum Internet befindet sich im Aufbau oder wird geprüft.

Default:

Auto

2.37.1.17.9.3 Downlink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Empfangs-Bandbreite (Downlink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

2.37.1.17.9.4 Uplink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Sende-Bandbreite (Uplink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

2.37.1.17.9.5 IPv4-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv4 erhält.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

Not-Available

IPv4-Adresstyp ist nicht verfügbar.

Public-Addr-Available

Öffentliche IPv4-Adresse ist verfügbar.

Port-Restr-Addr-Avail

Port-beschränkte IPv4-Adresse ist verfügbar.

Single-Nat-Priv-Addr-Avail

Private, einfach NAT maskierte IPv4-Adresse ist verfügbar.

Double-Nat-Priv-Addr-Avail

Private, doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Single-Nat-Addr-Avail

Port-beschränkte IPv4-Adresse und einfach NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Double-Nat-Addr-Avail

Port-beschränkte IPv4-Adresse und doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Availability-not-known

Die Verfügbarkeit eines IPv4-Adresstyps ist unbekannt.

Default:

Single-Nat-Priv-Addr-Avail

2.37.1.17.9.6 IPv6-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv6 erhält.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

Not-Available

IPv6-Adresstyp ist nicht verfügbar.

Available

IPv6-Adresstyp ist verfügbar.

Availability-not-known

Die Verfügbarkeit eines IPv6-Adresstyps ist unbekannt.

Default:

Not-Available

2.37.1.17.9.7 Venue-Group

Die Standort-Gruppe (Venue Group) beschreibt das Umfeld, in dem Sie den AP einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den Venue Group Code, werden vom 802.11u-Standard vorgegeben.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

- `Unspecified`: Unspezifiziert
- `Assembly`: Versammlung
- `Business`: Geschäft
- `Educational`: Ausbildung
- `Factory-and-Industrial`: Fabrik und Industrie
- `Institutional`: Institutional
- `Mercantile`: Handel
- `Resindential`: Wohnheim
- `Storage`: Lager
- `Utility-and-Miscellaneous`: Dienste und sonstiges
- `Vehicular`: Fahrzeug
- `Outdoor`: Außen

Default:

Unspecified

2.37.1.17.9.8 Venue-Type

Über den Standort-Typ-Code (Venue-Type) haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

Tabelle 12: Übersicht möglicher Werte für Standort-Gruppen und -Typen

Standort-Gruppe	Code = Standort-Typ-Code
Unspezifiziert	
Versammlung	■ 0 = Unspezifizierte Versammlung ■ 1 = Bühne ■ 2 = Stadion ■ 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) ■ 4 = Amphitheater ■ 5 = Vergnügungspark ■ 6 = Andachtsstätte ■ 7 = Kongresszentrum ■ 8 = Bücherei ■ 9 = Museum ■ 10 = Restaurant ■ 11 = Schauspielhaus ■ 12 = Bar

Standort-Gruppe	Code = Standort-Typ-Code
	■ 13 = Café ■ 14 = Zoo, Aquarium ■ 15 = Notfallleitstelle
Geschäft	■ 0 = Unspezifiziertes Geschäft ■ 1 = Arztpraxis ■ 2 = Bank ■ 3 = Feuerwache ■ 4 = Polizeiwache ■ 6 = Post ■ 7 = Büro ■ 8 = Forschungseinrichtung ■ 9 = Anwaltskanzlei
Ausbildung	■ 0 = Unspezifizierte Ausbildung ■ 1 = Grundschule ■ 2 = Weiterführende Schule ■ 3 = Hochschule
Fabrik und Industrie	■ 0 = Unspezifizierte Fabrik und Industrie ■ 1 = Fabrik
Institutional	■ 0 = Unspezifizierte Institution ■ 1 = Krankenhaus ■ 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) ■ 3 = Entzugsklinik ■ 4 = Einrichtungsverbund ■ 5 = Gefängnis
Handel	■ 0 = Unspezifizierter Handel ■ 1 = Ladengeschäft ■ 2 = Lebensmittelmarkt ■ 3 = KFZ-Werkstatt ■ 4 = Einkaufszentrum ■ 5 = Tankstelle
Wohnheim	■ 0 = Unspezifiziertes Wohnheim ■ 1 = Privatwohnsitz ■ 2 = Hotel oder Motel ■ 3 = Studentenwohnheim ■ 4 = Pension
Lager	■ 0 = Unspezifiziertes Lager
Dienste und sonstiges	■ 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	■ 0 = Unspezifiziertes Fahrzeug ■ 1 = Personen- oder Lastkraftwagen ■ 2 = Flugzeug ■ 3 = Bus ■ 4 = Fähre ■ 5 = Schiff oder Boot ■ 6 = Zug ■ 7 = Motorrad
Außen	■ 0 = Unspezifizierter Außenbereich

Standort-Gruppe	Code = Standort-Typ-Code
	■ 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) ■ 2 = Stadtpark ■ 3 = Rastplatz ■ 4 = Verkehrsregelung ■ 5 = Bushaltestelle ■ 6 = Kiosk

Default:

0

2.37.1.17.9.9 Venue-Name

Geben Sie in diesem Feld einen oder mehrere gültige Listeneinträge aus der Tabelle **Venue-Name** an, welche den Standort des Gerätes spezifizieren. Dabei erfasst der Parameter alle Listeneinträge, die dem hier angegebenem Vanue-Namen entsprechen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **General**

Mögliche Werte:

Name aus Tabelle **Setup** > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Venue-Name**, max. 32 Zeichen. Mehrere Namen trennen Sie durch eine mit rautenseparierte ('#') Liste.

Default:

2.37.1.17.10 Auth-Parameter

Diese Tabelle beinhaltet eine festgelegte Liste der möglichen Authentifizierungsparameter für die NAI-Realms, auf die Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** als kommaseparierte Liste referenzieren.

Tabelle 13: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im RFC 1994
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im RFC 2433
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im RFC 2759
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort

Parameter	Sub-Parameter	Erläuterung
TunnelEAPCredentials.*	None	Keine Zugangsdaten erforderlich
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

*) Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.10.1 Name

Dieser Eintrag zeigt den Namen des Authentifizierungsparameters, auf den Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** als kommaseparierte Liste referenzieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Auth-Parameter**

2.37.1.17.11 Connection-Capability

Diese Tabelle beinhaltet eine festgelegte Liste der Verbindungsfähigkeiten, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** als kommaseparierte Liste referenzieren. Mögliche Statuswerte für die einzelnen Dienste sind 'closed' (**-C**), 'open' (**-O**) oder 'unknown' (**-U**).

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u**

2.37.1.17.11.1 Name

Dieser Eintrag zeigt den Namen der Verbindungsfähigkeit, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** als kommaseparierte Liste referenzieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **IEEE802.11u** > **Connection-Capability**

2.37.1.18 Konfig-Zuweisungs-Gruppen

Diese Tabelle enthält die Zuweisungs-Gruppen, anhand derer der WLC hinzukommenden APs automatisch eine Netzkonfiguration, ein WLAN-Profil und ein Client-Steering-Profil zuweist. Dazu definieren Sie für die einzelnen Zuweisungs-Gruppen je einen IP-Adressbereich, in dem die betreffende Gruppe greift. Auf diese Weise haben Sie z. B. in einem zentral gemanagten WLAN die Möglichkeit, anhand des Adressbereiches hinzukommenden APs automatisch eine standortspezifische Konfiguration (z. B. Filiale-A, Filiale-B, etc.) zuzuweisen.

Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt LCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

Achten Sie darauf, dass in der AP-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

Pfad Telnet:

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

2.37.1.18.1 Name

Name der Zuweisungs-Gruppe, auf die Sie aus anderen Tabellen referenzieren.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.18.2 Profil

Name des WLAN-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zuweist.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

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

Default-Wert:

leer

2.37.1.18.3 AP-Intranet

Name des IP-Parameter-Profils, das der WLC über die Zuweisungs-Gruppe einem hinzukommenden AP automatisch zuweist.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **AP-Intranets**

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

Besondere Werte:

DHCP

Der AP bezieht seine Netzkonfiguration über DHCP.

Default-Wert:

leer

2.37.1.18.4 IPv4-Referenz-Pool-Start

Anfang des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

2.37.1.18.5 IPv4-Referenz-Pool-Ende

Ende des IPv4-Adressbereichs, in dem die betreffende Zuweisungs-Gruppe greift. Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

2.37.1.18.6 Client-Steering-Profil

Client-Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **Client-Steering** > **Profile**

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

Default-Wert:

leer

2.37.1.18.7 iBeacon-Profile

Tragen Sie hier das auf dem Gerät konfigurierte iBeacon-Profil ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Konfig-Zuweisungs-Gruppen**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.20 Tag-Gruppen

Diese Tabelle enthält die Tag-Gruppen, die der WLC automatisch den einem WLAN-Profil angehörigen APs zuweist. Anhand von Tag-Gruppen haben Sie die Möglichkeit, z. B. Aktionen, die Sie auf dem WLC ausführen, auf eine bestimmte Auswahl von APs zu beschränken.

Pfad Telnet:

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

2.37.1.20.1 Name

Über diesen Parameter definieren Sie den Namen des anzulegenden des Tags.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Tag-Gruppen**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.21 LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie hier entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.

Pfad Telnet:

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

2.37.1.21.1 Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

2.37.1.21.4 LED-Modus

Bestimmen Sie hier die LED-Betriebsart.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

An
Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Aus
Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Zeitgesteuert-Aus
Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustartes auf kritische Fehler hinweisen.

Default-Wert:

An

2.37.1.21.5 LED-Ausschalten-Sekunden

In der Betriebsart **Verzögert aus** können Sie hier die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll. Das ist dann hilfreich, wenn die LEDs während des Neustartes auf kritische Fehler hinweisen.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

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

Default-Wert:

300

2.37.1.22 LBS

Konfigurieren Sie hier die Einstellungen für die LANCOM Location Based Services (LBS).

Pfad Telnet:

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

2.37.1.22.1 Allgemein

In diesem Verzeichnis konfigurieren Sie die allgemeinen Einstellungen für die LANCOM Location Based Services (LBS).

Pfad Telnet:

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

2.37.1.22.1.1 Name

Geben Sie hier eine Beschreibung des Gerätes ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.37.1.22.1.2 Aktiv

Aktiviert oder deaktiviert die ortsbasierten Dienste.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.37.1.22.1.3 TLS-Verbindung-Verwenden

Diese Einstellung legt fest, ob die Verbindung zur LBSEngine SSL/TLS-gesichert ist.

Das Gerät übernimmt eine Änderung nicht im laufenden Betrieb, sondern erst nach einer erneuten Aktivierung der LBS.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

ja
nein

2.37.1.22.1.4 LBS-Server-Adresse

Geben Sie hier die Adresse des LBS-Servers ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.22.1.5 LBS-Server-Port

Geben Sie hier den Port des LBS-Servers ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

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

Default-Wert:

9090

2.37.1.22.2 Device-Location

In dieser Tabelle bestimmen Sie die Standortkoordinaten des Gerätes. Die Angabe erfolgt im geographischen Koordinatensystem (Grad, Minute, Sekunde, Orientierung).

Pfad Telnet:

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

2.37.1.22.2.1 Name

Geben Sie hier eine Beschreibung des Gerätes ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.37.1.22.2.2 Etage

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

2.37.1.22.2.3 Hoehe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

2.37.1.22.2.4 Breitengrad

Dieser Wert gibt den Winkel des Breitengrades in Grad an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

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

0 … 90

Default-Wert:

0

2.37.1.22.2.5 Breitengrad-Minuten

Dieser Wert gibt die Minute des Breitengrades an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

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

0 … 60

Default-Wert:

0

2.37.1.22.2.6 Breitengrad-Sekunden

Dieser Wert gibt die Sekunde des Breitengrades an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

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

0 … 60

Default-Wert:

0

2.37.1.22.2.7 Breitengrad-Hemisphaere

Dieser Wert gibt die Orientierung des Breitengrades (Latitude) an. Mögliche Werte sind:

- N: nördliche Breite
- S: südliche Breite

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

N
S

Default-Wert:

N

2.37.1.22.2.8 Laengengrad

Dieser Wert gibt den Winkel des Längengrades in Grad an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`
0 … 90

Default-Wert:

0

2.37.1.22.2.9 Laengengrad-Minuten

Dieser Wert gibt die Minute des Längengrades an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`
0 … 60

Default-Wert:

0

2.37.1.22.2.10 Laengengrad-Sekunden

Dieser Wert gibt die Sekunde des Längengrades an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

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

0 … 60

Default-Wert:

0

2.37.1.22.2.8 Laengengrad-Hemisphaere

Dieser Wert gibt die Orientierung des Längengrades (Longititude) an. Mögliche Werte sind:

- W: Westliche Länge
- O: Östliche Länge

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

O
W

Default-Wert:

W

2.37.1.22.2.12 Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.37.1.23 Wireless-ePaper-Profile

Pfad Telnet:

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

2.37.1.23.1 Name

Geben Sie hier den Namen des Wireless ePaper-Profils an.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-ePaper-Profile**

Mögliche Werte:

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

Default-Wert:

DEFAULT

2.37.1.23.2 Aktiv

Legen Sie fest, ob das gewählte Wireless ePaper-Profil aktiv oder inaktiv ist. Inaktive Profile überträgt der WLC nicht zu einem AP.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-ePaper-Profile**

Mögliche Werte:

nein

Das gewählte Wireless ePaper-Profil ist nicht aktiv.

ja

Das gewählte Wireless ePaper-Profil ist aktiv.

Default-Wert:

ja

2.37.1.23.3 Port

Tragen Sie den für das Wireless ePaper-Modul verwendeten Port ein.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Wireless-ePaper-Profile**

Mögliche Werte:

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

1 … 65535 Integer-Wert

Default-Wert:

7353

2.37.1.24 iBeacon-Profile

Pfad Telnet:

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

2.37.1.24.1 Name

Geben Sie hier den Namen des iBeacon-Profils an, das an die APs übermittelt werden soll.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **iBeacon-Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.37.1.24.2 Aktiv

Legen Sie fest, ob das gewählte iBeacon-Profil aktiv oder inaktiv ist. Inaktive Profile überträgt der WLC nicht zu einem AP

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **iBeacon-Profile**

Mögliche Werte:

nein

Das gewählte iBeacon-Profil ist nicht aktiv.

ja

Das gewählte iBeacon-Profil ist aktiv.

Default-Wert:

nein

2.37.1.24.3 Major

Geben Sie die eindeutige Major-ID des iBeacon-Profils an, die der WLC an die APs übertragen soll.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **iBeacon-Profile**

Mögliche Werte:

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

Default-Wert:

0

2.37.1.24.4 UUID

Geben Sie hier den "Universally Unique Identifier" (UUID) des iBeacon-Modul an, der an die APs übertragen werden soll.

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **iBeacon-Profile**

Mögliche Werte:

max. 36 Zeichen aus `[0-9][a-f][A-F]-`

Default-Wert:

00000000-0000-0000-0000-000000000000

2.37.5 CAPWAP-Port

Port-Nummer für den CAPWAP Dienst

SNMP-ID: 2.37.5

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- 0 bis 65535

Default: 1027

Nicht per LANconfig konfigurierbar

2.37.6 AP-automatisch-einbinden

Ermöglicht dem WLC, allen neuen AP eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

Ermöglicht dem WLC, allen neuen AP ohne gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

- Für den AP ist unter seiner MAC-Adresse eine Konfiguration in der AP-Tabelle eingetragen.

- Die Option 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.

SNMP-ID: 2.37.6

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- Ja
- Nein

Default: Nein

Mit der Kombination der Einstellungen für Auto-Accept und Default-Konfiguration können Sie verschiedene Situationen für die Einrichtung und den Betrieb der AP abdecken:

Auto-Accept EIN, Default-Konfiguration EIN: Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn keine AP unkontrolliert mit dem LAN verbunden werden können und so unbeabsichtigt in die WLAN-Struktur aufgenommen werden.

Auto-Accept EIN, Default-Konfiguration AUS: Kontrollierte Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie alle erlaubten AP mit ihrer MAC-Adresse in die AP-Tabelle eingetragen haben und diese automatisch in die WLAN-Struktur aufgenommen werden sollen.

Auto-Accept AUS, Default-Konfiguration AUS: Normalbetrieb: Es werden keine neuen AP ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

2.37.7 AP-einbinden

Über diese Aktion veranlassen Sie die Einbindung eines neuen APs. Je nach Firmware-Stand Ihres Gerätes akzeptiert die Aktion unterschiedliche Argumente. Die Angabe einer MAC-Adresse ist in jedem Fall erforderlich; die Angabe weiterer Argumente hingegen ist optional.

Syntax in Versionen vor LCOS 9.00

```
[-c] <WTP-MAC> [<Profile>] [<Name>] [<IP>] [<Netmask>] [<Gateway>]
```

Syntax in Versionen nach LCOS 9.00

```
<WTP-MAC> [<WTP-MAC-2> … <WTP-MAC-n> ] [-c] [-l <Location>] [-p <Profile>] [-i
<IP>]
[-n <Name>] [-m <Netmask>] [-g <Gateway>] [-1 <Wlan1Channels>] [-2 <Wlan2Channels>]
```

Sofern Sie mehrere MAC-Adressen definieren, ignoriert das Gerät die Argumente `[-i <IP>]` und `[-n <Name>]`.

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Argumente:

-c

Der WLC generiert keinen Konfigurationseintrag für den AP.

-l <Location>

Der WLC ergänzt die AP-Konfiguration um den angegeben Standort.

Es wird empfohlen, die Ortsangaben als eindeutiges Feld-Werte-Paar im Gerät zu hinterlegen, um z. B. an der Konsole die Filterfunktion im LCOS nutzen zu können. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

-p <Profile>

Der WLC ergänzt die AP-Konfiguration um das angegebene WLAN-Profil.

-i <IP>

Der WLC ergänzt die AP-Konfiguration um die angegeben IPv4-Adresse.

-n <Name>

Der WLC ergänzt die AP-Konfiguration um die angegebene Gerätebezeichnung.

-m <Netmask>

Der WLC ergänzt die AP-Konfiguration um die angegeben Netzmaske.

-g <Gateway>

Der WLC ergänzt die AP-Konfiguration um die angegeben Gateway-Adresse (IPv4).

-1 <Wlan1Channels>

Der WLC ergänzt die AP-Konfiguration um die 1. Kanalliste.

-2 <Wlan2Channels>

Der WLC ergänzt die AP-Konfiguration um die 2. Kanalliste.

2.37.8 Defaultkonfiguration-verwenden

Ermöglicht dem WLC, allen neuen AP (also ohne gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der WLC alle im LAN gefundenen AP im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLC verwalteten AP).

SNMP-ID: 2.37.8

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- Ja
- Nein

Default: Nein

Mit dieser Option können möglicherweise auch unbeabsichtigte AP in die WLAN-Struktur aufgenommen werden. Daher sollte diese Option nur während der Startphase bei der Einrichtung einer zentral verwalteten WLAN-Struktur aktiviert werden.

2.37.9 AP-Verbindung-trennen

Do-Kommando zum Trennen von Aps. Als Parameter muss die MAC-Adresse angegeben werden.

SNMP-ID: 2.37.9

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- Syntax: do AP-Verbindung-trennen <WTP-MAC>

Default: leer

2.37.10 Benachrichtigung

Dieses Menü enthält die Konfiguration des Benachrichtungs-Systems des WLAN-Managements.

SNMP-ID: 2.37.10

Pfad Telnet: /Setup/WLAN-Management

2.37.10.1 E-Mail

Aktiviert die Benachrichtigung über E-Mail.

SNMP-ID: 2.37.10.1

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.37.10.2 Syslog

Aktiviert die Benachrichtigung über SYSLOG.

SNMP-ID: 2.37.10.2

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.37.10.3 E-Mail-Empfaenger

An diese E-Mail-Adresse werden die Benachrichtigungen über die Ereignisse im WLC gesendet.

SNMP-ID: 2.37.10.3

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung

Mögliche Werte:

- Gültige E-Mail-Adresse bis zu 63 ASCII-Zeichen

Default: Leer

Zur Nutzung der Benachrichtigung über E-Mail muss ein SMTP-Konto eingerichtet sein.

2.37.10.4 Erweitert

Hier definieren Sie, über welche Ereignisse Sie informiert werden möchten.

SNMP-ID: 2.37.10.4

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung

2.37.10.4.1 Name

Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll.

SNMP-ID: 2.37.10.4.1

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung/Erweitert

Mögliche Werte:

- E-Mail
- Syslog

Default: leer

Besondere Werte: Wert ist Fix

2.37.10.4.2 Aktive-Radios

Aktiviert die Benachrichtigung über aktive AP.

SNMP-ID: 2.37.10.4.2

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung/Erweitert

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.37.10.4.3 Fehlende-AP

Aktiviert die Benachrichtigung über verlorene AP.

SNMP-ID: 2.37.10.4.3

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung/Erweitert

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.37.10.4.4 Neue-AP

Aktiviert die Benachrichtigung über neue AP.

SNMP-ID: 2.37.10.4.4

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung/Erweitert

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.37.10.5 Sende-SNMP-Trap-fuer-Stationstabellenereignis

Geben Sie hier an, wann Sie über Ereignisse bezüglich der Einträge der Stationstabelle informiert werden.

Pfad Telnet: /Setup/WLAN-Management/Benachrichtigung/Sende-SNMP-Trap-fuer-Stationstabellenereignis

Mögliche Werte:

- Hinzufuegen/loeschen_eines_Eintrags
- alle_Ereignisse

Default: Hinzufuegen/loeschen_eines_Eintrags

2.37.19 Starte-automatische-Funkfeldoptimierung

automatisch Funktfeldoptimierung starten. Optional kann die Optimierung auf eine AP eingeschränkt werden, indem man dessen MAC-Adresse als Parameter angibt.

SNMP-ID: 2.37.19

Pfad Telnet: /Setup/WLAN-Management

Mögliche Werte:

- Syntax: do Starte-automatische-Funkfeldoptimierung [<WTP-MAC>]

Default: leer

2.37.21 Zugriffsregeln

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder gezielt bestimmte Stationen freischalten.

Pfad Telnet:

Setup > **WLAN-Management**

2.37.21.1 MAC-Adress-Muster

Geben Sie hier die MAC-Adresse einer Station ein.

Die Verwendung von Wildcards ist möglich.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Mögliche Argumente:

MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

2.37.21.2 Name

Sie können zu jeder Station einen beliebigen Namen eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

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

2.37.21.3 Kommentar

Sie können zu jeder Station einen beliebigen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

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

2.37.21.4 WPA-Passphrase

Hier können Sie optional für jeden Eintrag eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

Bei WEP-gesicherten Netzwerken hat dieses Feld keine Bedeutung.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

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

2.37.21.5 Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.37.21.6 Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.37.21.7 VLAN-Id

Das Gerät weist diese VLAN-ID den Paketen zu, die der WLAN-Client mit der eingetragenen MAC-Adresse empfängt.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

0 … 4096

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

2.37.21.9 SSID-Muster

Dieser Eintrag reduziert oder erlaubt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen für diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Besondere Werte:

*****
Platzhalter für beliebig viele Zeichen

?
Platzhalter für genau ein Zeichen

Default-Wert:

leer

2.37.27 Zentrales-Firmware-Management

Dieses Menü enthält die Konfiguration des zentralen Firmware-Managements.

SNMP-ID: 2.37.27

Pfad Telnet: /Setup/WLAN-Management

2.37.27.11 Firmware-Depot-URL

Verzeichnis, in dem die aktuellen Firmware-Dateien liegen

SNMP-ID: 2.37.27.11

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- URL in der Form Server/Verzeichnis oder http://Server/Verzeichnis

Default: Leer

2.37.27.12 Script-Depot-URL

Pfad zum Verzeichnis mit den Skript-Dateien.

SNMP-ID: 2.37.27.12

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- URL in der Form Server/Verzeichnis oder http://Server/Verzeichnis

Default: Leer

2.37.27.13 Aktualisiere-Firmware-und-Skript-Information

Startet einen Update-Prozess über die verfügbaren Firmware- und Script-Informationen

SNMP-ID: 2.37.27.13

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- Syntax: do Aktualisiere-Firmware-und-Skript-Information

Do-Commando

2.37.27.14 Maximale-Anzahl-geladener-Firmwares

Maximale Anzahl der Firmwareversionen im Speicher.

SNMP-ID: 2.37.27.14

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- 1 bis 10

Default: 5

2.37.27.15 Firmware-Versionsverwaltung

Tabelle mit Gerätetyp, MAC-Adresse und Firmware-Version zur gezielten Steuerung der verwendeten Firmware-Dateien.

SNMP-ID: 2.37.27.15

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

2.37.27.15.2 Geraet

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

SNMP-ID: 2.37.27.15.2

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

Mögliche Werte:

- Alle bzw. Auswahl aus der Liste der verfügbaren Gerätetypen.

Default: Alle-Geraete

2.37.27.15.3 MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

SNMP-ID: 2.37.27.15.3

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

Mögliche Werte:

- Gültige MAC-Adresse

Default: Leer

2.37.27.15.4 Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll.

SNMP-ID: 2.37.27.15.4

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management/Firmware-Versionsverwaltung

Mögliche Werte:

- Firmware-Version in der Form X.XX

Default: Leer

2.37.27.15.5 Datum

Datum der entsprechenden Firmware-Version.

Pfad Telnet:

Setup > **WLAN-Management** > **Zentrales-Firmware-Management** > **Firmware-Versionsverwaltung**

Mögliche Werte:

max. 8 Zeichen aus `[0-9]`

Default-Wert:

Entspricht dem UPX-Header der Firmware (z. B. "01072014" für den 01.07.2014)

2.37.27.16 Skriptverwaltung

Tabelle mit Skript-Dateiname und WLAN-Profil zur Zuordnung der Skripte zu einem WLAN-Profil.

Die Konfiguration eines Wireless Routers und APs in der Betriebsart „Managed" erfolgt über WLAN-Profile. Mit einem Skript können auch diejenigen Detail-Parameter der gemanagten Geräte eingestellt werden, die nicht im Rahmen der vorgegebenen Parameter eines WLAN-Profils verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über die WLAN-Profile, um für die Wireless Router und APs mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

Da für jedes WLAN-Profil nur eine Skript-Datei angegeben werden kann, ist hier keine Versionierung möglich. Bei der Zuweisung eines Skripts zu einem Wireless Router oder AP wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLC bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen daher feststellen, ob die Skript-Datei erneut übertragen werden muss.

SNMP-ID: 2.37.27.16

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

2.37.27.16.1 Profil

Wählen Sie hier aus, für welches WLAN-Profil die in diesem Eintrag spezifizierte Skript-Datei verwendet werden soll.

SNMP-ID: 2.37.27.16.1

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management/Skriptverwaltung

Mögliche Werte:

- Auswahl aus der Liste der definierten WLAN-Profile, maximal 31 ASCII-Zeichen

Default: Leer

2.37.27.16.2 Name

Name der zu verwendenen Skript-Datei.

SNMP-ID: 2.37.27.16.2

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management/Skriptverwaltung

Mögliche Werte:

- Dateiname in der Form *.lcs, maximal 63 ASCII-Zeichen

Default: Leer

2.37.27.18 Aktualisierte-APs-neustarten

Reboot bei upgedateten Aps durchführen.

SNMP-ID: 2.37.27.18

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- Syntax: do Aktualisierte-APs-neustarten

Do-Commando

2.37.27.25 Firmware-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

SNMP-ID: 2.37.27.25

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

Default: Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

2.37.27.26 Skript-Loopback-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

SNMP-ID: 2.37.27.26

Pfad Telnet: /Setup/WLAN-Management/Zentrales-Firmware-Management

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

Default: Leer

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, wird die zugehörige IP-Adresse verwendet.

2.37.27.38 Max.-Anzahl-gleichzeitiger-Updates

Geben Sie hier an, wie viele Firmware Updates der WLC gleichzeitig durchführen darf.

Pfad Telnet:

Setup > **WLAN-Management** > **Zentrales-Firmware-Management**

Mögliche Werte:

1-30
10

Default-Wert:

10

2.37.29 Erlaube-WAN-Verbindungen

Um bei CAPWAP-Anfragen von unbekannten WAN-Gegenstellen diesen APs nicht versehentlich eine Default-Konfiguration mit internen Netzwerkeinstellungen zuzuweisen, konfigurieren Sie hier, wie der WLC mit solchen Anfragen aus dem WAN umgehen soll.

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

Ja

Der WLC übernimmt einen über WAN anfragenden AP in die AP-Verwaltung und übergibt bei entsprechender Einstellung eine Default-Konfiguration.

VPN

Der WLC übernimmt einen über WAN anfragenden AP in die AP-Verwaltung und übergibt bei entsprechender Einstellung eine Default-Konfiguration, wenn die WAN-Verbindung über einen VPN-Tunnel besteht.

Nein

Der WLC übernimmt einen über WAN anfragenden AP nicht in die AP-Verwaltung.

Default-Wert:

Nein

2.37.30 WTP-Password-synchron-halten

Bei Aktivierung dieser Funktion wird das Haupt-Geräte-Passwort des AP bei jeder Anmeldung gesetzt, um dieses synchron zum Passwort des WLCs zu halten. Ist die Funktion deaktiviert, wird das Haupt-Geräte-Passwort nur dann gesetzt, wenn im AP bei der Anmeldung kein Passwort gesetzt ist. Ein einmal gesetztes Passwort wird niemals überschrieben.

SNMP-ID: 2.37.30

Pfad Telnet: /Setup/WLAN-Management/WTP-Password-synchron-halten

Mögliche Werte:

- ja
- nein

Default: ja

2.37.31 Intervall-zur-Bereinigung-der-Statustabellen

Der WLC bereinigt regelmäßig die Statustabellen des Background-Scans und der gesehenen WLAN-Clients. Bei einem solchen Durchlauf entfernt der WLC alle Einträge, die älter als das hier eingetragene Intervall in Minuten sind.

Pfad Telnet: /Setup/WLAN-Management/Intervall-zur-Bereinigung-der-Statustabellen

Mögliche Werte:

- maximal 11 numerische Zeichen

Default: 1440 Minuten

2.37.32 Lizenzzahl

Dieser Wert zeigt die aktuelle Anzahl von Lizenzen für den WLC, die Sie auf diesem Gerät nutzen können.

SNMP-ID: 2.37.32

Pfad Telnet: /Setup/WLAN-Management/Lizenzzahl

Dieser Wert dient nur zu Ihrer Information, Sie können diesen Wert nicht verändern.

2.37.33 Lizenzlimit

Dieser Wert zeigt die maximal mögliche Anzahl von Lizenzen für den WLC, die Sie auf diesem Gerät nutzen können.

Pfad Telnet: /Setup/WLAN-Management/Lizenzlimit

Dieser Wert dient nur zu Ihrer Information, Sie können diesen Wert nicht verändern.

2.37.34 WLC-Cluster

Dieses Menü enthält die Einstellungen für die Datenverbindungen und Statusverbindungen zwischen mehreren WLCs (WLC-Cluster).

Pfad Telnet:

Setup > **WLAN-Management**

2.37.34.2 WLC-Daten-Tunnel-aktiviert

Mit dieser Option aktivieren oder deaktivieren Sie die Nutzung von Daten-Tunneln (L3-Tunneln) zwischen mehreren WLCs. Dies erlaubt Ihnen, ein transparentes Layer-2-Netz als Overlay-Netz über die Remote-WLCs auszudehnen.

Achten Sie darauf, die betreffenden WLC-Tunnel niemals zu bridgen, wenn sich die einzelnen WLCs in der selben Broadcastdomäne befinden. Andernfalls erzeugen Sie eine Schleife (Switching-Loop), die Ihr Netz durch Überlastung umgehend lahmlegt.

Um den Datendurchsatz und die Performanz des Netzes zu maximieren, leiten Sie den über die APs stattfindenden Datenverkehr direkt ins LAN weiter. In diesem Fall sind keine L3-Tunnel zwischen den WLCs notwendig, auch wenn diese in unterschiedlichen Layer-2-Netzen stehen.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Werte:

ja

Der WLC baut die Verbindung zu Remote-WLCs als L3-Tunnel auf.

nein

Der WLC baut die Verbindung zu Remote-WLCs nicht als L3-Tunnel auf.

Default-Wert:

nein

2.37.34.3 Statische WLC Liste

In dieser Tabelle hinterlegen Sie die statischen IPv4-Adressen der Remote-WLCs, zu denen Ihr WLC eine Verbindung aufbaut. Alternativ lässt sich die Tabelle auch dazu nutzen, um die von der **WLC-Discovery**-Tabelle praktizierte Suche im lokalen Netz zu umgehen.

Wenn Sie einen Remote-WLC über eine statische IPv4-Adresse an Ihren WLC anbinden, baut Ihr WLC zunächst einen Kontroll-Tunnel zu dieser Gegenstelle auf. Wenn Sie die Option für den Daten-Tunnel aktiviert haben, baut Ihr WLC anschließend automatisch einen Daten-Tunnel zu dieser Gegenstelle auf.

Die betreffenden WLCs können nur dann eine Verbindung zueinander aufbauen, wenn die Geräte über ein Zertifikat aus der gleichen Zertifikatshierarchie verfügen.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

2.37.34.3.1 IP-Adresse

Definieren Sie hier die IPv4-Adresse des Remote-WLCs, zu dem Ihr WLC eine Verbindung aufbaut.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische WLC Liste**

Mögliche Werte:

0.0.0.0 … 255.255.255.255

Default-Wert:

leer

2.37.34.3.2 Loopback-Addr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem Remote-WLC als Absender auftritt.

Standardmäßig verwendet Ihr Gerät seine Adresse aus dem jeweiligen ARF-Kontext, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der Ihr Gerät die Gegenstelle anspricht. Dies kann z. B. dann sinnvoll sein, falls Ihr Gerät über verschiedene Wege erreichbar ist und die Gegenstelle einen bestimmten Weg für ihre Antwort-Nachrichten wählen soll.

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

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische WLC Liste**

Mögliche Werte:

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

Besondere Werte:

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

Wenn in der Liste der IP-Netze oder in der Liste der Loopback-Adressen eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen die zugehörige IP-Adresse!

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

Default-Wert:

leer

2.37.34.3.3 Port

Definieren Sie den Port, über den Ihr WLC einen Daten-Tunnel zum Remote-WLC aufbaut.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **Statische-WLC-Liste**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Das Gerät verwendet Default-Port 1027.

Default-Wert:

0

2.37.34.4 WLC-Discovery

Über diese Tabelle schalten Sie für einzelne IPv4-Netze die automatische Suche nach WLCs, die sich im selben lokalen Netz befinden, ein oder aus.

Die Adressen der WLCs, die nicht im lokalen Netz stehen (Remote-WLCs), tragen Sie in der statischen WLC-Liste fest ein (SNMP-ID *2.37.34.3*). Die automatische Suche findet keine Remote-WLCs.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

2.37.34.4.1 Netz

Geben Sie den Namen des IPv4-Netzes an, in dem der WLC automatisch nach Remote-WLCs sucht.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

Netzname aus **Setup** > **TCP-IP** > **Netzliste**

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

Default-Wert:

leer

2.37.34.4.2 Aktiv

Mit dieser Option aktivieren oder deaktivieren Sie für das gewählte Netz die automatische Suche nach Remote-WLCs.

Die automatische Suche nach Remote-WLCs ist ein möglicher Weg für den Aufbau von WLC-Tunneln zwischen mehreren WLCs. Wenn Sie diese Option deaktivieren, kann der WLC über das betreffende Netz keine Verbindung zu einem anderen WLC automatisch aufbauen, auch wenn Sie die Nutzung der WLC-Tunnel generell aktiviert haben. Alternativ haben Sie die Möglichkeit, die gewünschten Gegenstellen in der statischen WLC-Liste zu definieren.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.37.34.4.3 Port

Definieren Sie den Port, über den die automatische Suche nach Remote-WLCs stattfindet.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster** > **WLC-Discovery**

Mögliche Werte:

0 … 65535

Besondere Werte:

0

Das Gerät verwendet Default-Port 1027.

Default-Wert:

0

2.37.34.5 WLC-Suche-auf-WTPs-anstossen

Über diese Aktion starten Sie auf sämtlichen gemanagten APs die Berechnung der idealen Verteilung der APs im WLC-Cluster. Das Ergebnis dieser Berechnung löst ggf. eine Neuverteilung der APs aus.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Argumente:

keine

2.37.34.6 WLC-Tunnel-aktiv

Über diesen Parameter aktivieren oder deaktivieren Sie die für das WLC-Clustering verwendeten WLC-Tunnel. Der Vorgang schaltet damit indirekt auch die Cluster-Funktionalität für den betreffenden WLC ein oder aus.

Pfad Telnet:

Setup > **WLAN-Management** > **WLC-Cluster**

Mögliche Werte:

nein
WLC-Cluster-Tunnel sind auf dem Gerät deaktiviert.

ja
WLC-Cluster-Tunnel sind auf dem Gerät aktiviert.

Default-Wert:

nein

2.37.35 RADIUS-Server-Profiles

Standardmäßig übernimmt Ihr WLC die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung zum RADIUS-Server. Damit die AP den entsprechenden RADIUS- Server direkt ansprechen können, definieren Sie in dieser Tabelle die nötigen RADIUS-Profile. Bei der Definition der logischen WLANs (SSIDs) haben Sie die Möglichkeit, pro SSID ein separates RADIUS-Profil zu wählen.

SNMP-ID: 2.37.35

Pfad Telnet: /Setup/WLAN-Management

2.37.35.1 Name

Name des RADIUS-Profils. Unter diesem Namen referenzieren Sie das RADIUS-Profil aus den logischen WLAN-Einstellungen.

SNMP-ID: 2.30.3.1

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.37.35.2 Account-IP

IP-Adresse des RADIUS-Servers, der das Accounting der Benutzeraktivitäten übernimmt. In der Default-Einstellung mit der IP-Adresse 0.0.0.0 sendet der AP die entsprechenden RADIUS-Anfragen an den WLC.

SNMP-ID: 2.37.35.2

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.37.35.3 Account-Port

Port des RADIUS-Servers, der das Accounting der Benutzeraktivitäten übernimmt.

SNMP-ID: 2.37.35.3

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 5 Ziffern

Default: 1813

2.37.35.4 Account-Secret

Kennwort für den RADIUS-Server, der das Accounting der Benutzeraktivitäten übernimmt.

SNMP-ID: 2.37.35.4

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 32 Zeichen

Default: leer

2.37.35.5 Account-Loopback

Hier können Sie optional eine Absenderadresse konfigurieren für den RADIUS-Server, der das Accounting der Benutzeraktivitäten übernimmt. Diese wird statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.37.35.5

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Als Adresse werden verschiedene Eingabeformen akzeptiert:
- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen.

- LBO... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Default: leer

2.37.35.6 Account-Protokoll

Protokoll für die Kommunikation zwischen dem AP und dem RADIUS-Server, der das Accounting der Benutzeraktivitäten übernimmt.

SNMP-ID: 2.37.35.6

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- RADSEC
- RADIUS

Default: RADIUS

2.37.35.7 Access-IP

IP-Adresse des RADIUS-Servers, der die Authentifizierung der Benutzerdaten übernimmt. In der Default-Einstellung mit der IP-Adresse 0.0.0.0 sendet der AP die entsprechenden RADIUS-Anfragen an den WLC.

SNMP-ID: 2.37.35.7

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

2.37.35.8 Access-Port

Port des RADIUS-Servers, der die Authentifizierung der Benutzerdaten übernimmt.

SNMP-ID: 2.37.35.8

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 5 Ziffern

Default: 1812

2.37.35.9 Access-Secret

Kennwort für den RADIUS-Server, der die Authentifizierung der Benutzerdaten übernimmt.

SNMP-ID: 2.37.35.9

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 32 Zeichen

Default: leer

2.37.35.10 Access-Loopback

Hier können Sie optional eine Absenderadresse konfigurieren für den RADIUS-Server, der die Authentifizierung der Benutzerdaten übernimmt. Diese wird statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

SNMP-ID: 2.37.35.10

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Als Adresse werden verschiedene Eingabeformen akzeptiert:
- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ

Wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen.

- LBO... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Default: leer

2.37.35.11 Access-Protokoll

Protokoll für die Kommunikation zwischen dem AP und dem RADIUS-Server, der die Authentifizierung der Benutzerdaten übernimmt.

SNMP-ID: 2.37.35.11

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- RADSEC
- RADIUS

Default: RADIUS

2.37.35.12 Backup

Name des Backup-RADIUS-Profils. Unter diesem Namen referenzieren Sie das Backup-RADIUS-Profil aus den logischen WLAN-Einstellungen. Der WLC verwendet die Einstellungen aus dem Backup-RADIUS-Profil, wenn die primären RADIUS-Server für Authentifizierung oder Accounting nicht auf Anfragen antworten.

SNMP-ID: 2.30.3.12

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.37.36 Capwap-Aktiv

Aktiviert oder deaktiviert den CAPWAP-Dienst auf Ihrem Gerät.

Um mehrere WLCs in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile (wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen Controller spiegeln lässt.

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.37.37 Praeferenz

Über diesen Parameter geben Sie den Präferenzwert an, nach dem ein AP innerhalb von WLC-Clustern die Priorität eines WLC bestimmt. Der AP wertet aus, welchen Präferenzwert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

0 … 255

Default-Wert:

0

2.37.40 Client-Steering

In diesem Verzeichnis konfigurieren Sie das Client-Steering über den WLC.

Pfad Telnet:

Setup > **WLAN-Management**

2.37.40.11 Trace-Mac

Um die Fehlersuche zu erleichtern, erscheint bei aktiviertem Trace (`trace # wlc-steering`) nur die hier eingetragene MAC-Adresse.

Pfad Telnet:

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

Mögliche Werte:

16 Zeichen aus `0123456789abcdef`

Default-Wert:

0000000000000000

2.37.40.17 Statistiken-anzeigen

Über diesen Parameter aktivieren bzw. deaktivieren Sie die Aufzeichnung von Client-Steering-Statistiken. Die Statistikdaten lassen sich anschließend z. B. mittels LANmonitor auswerten. Alternativ lassen sich die Statistikdaten auch unter **Status** > **WLAN-Management** > **Client-Steering** einsehen.

Die Statistikaufzeichnung erhöht die Last auf dem WLC. LANCOM empfiehlt daher, die Statistikaufzeichnung nicht dauerhaft zu aktivieren.

Pfad Telnet:

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

Mögliche Werte:

ja

Aktiviert die Aufzeichnung von Client-Steering-Statistiken.

nein

Deaktiviert die Aufzeichnung von Client-Steering-Statistiken.

Default-Wert:

nein

2.37.40.19 Profile

In dieser Tabelle verwalten Sie die Profile für das Client-Steering. Ein Client-Steering-Profil legt die Bedingungen fest, unter denen der WLC einen Client-Steering-Vorgang auslöst.

Pfad Telnet:

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

2.37.40.19.1 Name

Bezeichnung des Client-Steering-Profils.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.37.40.19.2 Toleranzschwelle

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

0

2.37.40.19.4 Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

100

2.37.40.19.5 Anzahl-Clients-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

100

2.37.40.19.6 Frequenzband-Gewichtung

Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

100

2.37.40.19.9 Bevorzugtes-Band

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

2,4GHz
Der WLC leitet den AP auf das Frequenzband 2,4 GHz.

5GHz
Der WLC leitet den AP auf das Frequenzband 5 GHz.

Default-Wert:

5GHz

2.37.40.19.10 Disassoziierungs-Schwellwert

Gibt den Schwellwert an, unter den der mit der Verbindung zum Client assoziierte Wert sinken muss, bevor der AP die Verbindung zum Client trennt und ein neuer Client-Steering-Vorgang beginnt.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 100 Prozent

Default-Wert:

30

2.37.40.19.11 Zeit-bis-Disassoziierung

Gibt die Anzahl der Sekunden an, in denen keine Datenübertragung zwischen AP und Client stattfinden darf, bevor der AP den Client trennt.

Pfad Telnet:

Setup > **WLAN-Management** > **Client-Steering** > **Profile**

Mögliche Werte:

0 … 10 Sekunden

Default-Wert:

1

2.37.40.20 Statistik-Mac-Filter

Über diesen Parameter definieren Sie eine Liste von MAC-Adressen, für die der WLC explizit Statistikdaten erfasst. Die Statistiken zu den aufgeführten MAC-Adressen schreibt der WLC in die **Event-Tabelle** unter **Status** > **WLAN-Management** > **Client-Steering**. Mehrere MAC-Adressen trennen Sie durch eine kommaseparierte Liste.

Die Erfassung von Statistikdaten aktivieren Sie unabhängig über den Parameter *2.37.40.17 Statistiken-anzeigen* auf Seite 803.

Pfad Telnet:

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

Mögliche Werte:

max. 251 Zeichen aus `[0-9][a-f]:-,`

Besondere Werte:

leer

Das Gerät erfasst Statistikdaten zu sämtlichen MAC-Adressen (Filter deaktiviert).

Default-Wert:

leer

2.38 LLDP

Dieses Untermenü beinhaltet alle Konfigurationsoptionen, die mit dem Link Layer Discovery Protocol (LLDP) zusammenhängen. Die Optionen ähneln den Konfigurationsoptionen nach dem LLDP MIB. Sollten Ihnen die hier enthaltenen Informationen nicht genügen, finden Sie weitere Details im IEEE-Standard 802.1AB.

Ob ein spezifisches Gerät LLDP unterstützt, können Sie dem entsprechenden Datenblatt entnehmen.

Pfad Telnet:

Setup > **LLDP**

2.38.1 Nachrichten-TX-Intervall

Dieser Wert definiert das Interval in Sekunden, in dem das Gerät regelmäßig LLDPDUs überträgt.

Wenn das Gerät während eines solchen Intervalls Änderungen der LLDP-Informationen ermittelt, kann das Gerät zusätzliche LLDP-Nachrichten versenden. Der Parameter `Tx-Verzoegerung` definiert die maximale Häufigkeit der LLDP-Nachrichten aufgrund dieser Änderungen.

Das Gerät verwendet das hier eingestellte `Nachrichten-TX-Intervall` auch zur Berechnung der Haltezeit für die empfangenen LLDP-Nachrichten mit Hilfe des `Nachrichten-TX-Halte-Faktor`,

Pfad Telnet:

Setup > **LLDP** > **Nachrichten-TX-Intervall**

Mögliche Werte:

0 bis 65535 Sekunden

Default:

30

2.38.2 Nachrichten-TX-Halte-Faktor

Dieser Wert dient zur Berechnung der Zeitspanne in Sekunden, nach der das Gerät die Informationen aus empfangenen LLDP-Nachrichten wieder verwirft (Haltezeit oder Time to Live - TTL). Das Gerät berechnet diesen Wert als Produkt aus dem hier angegebenen `Nachrichten-TX-Halte-Faktor` und dem aktuellen *`Nachrichten-TX-Intervall`*:

Haltezeit = `Nachrichten-TX-Halte-Faktor` x `Nachrichten-TX-Intervall`

In der Default-Einstellung beträgt die resultierende Haltezeit für die empfangenen LLDP-Nachrichten 120 Sekunden.

Pfad Telnet:

Setup > **LLDP** > **Nachrichten-TX-Haltefaktor**

Mögliche Werte:

0 bis 99

Default:

4

2.38.3 Reinit-Verzoegerung

Dieser Wert definiert die Zeit, während der das Gerät trotz eingeschaltetem LLDP die Übertragung von LLDPDUs unterdrückt.

Pfad Telnet:

Setup > **LLDP** > **Reinit-Verzoegerung**

Mögliche Werte:

0 bis 99 Sekunden

Default:

2

2.38.4 Tx-Verzoegerung

Prinzipiell versendet das Gerät LLDP-Nachrichten in dem als *`Nachrichten-TX-Intervall`* eingestellten Interval. Wenn das Gerät während eines solchen Intervalls Änderungen der LLDP-Informationen ermittelt, kann das Gerät zusätzliche LLDP-Nachrichten versenden.

Der hier eingestellte Wert definiert die maximale Häufigkeit in Sekunden, in der das Gerät LLDP-Nachrichten verwendet. Der Standardwert von 2 Sekunden führt also dazu, dass das Gerät maximal einmal alle 2 Sekunden LLDP-Nachrichten versendet, auch wenn das Gerät in der Zwischenzeit mehrere Änderungen ermittelt hat.

Pfad Telnet:

Setup > **LLDP** > **Tx-Verzoegerung**

Mögliche Werte:

0 bis 9999 Sekunden

Default:

2

2.38.5 Benachrichtigungs-Intervall

Dieser Wert definiert den Zeitabstand, in dem das Gerät Benachrichtigungen über Änderungen in den Gegenstellen-Tabellen versendet. Der Wert definiert die kleinste Zeitperiode zwischen den Benachrichtigungen. Der Standardwert von 5 Sekunden führt also dazu, dass das Gerät maximal eine Benachrichtigung alle 5 Sekunden versendet, auch wenn das Gerät in der Zwischenzeit mehrere Änderungen ermittelt hat.

Pfad Telnet:

Setup > **LLDP** > **Benachrichtigungs-Intervall**

Mögliche Werte:

0 bis 9999 Sekunden

Default:

5

2.38.6 Ports

Diese Tabelle beinhaltet alle port-abhängigen LLDP-Konfigurations-Optionen. Der Tabellen-Index ist ein String, nämlich der Schnittstellen-/Port-Name.

Pfad Telnet:

Setup > **LLDP** > **Ports**

2.38.6.1 Name

Der Name des Ports oder der Schnittstelle

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Name**

Mögliche Werte:

Abhängig von den Schnittstellen, z. B. LAN-1, WLAN-1

2.38.6.2 Admin-Status

Gibt an, ob PDU-Übertragung und/oder -Empfang auf diesem Port aktiv oder inaktiv ist. Dieser Parameter kann für jeden Port individuell festgelegt werden.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Admin-Status**

Mögliche Werte:

Aus

nur-Tx

nur-Rx

Rx/Tx

Default:

Aus

2.38.6.3 Benachrichtigungen

Stellen Sie hier ein, ob Änderungen in einer MSAP-Gegenstelle dieses Ports an mögliche Netzwerk-Management-Systeme gemeldet werden.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Benachrichtigungen**

Mögliche Werte:

nein

ja

Default:

nein

2.38.6.4 TLVs

Stellen Sie hier die Menge der optionalen Standard-TLVs ein, die an die PDUs übermittelt werden.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **TLVs**

Mögliche Werte:

Port-Beschreibung

System-Name

System-Beschreibung

System-Eigenschaften

keine

Default:

Port-Beschreibung

2.38.6.6 TLVs-802.3

Stellen Sie hier die Menge der optionalen Standard-TLVs-802.3 ein, die das Gerät an die PDUs übermittelt.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **TLVs-802.3**

Mögliche Werte:

PHY-Konfig-Status

Power-via-MDI

Link-Aggregierung

Max-Frame-Groesse

Keine

Default:

PHY-Konfig-Status

2.38.6.7 Max-Nachbarn

Dieser Parameter gibt die maximale Anzahl von LLDP-Nachbarn an.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Max-Nachbarn**

Mögliche Werte:

0 bis 65535

Default:

0

2.38.6.8 Akt.-Quellen

Dieser Parameter gibt die möglichen Quellen für LLDP-Updates an.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Akt.-Quellen**

Mögliche Werte:

Auto

nur-LLDP

nur andere

beide

Default:

Auto

2.38.6.9 TLVs-LCS

Diese Einstellungen definieren die Menge der optionalen Standard-TLVs-LCS, die das Gerät über PDUs übermittelt.

Pfad Telnet:

Setup > **LLDP** > **Ports** > **TLVs-LCS**

Mögliche Werte:

SSID

Radio-Kanal

PHY-Typ

Keine

Default:

SSID

2.38.7 Management-Adressen

Stellen Sie in dieser Tabelle ein, welche Management-Adresse(n) das Gerät über LLDPDUs übermittelt. Management-Adressen beziehen ihre Namen aus der TCP/IP-Netzwerkliste. Das Gerät übermittelt ausschließlich die Netzwerke und Management-Adressen in dieser Tabelle für LLDPDUs. Ein Netzwerk aus dieser Liste hat die Möglichkeit, die Port-Liste zu nutzen, um die Bekanntgabe der einzelnen Geräte-Adressen weiterführend zu limitieren.

Pfad Telnet:

Setup > **LLDP** > **Management-Addressen**

Die Definitionen des Adress-Bindings limitieren die Bekanntgabe von Management-Adressen unabhängig von den Port-Listen-Einstellungen. Das Gerät gibt ein IP-Netzwerk ausschließlich dann bekannt, wenn sich dieses an eine Schnittstelle anschließt. Dies ist unabhängig von den Einstellungen der Port-Liste.

2.38.7.1 Netzwerk-Name

Der Name des TCP/IP-Netzwerks, wie er in der TCP-IP-Netzwerk-Liste steht.

Pfad Telnet:

Setup > **LLDP** > **Management-Addressen** > **Netzwerk-Name**

Mögliche Werte:

max. 16 alphanumerische Zeichen

Default:

leer

2.38.7.2 Port-Liste

Die Liste der Schnittstellen und Ports, die zu der entsprechenden Management-Adresse gehören.

Pfad Telnet:

Setup > **LLDP** > **Management-Addressen** > **Port-Liste**

Mögliche Werte:

Mit Kommata getrennte Liste von Ports, max. 251 alphanumerische Zeichen, z. B. LAN-1 oder WLAN-1. Benutzen Sie Wildcards, um eine Gruppe von Ports zu definieren (z. B. "*_*").

Default:

leer

2.38.8 Protokolle

Diese Tabelle enthält die LLDP-Port-Einstellungen für die Spanning-Tree- und Rapid-Spanning-Tree-Protokolle.

Pfad Telnet:

Setup > **LLDP** > **Protokolle**

2.38.8.1 Protokoll

Dieser Parameter setzt das Protokoll, für das die LLDP-Ports aktiviert werden sollen.

Pfad Telnet:

Setup > **LLDP** > **Protokolle** > **Protokoll**

Mögliche Werte:

Spanning-Tree

Rapid-Spanning-Tree

Default:

Spanning-Tree, Rapid-Spanning-Tree

2.38.8.2 Port-Liste

Dieser Wert beschreibt die Ports, die LLDP mit dem zugehörigen Protokoll verwenden (Spanning-Tree oder Rapid-Spanning-Tree).

Pfad Telnet:

Setup > **LLDP** > **Protokolle** > **Port-Liste**

Mögliche Werte:

Mit Kommata getrennte Liste von Ports, max. 251 alphanumerische Zeichen, z. B. LAN-1 oder WLAN-1. Benutzen Sie Wildcards, um eine Gruppe von Ports zu definieren (z. B. "*_*").

Default:

leer

2.38.9 Sofortiges-Loeschen

Dieser Parameter aktiviert oder deaktiviert das direkte Löschen von LLDPDUs.

Pfad Telnet:

Setup > **LLDP** > **Sofortiges-Loeschen**

Mögliche Werte:

ja

nein

Default:

ja

2.38.10 In-Betrieb

Dieser Parameter aktiviert oder deaktiviert die Verwendung von LLDP.

Pfad Telnet:

Setup > **LLDP** > **In-Betrieb**

Mögliche Werte:

ja

nein

Default:

ja

2.39 Zertifikate

Dieses Menü enthält die Konfiguration der Zertifikate.

SNMP-ID: 2.39

Pfad Telnet: /Setup

2.39.1 SCEP-Client

Dieses Menü enthält die Konfiguration des SCEP-Clients.

SNMP-ID: 2.39.1

Pfad Telnet: /Setup/Zertifikate

2.39.1.1 Aktiv

Schaltet die Nutzung von SCEP ein oder aus.

SNMP-ID: 2.39.1.1

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- Ja
- Nein

Default: Nein

Besondere Werte: No

2.39.1.2 CA-Zertifikate-Aktualisieren-Vor-Ablauf

Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

SNMP-ID: 2.39.1.2

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- max. 10 Zeichen

Default: leer

2.39.1.3 CA-Zertifikate-Aktualisieren-Vor-Ablauf

Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

SNMP-ID: 2.39.1.3

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- max. 10 Zeichen

Default: 3

2.39.1.7 Zertifikate

Hier können Sie Zertifikate konfigurieren bzw. Neue hinzufügen.

SNMP-ID: 2.39.1.7

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

2.39.1.7.1 Name

Konfigurationsname des Zertifikats.

SNMP-ID: 2.39.1.7.1

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.39.1.7.2 CADN

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen LCOS-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

SNMP-ID: 2.39.1.7.2

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.7.3 Subject

Distinguished Name des Subjects des Antragstellers.

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen LCOS-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

SNMP-ID: 2.39.1.7.3

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.7.4 ChallengePwd

Kennwort (für das automatische Ausstellen der Geräte-Zertifikate auf dem SCEP-Server).

SNMP-ID: 2.39.1.7.4

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.7.5 SubjectAltName

Weitere Angaben zum Requester, z. B. Domain oder IP-Adresse.

SNMP-ID: 2.39.1.7.5

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.7.6 KeyUsage

Beliebige kommaseparierte Kombination aus: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly, critical (möglich aber nicht empfohlen)

SNMP-ID: 2.39.1.7.6

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.7.7 Systemzertifikate-Schlüssellänge

Länge der Schlüssel, die für das Gerät selbst erzeugt werden.

SNMP-ID: 2.39.1.7.7

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- 31 oder größer

Default: 0

2.39.1.7.8 Verwendung

Gibt den Verwendungszweck der eingetragenen Zertifikate an. Die hier eingetragenen Zertifikate werden dann nur für den entsprechenden Verwendungszweck abgefragt.

SNMP-ID: 2.39.1.7.8

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- VPN

Default: VPN

2.39.1.7.9 Extended-KeyUsage

Beliebige kommaseparierte Kombination aus: critical, serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, msCodeInd, msCodeCom, msCTLSign, msSGC, msEFS, nsSGC, 1.3.6.1.5.5.7.3.18 für WLAN-Controller, 1.3.6.1.5.5.7.3.19 für Access Points im Managed-Modus

SNMP-ID: 2.39.1.7.9

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.1.8 Reinit

Startet die manuelle Re-Initialisierung der SCEP-Parameter. Dabei werden wie bei der gewöhnlichen SCEP-Initialisierung auch die notwendigen RA- und CA-Zertifikate von der CA abgerufen und so im Dateisystem des Geräts abgelegt, dass Sie noch nicht für die Nutzung im VPN-Betrieb bereit stehen. Sofern das vorhandene Systemzertifikat zum abgerufenen CA-Zertifikat passt, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden. Sofern die vorhandenen Systemzertifikate nicht zum abgerufenen CA-Zertifikat passen, muss zunächst eine neue Zertifikatsanfrage beim SCEP-Server gestellt werden. Erst wenn so ein neues, zum CA-Zertifikat passendes Systemzertifikat

ausgestellt und abgerufen wurde, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.

SNMP-ID: 2.39.1.8

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

2.39.1.9 Aktualisieren

Startet manuell die Anfrage nach einem neuen Systemzertifikat, unabhängig von der verbleibenden Gültigkeitsdauer. Dabei wird ein neues Schlüsselpaar erzeugt.

SNMP-ID: 2.39.1.9

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

2.39.1.10 Bereinige-SCEP-Dateisystem

Startet die Bereinigung des SCEP-Dateisystems.

gelöscht werden: RA-Zertifikate, ausstehende Zertifikatsanfragen, neue und inaktive CA-Zertifikate, neue und inaktive private Schlüssel.

erhalten bleiben: aktuell im VPN-Betrieb genutzte Systemzertifikate, private Schlüssel dazu und die aktuell im VPN-Betrieb genutzten CA-Zertifikate.

SNMP-ID: 2.39.1.10

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

2.39.1.11 Wiederholen-Nach-Fehler-Intervall

Intervall in Sekunden für Wiederholungen nach jeglicher Art von Fehler.

SNMP-ID: 2.39.1.11

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- max. 10 Zeichen

Default: 22

2.39.1.12 Ausstehende-Anfragen-Prüfen-Intervall

Intervall in Sekunden für das Prüfen von ausstehenden Zertifikatsanfragen.

SNMP-ID: 2.39.1.12

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- max. 10 Zeichen

Default: 101

2.39.1.13 Trace-Stufe

Für den SCEP-Client-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Dazu wird ein Wert angegeben, bis zu welcher Stufe die Pakete im Trace ausgegeben werden sollen.

SNMP-ID: 2.39.1.13

Pfad Telnet: /Setup/Zertifikate/SCEP-Client

Mögliche Werte:

- alles: alle Tracemeldungen, auch reine Info- und Debug-Meldungen
- reduziert: nur Fehler- und Warnmeldungen
- nur-Fehler: nur Fehlermeldungen

Default:

alles

2.39.1.14 CAs

In dieser Tabelle definieren sie die verfügbaren CAs.

SNMP-ID: 2.39.1.14

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/CAs

2.39.1.14.1 Name

Geben Sie einen Namen ein, der diese Konfiguration kennzeichnet.

SNMP-ID: 2.39.1.14.1

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/Name

Mögliche Werte: max. 16 alphamnumerische Zeichen

Default: leer

2.39.1.14.2 URL

Hier muss die sogenannte 'Enrollment-URL' eingegeben werden. Um ein Zertifikat zu beantragen, muss der Router die Zertifizierungsstelle (CA - Certificate Authority) kontaktieren. Dazu wird eine URL benötigt, die von Anbieter zu Anbieter unterschiedlich ist und meist anhand der Dokumentation zur CA herauszufinden ist. Beispiel: http:/ /postman/certsrv/mscep/mscep.dll

SNMP-ID: 2.39.1.14.2

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/URL

Mögliche Werte:

- max. 251 alphanumerische Zeichen

Default: leer

2.39.1.14.3 DN

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM Systems/C=DE

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen LCOS-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

SNMP-ID: 2.39.1.14.3

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/DN

Mögliche Werte:

- max. 251 alphanumerische Zeichen

Default: leer

2.39.1.14.4 Enc-Alg

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen. Es stehen mehrere Verfahren zur Auswahl.

Verwenden Sie nach Möglichkeit eines der letzteren Verfahren (3DES, BLOWFISH, AES), wenn die Zertifizierungsstelle (CA) und alle Clients es unterstützen. Als Standard ist hier DES-Verschlüsselung voreingestellt, um die Interoperabilität zu wahren.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

DES

Data Encryption Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung. DES ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter Algorithmus. Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel, der Kombinationen von Substitutions-Chiffre, Transpositions-Chiffre und Exklusiv-Oder-Funktionen (XOR) ermöglicht. Der 64-Bit-Datensatz besteht aus einer effektiven Schlüssellänge von 56 Bits und 8 Parity-Bits, das zugrunde liegende Verschlüsselungsverfahren heißt Lucifer.

3DES

Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die zwei 64-Bit-Schlüssel verwendet.

BLOWFISH

Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.

AES

Advanced Encryption Standard: Der AES-Algorithmuss besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

Default-Wert:

DES

2.39.1.14.5 Identifier

Hier kann ein zusätzlicher Identifier eingegeben werden. Dieser Wert wird von manchen Webservern benötigt um die CA zuordnen zu können.

SNMP-ID: 2.39.1.14.5

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/Identifier

Mögliche Werte:

- max. 251 alphanumerische Zeichen

Default: leer

2.39.1.14.6 CA-Signaturalgorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest, gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwertes für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

2.39.1.14.7 RA-Autoapprove

Bei Auswahl dieser Option werden Neuanträge, bei bereits vorliegendem Systemzertifikat, mit diesem unterschrieben. Die Option muss sowohl beim Zertifikatnehmer (Client), als auch bei der Zertifizierungsstelle (CA-Server) eingeschaltet werden. Die CA authentifiziert den Client in diesem Falle ohne Angabe eines Challenge-Passwortes, sondern nur anhand des Zertifikats.

SNMP-ID: 2.39.1.14.7

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/RA-Autoapprove

Mögliche Werte:

- ja
- nein

Default: nein

2.39.1.14.8 CA-Fingerprintalgorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen.

Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

aus

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest, gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwertes für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

2.39.1.14.9 CA-Fingerprint

Hier kann der CA-Fingerprint eingetragen werden. Es handelt sich hierbei um den Hash-Wert, der sich bei Verwendung des Fingerprint-Algorithmus ergibt. Anhand dieses Hash-Wertes kann die Authentizität des erhaltenen CA-Zertifikats gesichert werden (wenn ein CA-Fingerprintalgorithmus gewählt ist). Mögliche Delimiter sind: ' :' ' -' ' ,' ' '

SNMP-ID: 2.39.1.14.9

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/CA-Fingerprint

Mögliche Werte:

- max. 59 alphanumerische Zeichen

Default: leer

2.39.1.14.11 Loopback-Addr.

Geben Sie eine Loopback-Adresse an.

SNMP-ID: 2.39.1.14.11

Pfad Telnet: /Setup/Zertifikate/SCEP-Client/Zertifikate/Loopback-Addr.

Mögliche Werte: max. 16 Zeichen

Default: leer

2.39.2 SCEP-CA

Dieses Menü enthält die Einstellungen für die SCEP-CA.

SNMP-ID: 2.39.2

Pfad Telnet: /Setup/Zertifikate/SCEP-CA

2.39.2.1 Aktiv

Aktivieren oder deaktivieren Sie den SCEP-Client.

SNMP-ID: 2.39.2.1

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Aktiv

Mögliche Werte:

- ja
- nein

Default: nein

2.39.2.2 CA-Zertifikate

Dieses Menü enthält die Einstellungen für die CA-Zertifikate.

SNMP-ID: 2.39.2.2

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate

2.39.2.2.1 CA-Distinguished-Name

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

SNMP-ID: 2.39.2.2.1

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/CA-Distinguished-Name

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.2.2.3 Alternativer-Name

Hier kann ein alternativer 'Subject-Name' eingegeben werden.

Beispiele: critical,DNS:host.company.de IP:10.10.10.10 DNS:host.company.de, IP:10.10.10.10 UFQDN:email:name@company.de

SNMP-ID: 2.39.2.2.3

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Alternativer-Name

2.39.2.2.4 RSA-Schluessellaenge

Hier muss die Schlüssellänge eingegeben werden. Dieser Wert bestimmt für neue Schlüssel die Länge in Bits.

SNMP-ID: 2.39.2.2.4

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/RSA-Schluessellaenge

Mögliche Werte:

- 1024
- 2048
- 3072
- 4096
- 8192

Default: 2048

Je nach zur Verfügung stehender Systemleistung dauert die Berechnung unterschiedlich lange, je größer die Anzahl Bits umso länger.

2.39.2.2.5 Gueltigkeitsdauer

Tragen Sie hier den Gültigkeitszeitraum für das ausgestellte Zertifikat in Tagen ein.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Gueltigkeitsdauer

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 1100

2.39.2.2.6 CA-Zertifikate-aktualisieren-vor-Ablauf

Tragen Sie hier den Zeitraum für die 'Erneuerung vor Ablauf' in Tagen ein.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/CA-Zertifikate-aktualisieren-vor-Ablauf

Mögliche Werte:

- maximal 2 numerische Zeichen

Default: 4

2.39.2.2.8 RA-Distinguished-Name

Hier muss der 'Distinguished Name' eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE

SNMP-ID: 2.39.2.2.8

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/RA-Distinguished-Name

Mögliche Werte:

- max. 251 Zeichen

Default: leer

2.39.2.2.9 Erstelle-neue-CA-Zertifikate

Führen Sie diesen Befehl aus, wenn Sie die Konfiguration der CA geändert haben.

Die CA erstellt nur dann automatisch neue Zertifikate, wenn die alten abgelaufen oder gar keine vorhanden sind. WennSie nachträglich die Schlüssellänge, den Namen oder andere Werte der CA-Zertifikate ändern, erstellen Sie über diesen Befehl die entsprechenden Zertifikatsdateien neu.

SNMP-ID: 2.39.2.2.9

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Erstelle-neue-CA-Zertifikate

2.39.2.2.10 Erstelle-PKCS12-Backup-Dateien

Für die Wiederherstellung der CA bzw. der RA im Backup-Fall werden die jeweiligen Root-Zertifikate mit den privaten Schlüsseln benötigt, die beim Systemstart automatisch vom WLC erzeugt werden.

Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PCKS12-Container gespeichert, der mit einer Passphrase geschützt ist.

Mit dem Befehl "Erstelle-PKCS12-Backup-Dateien" starten Sie den Export. Geben Sie als Parameter die gewünschte Passphrase an.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Erstelle-PKCS12-Backup-Dateien

2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen

Mit diesem Befehl können Sie die beiden PKCS12-Dateien mit den jeweiligen Root-Zertifikaten und den privaten Schlüsseln der CA bzw. der RA im Backup-Fall wiederherstellen.

SNMP-ID: 2.39.2.2.11

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/CA-Zertifikate/Zertifikate-aus-Backup-wiederherstellen

2.39.2.3 Verschluesselungsalgorithmus

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen. Es stehen mehrere Verfahren zur Auswahl.

Verwenden Sie nach Möglichkeit eines der letzteren Verfahren (3DES, BLOWFISH, AES), wenn die Zertifizierungsstelle (CA) und alle Clients es unterstützen. Als Standard ist hier DES-Verschlüsselung voreingestellt, um die Interoperabilität zu wahren.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

DES

Data Encryption Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung. DES ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter Algorithmus. Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel, der Kombinationen von Substitutions-Chiffre, Transpositions-Chiffre und Exklusiv-Oder-Funktionen (XOR) ermöglicht. Der 64-Bit-Datensatz besteht aus einer effektiven Schlüssellänge von 56 Bits und 8 Parity-Bits, das zugrunde liegende Verschlüsselungsverfahren heißt Lucifer.

3DES

Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die zwei 64-Bit-Schlüssel verwendet.

BLOWFISH

Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.

AES

Advanced Encryption Standard: Der AES-Algorithmuss besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

Default-Wert:

DES

2.39.2.4 RA-Automatische-Authentifikation

Bei Auswahl dieser Option werden Neuanträge, bei bereits vorliegendem Systemzertifikat, mit diesem unterschrieben. Die Option muss sowohl beim Zertifikatnehmer (Client), als auch bei der Zertifizierungsstelle (CA-Server) eingeschaltet werden. Die CA authentifiziert den Client in diesem Falle ohne Angabe eines Challenge-Passwortes, sondern nur anhand des Zertifikats.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/RA-Automatische-Authentifikation

Mögliche Werte:

- ja
- nein

Default: ja

2.39.2.5 Client-Zertifikate

Dieses Menü enthält die Einstellungen für die Client-Zertifikate.

SNMP-ID: 2.39.2.5

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Client-Zertifikate

2.39.2.5.1 Gueltigkeitsdauer

Bestimmen Sie hier die Gültigkeitsdauer des Zertifikats in Tagen.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Gueltigkeitsdauer

Mögliche Werte:

- maximal 5 numerische Zeichen

Default: 365

2.39.2.5.3 Challenge-Passwoerter

In dieser Tabelle erhalten Sie einen Überblick über die Challenge-Passwörter.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate**

2.39.2.5.3.1 Index

Geben Sie hier den Index für das Challenge-Passwort an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

leer

2.39.2.5.3.2 Subject-Distinguished-Name

Hier muss der „Distinguished Name“ eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE`

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.39.2.5.3.3 MAC-Adresse

Tragen Sie hier die MAC-Adresse des Clients ein, dessen Passwort in der Challange-Passwort-Tabelle verwaltet wird.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

max. 12 Zeichen aus `0123456789abcdef`

Default-Wert:

leer

2.39.2.5.3.4 Challenge

Geben Sie hier die Challenge (Passwort) für den Client an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.5.3.5 Challenge

Geben Sie hier die Gültigkeit des Passwortes an. Wenn Sie „einmalig“ auswählen, handelt es sich bei diesem Passwort um ein One-Time-Passwort (OTP), das nur für die einmalige Verwendung bei einer Authentifizierung gültig ist.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

einmalig
permanent

Default-Wert:

permanent

2.39.2.5.4 Allgemeines-Challenge-Passwort

Hier kann ein weiteres 'Passwort' eingetragen werden, das an die CA übertragen wird. Dieses kann standardmäßig zur Authentifizierung von Rücknahme-Anträgen benutzt werden. Auf CAs mit Microsoft-SCEP (mscep) können (falls dort aktiviert) die von der CA vergebenen Einmalpasswörter zur Antragsauthentifizierung eingetragen.

SNMP-ID: 2.39.2.5.4

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Client-Zertifikate/Allgemeines-Challenge-Passwort

Mögliche Werte:

- max. 16 Zeichen

Default: XuL[ksKcC3+'%PA2

2.39.2.6 Signatur-Algorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest, gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwertes für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

2.39.2.7 Fingerabdruck-Algorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen.

Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest, gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwertes für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

2.39.2.8 Zertifikatswiderruflisten

Hier finden Sie die Zertifikatswiderruflisten.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten

2.39.2.8.1 Update-Intervall

Tragen Sie hier das Aktualisierungs-Intervall in Sekunden für die Erstellung einer neuen CRL ein. Die untere Grenze hierfür liegt bei 600 Sekunden. .

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/Update-Intervall

Mögliche Werte:

- maximal 63 numerische Zeichen

Default: 86.400

2.39.2.8.2 CRL-Verteilungspunkt-Rechnername

Tragen Sie hier das Aktualisierungs-Intervall in Sekunden für die Erstellung einer neuen CRL ein. Die untere Grenze hierfür liegt bei 600 Sekunden.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/CRL-Verteilungspunkt-Rechnername

Mögliche Werte:

- maximal 63 numerische Zeichen

Default: 600

2.39.2.8.3 Erstelle-neue-Zertifikatswiderrufliste

Normalerweise erstellt die CA automatisch eine neue Zertifikatswiderrufliste (CRL) erstellt, wenn die alte CRL abgelaufen ist oder wenn sich der Inhalt der CRL ändert (durch SCEP-Operationen).

Führen Sie diesen Befehl aus, wenn Sie in der Zertifikatsstatusliste ein Zertifikat zurückgerufen haben.

SNMP-ID: 2.39.2.8.3

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Zertifikatswiderruflisten/Erstelle-neue-Zertifikatswiderrufliste

2.39.2.9 Reinitialisiere

Mit diesem Befehl reinitialisieren Sie die CA. Das Gerät prüft die Konfiguration und die Zertifikate, wenn nötig aktualisiert das Gerät die entsprechenden Werte bzw. Dateien.

Führen Sie diesen Befehl aus, wenn die CA wegen eines Konfigurationsfehlers nicht läuft, um die erneute Überprüfung nach einer Konfigurationsänderung auszulösen.

SNMP-ID: 2.39.2.9

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Reinitialisiere

2.39.2.10 Benachrichtigung

In diesem Menü finden Sie die Einstellungen zu Benachrichtigungen über Ereignisse im Zusammenhang mit den Zertifikaten.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Benachrichtigung

2.39.2.10.1 E-Mail

Aktivieren Sie hier, ob eine Benachrichtigung beim Eintreffen eines Ereignisses gesendet wird.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Benachrichtigung/E-Mail

Mögliche Werte:

- nein
- ja

Default: nein

2.39.2.10.2 Syslog

Aktivieren Sie hier die Protokollfunktion der Benachrichtigungen via SYSLOG.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Benachrichtigung/Syslog

Mögliche Werte:

- nein
- ja

Default: nein

Um die Protokollfunktion zu Nutzen, muss der SYSLOG-Client im Gerät entsprechend konfiguriert sein.

2.39.2.10.3 E-Mail-Empfaenger

Geben Sie hier die Emailadresse an, an die eine Benachrichtigung beim Eintreffen eines Ereignisses gesendet wird.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Benachrichtigung/E-Mail

Mögliche Werte:

- maximal 63 alphanumerische Zeichen

Default: leer

2.39.2.10.4 Sende-Backup-Erinnerung

Aktivieren Sie hier die Funktion, dass das Gerät automatisch eine Erinnerung zur Erstellung eines Backups an die eingetragene Emailadresse schickt.

Pfad Telnet: /Setup/Zertifikate/SCEP-CA/Benachrichtigung/Sende-Backup-Erinnerung

Mögliche Werte:

- nein
- ja

Default: nein

2.39.2.11 Root-CA

Über diesen Parameter legen Sie fest, ob die CA des betreffenden WLC die Root-CA darstellt oder nicht.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

nein
ja

Default-Wert:

ja

2.39.2.12 CA-Pfad-Laenge

Über diesen Parameter legen Sie fest, wie lang die Hierarchie der Sub-CAs unterhalb der Root-CA maximal sein darf (Länge der „Chain of Trust").

Ein Wert von `1` z. B. bewirkt, dass nur die Root-CA Zertifikate für Sub-CAs austellen kann. Die betreffenden Sub-CAs sind ihrerseits nicht mehr dazu in der Lage, an andere Sub-CAs Zertifikate auszustellen und die „Chain of Trust" auf diese Weise zu verlängern. Bei einem Wert von `0` hingegen ist auch die Root-CA nicht dazu in der Lage, Zertifikate für Sub-CAs auszustellen. In diesem Fall kann die Root-CA nur noch Endbenutzer-Zertifikate signieren.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

0 … 65535

Default-Wert:

1

2.39.2.13 Sub-CA

In diesem Menü nehmen Sie sämtliche Einstellungen vor, die für den Bezug eines Zertifikats für die Sub-CA notwendig sind.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

2.39.2.13.1 Auto-generiert-Request

Über diesen Parameter legen Sie fest, ob der WLC den Request nach einem Zertifikat für die Sub-CA automatisch an die Root-CA stellt.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.39.2.13.2 CADN

Geben Sie den Certificate Authority Distinguished Name (CADN) der übergeordneten CA (z. B. der Root-CA) an, von welcher der WLC das Zertifikat für die Sub-CA bezieht.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.39.2.13.3 Challenge-Pwd

Geben Sie das Challenge-Passwort an, mit dem die Sub-CA das Zertifikat von der übergeordneten CA (z. B. der Root-CA) bezieht. Das Challenge-Passwort für die übergeordnete CA setzen Sie unter LCOS im Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate**.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.39.2.13.4 Ext-Key-Usage

Definieren Sie weitere Verwendungs-Zwecke für die Schlüssel-Benutzung. Die erweiterte Schlüssel-Benutzung besteht aus einer kommaseparierten Liste von Verwendungs-Zwecken, für die der öffentliche Zertifikats-Schlüssel verwendbar ist.

Die Verwendungs-Zwecke können entweder deren Kurznamen oder die punktseparierte Form der OIDs sein. Obwohl jede beliebige OID verwendet werden kann, machen nur bestimmte Sinn (siehe unten). Speziell die folgenden PKIX-, NS- und MS-Werte sind von Bedeutung und können in jeder beliebigen Kombination aufgezählt werden:

Tabelle 14: Erweiterte Verwendungs-Zwecke: Bedeutsame Kurznamen

Wert	Bedeutung
serverAuth	SSL/TLS-Web-Server-Authentifizierung
clientAuth	SSL/TLS-Web-Client-Authentifizierung
codeSigning	Code-Signierung
emailProtection	E-Mail-Schutz (S/MIME)
timeStamping	Vertrauenswürdiges Zeitstempeln (Trusted Timestamping)
msCodeInd	Microsoft persönliche Code-Signierung (Authenticode)
msCodeCom	Microsoft kommerzielle Code-Signierung (Authenticode)
msCTLSign	Microsoft vertrauenswürdige Listen-Signierung (Trust List Signing)
msSGC	Microsoft Server-gestützte Verschlüsselung (Server Gated Crypto)
msEFS	Microsoft verschlüsseltes Dateisystem (Encrypted File System)
nsSGC	Netscape Server-gestützte Verschlüsselung (Server Gated Crypto)
critical	Ist diese Einschränkung gesetzt, muss die Schlüssel-Verwendungs-Erweiterung immer beachtet werden. Wenn die Erweiterung nicht unterstützt wird, wird das Zertifikat als nicht gültig abgelehnt.

Tabelle 15: Erweiterte Verwendungs-Zwecke: Sinnvolle OIDs für WLAN-Switching

Gerät	OID
WLC	1.3.6.1.5.5.7.3.18

Gerät	OID
Verwalteter AP (Managed AP)	1.3.6.1.5.5.7.3.19

Beispieleingabe: `critical,clientAuth,1.3.6.1.5.5.7.3.19`

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

Kommaseparierte Liste aus den o. g. Kurznamen und/oder OIDs. Max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.39.2.13.5 Cert-Key-Usage

Geben Sie den Verwendungszweck der eingetragenen Zertifikate an (Schlüssel-Benutzung). Der WLC fragt die Zertifikate für die Sub-CA dann ausschließlich für den entsprechenden Verwendungszweck ab.

Tabelle 16: Verwendungs-Zwecke: Kurznamen

Wert	Bedeutung
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
encipherOnly	
decipherOnly	
critical	Ist diese Einschränkung gesetzt, muss die Schlüssel-Verwendungs-Erweiterung immer beachtet werden. Wenn die Erweiterung nicht unterstützt wird, wird das Zertifikat als nicht gültig abgelehnt.

Beispieleingabe: `digitalSignature, nonRepudiation`

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

Kommaseparierte Liste aus den o. g. Kurznamen. Max. 100 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.39.2.13.8 CA-Url-Adresse

Geben Sie die URL (Adresse) an, unter der die übergeordnete CA zu finden ist. Stellt ein anderer WLC mit LCOS-Betriebssystem die CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

http://127.0.0.1/cgi-bin/pkiclient.exe

2.39.2.13.9 Neustart

Diese Aktion bewirkt einen Neustart der Sub-CA. Führen Sie diese Aktion nach Konfigurationsänderungen an der Sub-CA durch.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Sub-CA**

Mögliche Argumente:

keine

2.39.2.14 Web-Schnittstelle

In diesem Verzeichnis konfigurieren Sie die Einstellungen für die SCEP-CA-Web-Schnittstelle.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

2.39.2.14.1 Profile

In dieser Tabelle legen Sie Profile mit gesammelten Zertifikats-Eigenschaften an.

Standardmäßig sind bereits drei Profile für gängige Anwendungsszenarien angelegt.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle**

2.39.2.14.1.1 Profilname

Vergeben Sie hier einen eindeutigen Namen des Profils.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.2 Schluessel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

- critical
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly

Eine kommagetrennte Mehrfachauswahl ist möglich.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

critical,digitalSignature,keyEncipherment

2.39.2.14.1.3 Erw.-Schluessel-Verwendung

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

- critical
- serverAuth: SSL/TLS-Web-Server-Authentifizierung
- clientAuth: SSL/TLS-Web-Client-Authentifizierung
- codeSigning: Signierung von Programmcode
- emailProtection: E-Mail-Schutz (S/MIME)
- timeStamping: Daten mit zuverlässigen Zeitstempeln versehen
- msCodeInd: Microsoft Individual Code Signing (authenticode)
- msCodeCom: Microsoft Commercial Code Signing (authenticode)

- msCTLSign: Microsoft Trust List Signing
- msSGC: Microsoft Server Gated Crypto
- msEFS: Microsoft Encrypted File System
- nsSGC: Netscape Server Gated Crypto

Eine kommagetrennte Mehrfachauswahl ist möglich.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

2.39.2.14.1.4 RSA-Schluessellaenge

Gibt die Länge des Schlüssels an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

1024
2048
3072
4096
8192

Default-Wert:

2048

2.39.2.14.1.5 Gueltigkeitsperiode

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

365

2.39.2.14.1.6 CA

Gibt an, ob es sich um ein CA-Zertifikat handelt.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.39.2.14.1.7 Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.8 Land

Geben Sie die Staatenkennung ein (z. B. „DE“ für Deutschland).

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter **C**= (**C**ountry).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.9 Stadt

Geben Sie den Ort ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter **L**= (**L**ocality).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.10 Unternehmen

Geben Sie die das Zertifikat ausstellende Organisation ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter **O**= (**O**rganization).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.11 Abteilung

Geben Sie die das Zertifikat ausstellende Abteilung ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter **OU**= (**O**rganization **U**nit).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.12 Provinz-oder-Bundesland

Geben Sie das Bundesland ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter ST= (**ST**ate).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.13 E-Mail

Geben Sie eine E-Mail-Adresse ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `emailAddress=`.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.39.2.14.1.14 Nachname

Geben Sie einen Nachnamen ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter SN= (**S**ur**N**ame).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.15 Seriennummer

Geben Sie eine Seriennummer ein.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.16 Postleitzahl

Geben Sie die Postleitzahl des Ortes ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `postalCode=`.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 25 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.39.2.14.1.17 Vorlage

Wählen Sie hier ggf. eine passende Profil-Vorlage aus.

In der Profil-Vorlage ist festgelegt, welche Zertifikatsangaben notwendig und welche änderbar sind. Die Vorlagen-Erstellung erfolgt unter **Setup** > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.1.18 Subject-Alternative-Name

Geben Sie hier den Subject-Alternative-Namen (SAN) an. Der SAN enthält weitere Informationen, die Applikationen verwenden können.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.2 Vorlage

In dieser Tabelle definieren Sie Vorlagen für Zertifikat-Profile.

Hier legen Sie fest, welche der Profileigenschaften erforderlich und welche durch den Anwender zu editieren sind. Die folgenden Optionen stehen zur Auswahl:

- Nein: Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.
- Fest: Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.
- Ja: Das Feld ist sichtbar und durch den Anwender änderbar.
- Erzwingen: Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

Standardmäßig ist bereits eine Vorlage „Default" angelegt.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle**

2.39.2.14.2.1 Name

Vergeben Sie hier einen eindeutigen Namen für die Vorlage.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

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

Default-Wert:

leer

2.39.2.14.2.2 Schluessel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.3 Erw.-Schluessel-Verwendung

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.4 RSA-Schluessellaenge

Gibt die Länge des Schlüssels an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.5 Gueltigkeitsperiode

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.6 CA

Gibt an, ob es sich um ein CA-Zertifikat handelt.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.8 Land

Gibt die Staatenkennung an (z. B. „DE“ für Deutschland).

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.9 Stadt

Gibt den Ort an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.10 Unternehmen

Gibt die das Zertifikat ausstellende Organisation an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.11 Abteilung

Gibt die das Zertifikat ausstellende Abteilung an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.12 Provinz-oder-Bundesland

Gibt das Bundesland an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.13 E-Mail

Gibt die E-Mail-Adresse an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.14 Nachname

Gibt den Nachnamen an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.15 Seriennummer

Gibt die Seriennummer an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.16 Postleitzahl

Gibt die Postleitzahl an.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.2.14.2.17 Subject-Alternative-Name

Der „Subject-Alternative-Name" (SAN) verknüpft weitere Daten mit diesem Zertifikat.

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

2.39.3 CRLs

Dieses Menü enthält die Konfiguration der CRLs.

SNMP-ID: 2.39.3

Pfad Telnet: /Setup/Zertifikate

2.39.3.1 Aktiv

Aktiviert: Bei Prüfung eines Zertifikats wird die CRL (falls vorhanden) ebenfalls herangezogen.

SNMP-ID: 2.39.3.1

Pfad Telnet: /Setup/Zertifikate/CRLs

Mögliche Werte:

- Ja
- Nein

Default: Nein

Wenn diese Option aktiviert ist und keine gültige CRL gefunden werden kann, weil z. B. der Server nicht erreichbar ist, werden alle Verbindungen abgelehnt und bestehende Verbindungen unterbrochen.

2.39.3.4 Holen-Vor-Ablauf

Der Zeitpunkt vor dem Ablauf der CRL, ab dem versucht wird, eine neue CRL zu laden. Dieser Wert wird um einen Zufallskomponente erhöht, um gehäufte Anfragen an den Server zu vermeiden. Be Erreichen dieses Zeitpunkts wird ein evtl. aktiviertes regelmäßiges Update angehalten.

SNMP-ID: 2.39.3.4

Pfad Telnet: /Setup/Zertifikate/CRLs

Mögliche Werte:

- max. 10 Zeichen

Default: 300

Wenn die CRL im ersten Versuch nicht geladen werden kann, werden in kurzen Zeitabständen neue Versuche gestartet.

2.39.3.5 Automatische-Auffrisch-Periode

Die Länge des Zeitraums, nach dessen Ablauf periodisch versucht wird, eine neue CRL zu erhalten. Hiermit können eventuell außer der Reihe veröffentlichte CRLs frühzeitig heruntergeladen werden. Mit einem Eintrag von '0' wird das regelmäßige Abruf ausgeschaltet.

SNMP-ID: 2.39.3.5

Pfad Telnet: /Setup/Zertifikate/CRLs

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Wenn die CRL bei regelmäßigen Update nicht geladen werden kann, werden keine Versuche bis zum nächsten regelmäßigen Termin gestartet.

2.39.3.6 Gueltigkeitszeitueberschreitung

Zertifikatsbasierte Verbindungen werden auch nach Ablauf der CRL-Gültigkeit noch innerhalb des hier eingetragenen Zeitraums zugelassen. Mit dieser Toleranz-Zeit kann verhindert werden, dass z. B. bei kurzfristig nicht erreichbarem CRL-Server die Verbindungen abgelehnt oder getrennt werden.

SNMP-ID: 2.39.3.6

Pfad Telnet: /Setup/Zertifikate/CRLs

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: Innerhalb des hier eingestellten Zeitraums kann mit Hilfe der in der CRL bereits gesperrten Zertifikate weiterhin eine Verbindung aufrecht erhalten bzw. eine neue Verbindung aufgebaut werden.

In der hier definierten Zeitspanne können auch abgelaufene Zertifikate genutzt werden, um einer Verbindung aufrecht zu erhalten oder neu aufzubauen.

2.39.3.7 CRL-Jetzt-Abholen

Holt die aktuelle CRL von der im Root-Zertifikat angegebenen URL bzw. von der Alternativ-URL, sofern diese Funktion eingerichtet ist.

SNMP-ID: 2.39.3.7

Pfad Telnet: /Setup/Zertifikate/CRLs

2.39.3.8 Alternative-URL-Tabelle

In dieser Tabelle finden Sie die Liste der alternativen URLs.

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. Im LCOS können in einer Tabelle alternative URLs angegeben werden. Nach dem Systemstart werden die entsprechenden CRLs automatisch von diesen URLs abgeholt und zusätzlich zu den in den Zertifikaten angegebenen Listen verwendet.

SNMP-ID: 2.39.3.8

Pfad Telnet: /Setup/Zertifikate/CRLs/Alternative-URL-Tabelle

2.39.3.8.1 Alternative-URL

Geben Sie hier die alternative URL an, von der eine CRL abgeholt werden kann.

SNMP-ID: 2.39.3.8.1

Pfad Telnet: /Setup/Zertifikate/CRLs/Alternative-URL-Tabelle/Alternative-URL

Mögliche Werte:

- Gültige URL, max. 251 Zeichen.

Default: leer

2.39.3.9 Loopback-Adresse

Definieren Sie hier optional eine Sender-Adresse, die dem Empfänger anstelle der automatisch erzeugten Adresse angezeigt wird.

SNMP-ID: 2.39.3.9

Pfad Telnet: /Setup/Zertifikate/CRLs/Loopback-Adresse

Mögliche Werte:

- Name des IP-Netzwerks, dessen Adresse benutzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse des ersten DMZ
- LB0 - LBF für die 16 Loopback-Adressen
- Jede gültige IP-Adresse

Default: leer

Wenn es eine Schnittstelle namens "DMZ" gibt, dann wird deren Adresse genommen, wenn Sie "DMZ" auswählen.

2.39.6 OCSP-Client

Dieses Menü enthält die Einstellungen für den OCSP-Client.

SNMP-ID: 2.39.6

Pfad Telnet: /Setup/Zertifikate

2.39.6.1 CA-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

SNMP-ID: 2.39.6.1

Pfad Telnet: /Setup/Zertifikate/OCSP-Client

2.39.6.1.1 Profilname

Geben Sie hier den Namen eines CA-Profils ein, welches der OCSP-Client für eine bestimmte CA verwendet.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

Maximal 32 alphanumerische Zeichen

Default:

2.39.6.1.2 CA-DN

Geben Sie hier den Distinguished Name der CA ein, deren Zertifikate der OCSP-Client mit diesem Profil prüft.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

Maximal 251 alphanumerische Zeichen

Default:

2.39.6.1.3 AIA-Bevorzugen

Die Zertifikate für den VPN-Verbindungsaufbau führen optional den URL des zuständigen OCSP-Responders im Feld Auhority Info Access (AIA) mit. Stellen Sie hier ein, ob der OCSP-Client vorrangig den URL aus diesem Eintrag der CA-Profiltabelle verwendet oder den URL aus dem AIA-Feld sofern vorhanden.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

- **nein**: Der OCSP-Client verwendet immer den URL aus diesem Eintrag der CA-Profiltabelle und lässt den URL im AIA-Feld unbeachtet.

- **ja**: Der OCSP-Client verwendet (sofern angegeben) den URL aus dem AIA-Feld und lässt den URL aus diesem Eintrag der CA-Profiltabelle unbeachtet.

Default:

nein

2.39.6.1.4 Responder-Profilname

Wählen Sie hier das Responder-Profil aus, mit dem der OCSP-Client die Zertifikate dieser CA prüft.

Wenn das Feld für den Responder-Profilnamen frei bleibt, prüft das Gerät die verwendeten Zertifikate für die in diesem Eintrag definierte CA nicht mit OCSP, sondern mit Hilfe einer CRL.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

Auswahl aus der Liste der Profilnamen in der Tabelle *2.39.6.2 Responder-Profiltabelle*, maximal 32 alphanumerische Zeichen

Default:

2.39.6.1.5 Quellinterface

Hier können Sie optional eine Absenderadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

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

  Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' existiert, verwendet das Gerät stattdessen die zugehörige IP-Adresse!
- `LB0`...`LBF` für eine der 16 Loopback-Adressen oder deren Name
- Beliebige IPv4-Adresse

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

Default:

0.0.0.0

2.39.6.1.6 Cert-Pruefung

Stellen Sie hier ein, wie sich das Gerät bei einer nicht erfolgreichen Prüfung des Zertifikats verhält. Der OCSP-Client fragt zunächst beim Verbindungsaufbau die Gültigkeit des verwendeten Zertifikats beim OCSP-Responder an. Wenn das Zertifikat in Kürze abläuft, fragt der OCSP-Client rechtzeitig vor dem Ablaufdatum automatisch die Gültigkeit erneut ab.

Überprüfen und protokollieren Sie die Ergebnisse der Zertifikatsprüfung beim OCSP-Responder bei Bedarf mit SYSLOG, SNMP-Traps und entsprechenden Traces.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

- **Streng**: Wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau als nicht gültig meldet, baut das Gerät keine Verbindung zur Gegenstelle auf. Wenn der OCSP-Responder während einer bestehenden Verbindung auf eine erneute Anfrage vor dem Ende des Ablaufdatums die Gültigkeit des verwendeten Zertifikats nicht rechtzeitig bestätigt, baut das Gerät die Verbindung ab.
- **Lose**: Wenn der OCSP-Responder die Anfrage für das verwendete Zertifikat beim Verbindungsaufbau als nicht gültig meldet, baut das Gerät trotzdem eine Verbindung zur Gegenstelle auf. Wenn der OCSP-Responder während einer bestehenden Verbindung auf eine erneute Anfrage vor dem Ende des Ablaufdatums die Gültigkeit des verwendeten Zertifikats nicht rechtzeitig bestätigt, baut das Gerät die Verbindung dennoch nicht ab.

Default:

Streng

2.39.6.1.7 Syslog-Events

Der OCSP-Client kann optional SYSLOG-Nachrichten mit Informationen über die Ergebnisse der Zertifikatsprüfungen beim OCSP-Responder erzeugen.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **CA-Profiltabelle**

Mögliche Werte:

- **ja**: Der OCSP-Client erzeugt SYSLOG-Nachrichten.
- **nein**: Der OCSP-Client erzeugt keine SYSLOG-Nachrichten.

Default:

ja

2.39.6.2 Responder-Profiltabelle

Diese Tabelle enthält die Informationen über die Certificate Authorities (CAs), deren Zertifikate der OCSP-Client mit einer Anfrage an einen OCSP-Responder prüft.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client**

2.39.6.2.1 Profilname

Geben Sie hier den Namen eines OCSP-Responder-Profils ein, das der OCSP-Client in der CA-Profiltabelle referenziert.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **Responder-Profiltabelle**

Mögliche Werte:

Maximal 32 alphanumerische Zeichen

Default:

2.39.6.2.2 URL

Geben Sie hier den URL an, über welchen der OCSP-Client den OCSP-Responder erreicht.

Pfad Telnet:

Setup > **Zertifikate** > **OCSP-Client** > **Responder-Profiltabelle**

Mögliche Werte:

Gültige URL mit maximal 251 alphanumerische Zeichen

Default:

2.40 GPS

Hier finden Sie die Einstellungen für GPS.

SNMP-ID: 2.40

Pfad Telnet: /Setup/GPS

2.40.1 Aktiv

Aktivieren oder deaktivieren Sie hier die GPS-Funktion. Sie können das GPS-Modul unabhängig von der gewählten Verifikations-Methode der Standort-Verifikation einschalten, um die aktuellen Standortkoordinaten beispielsweise mit LANmonitor zu überwachen.

Pfad Telnet:

Setup > **GPS**

Mögliche Werte:

Nein

Ja

Default:

Nein

2.41 UTM

Hier finden Sie die Einstellung zu UTM.

SNMP-ID: 2.41

Pfad Telnet: /Setup/

2.41.2 Content-Filter

Hier finden Sie die Einstellungen für den Content-Filter.

SNMP-ID: 2.41.2

Pfad Telnet: /Setup/UTM/

2.41.2.1 Aktiv

Hier können Sie den Content Filter aktivieren.

Pfad Telnet: /Setup/UTM/Content-Filter/Aktiv

Mögliche Werte:

- Ja: Aktiviert den Content Filter.
- Nein: Deaktiviert den Content Filter.

Default:

- Nein

2.41.2.2 Globale Einstellungen

NEW

Hier finden Sie die globalen Einstellungen für den Content-Filter.

SNMP-ID: 2.41.2.2

Pfad Telnet: /Setup/UTM/Content-Filter/

2.41.2.2.1 Admin-Email

Um die E-Mail Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Wenn kein E-Mail Empfänger angegeben wird, dann wird keine E-Mail verschickt.

2.41.2.2.5 Aktion bei Fehler

Hier können Sie bestimmen, was bei einem Fehler passieren soll. Kann der Bewertungsserver beispielsweise nicht kontaktiert werden, kann der Benutzer in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- Blockieren, Durchlassen

Default: Blockieren

2.41.2.2.6 Aktion bei Lizenzüberschreitung

Hier können Sie bestimmen, was bei Überschreitung der lizensierten Benutzeranzahl passieren soll. Die Benutzer werden über die IP-Adresse identifiziert. Das heißt, dass die IP-Adressen, die eine Verbindung durch den LANCOM Content Filter aufbauen, gezählt werden. Baut z. B. bei einer 10er Option ein elfter Benutzer eine Verbindung auf, findet keine Prüfung mehr durch den LANCOM Content Filter statt. Der Benutzer, für den keine Lizenz mehr zur Verfügung steht, kann in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- Blockieren, Durchlassen

Default: Blockieren

Die Benutzer des Content-Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 5 Minuten keine Verbindung durch den Content-Filter mehr aufgebaut wurde.

2.41.2.2.7 Aktion bei Lizenzablauf

Die Lizenz zur Nutzung des LANCOM Content Filters gilt für einen bestimmten Zeitraum. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mailadresse, die konfiguriert ist unter LANconfig: Meldungen > Allgemein).

Hier können Sie bestimmen, was bei Ablauf der Lizenz passieren soll (blockieren oder ungeprüft durchlassen). Der Benutzer kann in Folge dieser Einstellung bei Ablauf der für ihn verwendeten Lizenz entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- Blockieren, Durchlassen

Default: Blockieren

2.41.2.2.9 Benachrichtigung

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, über welchen Weg Meldungen ausgegeben werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/

Fehler:

- Bei SYSLOG: Quelle “System”, Priorität “Alarm”.
- Default: Benachrichtigung SYSLOG

Lizenzüberschreitung:

- Bei SYSLOG: Quelle “Verwaltung”, Priorität “Alarm”.
- Default: Benachrichtigung E-MAIL, SNMP und SYSLOG

Lizenzablauf:

- Bei SYSLOG: Quelle “Verwaltung”, Priorität “Alarm”.
- Default: Benachrichtigung E-MAIL, SNMP und SYSLOG

Override:

- Bei SYSLOG: Quelle “Router”, Priorität “Alarm”.
- Default: Keine Benachrichtigung

Proxy-Limit:

- Bei SYSLOG: Quelle "Router", Priorität "Info"
- Default: Benachrichtigung SYSLOG

2.41.2.2.9.1 Grund

Wählen Sie hier einen der vordefinierten Werte für den Grund der Benachrichtigung aus.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

2.41.2.2.9.2 Email

Geben Sie hier an, ob Sie eine Benachrichtigung per Email bekommen möchten.

Je nach Grund ist diese Option unterschiedlich vorbelegt.

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen** > **Benachrichtigungen**

Mögliche Werte:

Aus
Sofort
Täglich

2.41.2.2.9.3 SNMP

Hier können Sie einstellen, ob Sie eine Benachrichtigung per SNMP bekommen möchten.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

Mögliche Werte:

- ja, nein

Default: je nach Grund unterschiedlich vorbelegt.

2.41.2.2.9.4 Syslog

Hier können Sie einstellen, ob Sie eine Benachrichtigung per SYSLOG bekommen möchten.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Benachrichtigung

Mögliche Werte:

- ja
- nein

Default: je nach Grund unterschiedlich vorbelegt.

2.41.2.2.10 Blocktext

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Blocktext definiert wird. Die Auswahl des verwendeten Blocktextes wird anhand des übermittelten Spracheinstellung des Browsers (User Agents) vorgenommen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

2.41.2.2.10.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Blocktext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

10 alphanumerische Zeichen

Default:

leer

2.41.2.2.10.2 Text

Geben Sie hier den Text ein, der als Blocktext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Blocktext

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Blocktext auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-OVERRIDEURL/> für den URL zum Freischalten des Overrides (dieser kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- ERR: wenn ein Fehler aufgetreten ist.

Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie einen alternativen Block-URL konfiguriert haben.

- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen lang sein darf.

Beispiel:

- <CF-URL/> wird wegen der Kategorien <CF-CA/> verboten.
Ihr Contentfilterprofil ist <CF-PR/>.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>

Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternativer Block-URL) verwendet werden.

2.41.2.2.11 URL wenn blockiert

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Blockierens wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Blocktext verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- gültige URL-Adresse

Default: leer

2.41.2.2.12 Loopback-wenn-blockiert

Hier können Sie optional eine Absende-Adresse für die Blockiert-URL konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- Name der IP-Netzwerke, deren 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 wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default: leer

Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

2.41.2.2.13 Override-aktiv

Hier können Sie die Override-Funktion aktivieren und weitere Einstellungen für diese Funktion vornehmen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- ja, nein

Default: nein

2.41.2.2.14 Overridedauer

Der Override kann hier zeitlich begrenzt werden. Nach Ablauf der Zeitspanne wird jedes Betreten der gleichen Domain und/oder Kategorie wieder verboten. Mit einem erneuten Klick auf den Override-Button kann die Seite wieder für die Override-Dauer betreten werden, der Administrator erhält je nach Einstellung eine erneute Benachrichtigung.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/

Mögliche Werte:

- 1-1440 (Minuten)
- max. 4 Zeichen

Default: 5 Minuten

2.41.2.2.15 Overridetyp

Hier können Sie den Override-Typ einstellen, für den der Override gelten soll. Er kann für die Domain oder die Kategorie der zu blockierenden Seite oder für beides erlaubt werden.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- Kategorie: Während der Override-Dauer sind alle URLs erlaubt, die unter die angezeigten Kategorien fallen (zuzüglich derer, die auch ohne den Override schon erlaubt gewesen wären).
- Domain: Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.
- Kategorie und Domain: Während der Override-Dauer sind alle URLs erlaubt, die sowohl zu dieser Domain als auch zu den freigeschalteten Kategorien gehören. Dies ist die stärkste Einschränkung.

Default: Kategorie und Domain

2.41.2.2.17 Im-Flashrom-speichern

Schalten Sie diese Option ein, damit die Kategoriestatistik im Flash-ROM abgelegt wird.

Dadurch gehen die Daten auch durch Ausschalten des Gerätes oder bei einem Stromausfall nicht verloren.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Im-Flashrom-speichern

Mögliche Werte:

- Ja: Aktiviert das Speichern im Flash-ROM.
- Nein: Deaktiviert das Speichern im Flash-ROM.

Default: Nein

2.41.2.2.19 Fehlertext

Hier können Sie einen Text definieren, der bei einem Fehler zur Anzeige kommt.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

2.41.2.2.19.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Fehlertext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

10 alphanumerische Zeichen

Default:

leer

2.41.2.2.19.2 Text

Geben Sie hier den Text ein, der als Fehlertext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Fehlertext

Mögliche Werte:

254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Fehlertext auch HTML-Tags verwenden.

Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

- <CF-URL/> für den verbotenen URL
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des blockierten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.
- <CF-PROFILE/> für den Profilnamen
- <CF-ERROR/> für die Fehlermeldung

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten
- OVERRIDEERROR: der Fehler ist beim Freischalten eines Override aufgetreten

Beispiel:

<CF-URL/> wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

<CF-URL>: blockierter URL <CF-HOST> oder <CF-DOMAIN>: Hostteil des blockierten URL <CF-PROFILE>: Contentfilterprofil des Benutzers <CF-DURATION>: Overridedauer in Minuten <CF-ERROR>: Fehlermeldung <CF-IF> bis </CF-IF>: bedingte Auswertung mit logischem ODER der folgenden Parameter: CHECKERROR: der Fehler ist beim Prüfen des URL aufgetreten (wie früher) OVERRIDEERROR: der Fehler ist beim Freischalten eines Overrides aufgetreten

2.41.2.2.20 Overridetext

Hier können Sie einen Text definieren, der als Bestätigung für den Benutzer bei einem Override angezeigt wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

2.41.2.2.20.1 Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Overridetext

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z. B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten

Der Contentfilter verarbeitet nur den ersten Teil des Country-Codes bis zum '-', d.h. "en", "en-GB" und "en-US" sind für den Contentfilter identisch. Der Contentfilter unterscheidet nicht zwischen Groß- und Kleinschreibung. Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

10 alphanumerische Zeichen

Default:

leer

2.41.2.2.20.2 Text

Geben Sie hier den Text ein, der als Overridetext für diese Sprache verwendet werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Overridetext

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

leer

Besondere Werte:

Sie können für den Blocktext auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z. B. verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für den ursprünglich verbotenen URL, der jetzt aber freigeschaltet ist
- <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
- <CF-BUTTON/> zeigt einen Override-Button, der auf den ursprünglich aufgerufenen URL weiterleitet.
- <CF-LINK/> zeigt einen Override-Link an, der auf den ursprünglich aufgerufenen URL weiterleitet.

- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain des freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.

Zum Ein- und Ausblenden von Teilen des HTML-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute können sein:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- FORBIDDEN: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- CATEGORY: wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- DOMAIN: wenn der Override-Typ "Domain" ist und der Override erfolgreich war
- BOTH: wenn der Override-Typ "Kategorie und Domain" ist und der Override erfolgreich war
- ERROR: falls der Override fehlgeschlagen ist
- OK: falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z. B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

Beispiel:

<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> für <CF-DU/> Minuten freigeschaltet.
<CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:
<CF-ERR/></CF-IF>

2.41.2.2.23 Schnappschuss

Hier können Sie den Content-Filter-Schnappschuss aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

2.41.2.2.23.1 Aktiv

Hier können Sie den Content-Filter-Schnappschuss aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss/Aktiv

Mögliche Werte:

- Ja: Aktiviert den Schnappschuss.
- Nein: Deaktiviert den Schnappschuss.

Default:

- Ja

2.41.2.2.23.2 Typ

Wählen Sie hier, ob der SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

Mögliche Werte

Monatlich, Wöchentlich, Täglich

Default:

Monatlich

2.41.2.2.23.3 Zeit

Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

Mögliche Werte:

- max. 5 Zeichen
- Format HH:MM

Default:

00:00

2.41.2.2.23.4 Tag

Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag an dem der SnapShot angefertigt werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

Mögliche Werte:

max. 2 Zeichen

Default:

1

Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

2.41.2.2.23.5 Wochentag

Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Schnappschuss

Mögliche Werte:

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

Default: Sonntag

2.41.2.2.24 Proxyverbindungs-Limit

Stellen Sie hier die Anzahl der Proxy-Verbindungen ein, die maximal gleichzeitig aufgebaut werden dürfen. Die Last kann somit auf dem System eingeschränkt werden. Es wird eine Benachrichtigung ausgelöst, wenn diese Anzahl überschritten wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Proxyverbindungs-Limit

Mögliche Werte:

- 0 bis 999999 Verbindungen

Default: geräteabhängig

2.41.2.2.25 Verarbeitungs-Timeout-in-ms

Stellen Sie hier die Zeit in Millisekunden ein, die der Proxy maximal für die Bearbeitung benötigen darf. Wird diese Zeit überschritten, wird dies durch eine entsprechende Zeitüberschreitungs-Fehlerseite quittiert.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen/Verarbeitungs-Timeout-in-ms

Mögliche Werte:

- 0 bis 999999 Millisekunden

Default:

- 3000 Millisekunden

Besondere Werte:

- Der Wert 0 steht für keine Zeitbegrenzung. Werte kleiner als 100 Millisekunden sind nicht sinnvoll.

2.41.2.2.21 URL bei Fehler

Hier können Sie einen alternativen URL eintragen. Im Falle eines Fehlers wird dann statt der Standard-Webseite der hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z. B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Mögliche Werte:

- gültige URL-Adresse

Default: leer

2.41.2.2.22 Loopback bei Fehler

Hier können Sie optional eine Absenderadresse für den Fehler-URL konfigurieren, der statt der ansonsten automatisch für die Ziel-Adresse gewählten Absenderadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absenderadresse angeben.

Pfad Telnet: /Setup/UTM/Content-Filter/Globale-Einstellungen

Englische Bezeichnung: Loopback-To-Use-On-Override

Mögliche Werte:

- Name der IP-Netzwerke, deren 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 wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default: leer

Die hier eingestellte Absenderadresse wird für jede Gegenstelle unmaskiert verwendet.

2.41.2.2.28 Loopback-zum-Ratingserver

Über diese Einstellung definieren Sie optional die Loopback-Adresse, die das Gerät benutzt, um sich mit dem Ratingserver zu verbinden. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

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

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Mögliche Werte:

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

  Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!
- `LB0...LBF` für eine der 16 Loopback-Adressen oder deren Name
- Beliebige IPv4-Adresse

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

Default:

2.41.2.2.29 Wildcard

Bei Webseiten mit Wildcard-Zertifikaten (bestehend aus CN-Einträgen wie z. B. `*.mydomain.de`) wird durch das Einschalten dieser Funktion die Haupt-Domain (`mydomain.de`) zur Prüfung herangezogen. Die Prüfung erfolgt dabei in dieser Reihenfolge:

- Prüfung des Servernamens im „Client Hello“ (abhängig vom verwendeten Webbrowser)
- Prüfung des CN im empfangenen SSL-Zertifikat
- Einträge mit Wildcards werden dabei ignoriert
- Ist der CN nicht verwertbar, wird das Feld „Alternative Name“ ausgewertet
- DNS Reverse Lookup der zugehörigen IP-Adresse und Prüfung des so erlangten Hostnamens
- Sind im Zertifikat Wildcards enthalten, wird stattdessen die Haupt-Domain geprüft (entspricht der oben beschriebenen Funktion)
- Prüfung der IP-Adresse

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.41.2.3 Profile

Hier finden Sie die Profil-Einstellungen für den Content-Filter.

2.41.2.3.1 Profile

Hier können Sie Content-Filter-Profile erstellen, die zur Überprüfung von Webseiten auf nicht zugelassene Inhalte genutzt werden. Ein Content-Filter-Profil hat immer einen Namen und ordnet verschiedenen Zeitabschnitten das jeweils gewünschte Kategorieprofil sowie optional eine Black- und eine Whitelist zu.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.

Bitte beachten Sie, dass Sie zur Nutzung der Profile im Content Filter entsprechende Einstellungen in der Firewall vornehmen müssen.

2.41.2.3.1.1 Name

Geben Sie hier den Namen des Content-Filter-Profils an, über das es in der Firewall referenziert wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Mögliche Werte:

- Name eines Profils
- maximal 31 Zeichen

Default:

leer

2.41.2.3.1.2 Zeitschema

Wählen Sie den Zeitrahmen für das Content-Filter-Profil. Voreingestellt sind die Zeitrahmen “Always” und “Never”. Weitere Zeitrahmen können Sie konfigurieren unter: /Setup/Zeit/Zeitrahmen.

Zu einem Content-Filter-Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Mögliche Werte:

- Always
- Never
- Name eines Zeitrahmenprofils
- maximal 31 Zeichen

Default: leer

Wenn sich bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil die Zeitrahmen überlappen, werden in diesem Zeitraum alle Seiten gesperrt, die durch einen der aktiven Einträge gesperrt werden. Bleibt bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil ein Zeitraum undefiniert, ist in diesem Zeitraum der ungeprüfte Zugriff auf alle Webseiten möglich.

2.41.2.3.1.3 Whitelist

Wählen Sie hier die Whitelist, die für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Whitelist-Tabelle aus.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Mögliche Werte:

- Name einer vorhandenen Whitelist
- maximal 31 Zeichen

Default: leer

2.41.2.3.1.4 Blacklist

Wählen Sie hier die Blacklist, die für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Blacklist-Tabelle aus.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Mögliche Werte:

- Name einer vorhandenen Blacklist
- maximal 31 Zeichen

Default: leer

2.41.2.3.1.5 Kategorieprofil

Wählen Sie hier das Kategorie-Profil, welches für dieses Content-Filter-Profil gelten soll. Geben Sie einen neuen Namen ein oder wählen Sie einen vorhandenen Eintrag aus der Tabelle der Kategorie-Profile aus.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Mögliche Werte:

- Name eines Kategorie-Profils
- maximal 31 Zeichen

Default: leer

2.41.2.3.2 Whitelists

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Die Einträge für die erlaubten Webseiten können maximal 252 Zeichen umfassen. Um längere Whitelist-Einträge zu definieren, können mehrere Einträge einen speziellen, gemeinsamen Namen verwenden. Geben Sie dazu den Namen der Whitelist ein gefolgt von einem #-Zeichen und einem beliebigen Suffix. Zum Beispiel legen Sie drei Whitelist-Einträge mit den Namen "MyWhitelist#1", "MyWhitelist#2" und "MyWhitelist#3" an. Im Content-Filter-Profil referenzieren Sie diese erweiterte Whitelist dann mit dem Namen "MyWhitelist".

2.41.2.3.2.1 Name

Hier muss der Name der Whitelist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Whitelists

Mögliche Werte:

- Name einer Whitelist
- maximal 31 Zeichen

Default:

leer

2.41.2.3.2.2 Whitelist

Hier können Sie Webseiten konfigurieren, die lokal geprüft und anschließend akzeptiert werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Whitelists

Mögliche Werte:

- gültige URL-Adresse(n)
- maximal 252 Zeichen

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z. B. findet www.beispiel.* die Webseiten www.beispiel.de, www.beispiel.en, www.beispiel.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.beispiel.e? die Webseiten www.beispiel.en und www.beispiel.es)

Bitte geben Sie die URL ohne führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

Einzelne URLs werden mit Leerzeichen getrennt.

Default:

leer

2.41.2.3.3 Blacklists

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile

Die Einträge für die verbotenen Webseiten können maximal 252 Zeichen umfassen. Um längere Blacklist-Einträge zu definieren, können mehrere Einträge einen speziellen, gemeinsamen Namen verwenden. Geben Sie dazu den Namen der Blacklist ein gefolgt von einem #-Zeichen und einem beliebigen Suffix. Zum Beispiel legen Sie drei Blacklist-Einträge mit den Namen "MyBlacklist#1", "MyBlacklist#2" und "MyBlacklist#3" an. Im Content-Filter-Profil referenzieren Sie diese erweiterte Blacklist dann mit dem Namen "MyBlacklist".

2.41.2.3.3.1 Name

Hier muss der Name der Blacklist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Blacklists

Mögliche Werte:

- Name einer Blacklist
- maximal 31 Zeichen

Default:

leer

2.41.2.3.3.2 Blacklist

Hier werden die URLs eingetragen, die über diese Blacklist verboten werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Blacklists

Mögliche Werte:

- gültige URL-Adresse(n)
- maximal 252 Zeichen

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z. B. findet www.beispiel.* die Webseiten www.beispiel.de, www.beispiel.en, www.beispiel.es etc.)
- ? für ein beliebiges Zeichen (z. B. findet www.beispiel.e? die Webseiten www.beispiel.en und www.beispiel.es)

Bitte geben Sie die URL ohne führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z. B. www.mycompany.de/ . Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

Einzelne URLs werden mit Leerzeichen getrennt.

Default:

leer

2.41.2.3.4 Kategorieprofile

Hier erstellen Sie ein Kategorieprofil und legen fest, welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede Gruppe können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/

2.41.2.3.4.1 Name

Hier wird der Name der Kategorieprofils angegeben, über den sie im Content-Filter-Profil referenziert wird.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Mögliche Werte:

- Name eines Kategorieprofils
- maximal 31 Zeichen

Default:

leer

2.41.2.3.4.100 Not_Categorized

Legen Sie hier fest, wie der Content-Filter URLs behandlen soll, die der Ratingserver noch nicht kennt und für die er deshalb keine Kategorien liefern kann.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Mögliche Werte:

Erlaubt, Verboten, Override

Default: Erlaubt

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

2.41.2.3.4.101 Pornography/Erotic/Sex

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.103 Swimwear/Lingerie

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.104 Shopping

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.105 Auctions/Classified_Ads

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.106 Governmental/Non-Profit_Organizations

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.108 Cities/Regions/Countries

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.109 Education

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.110 Political_Parties

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.111 Religion/Spirituality

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.113 Illegal_Activities

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.114 Computer_Crime/Warez/Hacking

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.115 Political_Extreme/Hate/Discrimination

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.117 Violence/Extreme

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.118 Gambling/Lottery

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.119 Computer_Games

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.120 Toys

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.121 Cinema/Television/Social_Media

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.122 Recreational_Facilities/Theme_Parks

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.123 Arts/Museums/Theaters

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.124 Music/Radio_Broadcast

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.125 Literature/Books

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.126 Humor/Cartoons

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.127 News/Magazines

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.128 Webmail/Unified_Messaging

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.129 Chat

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.130 Blogs/Bulletin_Boards

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.131 Mobile_Telephony

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.132 Digital_Postcards

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.133 Search_Engines/Web_Catalogs/Portals

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.134 Software/Hardware

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.135 Communication_Services

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.136 IT_Security/IT_Information

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.137 Web_Site_Translation

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.138 Anonymous_Proxies

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.139 Illegal_Drugs

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.140 Alcohol/Tobacco

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.143 Dating/Networks

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.144 Restaurants/Entertainment_Venues

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.144

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.145 Travel

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.145

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.146 Fashion/Cosmetics/Jewelry

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.146

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.147 Sports

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.147

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.148 Architecture/Construction/Furniture

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.148

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.149 Environment/Climate/Pets

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.149

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.150 Personal_Web_Sites

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.150

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.151 Job_Search

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.151

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.152 Finance/Investment

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.152

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.150 Banking

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.154

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.155 Vehicles

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.155

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.156 Weapons/Military

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.156

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.157 Medicine/Health/Self-Help

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.157

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.158 Abortion

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.158

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.160 Spam_URLs

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.160

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.161 Malware

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.161

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.162 Phishing_URLs

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.162

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.163 Instant_Messaging

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.163

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.167 General_Business

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.167

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.174 Banner_Advertisements

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.174

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.180 Web_Storage

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

SNMP-ID: 2.41.2.3.4.180

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Erlaubt

2.41.2.3.4.181 Command/Control_Server

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelet werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Pfad Telnet: /Setup/UTM/Content-Filter/Profile/Kategorieprofile

Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

Erlaubt, Verboten, Override

Default:

Verboten

2.44 CWMP

Über das CPE WAN Management Protokoll (CWMP) lassen sich Endgeräte mit einem entsprechenden Konfigurationsserver über eine WAN-Verbindung fernkonfigurieren. Die Kommunikation zwischen dem Gerät (Customer Premises Equipment,

CPE) und dem Konfigurationsserver (Auto Configuration Server, ACS) erfolgt über SOAP/HTTP(S) in Form von Remote Procedure Calls (RPC).

Pfad Telnet:

Setup

2.44.1 NTP-Server

Dieses Verzeichnis zeigt die vom CWMP konfigurierten NTP-Server zur Zeitsynchronisation an.

Pfad Telnet:

Setup > **CWMP**

2.44.1.1 NTP-Server-1

Zeigt den ersten NTP-Server an.

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

2.44.1.2 NTP-Server-2

Zeigt den zweiten NTP-Server an.

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

2.44.1.3 NTP-Server-3

Zeigt den dritten NTP-Server an.

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

2.44.1.4 NTP-Server-4

Zeigt den vierten NTP-Server an.

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

2.44.1.5 NTP-Server-5

Zeigt den fünften NTP-Server an.

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

2.44.2 Aktiv

Aktiviert oder deaktiviert das CWMP.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.44.3 Datei-Uebertragung-erlaubt

Dieser Schalter erlaubt die Übertragung einer Firmware oder einer Skript-Datei vom ACS (Auto Configuration Server) zu diesem Gerät.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.44.4 Inform-Wiederholung-Limit

Geben Sie hier an, wie oft der CPE nach einem erfolglosen Übertragungsversuch versuchen soll, eine Inform-Meldung an den ACS zu übermitteln.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

10

Besondere Werte:

0

Wiederholung deaktiviert

2.44.5 Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

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

Besondere Werte:

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 IP-Adresse in der Form x.x.x.x.

Default-Wert:

leer

2.44.6 ACS-URL

Bestimmen Sie hier die Adresse des ACS (Auto Configuration Server), mit dem sich das Gerät verbindet. Die Eingabe der Adresse erfolgt im IPv4-, IPv6- oder FQDN-Format.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

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

Default-Wert:

leer

2.44.7 ACS-Benutzername

Vergeben Sie einen Benutzernamen, den das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.44.8 ACS-Passwort

Vergeben Sie ein Passwort, das das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.44.9 Periodisches-Inform-Aktiviert

Aktiviert oder deaktiviert das Senden von periodischen Inform-Nachrichten vom Gerät zum ACS (Auto Configuration Server).

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.44.10 Periodisches-Inform-Intervall

Dies ist das Intervall in Sekunden zwischen zwei durch das Gerät zum ACS (Auto Configuration Server) eingeleiteten periodischen Inform-Nachrichten. Der ACS erfragt daraufhin weitere Informationen vom Gerät.

Der Standard-Wert beträgt 1200 Sekunden, d. h. 20 Minuten. Wählen Sie diesen Wert nicht zu klein, da Inform-Nachrichten einen erhöhten Netzwerk-Verkehr verursachen. Das Intervall startet nicht, bevor Gerät und Server alle Informationen ausgetauscht haben.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

1200

Besondere Werte:

0

Inform-Nachrichten deaktiviert

2.44.11 Periodische-Inform-Zeit

Geben Sie die periodische Inform-Zeit an. Dieser Eintrag im „dateTime"-Format enthält die Zeit für die erste Inform-Nachricht. Beispiel: `0001-02-03T03:04:05+06:00`.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.44.12 Verbindungs-Anfrage-Benutzername

Wählen Sie einen der konfigurierten Geräte-Administratoren, den der ACS (Auto Configuration Server) beim Verbindungs-Aufbau zu diesem Gerät verwenden soll. Der ausgewählte Name muss ein aktivierter Geräte-Administrator mit entsprechenden Rechten sein, d.h., er muss Root-Zugriff zum Ändern der Firmware besitzen.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.44.13 Firmware-Updates-Verwalten

Dieser Schalter erlaubt dem ACS (Auto Configuration Server), Firmware-Änderungen am Gerät vorzunehmen.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.44.14 Benutzernamen-Aendern-erlaubt

Dieser Schalter erlaubt dem ACS (Auto Configuration Server), den Geräte-Administrator zu wechseln oder den Namen des Geräte-Administrators zu ändern, den er zur Verbindung mit dem Gerät verwendet.

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.44.15 Provisionierungs-Code

Zeigt den ACS-Provisionierungs-Code an.

Pfad Telnet:

Setup > **CWMP**

2.44.16 Parameter-Schluessel

Zeigt den Parameter-Schlüssel an.

Mit dem Parameter-Schlüssel behält der ACS einen Überblick über seine Änderungen.

Pfad Telnet:

Setup > **CWMP**

2.44.17 Command-Key

Zeigt den Command-Key des ACS an.

Pfad Telnet:

Setup > **CWMP**

2.52 COM-Ports

Dieses Menü enthält die Konfiguration der COM-Ports.

SNMP-ID: 2.52

Pfad Telnet: /Setup

2.52.1 Geraete

Die seriellen Schnittstellen können im Gerät für verschiedene Anwendungen genutzt werden, z. B. für den COM-Port-Server oder als WAN-Schnittstelle. In der Geräte-Tabelle können den einzelnen seriellen Geräten bestimmte Anwendungen zugewiesen werden.

SNMP-ID: 2.52.1

Pfad Telnet: /Setup/COM-Ports

2.52.1.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

SNMP-ID: 2.52.1.1

Pfad Telnet: /Setup/COM-Ports/Geraete

Mögliche Werte:

- Alle verfügbaren seriellen Schnittstellen.

Default: Outband

2.52.1.4 Dienst

Aktivierung des Ports für den COM-Port-Server.

SNMP-ID: 2.52.1.4

Pfad Telnet: /Setup/COM-Ports/Geraete

Mögliche Werte:

- WAN
- COM-Port server

Default: WAN

2.52.2 COM-Port-Server

Dieses Menü enthält die Konfiguration des COM-Port-Servers.

SNMP-ID: 2.52.2

Pfad Telnet: /Setup/COM-Ports

2.52.2.1 Betrieb

Diese Tabelle aktiviert den COM-Port-Server auf einem Port einer bestimmten seriellen Schnittstelle. Fügen Sie dieser Tabelle eine Zeile hinzu, um eine neue Instanz des COM-Port-Servers zu starten. Löschen Sie eine Zeile, um die entsprechende Server-Instanz abzubrechen.

SNMP-ID: 2.52.2.1

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server

2.52.2.1.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

SNMP-ID: 2.52.2.1.1

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Device-Type

Mögliche Werte:

- Alle verfügbaren seriellen Schnittstellen.

Default: Outband

2.52.2.1.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

SNMP-ID: 2.52.2.1.2

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Device-Type

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

2.52.2.1.4 Operating

Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

SNMP-ID: 2.52.2.1.4

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Device-Type

Mögliche Werte:

- Ja
- Nein

Default: Nein

2.52.2.2 COM-Port-Einstellungen

Diese Tabelle enthält die Einstellungen für die Datenübertragung auf der seriellen Schnittstelle.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.

SNMP-ID: 2.52.2.2

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server

2.52.2.2.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

SNMP-ID: 2.52.2.2.1

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- Alle verfügbaren seriellen Schnittstellen.

Default: Outband

2.52.2.2.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

SNMP-ID: 2.52.2.2.2

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

2.52.2.2.4 Bitrate

Verwendete Bitrate auf dem COM-Port.

SNMP-ID: 2.52.2.2.4

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- 110 bis 230400

Default: 9600

2.52.2.2.5 Daten-Bits

Anzahl der Daten-Bits.

SNMP-ID: 2.52.2.2.5

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- 7
- 8

Default: 8

2.52.2.2.6 Paritaet

Auf dem COM-Port verwendetes Prüfverfahren.

SNMP-ID: 2.52.2.2.6

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- keine
- gerade
- ungerade

Default: keine

2.52.2.2.7 Stop-Bits

Anzahl der Stop-Bits.

SNMP-ID: 2.52.2.2.7

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- 1
- 2

Default: 1

2.52.2.2.8 Handshake

Auf dem COM-Port verwendete Datenflusskontrolle.

SNMP-ID: 2.52.2.2.8

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- keiner
- RTS/CTS

Default: RTS/CTS

2.52.2.2.9 Bereit-Bedingung

Eine wichtige Eigenschaft eines seriellen Ports ist die Bereit-Bedingung. Der COM-Port-Server überträgt keine Daten zwischen dem seriellen Port und dem Netzwerk, solange er sich nicht im Zustand "Bereit" befindet. Außerdem wird der Wechsel zwischen den Zuständen "Bereit" und "Nicht-Bereit" verwendet, um im Client-Modus TCP-Verbindungen aufzubauen bzw. abzubrechen. Die Bereitschaft des Ports kann auf zwei verschiedene Arten ermittelt werden. Im DTR-Modus (Default) wird nur der DTR-Handshake überwacht. Die serielle Schnittstelle wird solange als bereit angesehen, wie die DTR-Leitung aktiv ist. Im Daten-Modus wird die serielle Schnittstelle als bereit betrachtet, sobald sie Daten empfängt. Wenn für die eingestellte Timeout-Zeit keine Daten empfangen werden, fällt der Port zurück in den Zustand "Nicht-Bereit".

SNMP-ID: 2.52.2.2.9

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- DTR
- Daten

Default: DTR

2.52.2.2.10 Bereit-Daten-Timeout

Der Timeout schaltet den Port wieder in den Zustand Nicht-Bereit, wenn keine Daten empfangen werden. Mit einem Timeout von Null wird diese Funktion ausgeschaltet. In diesem Fall ist der Port immer bereit, wenn der Daten-Modus gewählt ist.

SNMP-ID: 2.52.2.2.10

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/COM-Port-Einstellungen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: 0 schaltet den Bereit-Daten-Timeout aus.

2.52.2.3 Netzwerk-Einstellungen

Diese Tabelle enthält alle Einstellungen, die das Verhalten des COM-Ports im Netzwerk definieren.

Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.

SNMP-ID: 2.52.2.3

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server

2.52.2.3.1 Device-Type

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

SNMP-ID: 2.52.2.3.1

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- Alle verfügbaren seriellen Schnittstellen.

Default: Outband

2.52.2.3.2 Port-Nummer

Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

SNMP-ID: 2.52.2.3.2

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

2.52.2.3.4 TCP-Modus

Jede Instanz des COM-Port-Servers überwacht im Server-Modus den definierten Listen-Port auf eingehende TCP-Verbindungen. Pro Instanz ist nur eine aktive Verbindung erlaubt, alle anderen Verbindungsanfragen werden abgelehnt. Im Client-Modus versucht die Instanz eine TCP-Verbindung über einen definierten Port zur angegebenen Gegenstelle aufzubauen, sobald der Port bereit ist. Die TCP-Verbindung wird wieder geschlossen, sobald der Port nicht mehr bereit ist. In beiden Fällen schließt das Gerät die offenen Verbindungen bei einem Neustart.

SNMP-ID: 2.52.2.3.4

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- Server
- Client

Default: Server

2.52.2.3.5 Listen-Port

Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

SNMP-ID: 2.52.2.3.5

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.52.2.3.6 Aufbau-Host-Name

Zu diesem Host baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand "Bereit" befindet.

SNMP-ID: 2.52.2.3.6

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- DNS-Name
- IP-Adresse

Default: leer

2.52.2.3.7 Aufbau-Port

Über diesen TCP-Port baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand "Bereit" befindet.

SNMP-ID: 2.52.2.3.7

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- max. 10 Zeichen

Default: 0

2.52.2.3.8 Loopback-Addr.

Über diese Adresse kann der COM-Port angesprochen werden. Dies ist die eigene IP-Adresse, die als Quelladresse beim Verbindungsaufbau benutzt wird. Sie wird z. B. verwendet, um die IP-Route festzulegen, über die die Verbindung aufgebaut wird.

SNMP-ID: 2.52.2.3.8

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- max. 16 Zeichen

Default: leer

2.52.2.3.9 RFC2217-Erweiterungen

Die RFC2217-Erweiterungen können für beide TCP-Modi aktiviert werden. Wenn diese Erweiterungen eingeschaltet sind, signalisiert ein Gerät seine Bereitschaft, Telnet Steuerungssequenzen zu akzeptieren, mit der Sequenz IAC DO

COM-PORT-OPTION. In der Folge werden auf dem COM-Port die entsprechenden Optionen verwendet, die konfigurierten Default-Werte werden überschrieben. Außerdem versucht der Port, für Telnet das lokale Echo und den Line Mode zu verhandeln. Die Verwendung der RFC2217-Erweiterungen ist auch bei nicht kompatibler Gegenstelle unkritisch, möglicherweise werden dann unerwartete Zeichen bei der Gegenstelle angezeigt. Als Nebeneffekt führt die Verwendung der RFC2217-Erweiterungen dazu, dass der Port einen regelmäßigen Alive-Check durchführt, indem Telnet-NOPs zur Gegenstelle gesendet werden.

SNMP-ID: 2.52.2.3.9

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- Ja
- Nein

Default: Ja

2.52.2.3.10 Newline-Konversion

Wählen Sie hier aus, welches Zeichen auf dem seriellen Port ausgegeben wird, wenn der Binär-Modus aktiviert ist.

Die Einstellung ist abhängig von der Anwendung, die über den seriellen Port kommunizieren wird. Wenn an den Port ein weiteres Gerät angeschlossen ist, können Sie hier entweder CRLF oder nur CR wählen, da die Outband-Schnittstelle dieser Geräte ein “Carriage Return” zur automatischen Bestimmung der Datenübertragungsgeschwindigkeit erwartet. Manche Unix-Anwendungen würden CRLF allerdings als unerlaubte doppelte Zeilenschaltung interpretieren, in diesem Fall wählen Sie CR oder LF.

SNMP-ID: 2.52.2.3.10

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- CRLF
- CR
- LF

Default:

CRLF

Diese Einstellung wird nur ausgewertet, wenn für diesen seriellen Port der Binär-Modus deaktiviert ist.

2.52.2.3.12 TCP-Wdh.-Timeout

Maximale Zeit für den Retransmission-Timeout. Dieser Timeout gibt an, in welchen Intervallen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

SNMP-ID: 2.52.2.3.12

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- 0 bis 99 Sekunden
- maximal 2 Zeichen

Besondere Werte:

- 0 verwendet den Standardwert nach RFC 1122 (60 Sekunden).

Default:

- 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

2.52.2.3.13 TCP-Wdh.-Zahl

Maximale Anzahl der Versuche, mit denen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

SNMP-ID: 2.52.2.3.13

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- 0 bis 9
- maximal 1 Zeichen

Besondere Werte:

- 0 verwendet den Standardwert nach RFC 1122 (5 Versuche).

Default:

- 0

Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

2.52.2.3.14 TCP-Keepalive

Der RFC 1122 definiert ein Verfahren, mit dem die Verfügbarkeit von TCP-Verbindungen geprüft werden kann (TCP-Keepalive). Ein inaktiver Transmitter sendet nach diesem Verfahren Anfragen nach dem Empfängerstatus an die Gegenstelle. Wenn die TCP-Sitzung zur Gegenstelle verfügbar ist, antwortet diese mit ihrem Empfängerstatus. Wenn die TCP-Sitzung zur Gegenstelle nicht verfügbar ist, wird die Anfrage in einem kürzeren Intervall solange wiederholt, bis die Gegenstelle mit ihrem Empfängerstatus antwortet (danach wird wieder ein längeres Intervall verwendet). Sofern die zugrunde liegende Verbindung funktioniert, die TCP-Sitzung zur Gegenstelle allerdings nicht verfügbar ist, sendet die Gegenstelle ein RST-Paket und löst so den Abbau der TCP-Sitzung bei der anfragenden Applikation aus.

SNMP-ID: 2.52.2.3.14

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- inaktiv: Der TCP-Keepalive wird nicht verwendet.
- aktiv: Der TCP-Keepalive ist aktiv, nur RST-Pakete führen zum Abbau von TCP-Sitzungen.
- proaktiv: Der TCP-Keepalive ist aktiv, wiederholt die Anfrage nach dem Empfängerstatus der Gegenstelle aber nur für den als "TCP-Wdh.-Zahl" eingestellten Wert. Sofern nach dieser Anzahl von Anfragen keine Antwort mit dem Empfängerstatus vorliegt, wird die TCP-Sitzung als "nicht verfügbar" eingestuft und an die Applikation gemeldet. Wird während der Wartezeit ein RST-Paket empfangen, so löst dieses vorzeitig den Abbau der TCP-Sitzung aus.

Default:

- inaktiv

Für Serverapplikationen wird die Einstellung “aktiv” empfohlen.

2.52.2.3.15 TCP-Keepalive-Intervall

Dieser Wert gibt an, in welchen Intervallen die Anfragen nach dem Empfängerstatus versendet werden, wenn die erste Anfrage nicht erfolgreich beantwortet wurde. Der dazu gehörende Timeout wird gebildet als Intervall / 3 (maximal 75 Sekunden).

SNMP-ID: 2.52.2.3.15

Pfad Telnet: /Setup/COM-Ports/COM-Port-Server/Netzwerk-Einstellungen

Mögliche Werte:

- maximal 10 Ziffern

Default:

- 0

Besondere Werte:

- 0 verwendet den Standardwert nach RFC 1122 (Intervall 7200 Sekunden, Timeout 75 Sekunden).

2.52.2.3.16 Binaermodus

Über diese Einstellung bestimmen Sie, ob das Gerät serielle Daten binär weiterleitet und somit keine CR/LF-Anpassung (CR/LF = Carriage Return/Line Feed) erfolgt. Da der Binärmodus bei manchen seriellen Gegenstellen zu Problemen führt, sollten Sie die Voreinstellung **Auto** beibehalten.

Pfad Telnet:

Setup > **COM-Ports** > **COM-Port-Server** > **Netzwerk-Einstellungen**

Mögliche Werte:

Auto: Der COM-Port-Server schaltet für die Datenübertragung zunächst in den ASCII-Modus, führt aber über die Telnet-Optionen mit der Gegenstelle eine Verhandlung darüber, ob er in den Binärmodus umschalten darf.

ja: Der COM-Port-Server schaltet für die Datenübertragung in den Binärmodus und führt über die Telnet-Optionen mit der Gegenstelle keine Verhandlung darüber aus.

nein: Der COM-Port-Server schaltet für die Datenübertragung in den ASCII-Modus und führt über die Telnet-Optionen mit der Gegenstelle keine Verhandlung darüber aus.

Default:

Auto

2.52.3 WAN

Dieses Menü enthält die Konfiguration des Wide-Area-Networks (WAN).

SNMP-ID: 2.52.3

Pfad Telnet: /Setup/COM-Ports

2.52.3.1 Geraete

Die Tabelle mit den WAN-Geräten dient nur als Status-Tabelle. Alle Hotplug-Geräte (über USB oder CardBus angeschlossen) tragen sich selbst in diese Tabelle ein.

SNMP-ID: 2.52.3.1

Pfad Telnet: /Setup/COM-Ports/WAN

2.52.3.1.1 Device-Type

Liste der im Gerät verfügbaren seriellen Schnittstellen.

SNMP-ID: 2.52.3.1.1

Pfad Telnet: /Setup/COM-Ports/WAN/Geraete

Mögliche Werte:

- Alle verfügbaren seriellen Schnittstellen.

2.52.3.1.3 Aktiv

Status des angeschlossenen Gerätes.

SNMP-ID: 2.52.3.1.3

Pfad Telnet: /Setup/COM-Ports/WAN/Geraete

Mögliche Werte:

- Ja
- Nein

2.53 Temperatur-Monitor

Hier finden Sie die Einstellungen für den Temperatur-Monitor.

SNMP-ID: 2.53

Pfad Telnet: /Setup/Temperatur-Monitor

2.53.1 Obergrenze-Grad

Bei Überschreiten der hier eingestellten Temperatur sendet das Gerät einen SNMP-Trap vom Typ "trpTempMonOverTemp" aus.

Pfad Telnet: /Setup/Temperatur-Monitor/Obergrenze-Grad

Mögliche Werte:

- 0 bis 127 ° Celsius

Default: 70

2.53.2 Untergrenze-Grad

Bei Unterschreiten der hier eingestellten Temperatur sendet das Gerät einen SNMP-Trap vom Typ "trpTempMonUnderTemp" aus.

Pfad Telnet: /Setup/Temperatur-Monitor/Untergrenze-Grad

Mögliche Werte:

- 0 bis 127 ° Celsius

Default: 0

2.54 TACACS

2.54.2 Authorisierung

WEBconfig: /Setup/TACACS+

WEBconfig englisch: /Setup/TACACS+

Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte: aktiviert, deaktiviert

Default: deaktiviert

Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Authorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.

2.54.3 Accounting

WEBconfig: /Setup/TACACS+

Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

Mögliche Werte: aktiviert, deaktiviert

Default: deaktiviert

Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.

2.54.6 Shared-Secret

WEBconfig: /Setup/TACACS+

Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte: 31 alphanumerische Zeichen

Default: Leer

Das Kennwort muss im Gerät und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.

2.54.7 Verschlüsselung

WEBconfig: /Setup/TACACS+

WEBconfig englisch: /Setup/TACACS+

Aktiviert oder deaktiviert die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

- aktiviert
- deaktiviert

Default: aktiviert

Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen. Wenn die Verschlüsselung hier aktiviert wird, muss außerdem das Kennwort für die Verschlüsselung passend zum Kennwort auf dem TACACS+-Server eingetragen werden.

2.54.9 Server

Zur Nutzung der TACACS+-Funktionen können zwei Server definiert werden. Dabei dient ein Server als Backup, falls der andere Server ausfällt. Beim Login über Telnet oder WEBconfig kann der Anwender den zu benutzenden Server auswählen.

Dieses Menü enthält die Einstellungen für die TACACS-Server.

SNMP-ID: 2.54.9

Pfad Telnet: /Setup/TACACS+

2.54.9.1 Server-Adresse

Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

SNMP-ID: 2.54.9.1

Pfad Telnet: /Setup/Tacacs+/Server-Adresse

Mögliche Werte Telnet:

- Gültiger DNS-auflösbarer Name oder gültige IP-Adresse.

Default: Leer

2.54.9.2 Loopback-Adresse

Hier können Sie optional eine Loopback-Adresse konfigurieren.

SNMP-ID: 2.54.9.2

Pfad Telnet: /Setup/Tacacs+/Loopback-Adresse

Mögliche Werte Telnet:

- 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

Default: Leer

2.54.9.3 Kompatibilitätsmodus

TACACS+-Server werden in einer freien und in einer kommerziellen Version angeboten, die jeweils unterschiedliche Nachrichten verwenden. Der Kompatibilitätsmodus ermöglicht die Verarbeitung der Nachrichten von den freien TACACS+-Servern.

SNMP-ID: 2.54.9.3

Pfad Telnet: /Setup/Tacacs+/Kompatibilitätsmodus

Mögliche Werte Telnet:

- aktiviert
- deaktiviert

Default: deaktiviert

2.54.10 Rückgriff auf lokale Benutzer

WEBconfig: /Setup/TACACS+

WEBconfig englisch: /Setup/TACACS+

Für den Fall, dass die definierten TACACS+-Server nicht erreichbar sind, kann ein Rückgriff auf die lokalen Benutzerkonten im Gerät erlaubt werden. So ist der Zugriff auf die Geräte auch bei Ausfall der TACACS+-Verbindung möglich, z. B. um die TACACS+-Nutzung zu deaktivieren oder die Konfiguration zu korrigieren.

Mögliche Werte: erlaubt, verboten

Default: erlaubt

Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort im Gerät gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

2.54.11 SNMP-GET-Anfragen-Authorisierung

WEBconfig: /Setup/TACACS+

WEBconfig englisch: /Setup/TACACS+

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Authorisierung zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS eine Authorisierung über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Authorisierung über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe keine Authorisierung über den TACACS+-Server erforderlich.

Default: nur_für_SETUP_Baum

2.54.12 SNMP-GET-Anfragen-Accounting

WEBconfig: /Setup/TACACS+

WEBconfig englisch: /Setup/TACACS+

Zahlreiche Netzwerkmanagementtools nutzen SNMP, um Informationen aus den Netzwerkgeräten abzufragen. Auch der LANmonitor greift über SNMP auf die Geräte zu, um Informationen über aktuelle Verbindungen etc. darzustellen oder Aktionen wie das Trennen einer Verbindung auszuführen. Da über SNMP ein Gerät auch konfiguriert werden kann, wertet TACACS+ diese Zugriffe als Vorgänge, die eine Authorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Authorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für das Accounting zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mit dem Eintrag einer Read-Only-Community unter /Setup/SNMP kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only-Community wird dazu im LANmonitor als Benutzername eingetragen.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von LCOS ein Accounting über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe ein Accounting über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe kein Accounting über den TACACS+-Server erforderlich.

Default: nur_für_SETUP_Baum

2.54.13 Umgehe-Tacacs-fuer-CRON/Skripte/Aktions-Tabelle

Hier können Sie die Umgehung der TACACS-Autorisierung und des TACACS+-Accounting für verschiedene Aktionen aktivieren bzw. deaktivieren.

SNMP-ID: 2.54.13

Pfad Telnet: /Setup/Tacacs+

Mögliche Werte:

- aktiviert
- deaktiviert

Default: deaktiviert

Bitte beachten Sie, dass die Funktion von TACACS+ für das gesamte System über diese Optionen beeinflusst wird. Beschränken Sie die Nutzung von CRON, der Aktionstabelle und von Scripten auf jeden Fall auf einen absolut vertrauenswürdigen Kreis von Administratoren!

2.54.14 Wert-zu-Authorisierungsanfrage-hinzufuegen

Wenn Sie diese Funktion deaktivieren, dann prüft TACACS+ nur beim Login die Benutzerrechte des Nutzers. Bei der Eingabe von Werten prüft das Gerät dann nicht erneut, ob der Benutzer die Berechtigung hat bestimmte Werte zu ändern.

Pfad Telnet: /Setup/Tacacs+/Wert-zu-Authorisierungsanfrage-hinzufuegen

Mögliche Werte:

- aktiviert: TACACS+ prüft bei der Übergabe von Werten, ob der Benutzer die Rechte hat diese zu ändern
- deaktiviert: TACACS+ prüft die Identität des Nutzers lediglich beim Login

Default: aktiviert

2.59 WLAN-Management

Dieses Menü enthält die Konfiguration des WLAN-Managements für Access Points.

2.59.1 Statische-WLC-Konfiguration

In dieser Tabelle können Sie die WLAN-Controller (WLCs) angeben, mit denen ein gemanagter Access Point vornehmlich Verbindung aufnehmen soll. Befinden sich Access Point und WLC im gleichen IP-Netzwerk ist hier keine Einstellung erforderlich.

Diese Einstellung ist nur dann von Bedeutung, wenn sich mindestens ein WLAN-Interface des Geräts in der Betriebsart "Managed" befindet.

SNMP-ID: 2.59.1

Pfad Telnet: /Setup/WLAN-Management/Statische-WLC-Konfiguration

2.59.1.1 IP-Adresse

Hier wird der Name des CAPWAP-Services angegeben, über den der DNS-Server die WLAN-Controller auflöst.

Der Name ist so voreingestellt, dass Sie hier nichts ändern müssen. Der Parameter bietet jedoch grundsätzlich die Möglichkeit auch CAPWAP-Services anderer Hersteller hier zu verwenden.

SNMP-ID: 2.59.1.1

Pfad Telnet: /Setup/WLAN-Management/Statische-WLC-Konfiguration/IP-Adresse

Mögliche Werte:

- Gültige IP-Adresse oder auflösbarer Name eines WLC-Controllers

Default: WLC-Address

2.59.1.2 Port

Hier können Sie den Port angeben, der für die Kommunikation mit dem WLAN-Controller verwendet werden soll.

SNMP-ID: 2.59.1.2

Pfad Telnet: /Setup/WLAN-Management/Statische-WLC-Konfiguration/Port

Mögliche Werte:

- Gültige Port-Bezeichnung

Default: 1027

2.59.1.3 Loopback-Addr.

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

SNMP-ID: 2.59.1.3

Pfad Telnet: /Setup/WLAN-Management/Statische-WLC-Konfiguration/Loopback-Addr.

Mögliche Werte:

- Name der IP-Netzwerke, deren 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 wird deren Adresse genommen).
- LB0 ... LBF für die 16 Loopback-Adressen.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Default: leer

Die hier eingestellte Absendeadresse wird für jede Gegenstelle **unmaskiert** verwendet.

2.59.4 AutoWDS

Diese Tabelle enthält die lokalen Werkseinstellungen Ihres Gerätes für die Suche nach und Authentifikation an einem AutoWDS-Basisnetz. Über die Timeout-Zeiten legen Sie fest, ob Ihr Gerät dabei die vorkonfigurierte Integration, die Express-Integration oder eine abgestufte Kombination aus beidem verfolgt.

Solange Ihr Gerät noch keine AutoWDS-Einstellungen von einem WLC erhalten hat, benutzt das Gerät die hier hinterlegten Voreinstellungen. Sobald Ihr Gerät jedoch ein AutoWDS-Profil von einem WLC erhält, genießt dessen Konfiguration die höhere Priorität, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

Die hier festgelegten Parameter betreffen ausschließlich die initiale Anmeldung eines hinzukommenden Slave-AP an einem Master-AP zur Suche nach einem WLC. Sie betreffen nicht die später aufgebauten P2P-Strecke zu einem Master-AP; hierzu verwendet Ihr Gerät dann die erhaltene WLC-Konfiguration.

Ob das Gerät vom WLC eine AutoWDS-Konfiguration erhalten hat, lässt sich anhand der Status-Tabelle **AutoWDS-Profil** (SNMP-ID 1.59.106) überprüfen.

Pfad Telnet:

Setup > **WLAN-Management**

2.59.4.1 Aktiv

Schalten Sie die AutoWDS-Funktion auf Ihrem Gerät ein- oder aus. Im deaktivierten Zustand versucht das Gerät nicht selbstständig, sich in ein gemanagtes WLAN zu integrierten, und führt auch keine Scans nach aktiven AutoWDS-Netzen durch.

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

2.59.4.2 Preconf-SSID

Tragen Sie die SSID des AutoWDS-Basisnetzes ein, nach dem Ihr Gerät im Sinne einer vorkonfigurierten Integration sucht. Dazu müssen Sie AutoWDS aktiviert und die *Wartezeit bis zur vorkonfigurierten Suche* größer `0` gesetzt haben.

Nach Ablauf der Wartezeit schaltet das Gerät sämtliche physikalischen WLAN-Schnittstellen in den Client-Modus und beginnt mit der Suche nach der eingetragenen SSID. Findet das Gerät eine übereinstimmende SSID, versucht es daraufhin, sich mit der eingetragenen WPA2-Passphrase am betreffenden WLAN zu authentisieren.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.59.4.3 Preconf-Key

Geben Sie die WPA2-Passphrase an, die Ihr Gerät für die Authentifikation am vorkonfigurierten AutoWDS-Basisnetz benutzt.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.59.4.4 Zeit-bis-Preconf-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und entsprechend den Werten der Vorkonfiguration (der lokal hinterlegten SSID und Passphrase) nach einem AutoWDS-Basisnetz scannt, sofern noch keine Konfigurationsbestandteile von einem WLC vorliegen. Findet der AP eine übereinstimmende SSID, versucht das Gerät, sich mit der dazugehörigen WPA2-Passphrase zu authentisieren, um anschließend einen Konfigurationsprozess durchzuführen.

Parallel zu diesem Prozess beginnt die eingestellte *Wartezeit für den Beginn der Express-Integration* herabzuzählen.

Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit und den Prozess zur vorkonfigurierte Integration. Das Gerät beginnt sofort damit, die Wartezeit für den Beginn der Express-Integration herabzuzählen.

Default-Wert:

0

2.59.4.5 Zeit-bis-Express-Scan

Definieren Sie die Wartezeit, nach welcher der AP in den Client-Modus wechselt und nach einem beliebigen AutoWDS-Basisnetz scannt, sofern noch keine Konfigurationsbestandteile von einem WLC vorliegen und die *Wartezeit für den Beginn der vorkonfigurierten Integration* (sofern gesetzt) abgelaufen ist. Findet der AP eine geeignete SSID, versucht das Gerät, sich am WLAN zu authentisieren, um anschließend einen Rekonfigurationsprozess durchzuführen. Für die Authentisierung verwendet das Gerät einen Express-Pre-Shared-Key, welcher fest in die Firmware implementiert ist.

Pfad Telnet:

Setup > **WLAN-Management** > **AutoWDS**

Mögliche Werte:

0 … 4294967295 Sekunden

Besondere Werte:

0

Dieser Wert deaktiviert die Wartezeit und den Prozess zur vorkonfigurierte Integration.

Default-Wert:

1

2.59.5 CAPWAP-Port

Definieren Sie in diesem Eintrag den CAPWAP-Port für den WLAN-Controller.

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

0 … 65535

Default-Wert:

1027

2.59.120 Log-Eintraege

Diese Parameter definiert die maximale Anzahl der Log-Einträge des Geräts.

Pfad Telnet: /Setup/WLAN-Management/Log-Eintraege

Mögliche Werte:

- 0 bis 9999

Default: 200

2.60 Automatisches-Laden

In diesem Menü finden Sie die Einstellungen für das automatische Laden von Firmware, Konfiguration oder Skript von externen Datenträgern oder von einer URL.

SNMP-ID: 2.60

Pfad Telnet: /Setup/Automatisches-Laden

2.60.1 Netzwerk

In diesem Menü finden Sie die Einstellungen für das Laden von Firmware, Konfiguration oder Skripten über das Netzwerk.

Die in diesem Bereich definierten Einstellungen werden verwendet, wenn auf der Kommandozeile die Befehle LoadFirmware, LoadConfig oder LoadScript aufgerufen werden. Diese Befehle laden Firmware, Konfiguration oder Skript mit Hilfe des TFTP- oder HTTP(S)-Clients in das Gerät.

SNMP-ID: 2.60.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk

Das Laden von Firmware, Konfiguration oder Skript mit Hilfe des TFTP- oder HTTP(S)-Clients ist nur erfolgreich, wenn die URL zum Laden der jeweiligen Datei vollständig konfiguriert ist und diese URL beim Ausführen des Befehls erreichbar ist. Alternativ kann die URL beim Aufruf des Befehls als Parameter übergeben werden.

Die im Bereich /Setup/Automatisches-Laden/Netzwerk eingestellten Werte für Bedingung, URL und Minimal-Version stellen Default-Werte dar. Diese Werte werden ausschließlich dann verwendet, wenn beim Aufruf der Befehle LoadFirmware, LoadConfig oder LoadScript auf der Kommandozeilekeine anderen entsprechenden Parameter übergeben werden.

2.60.1.1 Firmware

In diesem Menü finden Sie die Einstellungen für das Laden einer Firmware über das Netzwerk.

SNMP-ID: 2.60.1.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Firmware

2.60.1.1.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der die unter /Setup/Automatisches-Laden/Netzwerk/Firmware/URL angegebene Firmware geladen wird, wenn der Befehl LoadFirmware ausgeführt wird.

SNMP-ID: 2.60.1.1.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Firmware

Mögliche Werte:

- unbedingt: Die Firmware wird auf jeden Fall auf den Speicherplatz der inaktiven Firmware geladen und ausgeführt. Diese Einstellung deaktiviert die Versionsprüfung, die angegebene Firmware wird auf jeden Fall geladen.
- wenn-unterschiedlich: Die Firmware wird dann auf den Speicherplatz der inaktiven Firmware geladen und ausgeführt, wenn sie eine andere Version enthält als die im Gerät aktive und die inaktive Firmware. Wenn die Version der angegebenen Firmware einer der beiden vorhandenen Firmware-Versionen entspricht, wird die angegebene Firmware nicht geladen. Der Befehl LoadFirmware verwendet für den Vergleich die Firmware-Version (z. B. "8.10"), den Releasecode (z. B. "RU1") und das Dateidatum.
- wenn-neuer: Die Firmware wird nur dann geladen und ausgeführt, wenn sie neuer ist als die aktuell im Gerät aktive Firmware. Die Firmware wird dann auf den Speicherplatz der inaktiven Firmware geladen, wenn sie neuer ist als die im Gerät aktive und die inaktive Firmware. Wenn die Version der angegebenen Firmware älter ist als eine der beiden vorhandenen Firmware-Versionen, wird die angegebene Firmware nicht geladen.

Default: unbedingt

Wenn der Befehl LoadFirmware zweimal nacheinander mit der Einstellung "unbedingt" ausgeführt wird enthalten beide Speicherplätze für die Firmware die gleiche Version.

2.60.1.1.2 Minimal-Version

Stellen Sie hier die Minimal-Version der Firmware für das Laden über das Netzwerk ein.

SNMP-ID: 2.60.1.1.2

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Minimal-Version

Mögliche Werte:

- max. 14 Zeichen

Default: leer

Firmware-Versionen mir einer niedrigeren Versionsbezeichnung werden ignoriert.

2.60.1.1.3 URL

Geben Sie hier die URL der Firmware an, die mit dem Befehl LoadFirmware über das Netzwerk geladen wird.

SNMP-ID: 2.60.1.1.3

Pfad Telnet: /Setup/Automatisches-Laden/Firmware/URL

Mögliche Werte:

- max. 127 Zeichen, beginnend mit "tftp://", "http://" oder "https://"

Default: leer

Der TFTP- bzw. HTTP(S)-Client lädt die hier eingetragene Datei nur, wenn dem Befehl LoadFirmware keine URL als Parameter übergeben wurde. Wird eine URL als Parameter angegeben, kann gezielt eine andere Datei geladen werden.

2.60.1.2 Konfiguration

In diesem Menü finden Sie die Einstellungen für das Laden einer Konfiguration über das Netzwerk.

SNMP-ID: 2.60.1.2

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Konfiguration

2.60.1.2.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der die unter /Setup/Automatisches-Laden/Netzwerk/Konfiguration/URL angegebene Konfiguration beim Start des Gerätesgeladen wird.

SNMP-ID: 2.60.1.2.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Konfiguration

Mögliche Werte:

- unbedingt: Die Konfiguration wird auf jeden Fall geladen.
- wenn-unterschiedlich: Die Konfiguration wird nur dann geladen, wenn sie eine andere Versionsnummer enthält als die aktuell im Gerät aktive Konfiguration.

Default: unbedingt

2.60.1.2.2 URL

Geben Sie hier die URL der Konfigurationsdatei an, die das Gerät über das Netzwerk lädt.

Pfad Telnet:

Setup > **Automatisches-Laden** > **Netzwerk** > **Konfiguration**

Mögliche Werte:

Gültige URL, max. 127 Zeichen

Default:

2.60.1.3 Skript

In diesem Menü finden Sie die Einstellungen für das Laden eines Skriptes über das Netzwerk.

SNMP-ID: 2.60.1.3

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Skript

2.60.1.3.1 Bedingung

Wählen Sie hier die Bedingung aus, nach der das unter /Setup/Automatisches-Laden/Netzwerk/Konfiguration/URL angegebene Skript ausgeführt wird, wenn der Befehl LoadScript ausgeführt wird.

SNMP-ID: 2.60.1.3.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/Skript

Mögliche Werte:

- unbedingt: Das Skript wird auf jeden Fall ausgeführt. Diese Einstellung deaktiviert den Vergleich der Prüfsumme, das angegebene Skript wird auf jeden Fall ausgeführt.Dabei belässt der Befehl LoadScript die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes unverändert.
- wenn-unterschiedlich: Das Skript wird nur dann ausgeführt, wenn es sich vom zuletzt ausgeführten Skript unterscheidet.Der Unterschied zum zuletzt ausgeführten Skript wird über eine Prüfsumme festgestellt. Das Skript wird dazu grundsätzlich vollständig heruntergeladen. Dann vergleicht der Befehl LoadScript die Prüfsumme des geladenen Skriptes mit der im Gerät gespeicherten Prüfsumme des zuletzt ausgeführten Skriptes. Wenn das Skript ausgeführt wird aktualisiert der Befehl LoadScript die im Gerät gespeicherte Prüfsumme.

Default: unbedingt

2.60.1.3.2 URL

Geben Sie hier die URL der Skriptdatei an, die das Gerät über das Netzwerk lädt.

Pfad Telnet:

Setup > **Automatisches-Laden** > **Netzwerk** > **Skript**

Mögliche Werte:

Gültige URL, max. 127 Zeichen

Default:

2.60.1.4 TFTP-Client

In diesem Menü finden Sie die Konfiguration für den TFTP-Client.

SNMP-ID: 2.60.1.4

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/TFTP-Client

2.60.1.4.1 Bytes-pro-Hashmark

Stellen Sie hier ein, nach welcher Anzahl von erfolgreich geladenen Bytes der TFTP-Client bei der Ausführung von LoadFirmware, LoadConfig oder LoadScript ein Hash-Zeichen (#) auf der Kommandozeile ausgibt. Mit diesen Hash-Zeichen erzeugt der TFTP-Client einen Fortschrittsbalken beim Download von Firmware, Konfiguration oder Skript.

SNMP-ID: 2.60.1.4.1

Pfad Telnet: /Setup/Automatisches-Laden/Netzwerk/TFTP-Client

Mögliche Werte:

- 4 Zeichen

Default: 8192

Dieser Wert wird nur beim Laden über TFTP verwendet, nicht bei HTTP oder HTTPS. Bei HTTP oder HTTPS wird das Hash-Zeichen max. alle 100ms ausgeben, wenn ein Fortschritt stattgefunden hat.

2.60.3 Lizenz

In diesem Menü erfassen Sie die Angaben zum Lizenznehmer, welche das Gerät bei der automatischen Lizenzaktivierung durch LCOS in das Registrierungsformular einträgt.

Pfad Telnet:

Setup > **Automatisches-Laden**

2.60.3.1 URL

Über diese Einstellung definieren Sie die URL des Lizenzservers, den das Gerät für die automatische Lizenzaktivierung nutzt.

Pfad Telnet:

Setup > **Automatisches-Laden** > **Lizenz**

Mögliche Werte:

Gültige URL, max. 127 Zeichen

Default:

http://www2.lancom.de/newoptionreg.nsf/RegOpt

2.60.3.2 Loopback-Adr.

Geben Sie hier optional eine andere Adresse (Name oder IP) an, an die der Lizenz-Server seine Antwort-Nachrichten schickt.

Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

Pfad Telnet:

Setup > **Automatisches-Laden** > **Lizenz**

Mögliche Werte:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets
- `DMZ` für die Adresse der ersten DMZ

  Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!

- `LB0`...`LBF` für eine der 16 Loopback-Adressen oder deren Name

- Beliebige IPv4-Adresse

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet!

Default:

2.60.3.10 Firma

Tragen Sie hier die Firma des Lizenznehmers ein.

SNMP-ID: 2.60.3.10

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.11 Nachname

Tragen Sie hier den Nachnamen des Lizenznehmers ein.

SNMP-ID: 2.60.3.11

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.12 Vorname

Tragen Sie hier den Vornamen des Lizenznehmers ein.

SNMP-ID: 2.60.3.12

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.13 Straße und Hausnummer

Tragen Sie hier die Straße und die Hausnummer des Lizenznehmers ein.

SNMP-ID: 2.60.3.13

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.14 Postleitzahl

Tragen Sie hier die Postleitzahl des Lizenznehmers ein.

SNMP-ID: 2.60.3.14

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.15 Stadt

Tragen Sie hier die Stadt des Lizenznehmers ein.

SNMP-ID: 2.60.3.15

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.16 Land

Tragen Sie hier das Land des Lizenznehmers ein.

SNMP-ID: 2.60.3.16

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.3.17 E-Mail Adresse

Tragen Sie hier die E-Mail Adresse des Lizenznehmers ein, an die der Lizenzserver seine Bestätigungs-E-Mail schickt.

SNMP-ID: 2.60.3.17

Pfad Telnet: /Setup/Automatisches-Laden/Lizenz

2.60.56 USB

In diesem Menü finden Sie die Konfiguration für das automatische Laden von Firmware oder Konfiguration von externen Datenträgern.

SNMP-ID: 2.60.56

Pfad Telnet: /Setup/Automatisches-Laden/USB

2.60.56.1 Firmware-und-Loader

Mit dieser Option aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien von einem angeschlossenen USB-Medium. Speichern Sie die benötigten Loader- und/oder Firmware-Dateien im Verzeichnis "Firmware" in der obersten Ebene des angeschlossenen USB-Mediums.

SNMP-ID: 2.60.56.1

Pfad Telnet: /Setup/Automatisches-Laden/USB

Mögliche Werte:

- Inaktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und/oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

2.60.56.2 Konfiguration-und-Skript

Mit dieser Option aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien von einem angeschlossenen USB-Medium. Speichern Sie die benötigten Konfigurations- und/oder Skript-Dateien im Verzeichnis "Config" in der obersten Ebene des angeschlossenen USB-Mediums.

SNMP-ID: 2.60.56.2

Pfad Telnet: /Setup/Automatisches-Laden/USB

Mögliche Werte:

- Inaktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.
- Aktiv: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und/oder Skript-Dateien in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.
- Wenn-unkonfiguriert: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

- Wenn-unkonfiguriert

Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf “inaktiv” gesetzt.

Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

2.63 Paket-Capture

In diesem Menü finden Sie die Einstellungen zur Aufzeichnung des Netzwerk-Datenverkehrs via LCOScap und RPCAP.

Pfad Telnet:

Setup > **Paket-Capture**

2.63.1 LCOSCap-In-Betrieb

Mit dieser Einstellung aktivieren Sie die LCOSCAP-Funktionalität.

Pfad Telnet:

Setup > **Paket-Capture** > **LCOSCap-In-Betrieb**

Mögliche Werte:

ja

nein

Default:

ja

2.63.2 LCOSCap-Port

Mit dieser Einstellung bestimmen Sie den Port, den LCOSCAP nutzt.

Pfad Telnet:

Setup > **Paket-Capture** > **LCOSCap-Port**

Mögliche Werte:

5 Zeichen aus '0123456789'

Default:

41047

2.63.11 RPCap-In-Betrieb

Mit dieser Einstellung aktivieren Sie RPCAP. RPCAP ist ein von (der Windows-Version von) Wireshark unterstütztes Protokoll, mit dem Wireshark das Gerät direkt ansprechen kann, wodurch der Umweg über eine Capture-Datei entfällt. In Wireshark sprechen Sie die RPCAP-Schnittstelle über den Unterpunkt 'Remote interfaces' an.

Pfad Telnet:

Setup > **Paket-Capture**

Mögliche Werte:

ja

nein

Default:

nein

2.63.12 RPCap-Port

Mit dieser Einstellung bestimmen Sie den Port, den RPCAP nutzt.

Pfad Telnet:

Setup > **Paket-Capture**

Mögliche Werte:

0 bis 65535

Default:

2002

2.64 PMS-Interface

Über die Tabellen und Parameter in diesem Menü nehmen Sie sämtliche Einstellungen für die PMS-Schnittstelle vor (PMS = Property-Management-System).

Pfad Telnet:

Setup

2.64.1 Aktiv

Aktivieren oder deaktivieren Sie die PMS-Schnittstelle für das Gerät.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

nein

2.64.2 PMS-Typ

Bezeichnet das von Ihrem Property-Management-System verwendete Protokoll. Zur Zeit besteht ausschließlich die Unterstützung für das Hotel-Property-Management-System von Micros Fidelio über TCP/IP.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

TCP/IP

Default:

TCP/IP

2.64.3 PMS-Server-IP-Adresse

Geben Sie hier die IPv4-Adresse Ihres PMS-Servers ein.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

IPv4-Adresse

Default:

nein

2.64.4 Loopback-Address

Geben Sie hier optional eine andere Adresse (Name oder IP) an, an die der PMS-Server seine Antwort-Nachrichten schickt.

Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets
- `DMZ` für die Adresse der ersten DMZ

  Wenn eine Schnittstelle namens "DMZ" existiert, wählt das Gerät stattdessen deren Adresse!
- `LB0...LBF` für eine der 16 Loopback-Adressen oder deren Name
- Beliebige IPv4-Adresse

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet!

Default:

2.64.5 PMS-Port

Geben Sie hier den TCP-Port ein, über den Ihr PMS-Server erreichbar ist.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

0…65535

Default:

0

2.64.6 Trennzeichen

Über diesen Eintrag konfigurieren Sie das Trennzeichen, das Ihr PMS benutzt, um Datensätze an eine API weiterzureichen. Die Micros-Fidelio-Spezifikation z. B. verwendet standardmäßig den senkrechten Trennstrich (| , Hex 7C).

Sie sollten diesen Wert nach Möglichkeit nicht verändern. Ein falsches Trennzeichen führt dazu, dass das Gerät die von Ihrem PMS übermittelten Datensätze nicht mehr lesen kann und die PMS-Schnittstelle nicht funktioniert!

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

String, max. 1 Zeichen

Default:

|

2.64.7 Zeichensatz

Wählen Sie den Zeichensatz aus, in dem Ihr PMS die Nachnamen Ihrer Gäste an das Gerät übermittelt.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

CP850

W1252

Default:

CP850

2.64.8 Waehrung

Sofern Sie eine kostenpflichtigen Internetzugang anbieten, wählen Sie hier die Währungseinheit aus, mit der Sie die angebotenen Zeitkontingente (einstellbar über die Tarif-Tabelle) abrechnen. Diese Einheit erscheint ebenfalls auf der Portalseite. Achten Sie darauf, dass sie mit der Währung des PMS-Servers übereinstimmt.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

CENT

PENNY

Default:

CENT

2.64.9 Tarif

Sofern Sie eine kostenpflichtigen Internetzugang anbieten, verwalten Sie über diese Tabelle die Tarife für das Accounting.

Pfad Telnet:

Setup > **PMS-Interface**

2.64.9.1 Anzahl

Geben Sie hier die Höhe des Zeitkontingents ein, z. B. `1`. In Kombination mit der Einheit entspricht dies dann z. B. 1 Stunde.

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

0…99999999999999999

Default:

2.64.9.2 Einheit

Wählen Sie aus der Liste eine Einheit für das Zeitkontingent aus.

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

Stunde(n)

Tag(e)

Minute(n)

Default:

Stunde(n)

2.64.9.3 Tarifwert

Geben Sie hier die Höhe des Betrags ein, mit dem Sie die Zeitkontingente vergelten. In Kombination mit der gewählten Währung entspricht dies dann z. B. 50 Cent

Pfad Telnet:

Setup > **PMS-Interface** > **Tarif**

Mögliche Werte:

0…99999999999999999

Default:

2.64.10 Accounting

In diesem Menü konfigurieren Sie die Übermittlung der Abrechnungsinformationen vom Gerät an Ihr PMS.

Pfad Telnet:

Setup > **PMS-Interface**

2.64.10.1 Flashrom-Speichern

Aktivieren oder deaktivieren Sie, ob Ihr Gerät die Abrechnungsinformationen in regelmäßigen Abständen im internen Flash-ROM speichert. Dies geschieht standardmäßig stündlich, Sie können das betreffende Intervall aber über das Setup-Menü verändern. Aktivieren Sie diese Option, um bei einem Stromausfall den Komplettverlust von Accounting-Informationen zu vermeiden.

Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebendauer Ihres Gerätes reduziert!

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

nein

ja

Default:

nein

2.64.10.2 Flashrom-Speicherintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät die gesammelten Accounting-Informationen in seinem internen Flash-ROM sichert.

Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebendauer Ihres Gerätes reduziert!

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

15

2.64.10.3 Accounting-Tabelle-Reinigungsintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü von abgelaufenen Sitzungen befreit. Wenn der Wert `0` ist, ist die automatische Bereinigung deaktiviert.

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

60

2.64.10.4 Accounting-Tabelle-Updateintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü aktualisiert. Wenn der Wert `0` ist, ist die Aktualisierung deaktiviert und die Status-Tabelle zeigt keine Werte an.

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0…4294967295 Sekunden

Default:

15

2.64.11 Login-Formular

In diesem Menü nehmen Sie die PMS-spezifischen Einstellungen zur Login-/Portalseite, die Ihren Gäste beim unauthentifizierten Zugriff auf den Hotspot erscheint.

Pfad Telnet:

Setup > **PMS-Interface**

2.64.11.1 PublicSpot-Login-Formular

Aktivieren bzw. deaktivieren Sie, ob die Portalseite die Public-Spot-eigenen Anmeldemaske anzeigt. Wenn Sie diese Einstellung deaktivieren, können sich Public-Spot-Nutzer, die eine Kombination aus Benutzername und Passwort als Zugangsdaten verwenden (z. B. fest eingetragene oder über Voucher eingerichtete Nutzer), nicht mehr am Gerät anmelden.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

nein

ja

Default:

nein

2.64.11.2 PMS-Login-Formular

Wählen Sie aus, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

- `kostenlos`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenlosen Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dennoch dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren, um eine Internetnutzung durch Unbefugte zu erschweren.
- `kostenpflichtig`: Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenpflichtig Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren und einen Tarif auszuwählen.
- `kostenlos-VIP`: Wählen Sie diese Einstellung, wenn Sie einen eigentlich kostenpflichtigen Internetzugang für VIPs kostenlos anbieten wollen. Ihre VIPs erhalten dann zwar die Anmeldemaske für den kostenpflichtigen Zugang, es werden ihnen jedoch keine Gebühren in Rechnung gestellt.

Default:

kostenlos

2.64.11.3 Fidelio-kostenlos-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

Keiner

2.64.11.4 Fidelio-kostenpflichtig-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenpflichtige Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

Reservierungsnummer

2.64.11.5 Fidelio-kostenlos-VIP-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich eine VIP – zusätzlich zu ihrem Benutzernamen und ihrer Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung für VIPs anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner

Reservierungsnummer

Ankunftsdatum

Abreisedatum

Vorname

Profilnummer

Default:

Keiner

2.64.11.6 Kostenlos-VIP-Status

In dieser Tabelle verwalten Sie lokal die VIP-Kategorien aus Ihrem PMS.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

2.64.11.6.1 Status

Tragen Sie hier die VIP-Kategorie aus Ihrem PMS ein, deren Mitgliedern Sie einen kostenlosen Internetzugang zur Verfügung stellen wollen.

Haben Sie auf Ihrem PMS-Server z. B. drei mögliche VIP-Stati eingerichtet (VIP1, VIP2, VIP3), wollen allerdings nur den Hotelgästen aus Kategorie VIP2 einen freien Internetzugang anbieten, tragen Sie deren entsprechende Kennung hier ein.

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular** > **Kostenlos-VIP-Status**

Mögliche Werte:

String, max. 20 Zeichen

Default:

2.64.12 Gastname-Case-Sensitiv

Aktivieren oder deaktivieren Sie, ob das Gerät beim Abgleich des beim Login angegebenen Nachnamens mit dem Gastnamen in der PMS-Datenbank auf Groß- und Kleinschreibung achtet. Ist diese Einstellung aktiviert, wird einem Gast der Public-Spot-Zugang verweigert, wenn die Schreibweise seines Namens nicht der dem Hotel mitgeteilten Schreibweise entspricht.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

ja

2.64.13 Multi-Login

Aktivieren oder deaktivieren Sie, ob Sie einem Hotelgast erlauben, mehrere WLAN-Geräte mit den selben Zugangsdaten am Hotspot anzumelden.

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein

ja

Default:

nein

2.70 IPv6

In diesem Menü verwalten Sie die Einstellungen für IPv6.

Pfad Telnet:

Setup > **IPv6**

2.70.1 Tunnel

Mit dieser Einstellung verwalten Sie die Tunnelprotokolle, um den Zugang zum IPv6-Internet über eine IPv4-Internetverbindung bereitzustellen.

Pfad Telnet:

Setup > **IPv6** > **Tunnel**

2.70.1.1 6in4

Die Tabelle enthält die Einstellungen zum 6in4-Tunnel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4**

2.70.1.1.1 Gegenstelle

Beinhaltet den Namen des 6in4-Tunnels.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.1.1.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen aus dem Wertebereich 0 - 65534

Default:

0

2.70.1.1.3 Gateway-Adresse

Beinhaltet die IPv4-Adresse des entfernten 6in4-Gateways.

Der 6in4-Tunnel entsteht ausschließlich dann, wenn das Gateway über diese Adresse per Ping erreichbar ist.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gateway-Adresse**

Mögliche Werte:

IP-Adresse in IPv4-Notation mit max. 64 Zeichen

Default:

leer

2.70.1.1.4 IPv4-Rtg-tag

Bestimmen Sie hier das Routing-Tag, mit dem das Gerät die Route zum zugehörigen entfernten Gateway ermittelt. Das IPv4-Routing-Tag gibt an, über welche getaggte IPv4-Route die Datenpakete ihre Zieladresse erreichen. Folgende Zieladressen sind möglich:

- 6to4-Anycast-Adresse
- 6in4-Gateway-Adresse
- 6rd-Border-Relay-Adresse

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Wertebereich von 0 - 65534

Default:

0

2.70.1.1.5 Gateway-IPv6-Adresse

Beinhaltet die IPv6-Adresse des entfernten Tunnelendpunktes auf dem Transfernetz, z. B. "2001:db8::1".

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gateway-IPv6-Adresse**

Mögliche Werte:

IPv6-Adresse mit max. 43 Zeichen

Default:

leer

2.70.1.1.6 Lokale-IPv6-Adresse

Beinhaltet die lokale IPv6-Adresse des Geräts auf dem Transfernetz, z. B. "2001:db8::2/64".

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Lokale-IPv6-Adresse**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

2.70.1.1.7 Geroutetes-IPv6-Prefix

Enthält das Präfix, das vom entfernten Gateway zum lokalen Gerät geroutet wird und im LAN verwendet werden soll, z. B. "2001:db8:1:1::/64" oder "2001:db8:1::/48".

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Geroutetes-IPv6-Prefix**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

2.70.1.1.8 Firewall

Hier haben Sie die Möglichkeit die Firewall für jedes Tunnel-Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, wählen Sie **IPv6-Firewall/QoS aktiviert** im Menü **Firewall/QoS** > **Allgemein**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese in mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

2.70.1.2 6rd-Border-Relay

Ein Router kann grundsätzlich als 6rd-Client oder als 6rd-Border-Relay arbeiten. Ein 6rd-Client bzw. 6rd CE-Router (Customer Edge Router) verbindet sich über eine WAN-Verbindung zu einem Internet-Provider und propagiert das 6rd-Präfix an Clients im LAN. Ein 6rd-Border-Relay arbeitet im Netzwerk des Providers und stellt 6rd-Clients die Verbindung zum IPv6-Netzwerk bereit. Ein 6rd-Border Relay wird also immer dann verwendet, wenn 6rd-Routern eine IPv6-Verbindung bereitgestellt werden soll.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

2.70.1.2.1 Gegenstelle

Beinhaltet den Namen des 6rd-Border-Relay-Tunnels.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.1.2.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

2.70.1.2.3 IPv4-Loopback-Adresse

Bestimmen Sie die IPv4-Loopback-Adresse, d.h. die Adresse auf der das Gerät als 6rd-Border-Relay arbeiten soll.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **IPv4-Loopback-Adresse**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.1.2.4 6rd-Praefix

Definiert das von diesem Border-Relay verwendete Präfix für die 6rd-Domäne, z. B. 2001:db8::/32. Dieses Präfix muss ebenfalls auf allen zugehörigen 6rd-Clients konfiguriert werden.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **6rd-Praefix**

Mögliche Werte:

max. 24 Zeichen als Präfix einer IPv6 Adresse, mit bis zu 4 Blöcken aus je vier Hexadezimalzeichen

Default:

leer

2.70.1.2.5 IPv4-Masken-Laenge

Definiert die Anzahl der höchstwertigen Bits der IPv4-Adressen, die identisch innerhalb einer 6rd-Domäne sind. Bei Maskenlänge "0"existieren keine identischen Bits. In diesem Fall dient die gesamte IPv4-Adresse dazu, das delegierte 6rd-Präfix zu erzeugen.

Der Provider gibt die Maskenlänge vor.

Beispiel: Die IPv4-Adresse des Gerätes sei "192.168.1.99" (in hexadezimaler Form: "c0a8:163"). Dann sind beispielsweise folgende Kombinationen möglich:

6rd-Domäne	Masken-Länge	6rd-Präfix
2001:db8::/32	0	2001:db8:c0a8:163::/64

6rd-Domäne	Masken-Länge	6rd-Präfix
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **IPv4-Masken-Laenge**

Mögliche Werte:

max. 2 Ziffern im Bereich von 0 - 32

Default:

0: Das Gerät benutzt die vollständige IPv4-Adresse.

2.70.1.2.6 DHCPv4-Propagieren

Wenn Sie diese Funktion aktivieren, dann verteilt das 6rd-Border-Relay das Präfix über DHCPv4, insofern der DHCPv4-Client es anfragt.

Wenn Sie diese Funktion nicht aktivieren, müssen Sie die nötigen 6rd-Einstellungen auf den 6rd-Clients manuell konfigurieren.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **DHCPv4-Propagieren**

Mögliche Werte:

ja

nein

Default:

nein

2.70.1.2.7 Firewall

Hier haben Sie die Möglichkeit die Firewall für jedes Tunnel-Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, wählen Sie **IPv6-Firewall/QoS aktiviert** im Menü **Firewall/QoS** > **Allgemein**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese in mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

2.70.1.3 6rd

Die Tabelle enthält die Einstellungen zum 6rd-Tunnel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd**

2.70.1.3.1 Gegenstelle

Beinhaltet den Namen des 6rd-Tunnels.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.1.3.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

2.70.1.3.3 Border-Relay-Adresse

Enthält die IPv4-Adresse des 6rd-Border-Relays.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Border-Relay-Adresse**

Mögliche Werte:

IPv4-Adresse mit max. 64 Zeichen

Default:

leer

2.70.1.3.4 IPv4-Rtg-tag

Bestimmen Sie hier das Routing-Tag, mit dem das Gerät die Route zum zugehörigen entfernten Gateway ermittelt. Das IPv4-Routing-Tag gibt an, über welche getaggte IPv4-Route die Datenpakete ihre Zieladresse erreichen. Folgende Zieladressen sind möglich:

- 6to4-Anycast-Adresse
- 6in4-Gateway-Adresse
- 6rd-Border-Relay-Adresse

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

2.70.1.3.5 6rd-Praefix

Enthält das vom Provider für 6rd-Dienste verwendete Präfix, z. B. "2001:db8::/32".

Wird das 6rd-Präfix über DHCPv4 zugewiesen, so müssen Sie hier "::/32" eintragen.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **6rd-Praefix**

Mögliche Werte:

max. 24 Zeichen

Default:

leer

2.70.1.3.6 IPv4-Masken-Laenge

Definiert die Anzahl der höchstwertigen Bits der IPv4-Adressen, die identisch innerhalb einer 6rd-Domäne sind. Bei Maskenlänge "0"existieren keine identischen Bits. In diesem Fall dient die gesamte IPv4-Adresse dazu, das delegierte 6rd-Präfix zu erzeugen.

Der Provider gibt die Maskenlänge vor.

Beispiel: Die IPv4-Adresse des Gerätes sei "192.168.1.99" (in hexadezimaler Form: "c0a8:163"). Dann sind beispielsweise folgende Kombinationen möglich:

6rd-Domäne	Masken-Länge	6rd-Präfix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **IPv4-Masken-Laenge**

Mögliche Werte:

max. 2 Ziffern im Bereich von 0 - 32

Default:

0

2.70.1.3.7 Firewall

Hier haben Sie die Möglichkeit die Firewall für jedes Tunnel-Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, wählen Sie **IPv6-Firewall/QoS aktiviert** im Menü **Firewall/QoS** > **Allgemein**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese in mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

2.70.1.4 6to4

Die Tabelle enthält die Einstellungen zum 6to4-Tunnel.

Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Geräts hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen über einen 6to4-Tunnel **ausschließlich für Testzwecke** geeignet. Vermeiden Sie insbesondere Datenverbindungen über einen 6to4-Tunnel für den Einsatz in Produktivsystemen oder die Übertragung sensibler Daten.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4**

2.70.1.4.1 Gegenstelle

Beinhaltet den Namen des 6to4-Tunnels.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.1.4.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65535

Default:

0

2.70.1.4.3 Gateway-Adresse

Beinhaltet die IPv4-Adresse des 6to4-Relays bzw. 6to4-Gateways. Default-Wert ist die Anycast-Adresse "192.88.99.1". In der Regel können Sie diese Adresse unverändert lassen, da Sie damit immer automatisch das nächstgelegene 6to4-Relay im Internet erreichen.

Der 6to4-Tunnel wird nur aufgebaut, wenn das Gateway über diese Adresse per Ping erreichbar ist.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Gateway-Adresse**

Mögliche Werte:

IPv4-Adresse mit max. 64 Zeichen

Default:

192.88.99.1

2.70.1.4.4 IPv4-Rtg-tag

Bestimmen Sie hier das Routing-Tag, mit dem das Gerät die Route zum zugehörigen entfernten Gateway ermittelt. Das IPv4-Routing-Tag gibt an, über welche getaggte IPv4-Route die Datenpakete ihre Zieladresse erreichen. Folgende Zieladressen sind möglich:

- 6to4-Anycast-Adresse
- 6in4-Gateway-Adresse
- 6rd-Border-Relay-Adresse

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

2.70.1.4.5 Firewall

Hier haben Sie die Möglichkeit die Firewall für jedes Tunnel-Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, wählen Sie **IPv6-Firewall/QoS aktiviert** im Menü **Firewall/QoS** > **Allgemein**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv, selbst wenn Sie diese mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2 Router-Advertisement

Mit dieser Einstellung verwalten Sie die Router-Advertisements, mit denen das Gerät seine Verfügbarkeit im Netz als Router anzeigt.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement**

2.70.2.1 Praefix-Optionen

Die Tabelle enthält die Einstellungen der IPv6-Präfixe je Interface.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

2.70.2.1.1 Interface-Name

Definiert den Namen des logischen Interfaces.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

2.70.2.1.2 Praefix

Tragen Sie hier das Präfix ein, das in den Router-Advertisements übertragen wird, z. B. "2001:db8::/64".

Die Länge des Präfixes muss immer exakt 64 Bit betragen ("/64"), da ansonsten die Clients keine eigenen Adressen durch Hinzufügen ihrer "Interface Identifier" (mit 64 Bit Länge) generieren können.

Wollen Sie ein vom Provider delegiertes Präfix automatisch weiterverwenden, so konfigurieren Sie hier "::/64" und im Feld **PD-Quelle** den Namen des entsprechenden WAN-Interfaces.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

2.70.2.1.3 Subnetz-ID

Vergeben Sie hier die Subnetz-ID, die mit dem vom Provider erteilten Präfix kombiniert werden soll.

Weist der Provider z. B. das Präfix "2001:db8:a::/48" zu und vergeben Sie die Subnetz-ID "0001" (oder kurz "1"), so enthält das Router-Advertisement auf diesem Interface das Präfix "2001:db8:a:0001::/64".

Die maximale Subnetz-Länge bei einem 48 Bit langen, delegierten Präfix beträgt 16 Bit (65.536 Subnetze von "0000" bis "FFFF"). Bei einem delegierten Präfix von "/56" beträgt die maximale Subnetz-Länge 8 Bit (256 Subnetze von "00" bis "FF").

In der Regel dient die Subnetz-ID "0" zur automatischen Bildung der WAN-IPv6-Adresse. Deshalb sollten Sie bei der Vergabe von Subnetz-IDs für LANs bei "1" beginnen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

Max. 19 Zeichen

Default:

1

2.70.2.1.4 Adv.-OnLink

Gibt an, ob das Präfix "On Link" ist.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2.1.5 Adv.-Autonomous

Gibt an, ob ein Host das Präfix für eine "Stateless Address Autoconfiguration" verwenden kann. In diesem Fall kann er direkt eine Verbindung ins Internet aufbauen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2.1.6 PD-Quelle

Verwenden Sie hier den Namen des Interfaces, das ein vom Provider vergebenes Präfix empfängt. Dieses Präfix bildet zusammen mit dem im Feld **Praefix** eingetragenen Präfix ein Subnetz, das über Router-Advertisements veröffentlicht wird (DHCPv6-Präfix-Delegation).

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

2.70.2.1.7 Adv.-Pref.-Lifetime

Definiert die Dauer in Millisekunden, für die eine IPv6-Adresse als "Preferred" gilt. Diese Lifetime verwendet der Client auch für seine generierte IPv6-Adresse. Wenn die Lifetime des Präfix abgelaufen ist, nutzt der Client auch nicht mehr die entsprechende IPv6-Adresse. Ist diese "Preferred Lifetime" einer Adresse abgelaufen, so wird sie als "deprecated" markiert. Nur noch bereits aktive Verbindungen verwenden diese Adresse bis zum Verbindungsende. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

Max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

604800

2.70.2.1.8 Adv.-Valid-Lifetime

Definiert die Dauer in Sekunden, nach der die Gültigkeit einer IPv6-Adresse abläuft. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

Max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

2592000

2.70.2.1.9 Lifetime-herunterzaehlen

Wenn diese Option aktiviert ist, werden die Preferred- und Valid-Lifetime des Präfixes in gesendeten Router Advertisements automatisch über die Zeit heruntergezählt oder erhöht. Die Preferred- und Valid-Lifetime des Präfixes in den Router Advertisements werden mit den Zeiten vom bezogenen WAN-Präfix synchronisiert. Wird das bezogene Präfix vom Provider nicht aktualisiert, so werden Preferred- und Valid-Lifetime bis auf 0 heruntergezählt und damit ungültig. Sobald das das Gerät die Lebenszeiten des bezogenen Präfixes vom WAN aktualisiert, so wird auch das Präfix in den Router Advertisements erneut erhöht. Wenn die Option deaktiviert ist, werden Preferred- und Valid-Lifetime vom delegierten Präfix statisch übernommen, aber nicht reduziert oder erhöht. Bei WAN-Verbindungen über Tunnel (6to4, 6in4 und 6rd) hat dieser Parameter keine Auswirkung, da bei dieser Zugangsart die Präfixe nicht per DHCPv6-Präfix-Delegierung bezogen werden und somit keine Lebenszeiten besitzen. Deshalb werden dann die statisch konfigurierten Lebenszeiten der Parameter Preferred- und Valid-Lifetime des Präfixes verwendet. Ebenso hat der Parameter keine Auswirkung, wenn der Wert PD-Quelle leer ist, da in diesem Fall keine Synchronisierung mit dem bezogenen WAN-Präfix stattfindet.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Optionen**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2.2 Interface-Optionen

Die Tabelle enthält die Einstellungen der IPv6-Interfaces.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen**

2.70.2.2.1 Interface-Name

Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements gesendet werden sollen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Interface-Name**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

2.70.2.2.2 Adverts-Senden

Aktiviert das Senden von periodischen Router-Advertisements und das Antworten auf Router-Solicitations.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Optionen** > **Adverts-Senden**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2.2.3 Min-RTR-Intervall

Definiert die minimal erlaubte Zeit zwischen dem Senden von aufeinanderfolgenden Unsolicited-Multicast-Router-Advertisements in Sekunden. **Min-RTR-Intervall** und **Max-RTR-Intervall** bilden ein Zeitintervall, in dem das Gerät Router-Advertisements zufällig verteilt versendet.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Min-RTR-Intervall**

Mögliche Werte:

min. 3 Sekunden

max. 0,75 * **Max-RTR-Intervall**

max. 10 Ziffern

Default:

0,33 * **Max-RTR-Intervall** (wenn **Max-RTR-Intervall** >= 9 Sekunden)

Max-RTR-Intervall (wenn **Max-RTR-Intervall** < 9 Sekunden)

2.70.2.2.4 Max-RTR-Intervall

Definiert die maximal erlaubte Zeit zwischen dem Senden von aufeinanderfolgenden Unsolicited-Multicast-Router-Advertisements in Sekunden. **Min-RTR-Intervall** und **Max-RTR-Intervall** bilden ein Zeitintervall, in dem das Gerät Router-Advertisements zufällig verteilt versendet.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Max-RTR-Intervall**

Mögliche Werte:

min. 4 Sekunden

max. 1800 Sekunden

max. 10 Ziffern

Default:

600 Sekunden

2.70.2.2.5 Managed-Flag

Gibt an, ob das Flag "Managed Address Configuration" im Router-Advertisement gesetzt wird.

Bei gesetztem Flag veranlasst das Gerät die Clients, dass sie alle Adressen durch "Stateful Autoconfiguation" konfigurieren sollen (DHCPv6). In diesem Fall beziehen die Clients auch automatisch andere Informationen wie z. B. DNS-Server-Adressen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Managed-Flag**

Mögliche Werte:

ja

nein

Default:

nein

2.70.2.2.6 Other-Config-Flag

Gibt an, ob das Flag "Other Configuration" im Router-Advertisement gesetzt wird.

Bei gesetztem Flag veranlasst das Gerät die Clients, zusätzliche Informationen (außer Adressen für den Client) wie z. B. DNS-Server-Adressen über DHCPv6 beziehen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Other-Config-Flag**

Mögliche Werte:

ja

nein

Default:

ja

2.70.2.2.7 Link-MTU

Bestimmen Sie die gültige MTU auf dem entsprechenden Link.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Link-MTU**

Mögliche Werte:

max. 5 Ziffern im Bereich von 0 - 99999

Default:

1500

2.70.2.2.8 Reachable-Zeit

Definiert die Zeit in Sekunden, die der Router als erreichbar gelten soll.

Der Default-Wert "0" bedeutet, dass in den Router-Advertisements keine Vorgaben zur Reachable-Zeit existieren.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Reachable-Zeit**

Mögliche Werte:

max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

0

2.70.2.2.10 Hop-Limit

Definiert die maximale Anzahl von Routern, über die ein Datenpaket weitergeschickt werden darf. Ein Router entspricht hierbei einem "Hop".

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Hop-Limit**

Mögliche Werte:

max. 5 Ziffern im Bereich von 0 - 255

Default:

0: kein Hop-Limit definiert

2.70.2.2.11 Def.-Lifetime

Definiert die Zeit in Sekunden, für die der Router im Netz als erreichbar gelten soll.

Das Betriebssystem verwendet diesen Router nicht als Default Router, wenn Sie hier den Wert **0** eintragen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Def.-Lifetime**

Mögliche Werte:

max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

1800

2.70.2.2.12 Default-Router-Modus

Definiert das Verhalten, wie sich das Gerät als Standardgateway bzw. Router ankündigen soll.

Die Einstellungen haben folgende Funktionen:

- **auto**: Solange eine WAN-Verbindung besteht, setzt der Router eine positive Router-Lifetime in den Router-Advertisement-Nachrichten. Das führt dazu, dass ein Client diesen Router als Standard-Gateway verwendet. Besteht die WAN-Verbindung nicht mehr, so setzt der Router die Router-Lifetime auf "0". Ein Client verwendet dann diesen Router nicht mehr als Standard-Gateway. Dieses Verhalten ist konform zu RFC 6204.
- **immer**: Die Router-Lifetime ist unabhängig vom Status der WAN-Verbindung immer positiv, d. h. größer "0".
- **nie**: Die Router-Lifetime ist immer "0".

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Default-Router-Modus**

Mögliche Werte:

auto

immer

nie

Default:

auto

2.70.2.2.13 Router-Preference

Definiert die Präferenz dieses Routers. Clients tragen diese Präferenz in ihre lokale Routing-Tabelle ein.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Router-Preference**

Mögliche Werte:

low

medium

high

Default:

medium

2.70.2.2.14 RTR-Zeit

Definiert die Zeit in Sekunden zwischen aufeinanderfolgenden Sendungen von Neighbor-Solicitations-Nachrichten an einen Nachbarn, wenn die Adresse aufgelöst oder die Erreichbarkeit getestet wird.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Optionen**

Mögliche Werte:

0 bis 4294967295

Default:

0

2.70.2.3 Route-Optionen

Die Tabelle enthält die Einstellungen der Route-Optionen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen**

2.70.2.3.1 Interface-Name

Definiert den Namen des Interfaces, für das diese Route-Option gilt.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.2.3.2 Praefix

Vergeben Sie das Präfix für diese Route. Dieses darf maximal 64 Bit lang sein, wenn es zur Autokonfiguration dient.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Praefix**

Mögliche Werte:

IPv6-Präfix mit max. 43 Zeichen, z. B. 2001:db8::/64

Default:

leer

2.70.2.3.3 Route-Lifetime

Bestimmen Sie die Dauer in Sekunden, für welche die Route gültig sein soll.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Route-Lifetime**

Mögliche Werte:

max. 5 Ziffern im Bereich von 0 - 65335

Default:

0: Keine Route-Lifetime spezifiziert

2.70.2.3.4 Route-Preference

Dieser Parameter gibt an, welche die Priorität eine angebotene Route hat. Erhält ein Router zwei Routen mit unterschiedlichen Route-Preferences via Router Advertisement, dann wählt er die Route mit der höheren Priorität.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Route-Preference**

Mögliche Werte:

low

medium

high

Default:

medium

2.70.2.5 RDNSS-Optionen

Die Tabelle enthält die Einstellungen der RDNSS-Erweiterung (Recursive DNS Server).

Diese Funktion wird derzeit nicht von Windows unterstützt. Soll ein DNS-Server propagiert werden, geschieht dies über DHCPv6.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

2.70.2.5.1 Interface-Name

Name des Interfaces, auf dem das Gerät in Router-Advertisements die Informationen über den IPv6-DNS-Server ankündigt.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.2.5.2 Erster-DNS

IPv6-Adresse des ersten IPv6-DNS-Servers (Recursive DNS-Server, RDNSS, nach RFC 6106) für dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

Gültige IPv6-Adresse

Default:

leer

2.70.2.5.3 Zweiter-DNS

IPv6-Adresse des zweiten IPv6-DNS-Servers für dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

Gültige IPv6-Adresse

Default:

leer

2.70.2.5.4 DNS-Suchliste

Dieser Parameter definiert, welche DNS-Suchliste das Gerät in diesem logischen Netzwerk propagiert.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

Intern: Wenn Sie diese Option aktivieren, propagiert das Gerät die eigene DNS-Suchliste des internen DNS-Servers bzw. die eigene Domäne für dieses logische Netzwerk. Die eigene Domäne konfigurieren Sie unter **Setup** > **DNS** > **Domain**.

WAN: Wenn Sie diese Option aktivieren, propagiert das Gerät die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) für dieses logische Netzwerk. Diese Funktion steht nur dann zur Verfügung, wenn in der Präfix-Liste das entsprechende WAN-Interface unter **Präfix beziehen von** verknüpft ist.

Default:

Intern aktiviert, WAN deaktiviert.

2.70.2.5.5 Lifetime

Definiert die Dauer in Sekunden, die ein Client diesen DNS-Server zur Namensauflösung verwenden darf.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

- max. 5 Ziffern im Bereich von 0 - 65535
- 0: Abkündigung

Default:

900

2.70.2.6 Praefix-Pools

In diesem Verzeichnis können Sie Präfix-Pools für Einwahl-Benutzer bzw. die zugehörigen RAS-Schnittstellen (PPTP, PPPoE) definieren. Die Präfixe für Ethernet-Interfaces definieren Sie in WEBconfig unter **Setup** > **IPv6** > **Router** > **Router-Advertisements** > **Praefix-Optionen** bzw. im LANconfig unter **IPv6** > **Router-Advertisement** > **Präfix-Liste**.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements**

2.70.2.6.1 Interface-Name

Bestimmen Sie hier den Namen der RAS-Schnittstelle, für die dieser Präfix-Pool gelten soll.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.70.2.6.2 Start-Praefix-Pool

Definieren Sie hier das erste Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db8::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

Default-Wert:

leer

2.70.2.6.3 Ende-Praefix-Pool

Definieren Sie hier das letzte Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db9:FFFF::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 43 Zeichen aus `[A-F][a-f][0-9]:./`

Default-Wert:

::

2.70.2.6.4 Praefix-Laenge

Definieren Sie hier die Länge des Präfixes, das der Einwahl-Benutzer per Router-Advertisement zugewiesen bekommt. Die Größe des Einwahl-Pools richtet sich nur nach dem ersten und letzten Präfix. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool zugewiesen.

Damit ein Client aus dem Präfix per Autokonfiguration eine IPv6-Adresse bilden kann, muss die Präfix-Länge immer 64 Bit betragen.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 3 Zeichen aus `0123456789`

Default-Wert:

64

2.70.2.6.5 Adv.-OnLink

Gibt an, ob das Präfix "On Link" ist.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.70.2.6.6 Adv.-Autonomous

Gibt an, ob ein Client das Präfix für eine "Stateless Address Autoconfiguration (SLAAC)" verwenden kann.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.70.2.6.7 Adv.-Pref.-Lifetime

Legt die Dauer in Millisekunden fest, für die eine IPv6-Adresse als "Preferred" gilt. Diese Lifetime verwendet der Client auch für seine generierte IPv6-Adresse. Wenn die Lifetime des Präfix abgelaufen ist, nutzt der Client auch nicht mehr die entsprechende IPv6-Adresse. Ist diese "Preferred Lifetime" einer Adresse abgelaufen, so wird sie als "deprecated" markiert. Nur noch bereits aktive Verbindungen verwenden diese Adresse bis zum Verbindungsende. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

604800

2.70.2.6.8 Adv.-Valid-Lifetime

Definiert die Dauer in Sekunden, nach der die Gültigkeit einer IPv6-Adresse abläuft. Abgelaufene Adressen stehen für neue Verbindungen nicht mehr zur Verfügung.

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Praefix-Pools**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

2592000

2.70.3 DHCPv6

Dieses Menü enthält die Einstellungen für DHCP über IPv6.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6**

2.70.3.1 Server

Dieses Menü enthält die DHCP-Server-Einstellungen über IPv6.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.2 Adress-Pools

In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pool**

2.70.3.1.2.1 Adress-Pool-Name

Bestimmen Sie hier den Namen des Adress-Pools.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Adress-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

2.70.3.1.2.2 Start-Adress-Pool

Bestimmen Sie hier die erste Adresse des Pools, z. B. "2001:db8::1"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Start-Adress-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.1.2.3 Ende-Adress-Pool

Bestimmen Sie hier die letzte Adresse des Pools, z. B. "2001:db8::9"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Ende-Adress-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.1.2.5 Pref.-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als "bevorzugt" verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als "deprecated".

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Pref.-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

2.70.3.1.2.6 Valid-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als "gültig" verwenden soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Valid-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

2.70.3.1.2.7 PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

2.70.3.1.3 PD-Pools

In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

2.70.3.1.3.1 PD-Pool-Name

Bestimmen Sie hier den Namen des PD-Pools.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **PD-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

2.70.3.1.3.2 Start-PD-Pool

Bestimmen Sie hier das erste zu delegierende Präfix im PD-Pool, z. B. "2001:db8:1100::"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Start-PD-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.1.3.3 Ende-PD-Pool

Bestimmen Sie hier das letzte zu delegierende Präfix im PD-Pool, z. B. "2001:db8:FF00::"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Ende-PD-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.1.3.4 Praefix-Laenge

Bestimmen Sie hier die Länge der Präfixe im PD-Pool, z. B. "56" oder "60"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Praefix-Laenge**

Mögliche Werte:

maximal 3 Ziffern

Default:

56

2.70.3.1.3.5 Pref.-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als "bevorzugt" verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als "deprecated".

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Pref.-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

2.70.3.1.3.6 Valid-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als "gültig" verwenden soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Valid-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

2.70.3.1.3.7 PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

2.70.3.1.4 Interface-Liste

In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

2.70.3.1.4.1 Interface-Name-oder-Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET"

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Interface-Name**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN-Interfaces, maximal 39 Zeichen

Default:

leer

2.70.3.1.4.2 Aktiv

Aktiviert bzw. deaktiviert den DHCPv6-Server.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Aktiv**

Mögliche Werte:

nein

ja

Default:

ja

2.70.3.1.4.3 Erster-DNS

IPv6-Adresse des ersten DNS-Servers.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Erster-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

2.70.3.1.4.4 Zweiter-DNS

IPv6-Adresse des zweiten DNS-Servers.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Zweiter-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

leer

2.70.3.1.4.5 Adress-Pool-Name

Bestimmen Sie den Adress-Pool, den das Gerät für dieses Interface verwenden soll.

Verteilt der DHCPv6-Server seine Adressen 'stateful', müssen Sie entsprechende Adressen in die Tabelle **Setup** > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** eintragen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Adress-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

2.70.3.1.4.6 PD-Pool-Name

Bestimmen Sie den Präfix-Delegierungs-Pool, den das Gerät für dieses Interface verwenden soll.

Soll der DHCPv6-Server Präfixe an weitere Router delegieren, müssen Sie entsprechende Präfixe in der Tabelle **Setup** > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** eintragen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **PD-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

2.70.3.1.4.7 Rapid-Commit

Bei aktiviertem 'Rapid-Commit' antwortet der DHCPv6-Server direkt auf eine Solicit-Anfrage mit einer Reply-Nachricht.

Der Client muss explizit die Rapid-Commit-Option in seiner Anfrage setzen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Rapid-Commit**

Mögliche Werte:

nein

ja

Default:

nein

2.70.3.1.4.8 Preference

Befinden sich mehrere DHCPv6-Server im Netzwerk, so können Sie über die Präferenz steuern, welchen Server die Clients bevorzugen sollen. Der primäre Server muss dafür eine höhere Präferenz haben als die Backup-Server.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Preference**

Mögliche Werte:

0 bis 255

Default:

0

2.70.3.1.4.9 Renew-Time

Definiert die Zeit in Sekunden, zu der der Client den Server wieder kontaktieren soll (durch Renew-Nachricht), um seine vom Server erhaltene Adresse/Präfix zu verlängern. Der Parameter wird auch als T1 bezeichnet.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

0 bis 255

Default:

0 (automatisch)

2.70.3.1.4.10 Rebind-Time

Definiert die Zeit, zu der der Client einen beliebigen Server kontaktieren soll (durch Rebind-Nachricht), um seine erhaltene Adresse/Präfix verlängern zu lassen. Das Rebind-Ereignis tritt nur ein, falls der Client keine Antwort auf seine Renew-Anfrage erhalt. Der Parameter wird auch als T2 bezeichnet.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

0 bis 255

Default:

0 (automatisch)

2.70.3.1.4.11 Unicast-Adresse

Unicast-Adresse des DHCP-Servers. Der DHCP-Server setzt diese Adresse in der Server-Unicast-Option, um den Client zu erlauben per Unicast-Nachrichten mit dem Server zu kommunizieren. Standardmäßig wird Mulitcast verwendet.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

Gültige Unicast-Adresse

Default:

leer

2.70.3.1.4.12 DNS-Suchliste

Dieser Parameter definiert,welche DNS-Suchliste der DNS-Server an die Clients übermittelt.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

Keine: Der DNS-Server verteilt keine Suchliste an die Clients.

Intern: Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. "intern". Die eigene Domäne ist unter IPv4 > DNS > Allgemeine Einstellungen konfigurierbar.

WAN: Gibt an, ob die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Diese Funktion steht nur dann zur Verfügung, wenn in der Präfix-Liste das entsprechende WAN-Interface unter Präfix beziehen von verknüpft ist.

Default:

Intern

2.70.3.1.4.13 Reconfigure

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew/Rebind-Zeiten).

Ändert sich aber z. B. durch Trennung und Wiederaufbau der Internetverbindung oder Anforderung eines neuen Präfixes (Telekom-Privcay-Funktion) das WAN-Präfix, so hat der Server keine Möglichkeit, die Netzwerkgeräte darüber zu informieren, dass sich Präfix bzw. Adresse geändert haben. Das bedeutet, dass ein Client noch eine alte Adresse oder ein altes Präfix verwendet und damit nicht mehr mit dem Internet kommunizieren kann.

Die Reconfigure-Funktion ermöglicht dem DHCPv6-Server, die Clients im Netzwerk zu einer Erneuerung der Leases/Bindings aufzufordern.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Mögliche Werte:

Aus: Deaktiviert die Reconfigure-Funktion.

Verbieten: Clients, die die Reconfigure-Option in Anfragen gesetzt haben, werden vom Server abgelehnt und erhalten keine Adressen, Präfixe oder andere Optionen.

Erlauben: Hat ein Client die Reconfigure-Option in Anfragen gesetzt, so verhandelt der Server mit dem Client die nötigen Parameter, um zu einem späteren Zeitpunkt ein Reconfigure zu starten.

Erzwingen: Clients müssen die Reconfigure-Option in ihren Anfragen setzen, sonst lehnt der Server diese Clients ab. Dieser Modus ist dann sinnvoll, wenn Sie sichergehen wollen, dass der Server ausschließlich Clients bedient, die Reconfigure unterstützen. Dadurch ist gewährleistet, dass alle Clients zu einem späteren Zeitpunkt erfolgreich durch Reconfigure ihre Adressen, Präfixe oder weiteren Informationen aktualisieren können.

Default:

Aus

2.70.3.1.5 Confirm-Auf-Clients-Mit-Adressen-Beschraenken

Über diese Einstellung konfigurieren Sie das Verhalten des DHCPv6-Servers, wenn dieser eine Confirm-Nachricht von einem Client bekommt, dem dieser Server noch keine IP-Adresse zugewiesen hat. In der Einstellung **nein** beantwortet der Server die Nachricht mit einem "Not-on-link"-Status; in der Einstellung **ja** beantwortet er sie gar nicht.

Dieser Parameter wird ausschließlich für Entwicklungstests benötigt und ist für den normalen Betriebsablauf nicht relevant. Verändern Sie die Standardeinstellung niemals!

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

Mögliche Werte:

ja

nein

Default:

nein

2.70.3.1.6 Reservierungen

Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, definieren Sie in dieser Tabelle pro Client eine Reservierung.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

2.70.3.1.6.1 Interface-Name-oder-Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ können Sie auch die IPv6-Adresse des entfernten Relay-Agenten eintragen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN-Interfaces, maximal 39 Zeichen

Default:

leer

2.70.3.1.6.2 Adresse-oder-PD-Praefix

IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Maximal 43 Zeichen

Default:

leer

2.70.3.1.6.3 Client-ID

DHCPv6-Unique-Identifier (DUID) des Clients.

Bei DHCPv6 lassen sich Clients nicht mehr wie bei DHCPv4 anhand ihrer MAC-Adresse, sondern anhand der DUID identifizieren. Die DUID lässt sich auf dem jeweiligen Client auslesen, unter Windows beispielsweise mit dem Kommandozeilen-Befehl `show dhcpv6-client` oder im WEBconfig unter **Status** > **IPv6** > **DHCPv6** > **Client** > **Client-ID**.

Arbeitet das Gerät als DHCPv6-Server, finden sich die Client-IDs der Clients mit aktuellem Bezug von IPv6-Adressen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Adress-Zuteilungen**, bzw. mit aktuellem Bezug von IPv6-Präfixen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **PD-Zuteilungen**.

Der LANmonitor zeigt die Client-IDs der Clients unter **DHCPv6-Server** an.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Maximal 96 Zeichen

Default:

leer

2.70.3.1.6.5 Pref.-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als "bevorzugt" verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als "deprecated".

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

2.70.3.1.6.6 Valid-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als "gültig" verwenden soll.

Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte Bevorzugte Gültigkeit und Gültigkeitsdauer gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

2.70.3.1.6.7 PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

2.70.3.1.7 Adressrouten-Anlegen

Der DHCPv6-Server legt für IA_NA (Identity Association for Non-temporary Addresses) zugewiesene Adressen einen Eintrag in der Routing-Tabelle an. Diese Funktion wird beispielsweise dann benötigt, wenn der DHCPv6-Server IA_NA-Adressen auf PPP-Schnittstellen zuweisen soll und ein IPv6-Adresspool über mehrere PPP-Schnittstellen verwendet wird. Auf anderen Schnittstellen als Punkt-zu-Punkt wird dieser Schalter nicht benötigt.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.70.3.2 Client

Dieses Menü enthält die DHCP-Client-Einstellungen über IPv6.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client**

2.70.3.2.1 Interface-Liste

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Clients.

Normalerweise steuert bereits die Autokonfiguration das Client-Verhalten.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

2.70.3.2.1.1 Interface-Name

Vergeben Sie den Namen des Interfaces, auf dem der DHCPv6-Client arbeitet. Dies können LAN-Interfaces oder WAN-Interfaces (Gegenstellen) sein, z. B. "INTRANET" oder "INTERNET".

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Interface-Name**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN-Interfaces, maximal 16 Zeichen

Default:

leer

2.70.3.2.1.2 Aktiv

Bestimmen Sie hier, wie und ob das Gerät den Client aktiviert. Mögliche Werte sind:

- **Autoconf:** Das Gerät wartet auf Router-Advertisements und startet dann den DHCPv6-Client. Diese Option ist die Standardeinstellung.
- **Ja:** Das gerät startet den DHCPv6-Client sofort, sobald die Schnittstelle aktiv wird, ohne auf Router-Advertisements zu warten.
- **Nein:** Der DHCPv6-Client ist auf diesem Interface deaktiviert. Auch, wenn das Gerät Router-Advertisements empfängt, startet es den Client nicht.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Aktiv**

Mögliche Werte:

Autoconf

Nein

Ja

Default:

Autoconf

2.70.3.2.1.3 DNS-Anfragen

Legen Sie fest, ob der Client beim DHCPv6-Server nach DNS-Servern fragen soll.

Sie müssen diese Option aktivieren, damit das Gerät Informationen über einen DNS-Server erhält.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **DNS-Anfragen**

Mögliche Werte:

nein

ja

Default:

ja

2.70.3.2.1.4 Adresse-Anfragen

Legen Sie fest, ob der Client beim DHCPv6-Server nach einer IPv6-Adresse fragen soll.

Diese Option sollten Sie nur dann aktivieren, wenn der DHCPv6-Server die Adressen über dieses Interface stateful, d. h. nicht durch 'SLAAC', verteilt.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Adresse-Anfragen**

Mögliche Werte:

nein

ja

Default:

ja

2.70.3.2.1.5 PD-Anfragen

Legen Sie fest, ob der Client beim DHCPv6-Server nach einem IPv6-Präfix anfragen soll. Eine Aktivierung dieser Option ist nur dann sinnvoll, wenn das Gerät selber als Router arbeitet und Präfixe weiterverteilt. Auf WAN-Interfaces ist diese Option standardmäßig aktiviert, damit der DHCPv6-Client ein Präfix beim Provider anfragt, das er ins lokale Netzwerk weiterverteilen kann. Auf LAN-Interfaces ist diese Option standardmäßig deaktiviert, weil ein Gerät im lokalen Netzwerk eher als Client und nicht als Router arbeitet.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **PD-Anfragen**

Mögliche Werte:

nein

ja

Default:

nein

2.70.3.2.1.6 Rapid-Commit

Bei aktiviertem Rapid-Commit versucht der Client, mit nur zwei Nachrichten vom DHCPv6-Server eine IPv6-Adresse zu erhalten. Ist der DHCPv6-Server entsprechend konfiguriert, antwortet er auf diese Solicit-Anfrage sofort mit einer Reply-Nachricht.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Rapid-Commit**

Mögliche Werte:

nein

ja

Default:

ja

2.70.3.2.1.7 FQDN-Senden

Mit dieser Einstellung legen Sie fest, ob der Client seinen Gerätenamen per FQDN-Option (Fully Qualified Domain Name) an den DHCPv6-Server senden soll oder nicht.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

Mögliche Werte:

ja

nein

Default:

ja

2.70.3.2.1.8 Reconf-Erlauben

Mit dieser Einstellung legen Sie fest, ob die Clients des betreffenden Interfaces mit dem DHCPv6-Server ein Reconfigure aushandeln dürfen.

Wenn Sie diese Einstellung aktivieren, erlauben Sie einem DHCP-Server, sogenannte Reconfigure-Nachrichten an einen Client zu schicken. Der Client antwortet seinerseits mit einem Renew oder Rebind an den Server. In der Antwort auf dieses Renew oder Rebind kann der Server dem Client daraufhin ein(e) neue(s) IPv6-Adresse oder delegiertes IPv6-Präfix zuweisen, oder dieses verlängern.

Weitere Informationen zur dynamischen Rekonfiguration finden Sie im Referenzhandbuch im IPv6-Abschnitt zum DHCPv6-Server unter 'Reconfigure'.

Damit die dynamische Rekonfiguration funktioniert, müssen Sie sie für den Server ebenfalls aktivieren!

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

Mögliche Werte:

ja

nein

Default:

nein

2.70.3.2.1.9 Domainliste-Anfragen

Mit dieser Einstellung aktivieren Sie, ob ein Client die Liste der über das betreffende Interface verfügbaren Domainnamen vom DHCP-Server abrufen soll.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

Mögliche Werte:

ja

nein

Default:

ja

2.70.3.2.2 User-Class-Identifier

Vergeben Sie dem Gerät eine eindeutige User-Class-ID.

Ein User-Class-Identifier dient dazu, den Typ oder die Kategorie des Clients beim Server zu Identifizieren. Beispielsweise könnte der User-Class-Identifier dazu verwendet werden, um alle Clients der Mitarbeiter aus der Abteilung "Buchhaltung" oder alle Drucker an einem Standort zu identifizieren.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **User-Class-Identifier**

Mögliche Werte:

maximal 253 Zeichen

Default:

leer

2.70.3.2.3 Vendor-Class-Identifier

Vergeben Sie dem Gerät eine eindeutige Vendor-Class-ID.

Der Vendor-Class-Identifier dient dazu, den Hersteller der Hardware, auf der der DHCP-Client läuft, zu identifizieren.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Vendor-Class-Identifier**

Mögliche Werte:

maximal 253 Zeichen

Default:

Name des Geräteherstellers

2.70.3.2.4 Vendor-Class-Nummer

Bestimmt die Enterprise Number, mit der der Gerätehersteller bei der IANA (Internet Assigned Numbers Authority) registriert ist.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client**

Mögliche Werte:

maximal 10 Zeichen

Default:

2356

2.70.3.3 Relay-Agent

Dieses Menü enthält die DHCP-Relay-Agent-Einstellungen über IPv6.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent**

2.70.3.3.1 Interface-Liste

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Relay-Agents.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste**

2.70.3.3.1.1 Interface-Name

Definieren Sie den Name des Interfaces, auf dem der Relay-Agent Anfragen von DHCPv6-Clients entgegennimmt, z. B. "INTRANET".

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Interface-Name**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN-Interfaces, maximal 16 Zeichen

Default:

leer

2.70.3.3.1.2 Relay-Agent aktiviert

Definieren Sie mit dieser Option, wie und ob das Gerät den Relay-Agent aktiviert.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Relay-Agent aktiviert**

Mögliche Werte:

Ja: Relay-Agent ist aktiviert. Diese Option ist die Standardeinstellung.

Nein: Relay-Agent ist nicht aktiviert.

Default:

Ja

2.70.3.3.1.3 Interface-Adresse

Definieren Sie die eigene IPv6-Adresse des Relay-Agents auf dem Interface, das unter Interface-Name konfiguriert ist. Diese IPv6-Adresse wird als Absenderadresse in den weitergeleiteten DHCP-Nachrichten verwendet. Über diese Absenderadresse kann ein DHCPv6-Server einen Relay-Agenten eindeutig identifizieren. Die explizite Angabe der Interface-Adresse ist nötig, da ein IPv6-Host durchaus mehrere IPv6-Adressen pro Schnittstelle haben kann.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Interface-Adresse**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.3.1.4 Ziel-Adresse

Definieren Sie die IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder Linklokale Multicast-Adresse sein. Bei Verwendung einer Linklokalen

Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der Linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Ziel-Adresse**

Mögliche Werte:

maximal 39 Zeichen

Default:

ff02::1:2

2.70.3.3.1.5 Ziel-Interface

Definieren Sie das Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine Linklokale Multicast-Adresse konfiguriert wird, da Linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Ziel-Interface**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

2.70.3.3.2 Adressrouten-Anlegen

Der DHCPv6-Server legt für IA_NA (Identity Association for Non-temporary Addresses) zugewiesene Adressen einen Eintrag in der Routing-Tabelle an. Diese Funktion wird beispielsweise dann benötigt, wenn der DHCPv6-Server IA_NA-Adressen auf PPP-Schnittstellen zuweisen soll und ein IPv6-Adresspool über mehrere PPP-Schnittstellen verwendet wird. Auf anderen Schnittstellen als Punkt-zu-Punkt wird dieser Schalter nicht benötigt.

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent**

Mögliche Werte:

nein
ja

Default-Wert:

nein

2.70.4 Netzwerk

Hier können Sie für jedes logische Interface Ihres Gerätes weitere IPv6-Netzwerk-Einstellungen vornehmen.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk**

2.70.4.1 Adressen

In dieser Tabelle verwalten Sie die IPv6-Adressen.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen**

2.70.4.1.1 Interface-Name

Benennen Sie das Interface, dem Sie das IPv6-Netz zuordnen wollen.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.4.1.2 IPv6-Adresse-Praefixlaenge

Vergeben Sie eine IPv6-Adresse inklusive Präfixlänge für dieses Interface.

Die Präfixlänge beträgt standardmäßig 64 Bit ("/64"). Verwenden Sie für die IPv6-Adresse möglichst keine längeren Präfixe, da zahlreiche IPv6-Mechanismen im Gerät von maximal 64 Bit Länge ausgehen.

Eine mögliche Adresse lautet z. B. "2001:db8::1/64". Ein Interface kann mehrere IPv6-Adressen besitzen:

- eine "Global Unicast Adresse", z. B. "2001:db8::1/64",
- eine "Unique Local Adresse", z. B. "fd00::1/64".

"Link Local Adressen" sind pro Interface fest vorgegeben und nicht konfigurierbar.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **IPv6-Adresse-Praefixlaenge**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

2.70.4.1.3 Adresstyp

Bestimmen Sie den Typ der IPv6-Adresse.

Beim Adresstyp **EUI-64** wird die IPv6-Adresse gemäß der IEEE-Norm "EUI-64" gebildet. Die MAC-Adresse der Schnittstelle stellt damit einen eindeutig identifizierbaren Bestandteil der IPv6-Adresse dar. Ein korrektes Eingabeformat für eine IPv6-Adresse inkl. Präfixlänge nach EUI-64 würde lauten: "2001:db8:1::/64".

"EUI-64" ignoriert einen eventuell konfigurierten "Interface Identifier" der jeweiligen IPv6-Adresse und ersetzt ihn durch einen "Interface Identifier" nach "EUI-64".

Die Präfixlänge bei "EUI-64" muss zwingend "/64" sein.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Adresstyp**

Mögliche Werte:

Unicast

Anycast

EUI-64

Default:

Unicast

2.70.4.1.4 Name

Vergeben Sie einen aussagekräftigen Namen für diese Kombination aus IPv6-Adresse und Präfix.

Die Eingabe eines Namens ist optional.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.4.1.5 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

2.70.4.2 Parameter

In dieser Tabelle verwalten Sie die IPv6-Parameter.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter**

2.70.4.2.1 Interface-Name

Benennen Sie das Interface, für Sie die IPv6-Parameter konfigurieren wollen.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.4.2.2 IPv6-Gateway

Bestimmen Sie das verwendete IPv6-Gateway für dieses Interface.

Dieser Parameter überschreibt Gateway-Informationen, die das Gerät beispielsweise über Router-Advertisements empfängt.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **IPv6-Gateway**

Mögliche Werte:

- Global Unicast Adresse, z. B. 2001:db8::1
- Link lokale Adresse, welche Sie um das entsprechende Interface (%<INTERFACE>) ergänzen, z. B. fe80::1%INTERNET

Default:

::

2.70.4.2.3 Erster-DNS

Bestimmen Sie den ersten IPv6-DNS-Server für dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Erster-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

2.70.4.2.4 Zweiter-DNS

Bestimmen Sie den zweiten IPv6-DNS-Server für dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Zweiter-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

2.70.4.3 Loopback

Hier können Sie IPv6-Loopback-Adressen festlegen. Das Gerät sieht jede dieser Adressen als eigene Adresse an, die auch dann verfügbar ist, wenn z. B. eine physikalische Schnittstelle deaktiviert ist.

Pfad Telnet:

Setup > **IPv6** > **Netz**

2.70.4.3.1 Name

Vergeben Sie hier einen eindeutigen Namen für diese Loopback-Adresse.

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.70.4.3.2 IPv6-Loopback-Addr.

Geben Sie hier eine gültige IPv6-Adresse ein.

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 39 Zeichen aus `0123456789ABCDEFabcdef:./`

Default-Wert:

leer

2.70.4.3.3 Rtg-Tag

Geben Sie hier das Routing-Tag des Netzes an, zu dem die Loopback-Adresse gehört. Nur die Pakete mit dem entsprechenden Routing-Tag erreichen diese Adresse.

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

0

2.70.4.3.4 Kommentar

Tragen Sie hier einen optionalen Kommentar ein.

Pfad Telnet:

Setup > **IPv6** > **Netz** > **Loopback**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

2.70.5 Firewall

Dieses Menü enthält die Einstellungen für die Firewall.

Pfad Telnet:

Setup > **IPv6** > **Firewall**

2.70.5.1 Aktiv

Aktivieren bzw. deaktivieren Sie die Firewall.

Hier aktivieren Sie die Firewall global. Nur, wenn Sie die Firewall hier aktivieren, ist die Firewall aktiv. Wenn Sie die Firewall hier deaktivieren und gleichzeitig für einzelne Interfaces aktivieren, dann ist sie trotzdem für alle Interfaces inaktiv.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktiv**

Mögliche Werte:

ja

nein

Default:

ja

2.70.5.2 Forwarding-Regeln

Diese Tabelle enthält die Regeln, die die Firewall beim Forwarding von Daten anwenden soll.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

2.70.5.2.1 Name

Definiert den Namen für die Forwarding-Regel.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.2.2 Flags

Diese Optionen bestimmen, wie die Firewall die Regel behandelt. Die Optionen haben folgende Bedeutung:

- **deaktiviert**: Die Regel ist deaktiviert. Die Firewall überspringt diese Regel.
- **verkettet**: Nach dem Abarbeiten der Regel sucht die Firewall nach weiteren Regeln, die für die Ausführung in Frage kommen.
- **zustandslos**: Diese Regel beachtet die Zustände von TCP-Sessions nicht.

Sie können mehrere Optionen gleichzeitig auswählen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

deaktiviert

verkettet

zustandslos

Default:

keine Auswahl

2.70.5.2.3 Prio

Diese Angabe bestimmt die Priorität, mit der die Firewall die Regel anwendet. Ein höherer Wert bestimmt eine höhere Priorität.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 4 Zeichen aus 1234567890

Default:

0

2.70.5.2.4 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 5 Zeichen aus 1234567890

Default:

0

2.70.5.2.5 Aktion

Legt die Aktion fest, die die Firewall bei gültiger Regelbedingung ausführen soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Aktionen** sind bereits bestimmte Standard-Aktionen vorgegeben. Sie können dort auch zusätzlich eigene Aktionen definieren.

Sie können mehrere Aktionen durch Komma getrennt eingeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

2.70.5.2.7 Dienste

Diese Angabe bestimmt, für welche Dienste die Firewall diese Regel anwenden soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Dienste** sind bereits bestimmte Dienste vorgegeben. Sie können dort auch zusätzlich eigene Dienste definieren.

Sie können mehrere Dienste durch Komma getrennt eingeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

2.70.5.2.8 Quell-Stationen

Diese Angabe bestimmt, auf welche Quell-Stationen die Firewall die Regel anwenden soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Stationen** sind bereits bestimmte Stationen vorgegeben. Sie können dort auch zusätzlich eigene Stationen definieren.

Sie können mehrere Stationen durch Komma getrennt eingeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

2.70.5.2.9 Ziel-Stationen

Diese Angabe bestimmt, auf welche Ziel-Stationen die Firewall die Regel anwenden soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Stationen** sind bereits bestimmte Stationen vorgegeben. Sie können dort auch zusätzlich eigene Stationen definieren.

Sie können mehrere Stationen durch Komma getrennt eingeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

2.70.5.2.10 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

2.70.5.2.11 Quell-Tag

Das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) dient zur Identifikation des ARF-Kontextes aus dem ein Paket empfangen wurde. Dieses kann zur Einschränkung von Firewall-Regeln auf bestimmte ARF-Kontexte verwendet werden.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

0 bis 65535

Erläuterung:

- 65535: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 0 ist.

- 1…65534: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 1…65534 ist.
- 0: Wildcard. Die betreffende Firewall-Regel wird auf alle ARF-Kontexte angewandt (erwartetes Schnittstellen- bzw. Routing-Tag 0…65535).

Default:

0

2.70.5.3 Aktions-Liste

In dieser Tabelle können Sie Aktionen zu Gruppen zusammenfassen. Die Aktionen definieren Sie vorher unter **Setup** > **IPv6** > **Firewall** > **Aktionen**.

Sie können eine Aktion in dieser Liste nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

2.70.5.3.1 Name

Definiert den Namen einer Gruppe von Aktionen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.3.2 Beschreibung

Enthält die Liste der Aktionen, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

Mögliche Werte:

max. 252 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

2.70.5.5 Stations-Liste

In dieser Tabelle können Sie Stationen zu Gruppen zusammenfassen. Die Stationen definieren Sie vorher unter **Setup** > **IPv6** > **Firewall** > **Stationen**.

Sie können eine Station in dieser Liste nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

2.70.5.5.1 Name

Definiert den Namen einer Gruppe von Stationen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.5.2 Beschreibung

Enthält die Liste der Stationen, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

Mögliche Werte:

max. 252 Zeichen aus #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

2.70.5.6 Dienst-Liste

In dieser Tabelle können Sie Dienste zu Gruppen zusammenfassen. Die Dienste definieren Sie vorher unter **Setup** > **IPv6** > **Firewall** > **Dienste**.

Sie können einen Dienst in dieser Liste nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

2.70.5.6.1 Name

Definiert den Namen einer Gruppe von Diensten.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.6.2 Beschreibung

Enthält die Liste der Dienste, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

Mögliche Werte:

max. 252 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

2.70.5.7 Aktionen

Diese Tabelle enthält eine Liste der Aktionen, die die Firewall gemäß der Forwarding- und Inbound-Regeln ausführen kann.

Sie können unter **Setup** > **IPv6** > **Firewall** > **Aktions-Liste** mehrere Aktionen zusammenfassen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

2.70.5.7.1 Name

Definiert den Namen der Aktion.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.7.2 Limit

Bestimmt das Limit, bei dessen Überschreiten die Firewall die Filterregel anwendet.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 10 Zeichen aus 0123456789

Besondere Werte:

0: Die Regel tritt sofort in Kraft.

Default:

0

2.70.5.7.3 Einheit

Bestimmt die Einheit des Limits.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

kBit

kByte

Pakete

Sessions

Bandbreite (%)

Default:

Pakete

2.70.5.7.4 Zeit

Bestimmt, für welchen Messzeitraum die Firewall das Limit ansetzt.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

Sekunde

Minute

Stunde

absolut

Default:

absolut

2.70.5.7.5 Kontext

Bestimmt, in welchem Kontext die Firewall das Limit ansetzt. Mögliche Werte sind:

- **Session**: Das Limit bezieht sich nur auf den Datenverkehr der aktuellen Session.
- **Station**: Das Limit bezieht sich nur auf den Datenverkehr der Station.
- **global**: Alle Sessions, auf die diese Regel zutrifft, verwenden denselben Limit-Zähler.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

Session

Station

global

Default:

Session

2.70.5.7.6 Flags

Bestimmt die Eigenschaften des Limits dieser Aktion. Mögliche Werte sind:

- **reset**: Bei Überschreiten des Limits setzt die Aktion den Zähler zurück.
- **geteilt**: Alle Regeln, die sich auf dieses Limit beziehen, verwenden denselben Limit-Zähler.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

reset

geteilt

Default:

leer

2.70.5.7.7 Aktion

Bestimmt die Aktion, die die Firewall bei Erreichen des Limits ausführt.

Die folgende Auswahl ist möglich:

- **reject**: Die Firewall weist das Datenpaket zurück und sendet einen entsprechenden Hinweis an den Absender.
- **drop**: Die Firewall verwirft das Datenpaket ohne Benachrichtigung.
- **accept**: Die Firewall akzeptiert das Datenpaket.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

reject

drop

accept

Default:

.

2.70.5.7.11 DiffServ

Bestimmt die Priorität der Datenpakete (Differentiated Services, DiffServ), mit der die Firewall die Datenpakete übertragen soll.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

BE

EF

CS0 bis CS7

AF11 bis AF43

nein

Wert

Besondere Werte:

Wert: Sie können im Feld **DSCP-Wert** direkt den DSCP-Dezimalwert eintragen.

Default:

nein

2.70.5.7.12 DSCP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

Geben Sie hier einen Wert ein, wenn Sie im Feld **DiffServ** die Option "Wert" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 2 Zeichen aus 1234567890

Default:

0

2.70.5.7.13 Bedingungen

Bestimmt, welche Bedingung zusätzlich zur Ausführung der Aktion erfüllt sein müssen. Die Bedingungen können Sie unter **Setup** > **IPv6** > **Firewall** > **Bedingungen** definieren.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.7.14 Trigger-Aktionen

Bestimmt, welche Trigger-Aktionen die Firewall zusätzlich zur Filterung der Datenpakete starten soll. Die Trigger-Aktionen können Sie unter **Setup** > **IPv6** > **Firewall** > **Trigger-Aktionen** definieren.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.9 Stationen

Diese Tabelle enthält eine Liste der Quell-Stationen, auf deren eingehende Verbindungen die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

Sie können unter **Setup** > **IPv6** > **Firewall** > **Stations-Liste** mehrere Stationen zusammenfassen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

2.70.5.9.1 Name

Definiert den Namen der Station.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.9.2 Typ

Bestimmt den Stationstyp.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

lokales-Netzwerk

Gegenstelle

Praefix

Identifier

IP-Adresse

benamter-Host

Default:

lokales-Netzwerk

2.70.5.9.3 lokales-Netzwerk

Geben Sie hier den Namen des lokalen Netzwerkes ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 16 Zeichen aus #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.9.6 Gegenstelle/Host-Name

Geben Sie hier die Gegenstelle oder den Host-Namen ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 64 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.9.7 Adresse/Praefix

Tragen Sie hier die IP-Adresse oder das Präfix der Station ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 43 Zeichen aus ABCDEFabcdef0123456789:

Default:

leer

2.70.5.10 Dienste

Diese Tabelle enthält eine Liste der Dienste, für deren Verbindungs-Protokolle die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

Sie können unter **Setup** > **IPv6** > **Firewall** > **Dienst-Liste** mehrere Dienste zusammenfassen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

2.70.5.10.1 Name

Definiert den Namen des Dienstes.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.10.2 Protokoll

Definiert das Protokoll des Dienstes.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

TCP+UDP

TCP

UDP

Default:

TCP+UDP

2.70.5.10.3 Ports

Definiert die Ports des Dienstes. Trennen Sie mehrere Ports jeweils durch ein Komma.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

max. 64 Zeichen aus 0123456789,

Default:

leer

2.70.5.10.4 Src-Ports

Bestimmt, ob es sich bei den angegebenen Ports um Quell-Ports handelt.

In bestimmten Szenarien kann es sinnvoll sein, einen Quell-Port anzugeben. Normalerweise ist es aber unüblich, so dass die Auswahl "nein" zu empfehlen ist.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

nein

ja

Default:

nein

2.70.5.11 Protokolle

Diese Tabelle enthält eine Liste der Protokolle, für die die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

2.70.5.11.1 Name

Definiert den Namen des Protokolls.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.11.2 Protokoll

Definiert die Protokoll-Nummer.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

Mögliche Werte:

max. 3 Zeichen 0123456789

Default:

leer

2.70.5.12 Bedingungen

Diese Tabelle enthält eine Liste der Bedingungen, für die die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

2.70.5.12.1 Name

Definiert den Namen der Bedingung.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.12.2 Bedingungen

Bestimmt die Bedingungen, die erfüllt sein müssen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

nicht-verbunden

Default-Route

Backup-Verbindung

VPN-Route

gesendet

empfangen

Default:

leer

2.70.5.12.3 Transportrichtung

Bestimmt, ob die Transportrichtung sich auf den logischen Verbindungsaufbau oder die physikalische Datenübertragung über das jeweilige Interface bezieht.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

physikalisch

logisch

Default:

physikalisch

2.70.5.12.4 DiffServ

Bestimmt, welche Priorität die Datenpakete (Differentiated Services, DiffServ) besitzen müssen, damit die Bedingung erfüllt ist.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

BE

EF

CS0 bis CS7, CSx

AF11 bis AF43, AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx

nein

Wert

Besondere Werte:

CSx: Erweitert den Bereich auf alle Class Selectors.

AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx: Erweitert den Bereich auf die entsprechenden Assured-Forwarding-Klassen (so berücksichtigt z. B. AF1x die Klassen AF11, AF12, AF13)

Wert: Sie können im Feld **DSCP-Wert** direkt den DSCP-Dezimalwert eintragen.

Default:

ignorieren

2.70.5.12.5 DSCP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

Geben Sie hier einen Wert ein, wenn Sie im Feld **DiffServ** die Option "Wert" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 2 Zeichen aus 1234567890

Default:

0

2.70.5.13 Trigger-Aktionen

Diese Tabelle enthält eine Liste der Trigger-Aktionen, die die Firewall-Aktionen starten können.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

2.70.5.13.1 Name

Definiert den Namen der Trigger-Aktion.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.13.2 Benachrichtigungen

Bestimmt, ob und wie eine Benachrichtigung erfolgen soll.

Wenn Sie eine Benachrichtigung per E-Mail erhalten möchten, müssen Sie unter **Setup** > **IP-Router** > **Firewall** > **Admin-E-Mail** eine E-Mail-Adresse angeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

SNMP

SYSLOG

E-Mail

Default:

leer

2.70.5.13.3 Trennen

Bestimmt, ob die Firewall bei gültiger Filterbedingung die Verbindung zur Gegenstelle trennt.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

2.70.5.13.4 Quelle-Sperren

Bestimmt, ob die Firewall bei gültiger Filterbedingung die Quelle sperrt. Die Firewall trägt die gesperrte IP-Adresse, die Sperrzeit sowie die zugrunde liegende Regel in die **Hostsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

2.70.5.13.5 Sperrzeit

Bestimmt, für wie viele Minuten die Firewall die Quelle sperren soll.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

max. 8 Zeichen aus 0123456789

Besondere Werte:

0: deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Default:

0

2.70.5.13.6 Ziel-Schliessen

Bestimmt, ob die Firewall bei gültiger Filterbedingung den Zielport schließt. Die Firewall trägt die gesperrte Ziel-IP-Adresse, das Protokoll, den Ziel-Port, die Sperrzeit sowie die zugrunde liegende Regel in die **Portsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

2.70.5.13.7 Schliesszeit

Bestimmt, für wie viele Sekunden die Firewall das Ziel schließt.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

max. 8 Zeichen aus 0123456789

Besondere Werte:

0: deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Default:

0

2.70.5.14 ICMP-Dienste

Diese Tabelle enthält eine Liste der ICMP-Dienste.

Da ICMPv6 für zahlreiche IPv6-Funktionen eine zentrale Bedeutung besitzt, sind bereits grundlegende ICMPv6-Regeln standardmäßig voreingestellt. Sie können diese Regeln nicht löschen.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

2.70.5.14.1 Name

Definiert den Namen des ICMP-Dienstes.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.14.2 Typ

Definiert den Typ des ICMP-Dienstes.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 3 Zeichen aus 0123456789

Default:

0

2.70.5.14.3 Code

Definiert den Code des ICMP-Dienstes.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 3 Zeichen aus 0123456789

Default:

0

2.70.5.15 Inbound-Regeln

Diese Tabelle enthält die Regeln, die die Firewall bei Inbound-Verbindungen anwenden soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

2.70.5.15.1 Name

Definiert den Namen der Inbound-Regel.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

2.70.5.15.2 Aktiv

Diese Option aktiviert die Inbound-Regel.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

ja

nein

Default:

ja

2.70.5.15.3 Prio

Diese Angabe bestimmt die Priorität, mit der die Firewall die Regel anwendet. Ein höherer Wert bestimmt eine höhere Priorität.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 4 Zeichen aus 1234567890

Default:

0

2.70.5.15.5 Aktion

Legt die Aktion fest, die die Firewall bei gültiger Regelbedingung ausführen soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Aktionen** sind bereits bestimmte Standard-Aktionen vorgegeben. Sie können dort auch zusätzlich eigene Aktionen definieren.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

2.70.5.15.7 Dienste

Diese Angabe bestimmt, für welche Dienste die Firewall diese Regel anwenden soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Dienste** sind bereits bestimmte Dienste vorgegeben. Sie können dort auch zusätzlich eigene Dienste definieren.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

2.70.5.15.8 Quell-Stationen

Diese Angabe bestimmt, auf welche Quell-Stationen die Firewall die Regel anwenden soll. In der Tabelle **Setup** > **IPv6** > **Firewall** > **Stationen** sind bereits bestimmte Stationen vorgegeben. Sie können dort auch zusätzlich eigene Stationen definieren.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

2.70.5.15.10 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

2.70.5.15.11 Quell-Tag

Das Quell-Tag (erwartetes Schnittstellen- bzw. Routing-Tag) dient zur Identifikation des ARF-Kontextes aus dem ein Paket empfangen wurde. Dieses kann zur Einschränkung von Firewall-Regeln auf bestimmte ARF-Kontexte verwendet werden.

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

0 bis 65535

Erläuterung:

- 65535: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 0 ist.
- 1…65534: Die betreffende Firewall-Regel wird angewandt, wenn das erwartete Schnittstellen- bzw. Routing-Tag 1…65534 ist.
- 0: Wildcard. Die betreffende Firewall-Regel wird auf alle ARF-Kontexte angewandt (erwartetes Schnittstellen- bzw. Routing-Tag 0…65535).

Default:

0

2.70.5.20 Route-Optionen-zulassen

Mit dieser Einstellung legen Sie fest, ob die IPv6-Firewall Routing-Optionen akzeptieren oder verwerfen soll. Das Verwerfen von Routing-Optionen bewirkt immer die Meldung eines IDS-Events. Diese Aktion ist unabhängig von den Einstellungen im IDS selbst.

Pfad Telnet:

Setup > **IPv6** > **Firewall**

Mögliche Werte:

nein

ja

Default:

nein

2.70.5.21 Destination-Cache-Limit

Mit dieser Einstellung begrenzen Sie die Anzahl "unbeantworteter" Destination-Cache-Einträge. Wenn innerhalb des eingestellten *Destination-Cache-Timeouts* von einem Interface aus mehr als die hier konfigurierte Anzahl an Zieladressen angesprochen wird, von denen keine Antwort erfolgt, blockiert die Firewall alle weiteren **neuen** Zieladressen für dieses Interface. In der Standardeinstellung (s. u.) kann dies z. B. dann passieren, wenn zu viele Benutzer im LAN Anfragen an nicht erreichbare Server im Internet stellen.

Um die Destination-Cache-Prüfung global für alle Interfaces zu deaktivieren, tragen Sie als Limit den Wert `0` ein. Um die Prüfung für ein spezifisches Interface deaktivieren, schalten Sie die Firewall auf dem betreffenden Interface aus. In der Standardeinstellung z. B. (LAN: Firwall aus // WAN: Firewall ein) prüft das Gerät den Datenverkehr von Benutzern innerhalb des LANs nicht.

Der Default-Wert ist für die meisten Szenarien hinreichend groß gewählt, sodass das IDS nicht bereits im Normalbetrieb auslöst.

Pfad Telnet:

Setup > **IPv6** > **Firewall**

Mögliche Werte:

0 bis 99999

Default:

300

2.70.6 LAN-Interfaces

Die Tabelle enthält die Einstellungen für die LAN-Interfaces.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces**

2.70.6.1 Interface-Name

Benennen Sie das logische IPv6-Interface, das durch das physikalische Interface (Schnittstellen-Zuordnung) und die VLAN-ID definiert wird.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.6.2 Interface-ID

Wählen Sie die physikalische Schnittstelle aus, die zusammen mit der VLAN-ID das logische IPv6-Interface bilden soll.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-ID**

Mögliche Werte:

alle verfügbaren physikalischen Schnittstellen des Gerätes

Default:

LAN-1

2.70.6.3 VLAN-ID

Wählen Sie die VLAN-ID aus, die zusammen mit der physikalischen Schnittstelle das logische IPv6-Interface bilden soll.

Wenn Sie hier eine ungültige VLAN-ID eingeben, dann findet keine Kommunikation statt.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **VLAN-ID**

Mögliche Werte:

0 bis 4096

max. 4 Ziffern

Default:

0

2.70.6.4 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65535

Default:

0

2.70.6.5 Autoconf

Aktivieren bzw. deaktivieren Sie die "Stateless Address Autoconfiguration" für dieses Interface.

Falls das Gerät über dieses Interface Router-Advertisements versendet, erzeugt es auch bei aktivierter Autokonfiguration keine IPv6-Adressen.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Autoconf**

Mögliche Werte:

ja

nein

Default:

ja

2.70.6.6 Akzeptiere-RA

Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten.

Bei deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Akzeptiere-RA**

Mögliche Werte:

ja

nein

Default:

ja

2.70.6.7 Interface-Status

Aktivieren bzw. deaktivieren Sie dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-Status**

Mögliche Werte:

aktiv

inaktiv

Default:

aktiv

2.70.6.8 Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.

Wenn Sie das Forwarding deaktivieren, überträgt das Gerät auch keine Router-Advertisements über dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

2.70.6.9 MTU

Bestimmen Sie die gültige MTU für dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **MTU**

Mögliche Werte:

max. 4 Ziffern im Bereich von 0 - 9999

Default:

1500

2.70.6.10 Firewall

Hier haben Sie die Möglichkeit die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, wählen Sie **IPv6-Firewall/QoS aktiviert** im Menü **Firewall/QoS** > **Allgemein**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Firewall**

Mögliche Werte:

ja

nein

Default:

nein

2.70.6.11 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

2.70.6.12 DaD-Versuche

Bevor das Gerät eine IPv6-Adresse auf einem Interface verwendet, prüft es per 'Duplicate Address Detection (DAD)', ob diese IPv6-Adresse bereits im lokalen Netzwerk vorhanden ist. Auf diese Art vermeidet das Gerät Adresskonflikte im Netzwerk.

Diese Option gibt die Anzahl der Versuche an, mit denen das Gerät doppelte IPv6-Adressen im Netzwerk sucht.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **DaD-Versuche**

Mögliche Werte:

0 bis 9

Default:

1

2.70.6.13 RS-Anzahl

Konfiguriert die Anzahl der IPv6-Router-Solicitations, die das Gerät nach dem Start des IPv6-LAN-Interfaces versenden soll.

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces**

Mögliche Werte:

max. 1 Zeichen aus `[0-9]`

Default-Wert:

3

2.70.7 WAN-Interfaces

Die Tabelle enthält die Einstellungen für die LAN-Interfaces.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

2.70.7.1 Interface-Name

Bestimmen Sie hier den Namen der WAN-Gegenstelle. Diese Gegenstelle gibt den entsprechenden Namen vor.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

2.70.7.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

2.70.7.3 Autoconf

Aktivieren bzw. deaktivieren Sie die "Stateless Address Autoconfiguration" für dieses Interface.

Falls das Gerät über dieses Interface Router-Advertisements versendet, erzeugt es auch bei aktivierter Autokonfiguration keine Adressen.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Autoconf**

Mögliche Werte:

ja

nein

Default:

ja

2.70.7.4 Akzeptiere-RA

Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten.

Bei deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Akzeptiere-RA**

Mögliche Werte:

ja

nein

Default:

ja

2.70.7.5 Interface-Status

Aktivieren bzw. deaktivieren Sie dieses Interface.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Interface-Status**

Mögliche Werte:

aktiv

inaktiv

Default:

aktiv

2.70.7.6 Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

2.70.7.7 Firewall

Aktiviert die Firewall für dieses Interface.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

2.70.7.8 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

2.70.7.9 DaD-Versuche

Bevor das Gerät eine IPv6-Adresse auf einem Interface verwendet, prüft es per 'Duplicate Address Detection (DAD)', ob diese IPv6-Adresse bereits im lokalen Netzwerk vorhanden ist. Auf diese Art vermeidet das Gerät Adresskonflikte im Netzwerk.

Diese Option gibt die Anzahl der Versuche an, mit denen das Gerät doppelte IPv6-Adressen im Netzwerk sucht.

SNMP-ID:

2.70.7.9

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **DaD-Versuche**

Mögliche Werte:

max. 1 Ziffer

Default:

1

2.70.7.10 PD-Modus

In Mobilfunknetzwerken mit IPv6-Unterstützung ist erst ab 3GPP-Release 10 eine Unterstützung von DHCPv6-Präfix-Delegation vorgesehen. Damit ist es in Mobilfunknetzen vor Release 10 nur möglich, einem Endgerät genau ein /64-Präfix z. B. durch Router-Advertisements zuzuweisen. Bei Smartphones oder Laptops lässt sich mit dieser Methode einfach eine IPv6-Unterstützung realisieren. Router benötigen bei IPv6 aber mindestens ein weiteres Präfix, das sie an Clients ins LAN propagieren können.

Die IPv6-Präfix-Delegation vom WWAN ins LAN macht es möglich, dass Clients das auf der WAN-Mobilfunkseite zugewiesene /64-Präfix im LAN verwenden können. Damit ist ein Betrieb eines Routers in IPv6-Mobilfunknetzwerk ohne DHCPv6-Präfix-Delegation und Neighbor Discovery Proxy (ND-Proxy) möglich. Der Router kündigt das bezogene /64-Präfix per Router-Advertisement im LAN an, statt es auf dem WAN-Interface hinzuzufügen. Clients können dann aus diesem Präfix eine Adresse generieren und diese für die IPv6-Kommunikation benutzen.

Mit dieser Option legen Sie fest, wie der Router die Präfix-Delegation durchführt:

- DHCPv6: Die Präfix-Delegation erfolgt über DHCPv6
- Router-Advertisement: Die Präfix-Delegation erfolgt über Router-Advertisement, der DHCPv6-Client startet dabei nicht.

SNMP-ID:

2.70.7.10

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

Mögliche Werte:

DHCPv6

Router-Advertisement

Default:

DHCPv6

2.70.7.11 RS-Anzahl

Konfiguriert die Anzahl der IPv6-Router-Solicitations, die das Gerät nach dem Start des IPv6-WAN-Interfaces versenden soll.

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

Mögliche Werte:

max. 1 Zeichen aus `[0-9]`

Default-Wert:

3

2.70.10 Aktiv

Schaltet den IPv6-Stack global ein oder aus. Bei deaktiviertem IPv6-Stack führt das Gerät keine IPv6-bezogenen Funktionen aus.

Pfad Telnet:

Setup > **IPv6** > **Aktiv**

Mögliche Werte:

ja

nein

Default:

nein

2.70.11 Forwarding

Ist das Forwarding ausgeschaltet, übermittelt das Gerät keine Datenpakete zwischen IPv6-Interfaces.

Wenn Sie das Gerät als Router verwenden möchten, dann ist Forwarding zwingend erforderlich.

Pfad Telnet:

Setup > **IPv6** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

2.70.12 Router

Mit dieser Einstellung verwalten Sie die Router-Einstellungen.

Pfad Telnet:

Setup > **IPv6** > **Router**

2.70.12.1 Routing-Tabelle

Die Tabelle enthält die Einträge für das Routing von Paketen mit IPv6-Adresse.

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle**

2.70.12.1.1 Praefix

Tragen Sie hier als Präfix den Netzbereich ein, dessen Daten die aktuelle Gegenstelle erhalten soll, z. B. 2001:db8::/32

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Praefix**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

2.70.12.1.2 Routing-Tag

Geben Sie hier das Routing-Tag für diese Route an. Die so markierte Route ist nur aktiv für Pakete mit dem gleichen Tag. Die Datenpakete erhalten das Routing-Tag entweder über die Firewall oder anhand der verwendeten LAN- oder WAN-Schnittstelle.

Die Verwendung von Routing-Tags ist ausschließlich im Zusammenhang mit Routing-Tags in Firewall-Regeln oder Schnittstellen-Definitionen erforderlich.

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Routing-Tag**

Mögliche Werte:

max. 5 Zeichen

Default:

leer

2.70.12.1.3 Peer-oder-IPv6

Wählen Sie hier die Gegenstelle für diese Route aus. Geben Sie dazu eine der folgenden Optionen an:

- einen Interface-Namen
- eine IPv6-Adresse (z. B. 2001:db8::1)
- ein um eine Link-lokale Adresse erweitertes Interface (z. B. fe80::1%INTERNET)

Das Gerät speichert die Gegenstellen für das IPv6-Routing als (*WAN-Schnittstellen*).

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Peer-oder-IPv6**

Mögliche Werte:

max. 56 Zeichen

Default:

leer

2.70.12.1.4 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

2.70.12.2 Dest.-Cache-Timeout

Der 'Destination Cache Timeout' gibt an, wie lange das Gerät sich den Pfad zu einer Zieladresse merkt, wenn keine Pakete zu dieser Adresse gesendet werden.

Außerdem beeinflusst dieser Wert die Dauer, bis das Gerät Änderungen an den Einstellungen der Firewall übernimmt: Zustandsänderungen übernimmt es nach spätestens der Hälfte des 'Destination Cache Timeouts', im Schnitt bereits nach einem Viertel der Timeout-Zeit. Bei der Defaulteinstellung von 30 Sekunden wirken sich also Änderungen an der Firewall im Durchschnitt nach 7,5 Sekunden aus, spätestens aber nach 15 Sekunden.

Pfad Telnet:

Setup > **IPv6** > **Router** > **Dest.-Cache-Timeout**

Mögliche Werte:

max. 3 Zeichen

Default:

30 Sekunden

2.70.13 ICMPv6

Diese Tabelle beinhaltet die Einstellungen für ICMPv6.

Pfad Telnet:

Setup > **IPv6**

2.70.13.1 Interface-Name

Vergeben Sie den Namen des Interfaces, für das Sie ICMPv6 konfigurieren wollen. Dies können LAN-Interfaces oder WAN-Interfaces (Gegenstellen) sein, z. B. "INTRANET" oder "INTERNET".

Pfad Telnet:

Setup > **IPv6** > **ICMPv6**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN/WAN-Interfaces, maximal 16 Zeichen

Default:

2.70.13.2 Error-Bandbreite

Über diese Einstellung definieren Sie die Bandbreite (in Kbit/s), die dem ICMPv6-Protokoll für das Versenden von Fehlernachrichten zur Verfügung steht. Verkleinern Sie diesen Wert, um die Netzlast durch ICMPv6-Nachrichten zu reduzieren.

Pfad Telnet:

Setup > **IPv6** > **ICMPv6**

Mögliche Werte:

0 bis 99999

Default:

1000

2.70.13.3 Redirects

Über diese Einstellung aktivieren bzw. deaktivieren Sie ICMP-Redirects. ICMP IPv6 Neighbor-Redirect-Nachrichten ermöglichen dem Gerät, seine Hosts über einen direkteren (d. h. an der Zahl der Hops gemessenen, kürzeren) Weg zu einer Zieladresse zu informieren.

Pfad Telnet:

Setup > **IPv6** > **ICMPv6**

Mögliche Werte:

aktivieren

deaktivieren

Default:

aktivieren

2.70.14 RAS-Interface

In diesem Verzeichnis legen Sie die Einstellungen für die RAS-Zugänge über IPv6 fest.

Pfad Telnet:

Setup > **IPv6**

2.70.14.1 Interface-Name

Definieren Sie hier den Namen der RAS-Schnittstelle, über die die IPv6-Gegenstellen zugreifen.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.70.14.2 Rtg-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netz eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netz empfängt, erhalten intern diesen Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netz gültigen Routen auch ohne explizite Firewall-Regel.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

0

2.70.14.3 Interface-Status

Aktivieren oder deaktivieren Sie hier diese Schnittstelle.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

Aktiv
Inaktiv

Default-Wert:

Aktiv

2.70.14.4 Forwarding

Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.70.14.5 Firewall

Hier haben Sie die Möglichkeit, die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, schalten Sie unter **IPv6** > **Firewall** > **Aktiv** auf **ja**.

Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

ja
nein

Default-Wert:

ja

2.70.14.6 DaD-Versuche

Bevor das Gerät eine IPv6-Adresse auf einem Interface verwendet, prüft es per 'Duplicate Address Detection (DAD)', ob diese IPv6-Adresse bereits im lokalen Netz vorhanden ist. Auf diese Art vermeidet das Gerät Adresskonflikte im Netz.

Diese Option gibt die Anzahl der Versuche an, mit denen das Gerät doppelte IPv6-Adressen im Netz sucht.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

1 Zeichen aus `0123456789`

Default-Wert:

0

2.70.14.7 Gegenstelle

Bestimmen Sie hier eine Gegenstelle oder eine Liste von Gegenstellen für RAS-Einwahl-Benutzer.

Die folgenden Werte sind möglich:

- Eine einzelne Gegenstelle aus den Tabellen unter **Setup** > **WAN** > **PPTP-Gegenstellen** oder **Setup** > **PPPoE-Server** > **Namenliste**.
- Dem Platzhalter "*", der bewirkt, dass diese Schnittstelle für alle PPTP- und PPPoE-Gegenstellen gilt.
- Dem Platzhalter "*" als Suffix oder Präfix von Gegenstellen, z. B. "FIRMA*" oder "*TUNNEL".

Durch den Platzhalter-Mechanismus können Sie sogenannte Template-Schnittstellen realisieren, die für entsprechend angepasste Gegenstellen gültig sind. Der Name der IPv6-RAS-Schnittstelle ist somit an vielen Stellen in der IPv6-Konfiguration verwendbar.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.70.14.8 Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Pfad Telnet:

Setup > **IPv6** > **RAS-Interface**

Mögliche Werte:

16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.71 IEEE802.11u

Über die Tabellen und Parameter in diesem Menü nehmen Sie sämtliche Einstellungen für Verbindungen nach IEEE 802.11u und Hotspot 2.0 vor.

Pfad Telnet:

Setup

2.71.1 ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für IEEE802.11u bzw. ANQP. IEEE802.11u-Profile bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **IEEE802.11u-Profil** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.1.1 Name

Vergeben Sie hierüber einen Namen für das ANQP-Profil. Diesen Namen geben Sie später in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **ANQP-Profil** an.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.1.2 Include-in-Beacon-OUI

Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Additional-OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.1.3 Additional-OUI

Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

OI, max. 65 Zeichen. Mehrere OIs trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.1.4 Domain-List

Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B.
`providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hostpot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

String, max. 65 Zeichen. Mehrere Domains trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.1.5 NAI-Realm-List

Geben Sie in diesem Feld ein gültiges NAI-Realm-Profil an.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **NAI-Realms**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.1.6 Cellular-List

Geben Sie in diesem Feld ein gültiges Mobilfunknetzwerk-Profil an.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Cellular-Network-Information-List**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.1.7 Network-Auth-Type-List

Geben Sie in diesem Feld ein oder mehrere gültiges Authentifizierungs-Parameter an.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Network-Authentication-Type**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.3 Venue-Name

In diese Tabelle geben Sie allgemeine Informationen zum Standort des Access Points ein.

Mit Angaben zu den Standort-Informationen unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.3.1 Name

Über diesen Paramter geben Sie einen Namen für den Listeneintrag in der Tabelle.

Auf einem standalone Access Point überschreibt LCOS individuelle Namen stets mit der Bezeichnung VENUE, da es für einen einzelnen Access Point auch nur einen Standort geben kann.

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

VENUE

Default:

leer

2.71.3.2 Venue-Name

Tragen Sie für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein.

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

String, max. 65 Zeichen

Default:

leer

2.71.3.3 Language

Wählen Sie hier die Sprache aus, in der Sie die Informationen zum Standort hinterlegen.

Pfad Telnet:

Setup > **IEEE802.11u** > **Venue-Name**

Mögliche Werte:

Keine

Englisch

Deutsch

Chinesisch

Spanisch

Franzoesisch

Italienisch

Russisch

Niederlaendisch

Tuerkisch

Portugiesisch

Polnisch

Tschechisch

Arabisch

Default:

Keine

2.71.4 Cellular-Network-Information-List

Über diese Tabelle verwalten Sie die Profillisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **ANQP-Profile** einem ANQP-Profil zu.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.4.1 Name

Vergeben Sie hierüber einen Namen für das Mobilfunknetz-Profil, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Diesen Namen geben Sie später in der Tabelle **Setup** > **IEEE802.11u** > **ANQP-Profile** unter **Cellular-List** an.

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.4.2 Country-Code

Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. `262` für Deutschland.

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MCC, max. 3 Zeichen

Default:

2.71.4.3 Network-Code

Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Pfad Telnet:

Setup > **IEEE802.11u** > **Cellular-Network-Information-List**

Mögliche Werte:

Gültigen MNC, max. 32 Zeichen

Default:

2.71.5 Network-Authentication-Type

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.5.1 Network-Auth-Type

Wählen Sie aus der Liste den Kontext, vor dem die Weiterleitung gilt.

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

- `Accept-Terms-Cond`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.
- `Online-Enrollment`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer erst online registrieren muss.
- `Http-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.
- `DNS-Redirection`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.

Default:

Accept-Terms-Cond

2.71.5.2 Redirect-URL

Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

URL, max. 65 Zeichen

Default:

2.71.5.3 Name

Vergeben Sie hierüber einen Namen für den Tabelleneintrag, z. B. `AGB akzeptieren`.

Pfad Telnet:

Setup > **IEEE802.11u** > **Network-Authentication-Type**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.6 ANQP-General

In diesem Menü nehmen die Sie allgemeine Einstellungen zu ANQP vor.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.6.1 Venue-Group

Die Standort-Gruppe (Venue Group) beschreibt das Umfeld, in dem Sie den Access Point einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den Venue Group Code, werden vom 802.11u-Standard vorgegeben.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

- `Unspecified`: Unspezifiziert
- `Assembly`: Versammlung
- `Business`: Geschäft
- `Educational`: Ausbildung
- `Factory-and-Industrial`: Fabrik und Industrie
- `Institutional`: Institutional
- `Mercantile`: Handel
- `Resindential`: Wohnheim

- `Storage`: Lager
- `Utility-and-Miscellaneous`: Dienste und sonstiges
- `Vehicular`: Fahrzeug
- `Outdoor`: Außen

Default:

Unspecified

2.71.6.2 Venue-Type

Über den Standort-Typ-Code (Venue-Type) haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

Tabelle 17: Übersicht möglicher Werte für Standort-Gruppen und -Typen

Standort-Gruppe	Code = Standort-Typ-Code
Unspezifiziert	
Versammlung	■ 0 = Unspezifizierte Versammlung ■ 1 = Bühne ■ 2 = Stadion ■ 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) ■ 4 = Amphitheater ■ 5 = Vergnügungspark ■ 6 = Andachtsstätte ■ 7 = Kongresszentrum ■ 8 = Bücherei ■ 9 = Museum ■ 10 = Restaurant ■ 11 = Schauspielhaus ■ 12 = Bar ■ 13 = Café ■ 14 = Zoo, Aquarium ■ 15 = Notfallleitstelle
Geschäft	■ 0 = Unspezifiziertes Geschäft ■ 1 = Arztpraxis ■ 2 = Bank ■ 3 = Feuerwache ■ 4 = Polizeiwache ■ 6 = Post ■ 7 = Büro ■ 8 = Forschungseinrichtung ■ 9 = Anwaltskanzlei
Ausbildung	■ 0 = Unspezifizierte Ausbildung ■ 1 = Grundschule ■ 2 = Weiterführende Schule

Standort-Gruppe	Code = Standort-Typ-Code
	■ 3 = Hochschule
Fabrik und Industrie	■ 0 = Unspezifizierte Fabrik und Industrie ■ 1 = Fabrik
Institutional	■ 0 = Unspezifizierte Institution ■ 1 = Krankenhaus ■ 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) ■ 3 = Entzugsklinik ■ 4 = Einrichtungsverbund ■ 5 = Gefängnis
Handel	■ 0 = Unspezifizierter Handel ■ 1 = Ladengeschäft ■ 2 = Lebensmittelmarkt ■ 3 = KFZ-Werkstatt ■ 4 = Einkaufszentrum ■ 5 = Tankstelle
Wohnheim	■ 0 = Unspezifiziertes Wohnheim ■ 1 = Privatwohnsitz ■ 2 = Hotel oder Motel ■ 3 = Studentenwohnheim ■ 4 = Pension
Lager	■ 0 = Unspezifiziertes Lager
Dienste und sonstiges	■ 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	■ 0 = Unspezifiziertes Fahrzeug ■ 1 = Personen- oder Lastkraftwagen ■ 2 = Flugzeug ■ 3 = Bus ■ 4 = Fähre ■ 5 = Schiff oder Boot ■ 6 = Zug ■ 7 = Motorrad
Außen	■ 0 = Unspezifizierter Außenbereich ■ 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) ■ 2 = Stadtpark ■ 3 = Rastplatz ■ 4 = Verkehrsregelung ■ 5 = Bushaltestelle ■ 6 = Kiosk

Default:

0

2.71.6.5 IPv4-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv4 erhält.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

Not-Available
IPv4-Adresstyp ist nicht verfügbar.

Public-Addr-Available
Öffentliche IPv4-Adresse ist verfügbar.

Port-Restr-Addr-Avail
Port-beschränkte IPv4-Adresse ist verfügbar.

Single-Nat-Priv-Addr-Avail
Private, einfach NAT maskierte IPv4-Adresse ist verfügbar.

Double-Nat-Priv-Addr-Avail
Private, doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Single-Nat-Addr-Avail
Port-beschränkte IPv4-Adresse und einfach NAT maskierte IPv4-Adresse ist verfügbar.

Port-Restr-Double-Nat-Addr-Avail
Port-beschränkte IPv4-Adresse und doppelt NAT maskierte IPv4-Adresse ist verfügbar.

Availability-not-known
Die Verfügbarkeit eines IPv4-Adresstyps ist unbekannt.

Default:

Single-Nat-Priv-Addr-Avail

2.71.6.6 IPv6-Addr-Type

Über diesen Eintrag teilen Sie einer IEEE-802.11u-fähigen Station mit, ob diese nach erfolgreicher Authentifizierung am Hotspot des Betreibers eine IP-Adresse vom Typ IPv6 erhält.

Pfad Telnet:

Setup > **IEEE802.11u** > **ANQP-General**

Mögliche Werte:

Not-Available
IPv6-Adresstyp ist nicht verfügbar.

Available
IPv6-Adresstyp ist verfügbar.

Availability-not-known
Die Verfügbarkeit eines IPv6-Adresstyps ist unbekannt.

Default:

Not-Available

2.71.7 Hotspot2.0

In diesem Menü nehmen die Sie allgemeine Einstellungen zu Hotspot 2.0 vor.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.7.1 Operator-List

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.1.1 Name

Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.7.1.2 Operator-Name

Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

String, max. 65 Zeichen

Default:

leer

2.71.7.1.4 Language

Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**

Mögliche Werte:

Keine

Englisch

Deutsch

Chinesisch

Spanisch

Franzoesisch

Italienisch

Russisch

Niederlaendisch

Tuerkisch

Portugiesisch

Polnisch

Tschechisch

Arabisch

Default:

Keine

2.71.7.2 Connection-Capability

Diese Tabelle beinhaltet eine festgelegte Liste der Verbindungsfähigkeiten, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** als kommaseparierte Liste referenzieren. Mögliche Statuswerte für die einzelnen Dienste sind 'closed' (**-C**), 'open' (**-O**) oder 'unknown' (**-U**).

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.2.4 Name

Dieser Eintrag zeigt den Namen der Verbindungsfähigkeit, auf die Sie in der Tabelle **Hotspot2.0-Profile** im Eingabefeld **Connection-Capabilities** als kommaseparierte Liste referenzieren.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Connection-Capability**

2.71.7.4 Link-Status

Über diesen Eintrag geben Sie den Konnektivitäts-Status Ihres Gerätes mit dem Internet an.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

- `Auto`: Das Gerät ermittelt den Statuswert für diesen Parameter automatisch.
- `Link-Up`: Die Verbindung zum Internet ist herstellt.
- `Link-Down`: Die Verbindung zum Internet ist unterbrochen.
- `Link-Test`: Die Verbindung zum Internet befindet sich im Aufbau oder wird geprüft.

Default:

Auto

2.71.7.7 Downlink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Empfangs-Bandbreite (Downlink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

0 bis 4294967295, in KBit/s

Default:

0

2.71.7.8 Uplink-Speed

Über diesen Eintrag geben Sie den Nominalwert der Sende-Bandbreite (Uplink) an, die einem angemeldeten Client an Ihrem Hotspot maximal zur Verfügung steht. Die Bandbreite selbst definieren Sie z. B. über das Public-Spot-Modul.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

Mögliche Werte:

0 bis 4294967295, in kBit/s

Default:

0

2.71.7.9 Hotspot2.0-Profile

Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. Hotspot-2.0-Profile bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **HS20-Profil** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0**

2.71.7.9.1 Name

Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Diesen Namen geben Sie später in der Tabelle **Setup** > **Schnittstellen** > **WLAN** > **IEEE802.11u** unter **HS20-Profil** an.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profile**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.7.9.2 Operator-Name

Geben Sie in diesem Feld ein gültiges Profil für den Hotspot-Betreiber an.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Operator-List**, max. 65 Zeichen

Default:

2.71.7.9.3 Connection-Capabilities

Geben Sie in diesem Feld einen oder mehrere gültige Einträge aus zu den Verbindungs-Fähigkeiten an. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status "unbekannt" tragen.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profile**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Hotspot2.0** > **Connection-Capability**, max. 252 Zeichen.
Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.71.7.9.4 Operating-Class

Geben Sie hier den Code für die globale Betriebsklasse des Access Points an. Über die Betriebsklasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen Ihr Access-Point verfügbar ist. Beispiel:

- `81`: Betrieb bei 2,4 GHz mit Kanälen 1–13
- `116`: Betrieb bei 40 MHz mit Kanälen 36 und 44

Die für Ihr Gerät passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Pfad Telnet:

Setup > **IEEE802.11u** > **Hotspot2.0** > **Hotspot2.0-Profile**

Mögliche Werte:

Betriebsklassen-Code, max. 32 Zeichen

Default:

2.71.8 Auth-Parameter

Diese Tabelle beinhaltet eine festgelegte Liste der möglichen Authentifizierungsparameter für die NAI-Realms, auf die Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** als kommaseparierte Liste referenzieren.

Tabelle 18: Übersicht der möglichen Authentifizierungs-Parameter

Parameter	Sub-Parameter	Erläuterung
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im RFC 1994
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im RFC 2433
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im RFC 2759
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort
	None	Keine Zugangsdaten erforderlich
TunnelEAPCredentials.*		
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

*) Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.8.1 Name

Dieser Eintrag zeigt den Namen des Authentifizierungsparameters, auf den Sie in der Tabelle **NAI-Realms** im Eingabefeld **Auth-Parameter** als kommaseparierte Liste referenzieren.

Pfad Telnet:

Setup > **IEEE802.11u** > **Auth-Parameter**

2.71.9 NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.

Im Setup-Menü weisen Sie diese Liste über die Tabelle **ANQP-Profile** einem ANQP-Profil zu.

Pfad Telnet:

Setup > **IEEE802.11u**

2.71.9.1 Name

Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Diesen Namen geben Sie später in der Tabelle **Setup** > **IEEE802.11u** > **ANQP-Profile** unter **NAI-Realm-List** an.

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.9.2 NAI-Realm

Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in IETF RFC 2486 definiert und entspricht im einfachsten Fall `<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

String, max. 32 Zeichen

Default:

2.71.9.3 EAP-Method

Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

- `Kein`: Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.
- `EAP-TLS`: Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installieren muss.

- `EAP-SIM`: Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.
- `EAP-TTLS`: Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.
- `EAP-AKA`: Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.

Default:

Kein

2.71.9.4 Auth-Parameter

Geben Sie in das Feld die zur EAP-Methode passenden Authentifizierungs-Parameter durch eine kommaseparierte Liste ein, z. B. für EAP-TTLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` oder für EAP-TLS `Credentials.Certificate`.

Pfad Telnet:

Setup > **IEEE802.11u** > **NAI-Realms**

Mögliche Werte:

Name aus Tabelle **Setup** > **IEEE802.11u** > **Auth-Parameter**, max. 65 Zeichen. Mehrere Namen trennen Sie durch eine kommaseparierte Liste.

Default:

2.82 Crypto

Pfad Telnet:

Setup

2.82.1 Rng

Pfad Telnet:

Setup > **Crypto**

2.82.1.1 seed

Pfad Telnet:

Setup > **Crypto** > **Rng**

Mögliche Argumente:

Wert nicht aenderbar

2.82.1.2 reseed

Pfad Telnet:

Setup > **Crypto** > **Rng**

Mögliche Argumente:

Wert nicht aenderbar

2.82.1.3 reset

Pfad Telnet:

Setup > **Crypto** > **Rng**

Mögliche Argumente:

Wert nicht aenderbar

2.82.1.4 write-interval

Pfad Telnet:

Setup > **Crypto** > **Rng**

Mögliche Werte:

0 … 4294967295

Default-Wert:

8000

2.83 SMS

Dieses Menü enthält die Einstellungsmöglichkeiten für das SMS-Modul, welches den Versand und Empfang von Kurznachrichten (SMS) übernimmt.

Pfad Telnet:

Setup

2.83.1 SMSC-Adresse

Über diesen Parameter konfigurieren Sie eine abweichende Rufnummer für das "Short Message Service Center" (SMSC).

Standardmäßig verwendet das Gerät die in Ihrer USIM-Karte hinterlegte Rufnummer, welche Sie über den Statuswert **SMSC-Nummer** (SNMP-ID 1.83.5) abrufen. Durch Angabe einer abweichenden Rufnummer lässt sich die SMS jedoch gezielt an ein bestimmtes SMSC senden.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

Gültige SMSC-Rufnummer, max. 31 Zeichen

Default:

2.83.2 Eingangs-Groesse

Über diesen Parameter setzen Sie die maximale Anzahl an Kurznachrichten, die das Gerät im Nachrichteneingang aufbewahrt. Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 bis 999999

Besondere Werte:

0: Dieser Wert deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

Default:

100

2.83.3 Ausgangs-Groesse

Über diesen Parameter setzen Sie die maximale Anzahl an Kurznachrichten, die das Gerät im Nachrichtenausgang aufbewahrt. Beim Überschreiten der eingestellten Anzahl wird die älteste Nachricht gelöscht. In diesem Fall erfolgt **kein** SYSLOG-Eintrag.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 bis 999999

Besondere Werte:

0: Dieser Wert deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang aufbewahrt.

Default:

100

2.83.4 Ausgangs-Aufbewahrung

Über diesen Parameter konfigurieren Sie, wie das Gerät mit versendeten Kurznachrichten umgeht.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

- **Keine**: Versendete Kurznachrichten werden nicht gespeichert.
- **Alle**: Versendete Kurznachrichten werden dauerhaft gespeichert.

Default:

Alle

2.83.5 Mail-Weiterleitungs-Addr.

Über diesen Parameter richten Sie eine optionale E-Mail-Adresse ein, an die das Gerät eingehende Kurznachrichten weiterleitet.

Damit die E-Mail-Weiterleitung funktioniert, muss ein gültiges SMTP-Konto im Gerät konfiguriert sein.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

Gültige E-Mail-Adresse, max. 31 Zeichen

Default:

2.83.6 SMS-Weiterleitungs-Addr.

Über diesen Parameter haben Sie die Möglichkeit, eine optionale SMS-Rufnummer einzurichten, an die das Gerät eingehende Kurznachrichten weiterleitet.

Bitte beachten Sie, dass für den Versand von SMS-Nachrichten zusätzliche Kosten durch aufgebaute Verbindungen entstehen können.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

Gültige Rufnummer, max. 63 Zeichen

Default:

2.83.7 SMS-Weiterleitungs-Limit

Über diesen Parameter begrenzen Sie die Anzahl an weitergeleiteten SMS. Wird dieses Limit erreicht, versendet das Gerät noch eine zusätzliche SMS gesendet, welche die betreffende Rufnummer über das Erreichen des Limits informiert.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 bis 999999

Besondere Werte:

0: Dieser Wert deaktiviert das Limit, d. h. Nachrichten werden im unbegrenzten Umfang weitergeleitet.

Default:

20

2.83.8 Syslog

Über diesen Parameter legen Sie fest, ob und wie das Gerät eingehende Kurznachrichten im SYSLOG protokolliert.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

- **Nein**: Im SYSLOG erfolgt für eingehende Kurznachrichten kein Eintrag.
- **Absender**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer im SYSLOG erfasst.
- **Vollstaendig**: Der Eingang einer Kurznachricht wird zusammen mit der Absender-Rufnummer und dem vollständigen Nachrichtentext im SYSLOG erfasst.

Default:

Nein

2.83.9 Maximale-Sende-Versuche

Geben Sie an, wie viele Versuche das Gerät durchführt, um eine SMS zu versenden. Bei Erreichen der Sendeversuche verbleibt die Nachricht im Nachrichtenausgang und das Gerät generiert im Syslog eine entsprechende Fehlermeldung.

Pfad Telnet:

Setup > **SMS**

Mögliche Werte:

0 … 4294967295

Default-Wert:

2

Besondere Werte:

0

Unlimitierte Sendeversuche

2.200 Sip-Alg

Konfigurieren Sie hier die Einstellungen für den Sip-Alg.

Pfad Telnet:

Setup

2.200.1 Operating

Diese Einstellung legt fest, ob der Sip-Alg aktiviert ist.

Pfad Telnet:

Setup > **Sip-Alg**

Mögliche Werte:

ja
nein

Default-Wert:

nein

2.200.2 Firewall-ueberstimmen

Über diesen Parameter legen Sie fest, ob die Firewall für SIP-Pakete Reject-Regeln beachtet oder ob die Pakete in jedem Fall vom SIP-ALG weitergeleitet werden.

Pfad Telnet:

Setup > **Sip-Alg**

Mögliche Werte:

nein
Die Firewall beachtet für SIP-Pakete Reject-Regeln.

ja
Die Firewall beachtet für SIP-Pakete keine Reject-Regeln. Datenpakete werden in jedem Fall vom SIP-ALG weitergeleitet.

Default-Wert:

ja

3 Firmware

In diesem Menü finden Sie die Aktionen und Einstellmöglichkeiten zur Verwaltung der Geräte-Firmware.

Pfad Telnet: /Firmware

3.1 Versions-Tabelle

In dieser Tabelle finden Sie die Informationen über die Firmware-Version und Seriennummer des Gerätes.

Pfad Telnet: /Firmware/Versions-Tabelle

3.1.1 Ifc

Das Interface, auf das sich dieser Eintrag bezieht.

Pfad Telnet: /Firmware/Versions-Tabelle/Ifc

3.1.2 Modul

Vollständige Bezeichnung des Gerätetyps.

Pfad Telnet: /Firmware/Versions-Tabelle/Modul

3.1.3 Version

Aktuell im Gerät aktive Firmware-Version mit Angabe des Release-Datums.

Pfad Telnet: /Firmware/Versions-Tabelle/Version

3.1.4 Seriennummer

Seriennummer des Gerätes.

Pfad Telnet: /Firmware/Versions-Tabelle/Seriennummer

3.2 Tabelle-Firmsafe

In dieser Tabelle finden Sie für jede der beiden im Gerät gespeicherten Firmware-Versionen die Angaben über die Position im Speicherbereich (1 oder 2), die Angabe des Zustandes (aktiv oder inaktiv), die Versionsnummer, das Datum, die Größe und den Index (fortlaufende Nummer).

Pfad Telnet: /Firmware/Tabelle-Firmsafe

3.2.1 Position

Position im Speicherbereich für den aktuellen Eintrag.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Position

3.2.2 Status

Status des aktuellen Eintrags.

Mögliche Werte:

- Inaktiv: Diese Firmware befindet sich im Wartezustand und kann aktiviert werden.
- Aktiv: Diese Firmware wird derzeit vom Gerät verwendet.
- Lader: Bei diesem Eintrag handelt es sich nicht um eine Firmware, sonder um einen Lader mit unterstützenden Funktionen.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Status

3.2.3 Version

Versionsbezeichnung der Firmware für den aktuellen Eintrag.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Version

3.2.4 Datum

Release-Datum der Firmware für den aktuellen Eintrag.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Datum

3.2.5 Groesse

Größe der Firmware für den aktuellen Eintrag.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Groesse

3.2.6 Index

Index für den aktuellen Eintrag.

Pfad Telnet: /Firmware/Tabelle-Firmsafe/Index

3.3 Modus-Firmsafe

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Mit dem Firmwafe-Modus können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll.

Mögliche Werte:

- Unmittelbar: Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:

  Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.

  Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit neu.

- Login: Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.

  Im Unterschied zur ersten Variante wartet das Gerät anschließend für den eingestellten Firmsafe-Timeout auf einen erfolgreichen Login über Telnet, ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

Wenn das Gerät nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, aktiviert es automatisch wieder die bisherige Firmware und startet damit neu.

- Manuell: Bei der dritten Möglichkeit können Sie ebenfalls selbst eine Zeit bestimmen, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, dass die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird. Unter LANconfig aktivieren Sie die neue Firmware mit Gerät > Firmware-Verwaltung > Im Test laufende Firmware freischalten, unter Telnet unter 'Firmware/Firmsafe-Tabelle' mit dem Befehl 'set # active' (dabei ist # die Position der Firmware in der Firmsafe-Tabelle). Unter WEBconfig finden Sie die Firmsafe-Tabelle unter Expertenkonfiguration Firmware.

Default:

- unmittelbar

Das Laden einer zweiten Firmware ist nur dann möglich, wenn das Gerät über ausreichenden Speicherplatz für zwei vollständige Firmwareversionen verfügt. Aktuelle Firmwareversionen (ggf. mit zusätzlichen Software-Optionen) können bei älteren Hardwaremodellen manchmal mehr als die Hälfte des verfügbaren Speicherplatzes benötigen. In diesem Fall wird das asymmetrische Firmsafe verwendet.

Pfad Telnet: /Firmware/Modus-Firmsafe

3.4 Timeout-Firmsafe

Die Zeit in Sekunden für den Test einer neuen Firmware.

Mögliche Werte:

- 0 bis 99999 Sekunden.

Default:

- 300 Sekunden

Pfad Telnet: /Firmware/Timeout-Firmsafe

3.5 Secure Upload

Das Gerät überprüft beim Upload einer Firmware anhand einer Signatur im Header der UPX-Datei die Integrität (Secure Upload).

In diesem Verzeichnis konfigurieren Sie den Secure Upload.

Pfad Telnet:

Firmware

3.5.3 Longtermkey-Loeschen

Pfad Telnet:

Firmware > **Secure-Upload**

3.7 Feature-Word

Anzeige der Feature-Bits, die Aufschluß gibt über die im Gerät freigeschalteten Optionen.

Pfad Telnet: /Firmware/Feature-Word

4 Sonstiges

In diesem Menü finden Sie zusätzliche Funktionen aus dem LCOS-Menübaum.

Pfad Telnet: /Sonstiges

4.1 Manuelle-Wahl

In diesem Menü finden Sie die Aktionen für den manuellen Verbindungsaufbau.

Pfad Telnet: /Sonstiges/Manuelle-Wahl

4.1.1 Aufbau

Mit dieser Aktion können Sie manuell den Verbindungsaufbau zu einer Gegenstelle starten.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

Pfad Telnet: /Sonstiges/Manuelle-Wahl/Aufbau

4.1.2 Abbau

Mit dieser Aktion können Sie manuell die Verbindung zu einer Gegenstelle beenden.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

Pfad Telnet: /Sonstiges/Manuelle-Wahl/Abbau

4.1.4 Testruf

Mit dieser Aktion können Sie manuell den Verbindungsaufbau zu einer Gegenstelle testen.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gegenstelle an.

Pfad Telnet: /Sonstiges/Manuelle-Wahl/Testruf

4.2 System-Boot

Über diese Aktion bewirken Sie den manuellen Neustart des Gerätes.

Pfad Telnet:

Sonstiges

Mögliche Argumente:

keine

4.5 Kaltstart

Mit dieser Aktion können Sie das Gerät neu booten.

Pfad Telnet: /Sonstiges/Kaltstart

4.6 Voice-Call-Manager

In diesem Menü finden Sie die Aktionen für den Voice-Call-Manager.

Pfad Telnet: /Sonstiges/Voice-Call-Manager

4.6.1 Line

In diesem Menü finden Sie die Aktionen für die Leitungen des Voice-Call-Managers.

Pfad Telnet: /Sonstiges/Voice-Call-Manager/Line

4.6.1.1 Unregister

Mit dieser Aktion können Sie gezielt eine Leitung des Voice-Call-Managers de-registrieren.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Leitung an.

Pfad Telnet: /Sonstiges/Voice-Call-Manager/Line/Unregister

4.6.1.2 Register

Mit dieser Aktion können Sie gezielt eine Leitung des Voice-Call-Managers registrieren.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Leitung an.

Pfad Telnet: /Sonstiges/Voice-Call-Manager/Line/Register

4.6.2 Groups

In diesem Menü finden Sie die Aktionen für die Gruppen des Voice-Call-Managers.

Pfad Telnet: /Sonstiges/Voice-Call-Manager/Groups

4.6.2.1 show

Mit dieser Aktion können Sie gezielt eine Gruppe des Voice-Call-Managers anzeigen.

Geben Sie als Parameter der Aktion den Namen der entsprechenden Gruppe an.

Pfad Telnet: /Sonstiges/Voice-Call-Manager/Groups/show

4.7 Flash-Restore

Befindet sich das Gerät im Testmodus, können Sie die Konfiguration aus dem Flash wieder herstellen. Nutzen Sie dazu auf der Kommandozeilenebene den Befehl `do/Other/Flash-Restore`. Dieser Befehl stellt die ursprüngliche Konfiguration aus dem Flash vor der Ausführung des Kommandos "Flash No" wieder her.

Pfad Telnet:

Sonstiges > **Flash-Restore**