Addendum LCOS 8.80 RC1

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 8.80 RC1

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 8.80 gegenüber der vorherigen Version.

2 Konfiguration

2.1 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.

3 LCOS

3.1 Datei-Übertragung über SCP

SCP (Secure Copy) ist ein Protokoll zur sicheren Übertragung von Daten zwischen zwei Rechnern in einem Netzwerk. Administratoren nutzen SCP häufig beim Datenaustausch zwischen Servern bzw. zwischen Server und Arbeitplatzrechner. Mit einem geeigneten Tool (z.B. mit dem Putty-Zusatzprogramm pscp.exe unter Windows-Betriebssystemen) können Sie auch Daten zwischen ihrem PC/Notebook und einem LANCOM-Gerät über das SCP-Protokoll austauschen.

Laden Sie pscp.exe vond er Putty-Downloadseite, um die Dateiübertragung auf einem Windows-Betriebssystem auszuführen.

Öffnen Sie dann ein Kommandozeilen-Fenster mit dem Kommando `cmd`.

Wechseln Sie in das Verzeichnis, in dem Sie die Datei pscp.exe abgelegt haben und führen Sie folgenden Befehl aus, um einen Datei von Ihrem Windows-Rechner auf das Gerät zu übertragen. Geben Sie dabei die Optionen `-scp` und `-pw` gefolgt von Ihrem Kennwort ein:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw ******* c:\path\myfile.ext
 <Benutzer>@<IP-Adresse>:target
```

Wechseln Sie die Reihenfolge von Quelle und Ziel, um die Datei vom Gerät auf Ihren Rechner zu übertragen:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw *******
<Benutzer>@<IP-Adresse>:target c:\path\myfile.ext
```

Geben Sie z.B. den folgenden Befehl ein, um die Konfiguration aus dem Gerät auf Ihren Rechner unter dem Namen `config.lcs` zu speichern:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw *******
root@123.123.123.123:config c:\config.lcs
```

Geben Sie z.B. den folgenden Befehl ein, um eine neue Firmware von Ihren Rechner in das Gerät zu laden:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw *******  c:\firmware.upx
 root@123.123.123.123:firmware
```

Die folgende Tabelle zeigt, welche Dateien Sie konkret über SCP aus dem Gerät auslesen und welche Sie in das Gerät schreiben können:

Tabelle 1: Dateien für SCP-Dateiübertragung

Target	Lesen	Schreiben
ssl_cert	Ja	Ja
ssl_privkey		Ja
ssl_rootcert	Ja	Ja
ssl_pkcs12		Ja
ssh_rsakey		Ja
ssh_dsakey		Ja
ssh_authkeys		Ja
vpn_rootcert	Ja	Ja
vpn_devcert	Ja	Ja

Target	Lesen	Schreiben
vpn_devprivkey		Ja
vpn_pkcs12		Ja
vpn_pkcs12_2		Ja
vpn_pkcs12_3		Ja
vpn_pkcs12_4		Ja
vpn_pkcs12_5		Ja
vpn_pkcs12_6		Ja
vpn_pkcs12_7		Ja
vpn_pkcs12_8		Ja
vpn_pkcs12_9		Ja
vpn_add_cas		Ja
eaptls_rootcert	Ja	Ja
eaptls_devcert	Ja	Ja
eaptls_privkey		Ja
eaptls_pkcs12		Ja
radsec_rootcert	Ja	Ja
radsec_devcert	Ja	Ja
radsec_privkey		Ja
radsec_pkcs12		Ja
radiuss_accnt_total	Ja	Ja
scep_cert_list	Ja	Ja
scep_cert_serial	Ja	Ja
scep_ca_backup	Ja	
scep_ra_backup	Ja	
scep_ca_pkcs12		Ja
scep_ra_pkcs12		Ja
pbspot_template_welcome	Ja	Ja
pbspot_template_login	Ja	Ja
pbspot_template_error	Ja	Ja
pbspot_template_start	Ja	Ja
pbspot_template_status	Ja	Ja
pbspot_template_logoff	Ja	Ja
pbspot_template_help	Ja	Ja
pbspot_template_noproxy	Ja	Ja
pbspot_template_voucher	Ja	Ja
pbspot_formhdrimg	Ja	Ja
WLC_Script_1.lcs	Ja	Ja
WLC_Script_2.lcs	Ja	Ja

Target	Lesen	Schreiben
WLC_Script_3.lcs	Ja	Ja
default_pkcs12		Ja
rollout_wizard		Ja
rollout_template		Ja
rollout_logo		Ja
hip_cert_0		Ja
issue	Ja	Ja
config	Ja	Ja
firmware		Ja

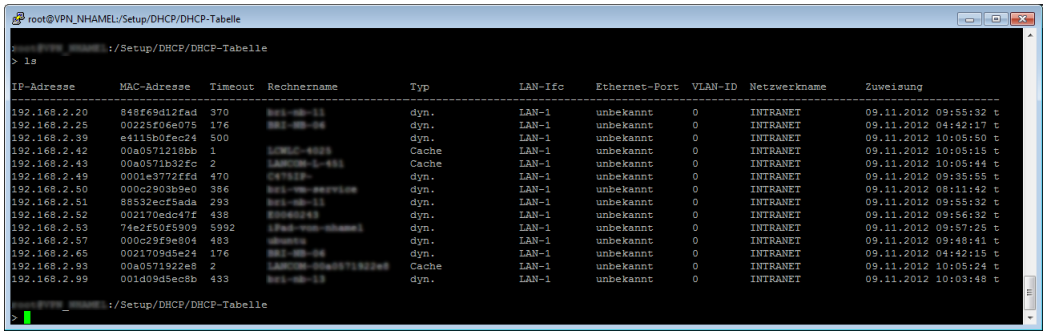
3.2 Anzeige von Statusinformationen des DHCP-Servers

Die Status-Tabelle des DHCP-Servers zeigt folgende Informationen über die Geräte an, denen der DHCP-Server eine IP-Adresse zugewiesen hat:

- IP-Adresse, welche der DHCP-Server dem Netzwerkgerät zugewiesen hat
- MAC-Adresse des Netzwerkgerätes
- Timeout, verbleibende Gültigkeitsdauer in Minuten
- Rechnername
- Typ der Adresszuweisung, dynamisch oder aus dem Cache
- LAN-Ifc, logische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- Ethernet-Port, physikalische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- VLAN-ID des Netzwerks
- Netzwerkname
- Zuweisung, Zeitpunkt zu dem der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat

Sie finden die Statusinformationen des DHCP-Servers an folgenden Stellen:

- Telnet: /Setup/DHCP/DHCP-Tabelle



- Webconfig: /Setup/DHCP/DHCP-Tabelle

LCOS-Menübaum

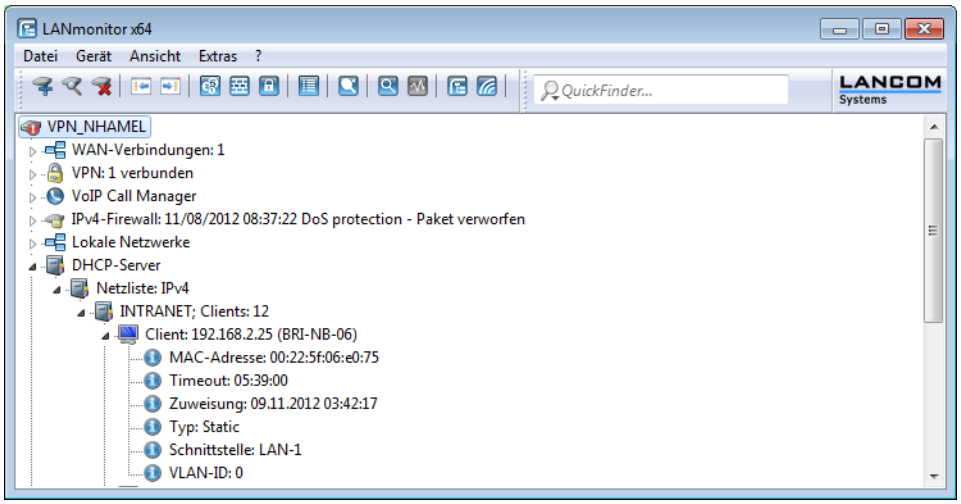
Setup

DHCP

DHCP-Tabelle

IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ	LAN-Ifc	Ethernet-Port	VLAN-ID	Netzwerkname	Zuweisung
192.168.2.25	00225f06e075	346	BRI-NB-06	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:17 tics
192.168.2.39	e4115b0fec24	321		dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:17:13 tics
192.168.2.42	00a0571218bb	2	LCWLC-4025	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:45 tics
192.168.2.43	00a0571b32fc	1	LANCOM-L-451	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:17 tics
192.168.2.49	0001e3772ffd	389	C475IP-	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 05:24:59 tics
192.168.2.50	000c2903b9e0	306	bri-vm-service	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:01:46 tics
192.168.2.51	88532ecf5ada	463	bri-nb-11	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:44:20 tics
192.168.2.52	002170edc47f	358	E0060243	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:53:53 tics
192.168.2.53	74e2f50f5909	5968	iPad-von-nhamel	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:43:35 tics
192.168.2.57	000c29f9e804	431	ubuntu	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:07:08 tics
192.168.2.65	0021709d5e24	346	BRI-NB-06	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:15 tics
192.168.2.93	00a0571922e8	2	LANCOM-00a0571922e8	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:16:00 tics

- LANmonitor: Aufgeteilt nach Netzwerkname unter DHCP-Server > Netzliste



4 LLDP

Das Protokoll LLDP (Link Layer Discovery Protocol) bietet eine einfache und zuverlässige Möglichkeit für den Austausch von Informationen zwischen benachbarten Geräten im Netzwerk und für die Bestimmung der Topologie von Netzwerken. LLDP stellt durch das im Standard IEEE 802.1AB definierte Verfahren Funktionen zur Identifizierung einzelner Geräte und ganzer Netzwerkstrukturen zur Verfügung. Da das Protokoll auf Schicht 2 (Sicherungsschicht) des OSI-Schichtenmodells arbeitet und somit für die physikalische Adressierung von Geräten sorgt, ist seine Funktionalität nicht auf logische Netze wie IP-Netze begrenzt. LLDP deckt prinzipiell alle physikalisch erreichbaren Geräte eines Netzes ab.

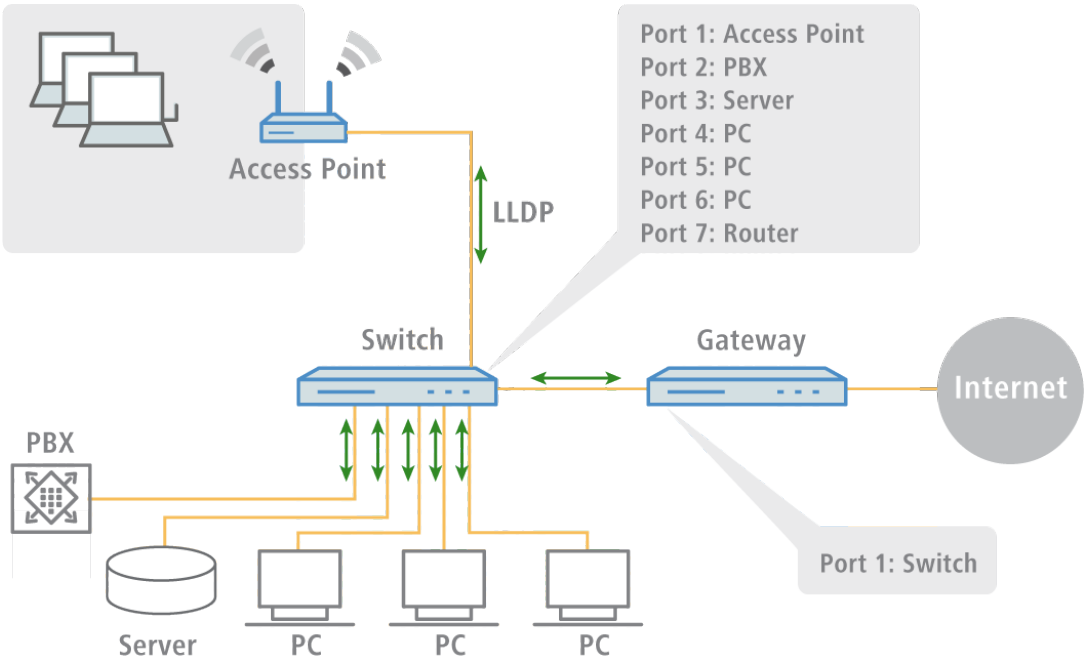
Insbesondere in komplexen Netzen bietet das herstellerunabhängige LLDP-Protokoll große Vorteile:

- Es ermöglicht die automatische Erkennung der in das Netz eingebundenen Komponenten wie Router, Switches und WLAN-Access Points.
- Es vereinfacht die Einbindung unterschiedlichster Geräte, die den LLDP-Standard unterstützen, in ein bestehendes Netzwerk: Durch den Einsatz einer zentralen Netzwerk-Management-Software und automatisch ablaufende Prüf- und Diagnoseprozesse verringert sich der zeitliche Aufwand für Aufbau, Betrieb und Wartung eines Netzes.
- Die von den Geräten versendeten Informationen ergeben in ihrer Gesamtheit einen Überblick über die Topologie (d. h. den Aufbau und die Anordnung) des Netzes. Eine zentrale Management-Software stellt dem Administrator ein virtuelles Abbild des Netzes zur Verfügung, das sich bei Änderungen an der Topologie selbständig aktualisiert.
- Mit Hilfe einer Management-Software kann der Administrator auch komplexe Netze überwachen und auf einfache Weise verwalten. Er kann anhand der Software feststellen, welche Komponenten und Geräte zusammengeschaltet sind und auftretende Störungen problemlos lokalisieren.
- LLDP kann die Kosten für Anschaffung, Aufbau oder Umgestaltung eines Netzes verringern, da die Unternehmen durch diesen offenen Standard nicht mehr an bestimmte Hersteller gebunden sind. Sie können einzelne Netzkomponenten danach auswählen, für welche Anwendung diese jeweils am besten geeignet sind. Diese Möglichkeit war bislang nicht gegeben, wenn ein proprietäres Protokoll zum Einsatz kam.

4.1 Funktionsweise

LLDP funktioniert nach einem einfachen Prinzip: Auf allen Geräten mit LLDP-Unterstützung arbeitet der so genannte LLDP-Agent. Diese Software-Komponente sendet zum einen in regelmäßigen Abständen eigene Informationen an alle Schnittstellen des Gerätes. Dies erfolgt entweder mittels Unicast oder Multicast, wobei Sie die Zieladressen je nach Bedarf

konfigurieren können. Zum anderen empfängt der LLDP-Agent laufend Informationen von benachbarten Geräten. Der Versand und der Empfang der betreffenden Datenpakete erfolgt unabhängig voneinander.



Die versendeten und empfangenen Datenpakete enthalten Informationen wie den Namen und die Beschreibung des Gerätes, die Kennung und Beschreibung von Ports, die IP- oder MAC-Adresse des Gerätes, die spezifischen Fähigkeiten des Gerätes (z. B. in Bezug auf Switching und Routing), VLAN-Kennungen und herstellerspezifische Details. Hierbei definiert LLDP grundlegende Informationen, die ein Datenpaket immer enthalten muss, sowie optionale zusätzliche Informationen.

Die einzelnen Geräte legen die empfangenen Informationen lokal in einer Datenstruktur ab, der so genannten MIB (Management Information Base). Eine MIB enthält somit Daten des eigenen LLDP-Agenten und des erkannten, direkten Nachbar-Agenten.

Der Informationsaustausch sorgt für eine ständige Identifikation der Geräte innerhalb des Netzwerks, da die Geräte ihre Datenpakete im Regelfall zyklisch (d. h. in konfigurierbaren Abständen) versenden. Darüber hinaus informieren sie ihre Netz-Nachbarn aber auch dann, wenn sich Änderungen innerhalb der Geräte oder an deren Netzanbindung ergeben.

Für den eigentlichen Prozess der Geräte-Identifizierung ist ausschlaggebend, dass jeder einzelne Verbindungspunkt in der Topologie als „Media Service Access Point" (MSAP) eindeutig identifiziert ist. Ein MSAP setzt sich aus einer Gerätekennung (Chassis-ID) und einer Portkennung (Port-ID) zusammen. Die eindeutige Ermittlung bzw. Zuordnung von Geräten basiert also darauf, dass jeder MSAP in der beobachteten Netzwerk-Topologie nur einmal vorkommen darf.

Der Administrator kann die von den Geräten gemeldeten Daten dann über eine zentrale Netzwerk-Management-Software auf seinem Rechner abfragen und erfassen, wobei die Abfrage der einzelnen MIBs über das SNMP-Protokoll erfolgt. Die Management-Software dokumentiert somit die gesamte Topologie des Netzes und ermöglicht eine automatische Abbildung dieser Topologie sowie die grafische Darstellung von aktuellen Diagnosedaten.

4.2 Aufbau der LLDP-Nachrichten

Der Austausch der Informationen erfolgt über spezifische Dateneinheiten, die so genannten LLDP Data Units (LLDPDU). Eine solche Dateneinheit besteht aus TLVs (Type-Length-Values), wobei jedes TLV-Feld einem bestimmten Typ entspricht und eine bestimmte Länge hat.

Gemäß LLDP-Standard IEEE 802.1AB müssen am Anfang einer LLDPU drei TLVs in der folgenden Reihenfolge stehen:

- Typ 1 = Chassis-ID
- Typ 2 = Port-ID
- Typ 3 = Time To Live

Im Anschluss an diese verbindlichen TLVs kann eine LLDPDU weitere, optionale TLVs enthalten:

- Typ 4 = Port Description
- Typ 5 = System Name
- Typ 6 = System Description
- Typ 7 = System Capabilities
- Typ 8 = Management Address

Am Ende einer LLDPDU muss dann zwingend folgende TLV stehen:

- Typ 0 = End of LLDPDU

Tabellarische Übersicht über die TLVs

TLV	Verwendung	Bezeichnung	Beispiel	Funktion
Typ1	Erforderlich	Chassis-ID	0018.2fa6.b28c	Identifiziert das Gerät
Typ 2	Erforderlich	Port-ID	Fi-0/12	Identifiziert den Port
Typ 3	Erforderlich	Time To Live	60 sec	Signalisiert dem empfangenden Gerät, wie lange die erhaltene Information gültig sein soll
Typ 4	Optional	Port Description	GigabitEthernet0/12	Zeigt Details über den Port wie etwa die Hardware-Version an
Typ 5	Optional	System Name	PN-I/O 3	Zeigt den vom Administrator vergebenen Namen des Gerätes an
Typ 6	Optional	System Description	LCOS Software, Version 8.9.1 SE	Zeigt Details über das Gerät wie etwa die Version der Netzwerk-Software an
Typ 7	Optional	System Capabilities	Router	Zeigt die primäre Funktion sowie die Fähigkeiten des Gerätes an
Typ 8	Optional	Management Address	192.168.0.1	Zeigt die IP- oder MAC-Adresse des Gerätes an
Typ 0	Erforderlich	End of LLDPDU	----------	Signalisiert das Ende der Dateneinheit

4.3 Unterstützte Betriebssysteme

Grundsätzlich funktioniert LLDP auf allen gängigen Systemen, sofern hierfür LLDP-Agenten bzw. eine entsprechende Software zur Auswertung der LLDP-Pakete zur Verfügung stehen. Für Linux gibt es diverse Open-Source-Projekte wie z. B. „LLDPD“, „Open-LLDP“ (mit Bindestrich) oder „ladvd“, die einen LLDP-Agenten bereitstellen.

Das Projekt „OpenLLDP“ zielt auf eine weitere Verbreitung und Akzeptanz des LLDP-Protokolls (IEEE 802.1AB) ab. Die Software unterstützt die Übertragung und den Empfang von LLDP-Nachrichten auf den Plattformen Linux, Mac OS X, FreeBSD und NetBSD. Allerdings scheint die Weiterentwicklung derzeit zu ruhen.

Die Microsoft-Betriebssysteme Vista und Windows 7 enthalten ein proprietäres Protokoll namens LLTD (Link Layer Topology Discovery), welches im Wesentlichen die gleiche Funktionalität wie LLDP aufweist. Auf Windows XP lässt sich die LLTD-Komponente über einen Patch nachinstallieren. Allerdings ist die Funktion des Patches gegenüber den

implementierten Varianten in Vista und Windows 7 eingeschränkt, da der „ LLTD Responder" nur IPv4-Adressen meldet, nicht jedoch IPv6-Adressen.

Will man auf Windows-Systemen LLDP installieren, kann man auf eine Shareware namens „haneWIN LLDP Agent" zurückgreifen. Mit dieser funktioniert LLDP auf allen Windows-Systemen ab Windows 2000, d. h. sowohl auf 32-Bit- wie auf 64-Bit-Systemen.

Die am weitesten verbreitete freie Software zur Auswertung und Analyse ist Wireshark. In der Grundversion ist Wireshark gratis und hat sich inzwischen als Standard etabliert. Die Software unterstützt zahlreiche Betriebssysteme und kann eine Vielzahl von Protokollen (u. a. auch LLDP) lesen und auswerten. Der Schwerpunkt der Grundversion von Wireshark liegt allerdings auf der Analyse von auftretenden Problemen innerhalb des Netzes. Benötigt man weitergehende Funktionen (wie z. B. die Visualisierung des Netzverkehrs in Form von farbigen Diagrammen), kann man kostenpflichtige Zusatzmodule erwerben.

4.4 Ergänzungen im Menüsystem

4.4.1 Ergänzungen im Setup-Menü

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.

SNMP-ID:

2.38

Pfad Telnet:

Setup > **LLDP**

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.

SNMP-ID:

2.38.7

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.

Netzwerk-Name

Der Name des TCP/IP-Netzwerks, wie er in der TCP-IP-Netzwerk-Liste steht.

SNMP-ID:

2.38.7.1

Pfad Telnet:

Setup > **LLDP** > **Management-Addressen** > **Netzwerk-Name**

Mögliche Werte:

max. 16 alphanumerische Zeichen

Default:

leer

Port-Liste

Die Liste der Schnittstellen und Ports, die zu der entsprechenden Management-Adresse gehören.

SNMP-ID:

2.38.7.2

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

Ports

Diese Tabelle beinhaltet alle port-abhängigen LLDP-Konfigurations-Optionen. Der Tabellen-Index ist ein String, nämlich der Schnittstellen-/Port-Name.

SNMP-ID:

2.38.6

Pfad Telnet:

Setup > **LLDP** > **Ports**

Name

Der Name des Ports oder der Schnittstelle

SNMP-ID:

2.38.6.1

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Name**

Mögliche Werte:

Abhängig von den Schnittstellen, z. B. LAN-1, WLAN-1

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.

SNMP-ID:

2.38.6.2

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Admin-Status**

Mögliche Werte:

Aus

nur-Tx

nur-Rx

Rx/Tx

Default:

Aus

Benachrichtigungen

Stellen Sie hier ein, ob Änderungen in einer MSAP-Gegenstelle dieses Ports an mögliche Netzwerk-Management-Systeme gemeldet werden.

SNMP-ID:

2.38.6.3

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Benachrichtigungen**

Mögliche Werte:

nein

ja

Default:

nein

Admin-Status

Stellen Sie hier die Menge der optionalen Standard-TLVs ein, die an die PDUs übermittelt werden.

SNMP-ID:

2.38.6.4

Pfad Telnet:

Setup > **LLDP** > **Ports** > **TLVs**

Mögliche Werte:

Port-Beschreibung

System-Name

System-Beschreibung

System-Eigenschaften

keine

Default:

Port-Beschreibung

TLVs-802.3

Stellen Sie hier die Menge der optionalen Standard-TLVs-802.3 ein, die das Gerät an die PDUs übermittelt.

SNMP-ID:

2.38.6.6

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

Max-Nachbarn

Dieser Parameter gibt die maximale Anzahl von LLDP-Nachbarn an.

SNMP-ID:

2.38.6.7

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Max-Nachbarn**

Mögliche Werte:

0 bis 65535

Default:

0

Akt.-Quellen

Dieser Parameter gibt die möglichen Quellen für LLDP-Updates an.

SNMP-ID:

2.38.6.8

Pfad Telnet:

Setup > **LLDP** > **Ports** > **Akt.-Quellen**

Mögliche Werte:

Auto

nur-LLDP

nur andere

beide

Default:

Auto

TLVs-LCS

Diese Einstellungen definieren die Menge der optionalen Standard-TLVs-LCS, die das Gerät über PDUs übermittelt.

SNMP-ID:

2.38.6.9

Pfad Telnet:

Setup > **LLDP** > **Ports** > **TLVs-LCS**

Mögliche Werte:

SSID

Radio-Kanal

PHY-Typ

Keine

Default:

SSID

Protokolle

Diese Tabelle enthält die LLDP-Port-Einstellungen für die Spanning-Tree- und Rapid-Spanning-Tree-Protokolle.

SNMP-ID:

2.38.8

Pfad Telnet:

Setup > **LLDP** > **Protokolle**

Protokoll

Dieser Parameter setzt das Protokoll, für das die LLDP-Ports aktiviert werden sollen.

SNMP-ID:

2.38.8.1

Pfad Telnet:

Setup > **LLDP** > **Protokolle** > **Protokoll**

Mögliche Werte:

Spanning-Tree

Rapid-Spanning-Tree

Default:

Spanning-Tree, Rapid-Spanning-Tree

Port-Liste

Dieser Wert beschreibt die Ports, die LLDP mit dem zugehörigen Protokoll verwenden (Spanning-Tree oder Rapid-Spanning-Tree).

SNMP-ID:

2.38.8.2

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

Benachrichtigungs-Intervall

Dieser Wert legt den Zeitabstand fest, in dem Benachrichtigungen über Änderungen in den Gegenstellen-Tabellen versendet werden. Der Wert definiert die kleinste Zeitperiode zwischen den Benachrichtigungen.

SNMP-ID:

2.38.5

Pfad Telnet:

Setup > **LLDP** > **Benachrichtigungs-Intervall**

Mögliche Werte:

0 bis 9999 Sekunden

Default:

5

In-Betrieb

Dieser Parameter aktiviert oder deaktiviert die Verwendung von LLDP.

SNMP-ID:

2.38.10

Pfad Telnet:

Setup > **LLDP** > **In-Betrieb**

Mögliche Werte:

ja

nein

Default:

nein

Nachrichten-TX-Halte-Faktor

Dieser Wert legt die TTL (time to live) fest, die mit LLDPDUs übertragen wird. Die TTL besteht aus dem Nachrichten-Übertragungs-Intervall und dem Übertragungs-Halte-Faktor.

SNMP-ID:

2.38.2

Pfad Telnet:

Setup > **LLDP** > **Nachrichten-TX-Haltefaktor**

Mögliche Werte:

0 bis 99

Default:

4

Nachrichten-TX-Intervall

Dieser Wert definiert das Interval in Sekunden, in dem das Gerät LLDPDUs überträgt.

SNMP-ID:

2.38.1

Pfad Telnet:

Setup > **LLDP** > **Nachrichten-TX-Intervall**

Mögliche Werte:

0 bis 65535 Sekunden

Default:

30

Reinit-Verzoegerung

Dieser Wert definiert die Zeit, während der das Gerät trotz eingeschaltetem LLDP die Übertragung von LLDPDUs unterdrückt.

SNMP-ID:

2.38.3

Pfad Telnet:

Setup > **LLDP** > **Reinit-Verzoegerung**

Mögliche Werte:

0 bis 99 Sekunden

Default:

2

Sofortiges-Loeschen

Dieser Parameter aktiviert oder deaktiviert das direkte Löschen von LLDPDUs.

SNMP-ID:

2.38.9

Pfad Telnet:

Setup > **LLDP** > **Sofortiges-Loeschen**

Mögliche Werte:

ja

nein

Default:

ja

Tx-Verzoegerung

Offen

SNMP-ID:

2.38.4

Pfad Telnet:

Setup > **LLDP** > **Tx-Verzoegerung**

Mögliche Werte:

0 bis 9999 Sekunden

Default:

2

5 IPv6

5.1 IPv6-Grundlagen

IPv4 (Internet Protocol Version 4) ist ein Protokoll zur eindeutigen Adressierung von Teilnehmern in einem Netzwerk und definierte bislang alle weltweit vergebenen IP-Adressen. Da der so gebotene Adressraum Grenzen hat, tritt das IPv6 (Internet Protocol Version 6) in die Fußstapfen des bisherigen Standards. IPv6 bietet durch einen anderen IP-Adressaufbau ein breiteres Spektrum für IP-Adressen und vergrößert somit die möglich Anzahl an Teilnehmern in Netzwerken weltweit.

5.1.1 Warum IP-Adressen nach dem Standard IPv6?

Folgende Gründe führten zur einer Entwicklung des neuen IPv6-Standards:

- IPv4 deckt einen Adressraum von etwa vier Milliarden IP-Adressen ab, mit denen Teilnehmern in Netzwerken eindeutige Identitäten erhalten. Bei der Implementierung des IPv4-Standards in den 80er-Jahren galt dieser Adressraum als überaus ausreichend. Durch das enorme Wachstum des World Wide Web und der unvorhergesehenen Vielzahl an Rechnern und kommunizierenden Geräten entsteht eine Adressknappheit, die der IPv6-Standard überbrücken soll.
- Der größere Adressraum des IPv6 erschwert das Scannen von IP-Adressen durch Viren und Trojaner. Auf diese Weise bietet das breitere Spektrum einen größeren Schutz vor Angriffen.
- Das IPv6 wurde nach sicherheitstechnischen Anforderungen implementiert. So enthält es das Sicherheitsprotokoll IPSec (IP Security). Dieses sorgt für eine sichere Kommunikation im Netzwerk auf dem 3. Layer, während viele Sicherheitsmechanismen des IPv4 erst auf höheren Ebenen greifen.
- Durch einfachere und feste Bezeichnungen der Datenpakete sparen Router Rechenleistung und beschleunigen somit ihren Datendurchsatz.
- IPv6 ermöglicht eine einfachere und schnellere Übertragung von Daten in Echtzeit und eignet sich somit für Multi-Media-Anwendungen wie Internet-Telefonie oder Internet-TV.
- So genannte mobile IPs ermöglichen es, sich mit einer festen IP-Adresse in verschiedenen Netzwerken anzumelden. So kann man sich mit seinem Laptop im Heimnetzwerk, im Café oder am Arbeitsplatz mit derselben IP-Adresse anmelden.

5.1.2 Aufbau einer IP-Adresse nach IPv6-Standard

Die neuen IPv6-Adressen sind 128 Bit lang und decken somit einen Adressbereich von rund 340 Sextillionen möglichen Netzwerkteilnehmern ab. Sie bestehen aus 8 Blöcken zu je 16 Bit und werden als hexadezimale Zahl notiert. Das folgende Beispiel zeigt eine mögliche IPv6-Adresse:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

Um die Lesbarkeit solcher IP-Adressen zu verbessern, entfallen Nullen, die am Anfang eines Ziffernblocks stehen. Darüber hinaus kann eine einzige Gruppe von Blöcken entfallen, die komplett aus Nullen bestehen. Für das oben gezeigte Beispiel wäre eine möglich Darstellungsweise demnach die folgende:

2001:db8::54f3:dd6b:1/64

Eine IPv6-Adresse besteht aus zwei Komponenten: einem Präfix und einem Interface Identifier. Das Präfix bezeichnet die Zugehörigkeit der IP-Adresse zu einem Netzwerk, während der Interface Identifier z. B. im Fall der Autokonfiguration aus einer Link Layer Adresse erzeugt wird und somit zu einer Netzwerkkarte gehört. Das Gerät kann Interface Identifier auch mit Hilfe von Zufallszahlen generieren. Dies erhöht die Sicherheit. Auf diese Weise können mehrere IPv6-Adressen einem Teilnehmer zugeordnet werden.

Das Präfix beschreibt den ersten Teil der IP-Adresse. Die Länge des Präfix steht als Dezimalzahl hinter einem Schrägstrich. Für das hier genannte Beispiel lautet das Präfix:

2001:db8::/64

Der übrige Teil der IP-Adresse stellt den Interface Identifier dar. Dieser lautet für das angebene Beispiel:

::54f3:ddb6:1

Gegenüber den IP-Adressen nach dem Standard IPv4 ergeben sich für den Aufbau der neuen IPv6-Adressen einige Änderungen:

- Während IPv4-Adressen einen Adressraum von 32 Bit abdecken, entsteht durch die neue Länge von 128 Bit ein deutlich größerer Adressbereich von IPv6. IPv6-Adressen sind daher viermal so lang wie eine IPv4-Adresse.
- Eine Schnittstelle kann mehrere IPv6-Adressen haben, bedingt durch die mögliche Zuweisung mehrerer Präfixe zu einem Interface Identifier. Im IPv4-Standard besitzt jede Schnittstelle ausschließlich eine IP-Adresse.
- IPv4-Adressen benötigen einen zentralen Server, der ihnen die IP-Adressen zuteilt. Dies ist üblicherweise ein DHCP-Server. IPv6 hingegen beherrscht eine Autokonfiguration, welche die Verwendung eines DHCP-Server überflüssig macht. Es besteht allerdings immer noch die Option einen DHCP-Server einzusetzen.

5.1.3 Migrationsstufen

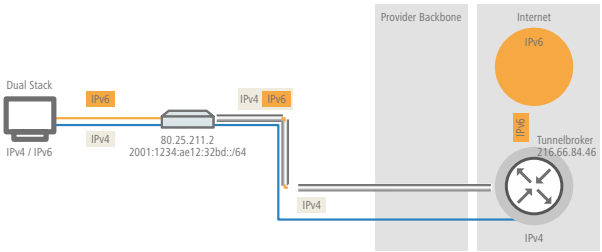
IPv6 ist in Netzwerken auf verschiedene Arten verfügbar. Man unterscheidet bei IPv6-Umgebungen zwischen nativem IPv6 und IPv6, das über einen Tunnel entsteht.

- **Reines (oder natives) IPv6:** Reines IPv6 bezeichnet ein Netzwerk, das nach Außen ebenfalls ausschließlich über IPv6 kommuniziert. Auf dieses können Teilnehmer mit IPv4-Adressen nur zugreifen, wenn sie über ein Gateway kommunizieren, dass zwischen IPv6- und IPv4-Netzwerken vermittelt.
- **IPv6 via Dual Stack:** Dual Stack bezeichnet den parallelen Betrieb von IPv4 und IPv6 in einem Netzwerk. Auf diese Weise vermittelt ein Router zwischen Geräten, die ausschließlich IPv4 oder IPv6 beherrschen. Die Clients wählen dann das entsprechende Protokoll.
- **IPv6 Tunneling:** Wenn ein Router keine Zugriff auf einen IPv6-Internetzugang hat, dann besteht die Möglichkeit mit Hilfe eines Tunnels auf ein IPv6-Netzwerk zuzugreifen.

5.2 IPv6-Tunneltechnologien

5.2.1 6in4-Tunnel

6in4 Tunnel dienen der Verbindung zweier Hosts, Router oder der Verbindung zwischen Host und Router. 6in4 Tunnel können somit zwei IPv6 Netzwerke über ein IPv4 Netzwerk verbinden. Die Abbildung zeigt einen statischen 6in4-Tunnel zwischen dem lokalen Router und einem 6in4-Gateway eines Tunnelbrokers.



Im Gegensatz zu 6to4 handelt es sich hierbei im einen dedizierten, bekannten Dienst und Betreiber. Die Endpunkte sind festgelegt und der Tunnelbroker weist ein statisches Präfix zu. Die Vorteile einer 6in4 Lösung sind also sowohl feste 6in4-Gateways als auch das Wissen um den Betreiber. Das feste Präfix des Tunnelbrokers bestimmt darüber hinaus die Anzahl der möglichen Subnetze, die genutzt werden können. Ein 64 Bit Präfix (z.B. 2001:db8::/64) erlaubt die Nutzung

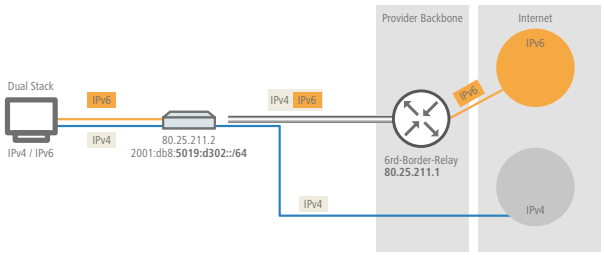
eines Subnetzes. Bei einem 48 Bit Präfix stehen sogar 16 Bit des 64 Bit Präfix-Anteils zur Verfügung. Damit lassen sich bis zu 65536 Subnetze realisieren.

Der Nachteil der 6in4-Technologie ist der höhere Administrationsaufwand. Eine Anmeldung beim gewählten Tunnelbroker ist notwendig. Hinzu kommt die statische Konfiguration der Tunnelendpunkte. Im Falle einer dynamisch bezogenen IPv4-Adresse müssen die Daten regelmäßig aktualisiert werden. Letzteres kann allerdings von einem Router, beispielsweise mit Hilfe eines Skriptes, automatisch erledigt werden.

6in4 stellt eine vergleichsweise sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Technologie ist somit auch zum Betrieb von Webservern geeingnet, die über IPv6 erreicht werden sollen. Der Nachteil ist lediglich der erhöhte adminstrative Aufwand. Diese Technologie ist somit auch für den professionellen Einsatz geeignet.

5.2.2 6rd-Tunnel

6rd (rapid deployment) ist eine Weiterentwicklung von 6to4. Die zugrunde liegende Funktionsweise ist identisch. Der Unterschied besteht darin, dass ein spezifisches Relay genutzt wird, welches der Provider betreibt. Dies löst die zwei grundlegenden Probleme der 6to4- Technologie, die mangelnde Sicherheit und Stabilität. Das Präfix wird bei 6rd etnweder manuell konfiguriert oder über DHCP (IPv4) übermittelt, was den Konfigurationsauswand weiter reduziert. Die Abbildung zeigt eine schematische Darstellung eines 6rd Szenarios.



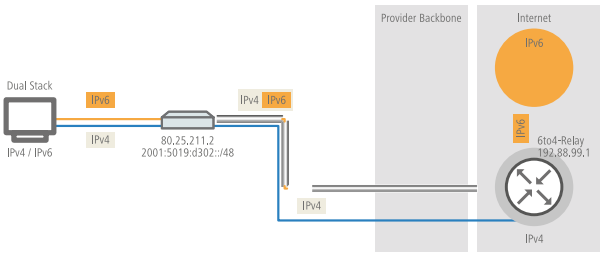
Der Provider weist dem Router ein Präfix (2001:db8::/32) zu, welches vom Router durch die IPv4-Adresse ergänzt wird. Die somit erzeugte IPv6-Adresse hat die Form: 2001:db8:5019:d302::/64. 6rd ist somit aus zwei Perspektiven interessant. Es ermöglicht dem Provider auf einfache Art und Weise seinen Kunden das IPv6 Internet zugänglich zu machen. Zusätzlich vereinfacht es die Nutzung für die Kunden erheblich. Sie müssen weder die Sicherheitsrisiken von 6to4 hinnehmen noch den Konfigurationsaufwand von 6in4 investieren.

5.2.3 6to4-Tunnel

Mit dem 6to4-Tunneling haben Sie die Möglichkeit auf einfache Weise eine Verbindung zwischen zwei IPv6-Netzwerken über ein IPv4-Netzwerk herzustellen. Dazu wird ein so genannter 6to4-Tunnel erstellt:

- Ein Router zwischen lokalen IPv6-Netzwerk und einem IPv4-Netzwerk dient als Vermittler zwischen den Netzwerken.
- Der Router hat sowohl eine öffentliche IPv4-Adresse, als auch eine IPv6-Adresse. Die IPv6-Adresse setzt sich aus einem IPv6-Präfix und der IPv4-Adresse in hexadezimaler Schreibweise zusammen. Hat ein Router z. B. die IPv4-Adresse 80.25.211.2 , so wird diese zunächst in hexadezimale Schreibweise umgerechnet: 5019:d302. Ergänzend dazu kommt ein IPv6-Präfix (z. B. 2002::/16), so dass die IPv6-Adresse für den Router wie folgt aussieht: 2002:5019:d302::/48.
- Schickt ein Gerät aus dem IPv6-Netzwerk Datenpakete über den Router an eine Zieladresse im IPv4-Netzwerk, dann schachtelt der Router die IPv6-Pakete zunächst in ein Paket mit einem IPv4-Header. Das geschachtelte Paket leitet

der Router anschließend an ein 6to4-Relay weiter. Das 6to4-Relay entpackt das Paket und leitet es an das gewünschte Ziel weiter. Die folgende Abbildung zeigt das Funktionsprinzip des 6to4-Tunneling:



6to4-Tunnel stellen eine dynamische Verbindung zwischen IPv6- und IPv4-Netzwerken her: die Antwortpakete werden möglicherweise über ein anderes 6to4-Relay zurückgeleitet, als auf dem Hinweg. Daher handelt es sich beim 6to4-Tunnel nicht um eine Punkt zu Punkt-Verbindung. Der Router sucht für jede neue Verbindung stets das nächstgelegene öffentliche 6to4-Relay. Dies geschieht über die Anycast-Adresse 192.88.99.1. Dieser Aspekt ist zum einen ein Vorteil des 6to4-Tunneling, stellt aber gleichzeitig auch einen Nachteil dar. Öffentliche 6to4-Relays benötigen keine Anmeldung und sind frei zugänglich. Desweiteren benötigt die dynamische Verbindung wenig Konfigurationsaufwand. Auf diese Weise ist es für jeden Nutzer möglich, einfach und schnell einen 6to4-Tunnel über ein öffentliches Relay zu erzeugen.

Andererseits führt die dynamische Verbindung dazu, dass der Nutzer keinen Einfluss auf die Wahl der 6to4-Relays hat. Daher besteht vom Provider des Relays die Möglichkeit, Daten mitzuschneiden oder zu manipulieren.

5.3 DHCPv6

Im Vergleich zu IPv4 benötigen Clients in einem IPv6-Netzwerk wegen der Autokonfiguration keine automatischen Adresszuweisungen über einen entsprechenden DHCP-Server. Da aber bestimmte Informationen wie DNS-Server-Adressen nicht per Autokonfiguration übertragen werden, ist es in bestimmten Anwendungsszenarien sinnvoll, auch bei IPv6 einen DHCP-Dienst im Netzwerk zur Verfügung zu stellen.

5.3.1 DHCPv6-Server

Die Verwendung eines DHCPv6-Servers ist bei IPv6 optional. Grundsätzlich unterstützt ein DHCPv6-Server zwei Betriebsarten:

- **Stateless**: Der DHCPv6-Server verteilt keine Adressen, sondern nur Informationen, z. B. DNS-Server-Adressen. Bei dieser Methode generiert sich ein Client seine IPv6-Adresse durch die 'Stateless Address Autokonfiguration (SLAAC)'. Dieses Verfahren ist besonders attraktiv u. a. für kleine Netzwerke, um den Verwaltungsaufwand möglichst gering zu halten.
- **Stateful**: Der DHCPv6-Server verteilt IPv6-Adressen, ähnlich wie bei IPv4. Dieses Verfahren ist deutlich aufwändiger, da ein DHCPv6-Server die Adressen vergeben und verwalten muss.

Ein DHCPv6-Server verteilt nur die Optionen, die ein IPv6-Client explizit bei ihm anfragt, d. h., der Server vergibt einem Client nur dann eine Adresse, wenn dieser explizit eine Adresse anfordert.

Zusätzlich kann der DHCPv6-Server Präfixe zur weiteren Verteilung an Router weitergeben. Dieses Verfahren wird als 'Präfix-Delegierung' bezeichnet. Ein DHCPv6-Client muss allerdings ebenfalls dieses Präfix explizit angefragt haben.

5.3.2 DHCPv6-Client

Durch die Autokonfiguration in IPv6-Netzwerken gestaltet sich die Konfiguration der angeschlossenen Clients sehr einfach und komfortabel.

Damit ein Client jedoch auch Informationen z. B. über DNS-Server erhalten kann, müssen Sie das Gerät so konfigurieren, dass es bei Bedarf den DHCPv6-Client aktiviert.

Die Einstellungen für den DHCPv6-Client sorgen dafür, dass das Gerät beim Empfang bestimmter Flags im Router-Advertisment den DHCPv6-Client startet, um spezielle Anfragen beim zuständigen DHCPv6-Server zu stellen:

- **M-Flag**: Erhält ein entsprechend konfiguriertes Gerät ein Router-Advertisment mit gesetztem 'M-Flag', dann fordert der DHCPv6-Client eine IPv6-Adresse sowie andere Informationen wie DNS-Server, SIP-Server oder NTP-Server beim DHCPv6-Server an.
- **O-Flag**: Bei einem 'O-Flag' fragt DHCPv6-Client beim DHCPv6-Server nur nach Informationen wie DNS-Server, SIP-Server oder NTP-Server, nicht jedoch nach einer IPv6-Adresse.

Wenn das 'M-Flag' gesetzt ist, muss nicht zwingend auch das 'O-Flag' gesetzt sein.

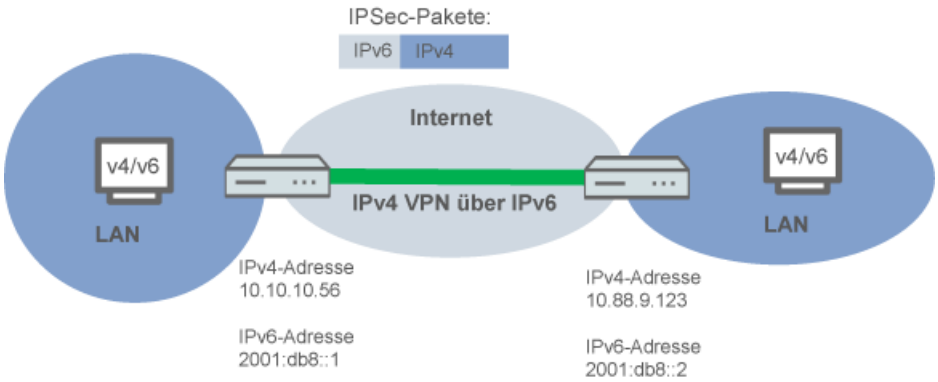
Bei IPv6 wird die Default-Route nicht über DHCPv6 verteilt, sondern über Router-Advertisements.

5.4 IPv4-VPN-Tunnel über IPv6

Bisher war es nicht möglich, zwei Gegenstellen über VPN zu verbinden, die für den Internetzugang private IPv4-Adressen verwenden (z.B. Mobilfunk).

Mit IPv6 ist diese Einschränkung nicht mehr vorhanden, da jedes IPv6-Gerät eine öffentliche IPv6-Adresse erhält. Somit kann über IPv6 ein IPv4-VPN-Tunnel eingerichtet werden, der zwei entfernte IPv4-Netzwerke verbindet, unabhängig von den IPv4-WAN-Adressen der entsprechenden Gegenstellen.

Im dargestellten Beispiel werden zwei lokale IPv4-Netzwerke über einen IPv4-VPN-Tunnel verbunden, welcher über eine IPv6-Internet-Verbindung aufgebaut wurde. Hierbei werden über die IPv6-Internetverbindung (nativ oder über Tunnelbroker) die IPv4-VPN-Pakete mit einem IPv6-Header an die Gegenstelle gesendet.

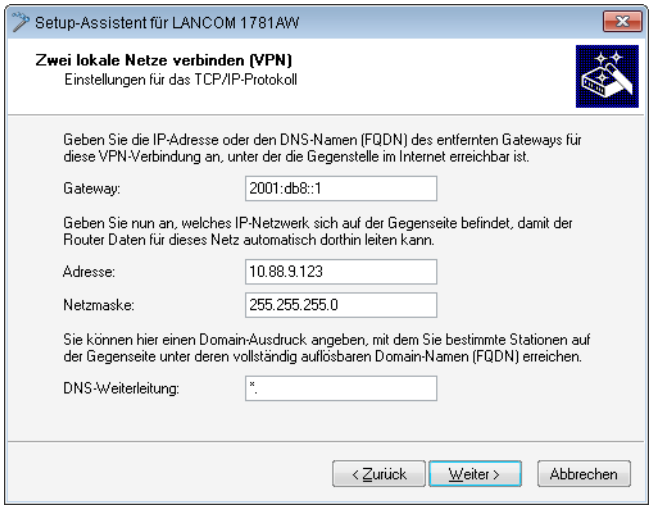


5.4 Setup-Assistent - IPv4-VPN-Verbindung über IPv6 einrichten

Der Setup-Assistent zur Verbindung zweier lokaler Netze unterstützt Sie bei der Einrichtung einer VPN-Verbindung.

1. Rufen Sie LANconfig z. B. aus der Windows-Startleiste auf mit **Start** > **Programme** > **LANCOM** > **LANconfig** . LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.
2. Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent** .
   LANconfig liest zunächst die Gerätekonfiguration aus und zeigt das Auswahlfenster der möglichen Anwendungen.
3. Wählen Sie die Aktion **Zwei lokale Netze verbinden**

4. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
5. Geben Sie als Gateway-Adresse die IPv6-Adresse des Gateways ein.



6. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
   Der Setup-Assistent schreibt die Konfiguration in das Gerät.

5.5 IPv6-Firewall

5.5.1 Funktion

Während die IPv4-Firewall ausschließlich das Forwarding der IP-Daten kontrolliert, regelt die IPv6-Firewall auch die Funktionen der Access-Listen aller IPv6-Server-Dienste. Die IPv6-Firewall entspricht damit eher dem klassischen Design von Firewalls, die die Inbound- und Outbound-Kommunikation sowie das Forwarding separat unterstützen. Da beim LANCOM dessen Konfiguration gezielt die Kommunikation steuert, verzichtet das LCOS auf eine Outbound-Firewall.

5.5.2 Konfiguration

Die Konfiguration der IPv6-Firewall entspricht weitgehend der Konfiguration der IPv4-Firewall, erfolgt jedoch getrennt von dieser.

Die Inbound- und Forwarding-Firewall verfügen jeweils über eine eigene Regeltabelle, die in Umfang und Aufbau in Teilen identisch und im Aufbau zur IPv4-Firewall vergleichbar sind.

Die Regeln sind nach absteigender Priorität sortiert, d. h., die Regel mit der höchsten Priorität steht in der Liste oben. Falls die Regel vorgibt, weitere Regeln zu beachten, führt die Firewall der Reihe nach auch die nachfolgenden Filterregeln aus. Ansonsten beendet die Firewall die Filterung, nachdem sie die aktuelle Regel angewendet hat.

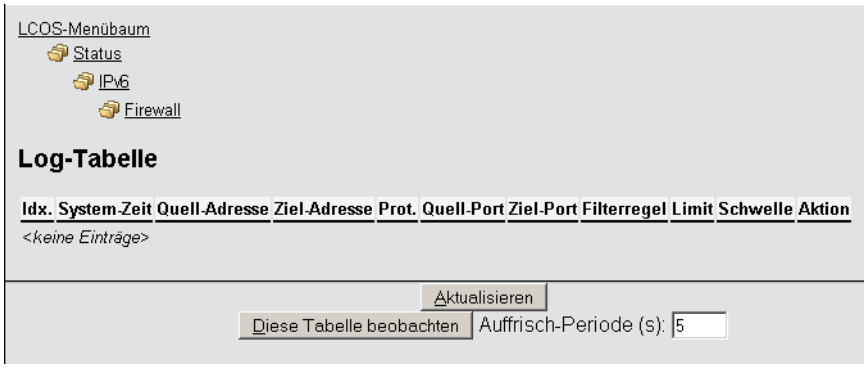
5.5.3 IPv6-Firewall-Tabelle

Die IPv6-Firewall stellt analog zur IPv4-Firewall eine Log-Tabelle für Ereignisse im IPv6-Umfeld bereit.

Die Syntax dieser Log-Tabelle entspricht der IPv4-Logtabelle mit Ausnahme des IP-Adressformats (IPv6-Adressen liegen in hexadezimaler, IPv4-Adressen in dezimaler Form vor).

IPv6-Firewall-Tabelle über WEBconfig auswerten

Sie können die IPv6-Log-Tabelle im WEBconfig über **LCOS-Menübaum** > **Status** > **IPv6** > **Firewall** > **Log-Tabelle** öffnen.



Die Einträge haben folgende Bedeutung:

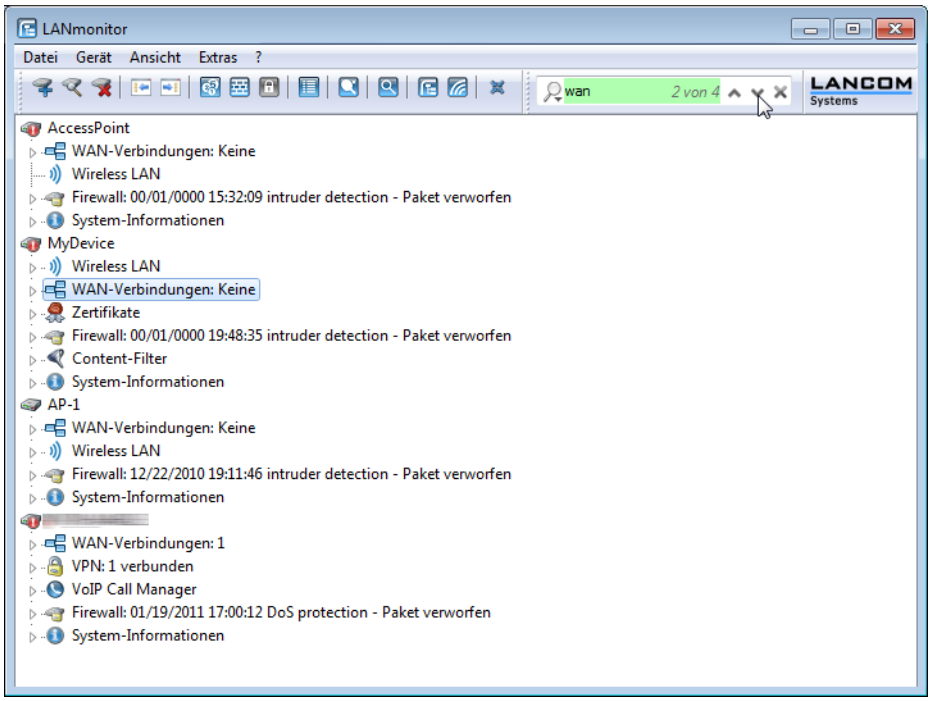
- **Idx.**: Fortlaufender Index. Darüber lässt sich die Tabelle auch über SNMP abfragen.
- **System-Zeit**: System-Zeit in UTC-Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt).
- **Quell-Adresse**: Quell-Adresse des gefilterten Pakets.
- **Ziel-Adresse**: Ziel-Adresse des gefilterten Pakets.
- **Prot.**: Protokoll (TCP, UDP etc.) des gefilterten Pakets.
- **Quell-Port**: Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Ziel-Port**: Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Filterregel**: Name der Regel, die den Eintrag erzeugt hat.
- **Limit**: Bitfeld, das das überschrittene Limit beschreibt, durch das die Firewall den Filter angewendet hat. Es sind zur Zeit folgende Werte definiert:
  - 0x01: Absolute Anzahl
  - 0x02: Anzahl pro Sekunde
  - 0x04: Anzahl pro Minute
  - 0x08: Anzahl pro Stunde
  - 0x10: globales Limit
  - 0x20: Byte-Limit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit)
  - 0x40: Limit gilt nur in Empfangsrichtung
  - 0x80: Limit gilt nur in Senderichtung
- **Schwelle**: überschrittener Grenzwert des auslösenden Limits.
- **Aktion**: Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind zur Zeit folgende Werte definiert:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Aufbaufilter
  - 0x00000400: Internet-(Defaultrouten-)Filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Quell-Adresse sperren
  - 0x00020000: Ziel-Adresse und -Port sperren
  - 0x20000000: Sende Syslog-Benachrichtigung
  - 0x40000000: Sende SNMP-Trap
  - 0x80000000: Sende E-Mail

Alle Firewall-Aktionen erscheinen ebenfalls im IP-Router-Trace. Einige LANCOM-Modelle verfügen ferner über eine Firewall-LED, die jedes gefilterte Paket signalisiert.

IPv6-Firewall-Tabelle über LANmonitor auswerten

Sie können sich die IPv6-Log-Tabelle eines Gerätes im LANmonitor anzeigen lassen.

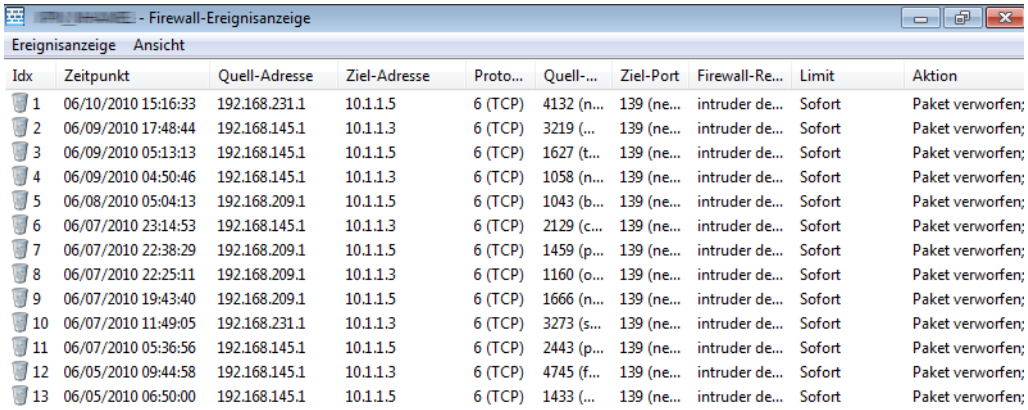
Starten Sie dazu den LANmontor mit **Start** > **Programme** > **LANCOM** > **LANmonitor** . Sie können den LANmonitor auch in LANconfig über das Kontextmenü für ein bestimmtes Gerät oder über die Tastenkombination `Strg + M` starten.



Über **Gerät** > **Firewall-Ereignisse anzeigen** können Sie sich die Firewall-Ereignisse eines markierten Geräts anzeigen lassen. Die Firewall-Ereignisanzeige listet die letzten 100 Aktionen der Firewall mit den folgenden Detailinformationen auf:

- Idx
- Zeitpunkt
- Quell-Adresse
- Ziel-Adresse
- Protokoll
- Quell-Port
- Ziel-Port
- Firewall-Regel
- Limit

- Aktion



Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Proto...	Quell-...	Ziel-Port	Firewall-Re...	Limit	Aktion
1	06/10/2010 15:16:33	192.168.231.1	10.1.1.5	6 (TCP)	4132 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
2	06/09/2010 17:48:44	192.168.145.1	10.1.1.3	6 (TCP)	3219 (...	139 (ne...	intruder de...	Sofort	Paket verworfen;
3	06/09/2010 05:13:13	192.168.145.1	10.1.1.5	6 (TCP)	1627 (t...	139 (ne...	intruder de...	Sofort	Paket verworfen;
4	06/09/2010 04:50:46	192.168.145.1	10.1.1.3	6 (TCP)	1058 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
5	06/08/2010 05:04:13	192.168.209.1	10.1.1.5	6 (TCP)	1043 (b...	139 (ne...	intruder de...	Sofort	Paket verworfen;
6	06/07/2010 23:14:53	192.168.145.1	10.1.1.3	6 (TCP)	2129 (c...	139 (ne...	intruder de...	Sofort	Paket verworfen;
7	06/07/2010 22:38:29	192.168.209.1	10.1.1.5	6 (TCP)	1459 (p...	139 (ne...	intruder de...	Sofort	Paket verworfen;
8	06/07/2010 22:25:11	192.168.209.1	10.1.1.3	6 (TCP)	1160 (o...	139 (ne...	intruder de...	Sofort	Paket verworfen;
9	06/07/2010 19:43:40	192.168.209.1	10.1.1.5	6 (TCP)	1666 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
10	06/07/2010 11:49:05	192.168.231.1	10.1.1.3	6 (TCP)	3273 (s...	139 (ne...	intruder de...	Sofort	Paket verworfen;
11	06/07/2010 05:36:56	192.168.145.1	10.1.1.5	6 (TCP)	2443 (p...	139 (ne...	intruder de...	Sofort	Paket verworfen;
12	06/05/2010 09:44:58	192.168.145.1	10.1.1.3	6 (TCP)	4745 (f...	139 (ne...	intruder de...	Sofort	Paket verworfen;
13	06/05/2010 06:50:00	192.168.145.1	10.1.1.5	6 (TCP)	1433 (...	139 (ne...	intruder de...	Sofort	Paket verworfen;

5.6 Ergänzungen im Setup-Menü

5.6.1 Tunnel

Mit dieser Einstellung verwalten Sie die Tunnelprotokolle, um den Zugang zum IPv6-Internet über eine IPv4-Internetverbindung bereitzustellen.

SNMP-ID:

2.70.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel**

6in4

Die Tabelle enthält die Einstellungen zum 6in4-Tunnel.

SNMP-ID:

2.70.1.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4**

Gegenstelle

Beinhaltet den Namen des 6in4-Tunnels.

SNMP-ID:

2.70.1.1.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.1.2

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen aus dem Wertebereich 0 - 65534

Default:

0

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.

SNMP-ID:

2.70.1.1.3

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gateway-Adresse**

Mögliche Werte:

IP-Adresse in IPv4-Notation mit max. 64 Zeichen

Default:

leer

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

SNMP-ID:

2.70.1.1.4

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Wertebereich von 0 - 65534

Default:

0

Gateway-IPv6-Adresse

Beinhaltet die IPv6-Adresse des entfernten Tunnelendpunktes auf dem Transfernetz, z.B. "2001:db8::1".

SNMP-ID:

2.70.1.1.5

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Gateway-IPv6-Adresse**

Mögliche Werte:

IPv6-Adresse mit max. 43 Zeichen

Default:

leer

Lokale-IPv6-Adresse

Beinhaltet die lokale IPv6-Adresse des Geräts auf dem Transfernetz, z.B. "2001:db8::2/64".

SNMP-ID:

2.70.1.1.6

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Lokale-IPv6-Adresse**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

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".

SNMP-ID:

2.70.1.1.7

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Geroutetes-IPv6-Prefix**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.1.8

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6in4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

6rd-Border-Relay

Ein LANCOM 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.

SNMP-ID:

2.70.1.2

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay**

Gegenstelle

Beinhaltet den Namen des 6rd-Border-Relay-Tunnels.

SNMP-ID:

2.70.1.2.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.2.2

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

IPv4-Loopback-Adresse

Bestimmen Sie die IPv4-Loopback-Adresse, d.h. die Adresse auf der das Gerät als 6rd-Border-Relay arbeiten soll.

SNMP-ID:

2.70.1.2.3

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **IPv4-Loopback-Adresse**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.2.4

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

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

SNMP-ID:

2.70.

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.

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.

SNMP-ID:

2.70.1.2.6

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **DHCPv4-Propagieren**

Mögliche Werte:

ja

nein

Default:

nein

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.

SNMP-ID:

2.70.1.2.7

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd-Border-Relay** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

6rd

Die Tabelle enthält die Einstellungen zum 6rd-Tunnel.

SNMP-ID:

2.70.1.3

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd**

Gegenstelle

Beinhaltet den Namen des 6rd-Tunnels.

SNMP-ID:

2.70.1.3.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.3.2

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

Border-Relay-Adresse

Enthält die IPv4-Adresse des 6rd-Border-Relays.

SNMP-ID:

2.70.1.3.3

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Border-Relay-Adresse**

Mögliche Werte:

IPv4-Adresse mit max. 64 Zeichen

Default:

leer

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

SNMP-ID:

2.70.1.3.4

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

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.

SNMP-ID:

2.70.1.3.5

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **6rd-Praefix**

Mögliche Werte:

max. 24 Zeichen

Default:

leer

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

SNMP-ID:

2.70.1.3.6

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd** > **IPv4-Masken-Laenge**

Mögliche Werte:

max. 2 Ziffern im Bereich von 0 - 32

Default:

0

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.

SNMP-ID:

2.70.1.3.7

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6rd4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.1.4

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4**

Gegenstelle

Beinhaltet den Namen des 6to4-Tunnels.

SNMP-ID:

2.70.1.4.1

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Gegenstelle**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.1.4.2

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65535

Default:

0

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.

SNMP-ID:

2.70.1.4.3

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Gateway-Adresse**

Mögliche Werte:

IPv4-Adresse mit max. 64 Zeichen

Default:

192.88.99.1

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

SNMP-ID:

2.70.1.4.4

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **IPv4-Rtg-tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

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.

SNMP-ID:

2.70.1.4.5

Pfad Telnet:

Setup > **IPv6** > **Tunnel** > **6to4** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

5.6.2 Router-Advertisement

Mit dieser Einstellung verwalten Sie die Router-Advertisements, mit denen das Gerät seine Verfügbarkeit im Netz als Router anzeigt.

SNMP-ID:

2.70.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement**

Praefix-Optionen

Die Tabelle enthält die Einstellungen der IPv6-Präfixe je Interface.

SNMP-ID:

2.70.2.1

Pfad Telnet:

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

Interface-Name

Definiert den Namen des logischen Interfaces.

SNMP-ID:

2.70.2.1.1

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Interface-Name**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.2.1.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Praefix**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.2.1.3

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Subnetz-ID**

Mögliche Werte:

Max. 19 Zeichen

Default:

1

Adv.-OnLink

Gibt an, ob das Präfix "On Link" ist.

SNMP-ID:

2.70.2.1.3

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Adv.-OnLink**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.2.1.5

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Adv.-Autonomous**

Mögliche Werte:

ja

nein

Default:

ja

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).

SNMP-ID:

2.70.2.1.6

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **PD-Quelle**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.2.1.7

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Adv.-Pref.-Lifetime**

Mögliche Werte:

Max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

604800

Adv.-Valid-Lifetime

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

SNMP-ID:

2.70.2.1.8

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Praefix-Optionen** > **Adv.-Valid-Lifetime**

Mögliche Werte:

Max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

2592000

Interface-Optionen

Die Tabelle enthält die Einstellungen der IPv6-Interfaces.

SNMP-ID:

2.70.2.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen**

Interface-Name

Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements gesendet werden sollen.

SNMP-ID:

2.70.2.2.1

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Interface-Name**

Mögliche Werte:

Max. 16 Zeichen

Default:

leer

Adverts-Senden

Aktiviert das Senden von periodischen Router-Advertisements und das Antworten auf Router-Solicitations.

SNMP-ID:

2.70.2.2.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Interface-Optionen** > **Adverts-Senden**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.2.2.3

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)

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.

SNMP-ID:

2.70.2.2.4

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

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.

SNMP-ID:

2.70.2.2.5

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Managed-Flag**

Mögliche Werte:

ja

nein

Default:

nein

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.

SNMP-ID:

2.70.2.2.6

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Other-Config-Flag**

Mögliche Werte:

ja

nein

Default:

ja

Link-MTU

Bestimmen Sie die gültige MTU auf dem entsprechenden Link.

SNMP-ID:

2.70.2.2.7

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Link-MTU**

Mögliche Werte:

max. 5 Ziffern im Bereich von 0 - 99999

Default:

1500

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.

SNMP-ID:

2.70.2.2.8

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Reachable-Zeit**

Mögliche Werte:

max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

0

Hop-Limit

Definiert die maximale Anzahl von Routern, über die ein Datenpaket weitergeschickt werden darf. Ein Router entspricht hierbei einem "Hop".

SNMP-ID:

2.70.2.2.10

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

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.

SNMP-ID:

2.70.2.2.11

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Def.-Lifetime**

Mögliche Werte:

max. 10 Ziffern im Bereich von 0 - 2147483647

Default:

1800

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.
- **immer**: Die Router-Lifetime ist unabhängig vom Status der WAN-Verbindung immer positiv, d. h. größer "0".
- **nie**: Die Router-Lifetime ist immer "0".

SNMP-ID:

2.70.2.2.12

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Default-Router-Modus**

Mögliche Werte:

auto

immer

nie

Default:

auto

Router-Preference

Definiert die Präferenz dieses Routers. Clients tragen diese Präferenz in ihre lokale Routing-Tabelle ein.

SNMP-ID:

2.70.2.2.13

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **Interface-Optionen** > **Router-Preference**

Mögliche Werte:

low

medium

high

Default:

medium

Route-Optionen

Die Tabelle enthält die Einstellungen der Route-Optionen.

SNMP-ID:

2.70.2.3

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen**

Interface-Name

Definiert den Namen des Interfaces, für das diese Route-Option gilt.

SNMP-ID:

2.70.2.3.1

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

Praefix

Vergeben Sie das Präfix für diese Route. Dieses darf maximal 64 Bit lang sein, wenn es zur Autokonfiguration dient.

SNMP-ID:

2.70.2.3.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Praefix**

Mögliche Werte:

IPv6-Präfix mit max. 43 Zeichen, z. B. 2001:db8::/64

Default:

leer

Route-Lifetime

Bestimmen Sie die Dauer in Sekunden, für welche die Route gültig sein soll.

SNMP-ID:

2.70.2.3.3

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

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.

SNMP-ID:

2.70.2.3.4

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisement** > **Route-Optionen** > **Route-Preference**

Mögliche Werte:

low

medium

high

Default:

medium

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.

SNMP-ID:

2.70.2.5

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Interface-Name

Name des Interfaces, auf dem der IPv6-DNS-Server Informationen in Router-Advertisements ankündigt.

SNMP-ID:

2.70.2.5.1

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

Erster-DNS

IPv6-Adresse des ersten IPv6-DNS-Servers (Recursive DNS-Server, RDNSS, nach RFC 6106) für dieses Interface.

SNMP-ID:

2.70.2.5.2

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

Gültige IPv6-Adresse

Default:

leer

Zweiter-DNS

IPv6-Adresse des zweiten IPv6-DNS-Servers für dieses Interface.

SNMP-ID:

2.70.2.5.3

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

Gültige IPv6-Adresse

Default:

leer

DNS-Suchliste

Dieser Parameter definiert, welche DNS-Suchliste das Gerät in diesem logischen Netzwerk propagiert.

SNMP-ID:

2.70.2.5.4

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.

Lifetime

Definiert die Dauer in Sekunden, die ein Client diesen DNS-Server zur Namensauflösung verwenden darf.

SNMP-ID:

2.70.2.5.5

Pfad Telnet:

Setup > **IPv6** > **Router-Advertisements** > **RDNSS-Optionen**

Mögliche Werte:

- max. 5 Ziffern im Bereich von 0 - 65535
- 0: Abkündigung

Default:

900

5.6.3 DHCPv6

Dieses Menü enthält die Einstellungen für DHCP über IPv6.

SNMP-ID:

2.70.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6**

Server

Dieses Menü enthält die DHCP-Server-Einstellungen über IPv6.

SNMP-ID:

2.70.3.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

Adress-Pools

In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll.

SNMP-ID:

2.70.3.1.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pool**

Adress-Pool-Name

Bestimmen Sie hier den Namen des Adress-Pools.

SNMP-ID:

2.70.3.1.2.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Adress-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

Start-Adress-Pool

Bestimmen Sie hier die erste Adresse des Pools, z. B. "2001:db8::1"

SNMP-ID:

2.70.3.1.2.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Start-Adress-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

Ende-Adress-Pool

Bestimmen Sie hier die letzte Adresse des Pools, z. B. "2001:db8::9"

SNMP-ID:

2.70.3.1.2.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Ende-Adress-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

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".

SNMP-ID:

2.70.3.1.2.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Pref.-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

Valid-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als "gültig" verwenden soll.

SNMP-ID:

2.70.3.1.2.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools** > **Valid-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

SNMP-ID:

2.70.3.1.2.7

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Adress-Pools**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

PD-Pools

In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll.

SNMP-ID:

2.70.3.1.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

PD-Pool-Name

Bestimmen Sie hier den Namen des PD-Pools.

SNMP-ID:

2.70.3.1.3.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **PD-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

Start-PD-Pool

Bestimmen Sie hier das erste zu delegierende Präfix im PD-Pool, z. B. "2001:db8:1100::"

SNMP-ID:

2.70.3.1.3.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Start-PD-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

Ende-PD-Pool

Bestimmen Sie hier das letzte zu delegierende Präfix im PD-Pool, z. B. "2001:db8:FF00::"

SNMP-ID:

2.70.3.1.3.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Ende-PD-Pool**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

Praefix-Laenge

Bestimmen Sie hier die Länge der Präfixe im PD-Pool, z. B. "56" oder "60"

SNMP-ID:

2.70.3.1.3.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Praefix-Laenge**

Mögliche Werte:

maximal 3 Ziffern

Default:

56

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".

SNMP-ID:

2.70.3.1.3.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Pref.-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

Valid-Lifetime

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als "gültig" verwenden soll.

SNMP-ID:

2.70.3.1.3.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools** > **Valid-Lifetime**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

SNMP-ID:

2.70.3.1.3.7

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **PD-Pools**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

Interface-Liste

In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.

SNMP-ID:

2.70.3.1.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste**

Interface-Name-oder-Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET"

SNMP-ID:

2.70.3.1.4.1

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

Aktiv

Aktiviert bzw. deaktiviert den DHCPv6-Server.

SNMP-ID:

2.70.3.1.4.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Aktiv**

Mögliche Werte:

nein

ja

Default:

ja

Erster-DNS

IPv6-Adresse des ersten DNS-Servers.

SNMP-ID:

2.70.3.1.4.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Erster-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

Zweiter-DNS

IPv6-Adresse des zweiten DNS-Servers.

SNMP-ID:

2.70.3.1.4.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Zweiter-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.3.1.4.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Adress-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.3.1.4.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **PD-Pool-Name**

Mögliche Werte:

maximal 31 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.3.1.4.7

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Rapid-Commit**

Mögliche Werte:

nein

ja

Default:

nein

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.

SNMP-ID:

2.70.3.1.4.8

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Interface-Liste** > **Preference**

Mögliche Werte:

0 bis 255

Default:

0

Reservierungen

Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, definieren Sie in dieser Tabelle pro Client eine Reservierung.

SNMP-ID:

2.70.3.1.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

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.

SNMP-ID:

2.70.3.1.6.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Auswahl aus der Liste der im Gerät definierten LAN-Interfaces, maximal 39 Zeichen

Default:

leer

Adresse-oder-PD-Praefix

IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.

SNMP-ID:

2.70.3.1.6.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Maximal 43 Zeichen

Default:

leer

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 `ipconfig /all`.

SNMP-ID:

2.70.3.1.6.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

Maximal 96 Zeichen

Default:

leer

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".

SNMP-ID:

2.70.3.1.6.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 10 Ziffern

Default:

3600

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.

SNMP-ID:

2.70.3.1.6.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 10 Ziffern

Default:

86400

PD-Quelle

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

SNMP-ID:

2.70.3.1.6.7

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservierungen**

Mögliche Werte:

maximal 16 Zeichen

Default:

leer

Client

Dieses Menü enthält die DHCP-Client-Einstellungen über IPv6.

SNMP-ID:

2.70.3.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client**

Interface-Liste

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Clients.

Normalerweise steuert bereits die Autokonfiguration das Client-Verhalten.

SNMP-ID:

2.70.3.2.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

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".

SNMP-ID:

2.70.3.2.1.1

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

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.

SNMP-ID:

2.70.3.2.1.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Aktiv**

Mögliche Werte:

Autoconf

Nein

Ja

Default:

Autoconf

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.

SNMP-ID:

2.70.3.2.1.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **DNS-Anfragen**

Mögliche Werte:

nein

ja

Default:

ja

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.

SNMP-ID:

2.70.3.2.1.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Adresse-Anfragen**

Mögliche Werte:

nein

ja

Default:

ja

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.

SNMP-ID:

2.70.3.2.1.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **PD-Anfragen**

Mögliche Werte:

nein

ja

Default:

nein

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.

SNMP-ID:

2.70.3.2.1.6

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste** > **Rapid-Commit**

Mögliche Werte:

nein

ja

Default:

ja

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.

SNMP-ID:

2.70.3.2.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **User-Class-Identifier**

Mögliche Werte:

maximal 253 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.3.2.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Vendor-Class-Identifier**

Mögliche Werte:

maximal 253 Zeichen

Default:

Name des Geräteherstellers

Vendor-Class-Nummer

Bestimmt die Enterprise Number, mit der der Gerätehersteller bei der IANA (Internet Assigned Numbers Authority) registriert ist.

SNMP-ID:

2.70.3.2.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client**

Mögliche Werte:

maximal 10 Zeichen

Default:

2356

5.6.4 Relay-Agent

Dieses Menü enthält die DHCP-Relay-Agent-Einstellungen über IPv6.

SNMP-ID:

2.70.3.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent**

Interface-Liste

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Relay-Agents.

SNMP-ID:

2.70.3.3.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste**

Interface-Name

Definieren Sie den Name des Interfaces, auf dem der Relay-Agent Anfragen von DHCPv6-Clients entgegennimmt, z. B. "INTRANET".

SNMP-ID:

2.70.3.3.1.1

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

Relay-Agent aktiviert

Definieren Sie mit dieser Option, wie und ob das Gerät den Relay-Agent aktiviert.

SNMP-ID:

2.70.3.3.1.2

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

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.

SNMP-ID:

2.70.3.3.1.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Interface-Adresse**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.3.3.1.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Ziel-Adresse**

Mögliche Werte:

maximal 39 Zeichen

Default:

ff02::1:2

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.

SNMP-ID:

2.70.3.3.1.5

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Relay-Agent** > **Interface-Liste** > **Ziel-Interface**

Mögliche Werte:

maximal 39 Zeichen

Default:

leer

5.6.5 Netzwerk

Hier können Sie für jedes logische Interface Ihres Gerätes weitere IPv6-Netzwerk-Einstellungen vornehmen.

SNMP-ID:

2.70.4

Pfad Telnet:

Setup > **IPv6** > **Netzwerk**

Adressen

In dieser Tabelle verwalten Sie die IPv6-Adressen.

SNMP-ID:

2.70.4.1

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen**

Interface-Name

Benennen Sie das Interface, dem Sie das IPv6-Netz zuordnen wollen.

SNMP-ID:

2.70.4.1.1

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.4.1.2

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **IPv6-Adresse-Praefixlaenge**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.4.1.3

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Adresstyp**

Mögliche Werte:

Unicast

Anycast

EUI-64

Default:

Unicast

Name

Vergeben Sie einen aussagekräftigen Namen für diese Kombination aus IPv6-Adresse und Präfix.

Die Eingabe eines Namens ist optional.

SNMP-ID:

2.70.4.1.4

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

SNMP-ID:

2.70.4.1.5

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Adressen** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

Parameter

In dieser Tabelle verwalten Sie die IPv6-Parameter.

SNMP-ID:

2.70.4.2

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter**

Interface-Name

Benennen Sie das Interface, für Sie die IPv6-Parameter konfigurieren wollen.

SNMP-ID:

2.70.4.2.1

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

IPv6-Gateway

Bestimmen Sie das verwendete IPv6-Gateway für dieses Interface.

Dieser Parameter überschreibt Gateway-Informationen, die das Gerät beispielsweise über Router-Advertisements empfängt.

SNMP-ID:

2.70.4.2.2

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:

::

Erster-DNS

Bestimmen Sie den ersten IPv6-DNS-Server für dieses Interface.

SNMP-ID:

2.70.4.2.3

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Erster-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

Zweiter-DNS

Bestimmen Sie den zweiten IPv6-DNS-Server für dieses Interface.

SNMP-ID:

2.70.4.2.4

Pfad Telnet:

Setup > **IPv6** > **Netzwerk** > **Parameter** > **Zweiter-DNS**

Mögliche Werte:

IPv6-Adresse mit max. 39 Zeichen

Default:

::

5.6.6 Firewall

Dieses Menü enthält die Einstellungen für die Firewall.

SNMP-ID:

2.70.5

Pfad Telnet:

Setup > **IPv6** > **Firewall**

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.

SNMP-ID:

2.70.5.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktiv**

Mögliche Werte:

ja

nein

Default:

ja

Forwarding-Regeln

Diese Tabelle enthält die Regeln, die die Firewall beim Forwarding von Daten anwenden soll.

SNMP-ID:

2.70.5.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Name

Definiert den Namen für die Forwarding-Regel.

SNMP-ID:

2.70.5.2.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

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.

SNMP-ID:

2.70.5.2.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

deaktiviert

verkettet

zustandslos

Default:

keine Auswahl

Prio

Diese Angabe bestimmt die Priorität, mit der die Firewall die Regel anwendet. Ein höherer Wert bestimmt eine höhere Priorität.

SNMP-ID:

2.70.5.2.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 4 Zeichen aus 1234567890

Default:

0

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.

SNMP-ID:

2.70.5.2.4

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 5 Zeichen aus 1234567890

Default:

0

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.

SNMP-ID:

2.70.5.2.5

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

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.

SNMP-ID:

2.70.5.2.7

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

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.

SNMP-ID:

2.70.5.2.8

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

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.

SNMP-ID:

2.70.5.2.9

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

SNMP-ID:

2.70.5.2.10

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Forwarding-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

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.

SNMP-ID:

2.70.5.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

Name

Definiert den Namen einer Gruppe von Aktionen.

SNMP-ID:

2.70.5.3.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Beschreibung

Enthält die Liste der Aktionen, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

SNMP-ID:

2.70.5.3.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktions-Liste**

Mögliche Werte:

max. 252 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

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.

SNMP-ID:

2.70.5.5

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

Name

Definiert den Namen einer Gruppe von Stationen.

SNMP-ID:

2.70.5.5.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Beschreibung

Enthält die Liste der Stationen, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

SNMP-ID:

2.70.5.5.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stations-Liste**

Mögliche Werte:

max. 252 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

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.

SNMP-ID:

2.70.5.6

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

Name

Definiert den Namen einer Gruppe von Diensten.

SNMP-ID:

2.70.5.6.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Beschreibung

Enthält die Liste der Dienste, die unter dem Gruppen-Namen zusammengefasst sind.

Trennen Sie die einzelnen Einträge jeweils durch ein Komma.

SNMP-ID:

2.70.5.6.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienst-Liste**

Mögliche Werte:

max. 252 Zeichen aus #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

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.

SNMP-ID:

2.70.5.7

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Name

Definiert den Namen der Aktion.

SNMP-ID:

2.70.5.7.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Limit

Bestimmt das Limit, bei dessen Überschreiten die Firewall die Filterregel anwendet.

SNMP-ID:

2.70.5.7.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 10 Zeichen aus 0123456789

Besondere Werte:

0: Die Regel tritt sofort in Kraft.

Default:

0

Einheit

Bestimmt die Einheit des Limits.

SNMP-ID:

2.70.5.7.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

kBit

kByte

Pakete

Sessions

Bandbreite (%)

Default:

Pakete

Zeit

Bestimmt, für welchen Messzeitraum die Firewall das Limit ansetzt.

SNMP-ID:

2.70.5.7.4

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

Sekunde

Minute

Stunde

absolut

Default:

absolut

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.

SNMP-ID:

2.70.5.7.5

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

Session

Station

global

Default:

Session

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.

SNMP-ID:

2.70.5.7.6

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

reset

geteilt

Default:

leer

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.

SNMP-ID:

2.70.5.7.7

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

reject

drop

accept

Default:

.

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”.

SNMP-ID:

2.70.5.7.11

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

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”.

SNMP-ID:

2.70.5.7.12

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 2 Zeichen aus 1234567890

Default:

0

Bedingungen

Bestimmt, welche Bedingung zusätzlich zur Ausführung der Aktion erfüllt sein müssen. Die Bedingungen können Sie unter **Setup** > **IPv6** > **Firewall** > **Bedingungen** definieren.

SNMP-ID:

2.70.5.7.13

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

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.

SNMP-ID:

2.70.5.7.14

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

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.

SNMP-ID:

2.70.5.9

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Name

Definiert den Namen der Station.

SNMP-ID:

2.70.5.9.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Typ

Bestimmt den Stationstyp.

SNMP-ID:

2.70.5.9.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

lokales-Netzwerk

Gegenstelle

Praefix

Identifier

IP-Adresse

benamter-Host

Default:

lokales-Netzwerk

lokales-Netzwerk

Geben Sie hier den Namen des lokalen Netzwerkes ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

SNMP-ID:

2.70.5.9.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 16 Zeichen aus #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Gegenstelle/Host-Name

Geben Sie hier die Gegenstelle oder den Host-Namen ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

SNMP-ID:

2.70.5.9.6

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 64 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Adresse/Praefix

Tragen Sie hier die IP-Adresse oder das Präfix der Station ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

SNMP-ID:

2.70.5.9.7

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

max. 43 Zeichen aus ABCDEFabcdef0123456789:

Default:

leer

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.

SNMP-ID:

2.70.5.10

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Name

Definiert den Namen des Dienstes.

SNMP-ID:

2.70.5.10.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Protokoll

Definiert das Protokoll des Dienstes.

SNMP-ID:

2.70.5.10.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

TCP+UDP

TCP

UDP

Default:

TCP+UDP

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*.

SNMP-ID:

2.70.5.10.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Dienste**

Mögliche Werte:

max. 64 Zeichen aus 0123456789,

Default:

leer

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.

SNMP-ID:

2.70.5.10.4

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Stationen**

Mögliche Werte:

nein

ja

Default:

nein

Protokolle

Diese Tabelle enthält eine Liste der Protokolle, für die die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

SNMP-ID:

2.70.5.11

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

Name

Definiert den Namen des Protokolls.

SNMP-ID:

2.70.5.11.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Protokoll

Definiert die Protokoll-Nummer.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

SNMP-ID:

2.70.5.11.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Protokolle**

Mögliche Werte:

max. 3 Zeichen 0123456789

Default:

leer

Bedingungen

Diese Tabelle enthält eine Liste der Bedingungen, für die die Firewall gemäß der Forwarding- und Inbound-Regeln Aktionen ausführen kann.

SNMP-ID:

2.70.5.12

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Name

Definiert den Namen der Bedingung.

SNMP-ID:

2.70.5.12.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Bedingungen

Bestimmt die Bedingungen, die erfüllt sein müssen.

SNMP-ID:

2.70.5.12.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

nicht-verbunden

Default-Route

Backup-Verbindung

VPN-Route

gesendet

empfangen

Default:

leer

Transportrichtung

Bestimmt, ob die Transportrichtung sich auf den logischen Verbindungsaufbau oder die physikalische Datenübertragung über das jeweilige Interface bezieht.

SNMP-ID:

2.70.5.12.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Bedingungen**

Mögliche Werte:

physikalisch

logisch

Default:

physikalisch

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”.

SNMP-ID:

2.70.5.7.11

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

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”.

SNMP-ID:

2.70.5.12.5

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 2 Zeichen aus 1234567890

Default:

0

Trigger-Aktionen

Diese Tabelle enthält eine Liste der Trigger-Aktionen, die die Firewall-Aktionen starten können.

SNMP-ID:

2.70.5.13

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Name

Definiert den Namen der Trigger-Aktion.

SNMP-ID:

2.70.5.13.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Benachrichtigungen

Bestimmt, ob und wie eine Benachrichtigung erfolgen soll.

Wenn Sie eine Benachrichtigung per Email erhalten möchten, müssen Sie unter **Setup** > **IP-Router** > **Firewall** > **Admin-Email** eine E-Mail-Adresse angeben.

SNMP-ID:

2.70.5.13.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

SNMP

Syslog

Email

Default:

leer

Trennen

Bestimmt, ob die Firewall bei gültiger Filterbedingung die Verbindung zur Gegenstelle trennt.

SNMP-ID:

2.70.5.13.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

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.

SNMP-ID:

2.70.5.13.4

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

Sperrzeit

Bestimmt, für wie viele Minuten die Firewall die Quelle sperren soll.

SNMP-ID:

2.70.5.13.5

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

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.

SNMP-ID:

2.70.5.13.6

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Trigger-Aktionen**

Mögliche Werte:

nein

ja

Default:

nein

Schliesszeit

Bestimmt, für wie viele Sekunden die Firewall das Ziel schließt.

SNMP-ID:

2.70.5.13.7

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

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.

SNMP-ID:

2.70.5.14

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Name

Definiert den Namen des ICMP-Dienstes.

SNMP-ID:

2.70.5.14.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 32 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Typ

Definiert den Typ des ICMP-Dienstes.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

SNMP-ID:

2.70.5.14.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 3 Zeichen aus 0123456789

Default:

0

Code

Definiert den Code des ICMP-Dienstes.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

SNMP-ID:

2.70.5.14.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **ICMP-Dienste**

Mögliche Werte:

max. 3 Zeichen aus 0123456789

Default:

0

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.

SNMP-ID:

2.70.5.15

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Name

Definiert den Namen der Inbound-Regel.

SNMP-ID:

2.70.5.15.1

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 36 Zeichen aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Aktiv

Diese Option aktiviert die Inbound-Regel.

SNMP-ID:

2.70.5.15.2

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

ja

nein

Default:

ja

Prio

Diese Angabe bestimmt die Priorität, mit der die Firewall die Regel anwendet. Ein höherer Wert bestimmt eine höhere Priorität.

SNMP-ID:

2.70.5.15.3

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 4 Zeichen aus 1234567890

Default:

0

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.

SNMP-ID:

2.70.5.15.5

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

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.

SNMP-ID:

2.70.5.15.7

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

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.

SNMP-ID:

2.70.5.15.8

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

SNMP-ID:

2.70.5.15.10

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Inbound-Regeln**

Mögliche Werte:

max. 64 Zeichen aus
#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`

Default:

leer

5.6.7 LAN-Interfaces

Die Tabelle enthält die Einstellungen für die LAN-Interfaces.

SNMP-ID:

2.70.6

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces**

Interface-Name

Benennen Sie das logische IPv6-Interface, das durch das physikalische Interface (Schnittstellen-Zuordnung) und die VLAN-ID definiert wird.

SNMP-ID:

2.70.6.1

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

Interface-ID

Wählen Sie die physikalische Schnittstelle aus, die zusammen mit der VLAN-ID das logische IPv6-Interface bilden soll.

SNMP-ID:

2.70.6.2

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-ID**

Mögliche Werte:

alle verfügbaren physikalischen Schnittstellen des Gerätes

Default:

LAN-1

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.

SNMP-ID:

2.70.6.3

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **VLAN-ID**

Mögliche Werte:

0 bis 4096

max. 4 Ziffern

Default:

0

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.

SNMP-ID:

2.70.6.4

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65535

Default:

0

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.

SNMP-ID:

2.70.6.5

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Autoconf**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.6.6

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Akzeptiere-RA**

Mögliche Werte:

ja

nein

Default:

ja

Interface-Status

Aktivieren bzw. deaktivieren Sie dieses Interface.

SNMP-ID:

2.70.6.7

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Interface-Status**

Mögliche Werte:

aktiv

inaktiv

Default:

aktiv

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.

SNMP-ID:

2.70.6.8

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

MTU

Bestimmen Sie die gültige MTU für dieses Interface.

SNMP-ID:

2.70.6.9

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **MTU**

Mögliche Werte:

max. 4 Ziffern im Bereich von 0 - 9999

Default:

1500

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. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

SNMP-ID:

2.70.6.10

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Firewall**

Mögliche Werte:

ja

nein

Default:

nein

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

SNMP-ID:

2.70.6.11

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

5.6.8 WAN-Interfaces

Die Tabelle enthält die Einstellungen für die LAN-Interfaces.

SNMP-ID:

2.70.7

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

Interface-Name

Bestimmen Sie hier den Namen der WAN-Gegenstelle. Diese Gegenstelle gibt den entsprechenden Namen vor.

SNMP-ID:

2.70.7.1

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Interface-Name**

Mögliche Werte:

max. 16 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.7.2

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Rtg-Tag**

Mögliche Werte:

max. 5 Zeichen im Bereich von 0 - 65534

Default:

0

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.

SNMP-ID:

2.70.7.3

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Autoconf**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.6.6

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Akzeptiere-RA**

Mögliche Werte:

ja

nein

Default:

ja

Interface-Status

Aktivieren bzw. deaktivieren Sie dieses Interface.

SNMP-ID:

2.70.7.5

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Interface-Status**

Mögliche Werte:

aktiv

inaktiv

Default:

aktiv

Forwarding

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

SNMP-ID:

2.70.7.6

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

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.

SNMP-ID:

2.70.7.7

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Firewall**

Mögliche Werte:

ja

nein

Default:

ja

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

SNMP-ID:

2.70.7.8

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

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** > **WAN-Interfaces** > **DaD-Versuche**

Mögliche Werte:

max. 1 Ziffer

Default:

1

5.6.9 Aktiv

Schaltet den IPv6-Stack global ein oder aus. Bei deaktiviertem IPv6-Stack führt das Gerät keine IPv6-bezogenen Funktionen aus.

SNMP-ID:

2.70.10

Pfad Telnet:

Setup > **IPv6** > **Aktiv**

Mögliche Werte:

ja

nein

Default:

nein

5.6.10 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.

SNMP-ID:

2.70.11

Pfad Telnet:

Setup > **IPv6** > **Forwarding**

Mögliche Werte:

ja

nein

Default:

ja

5.6.11 Router

Mit dieser Einstellung verwalten Sie die Router-Einstellungen.

SNMP-ID:

2.70.12

Pfad Telnet:

Setup > **IPv6** > **Router**

Routing-Tabelle

Die Tabelle enthält die Einträge für das Routing von Paketen mit IPv6-Adresse.

SNMP-ID:

2.70.12.1

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle**

Praefix

Tragen Sie hier als Präfix den Netzbereich ein, dessen Daten die aktuelle Gegenstelle erhalten soll, z. B. 2001:db8::/32

SNMP-ID:

2.70.12.1.1

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Praefix**

Mögliche Werte:

max. 43 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.12.1.2

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Routing-Tag**

Mögliche Werte:

max. 5 Zeichen

Default:

leer

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*).

SNMP-ID:

2.70.12.1.3

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Peer-oder-IPv6**

Mögliche Werte:

max. 56 Zeichen

Default:

leer

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

SNMP-ID:

2.70.12.1.4

Pfad Telnet:

Setup > **IPv6** > **Router** > **Routing-Tabelle** > **Kommentar**

Mögliche Werte:

max. 64 Zeichen

Default:

leer

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.

SNMP-ID:

2.70.12.2

Pfad Telnet:

Setup > **IPv6** > **Router** > **Dest.-Cache-Timeout**

Mögliche Werte:

max. 3 Zeichen

Default:

30 Sekunden

5.6.12 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

5.7 Ergänzungen im Status-Menü

5.7.1 Log-Tabelle

Diese Tabelle enthält eine Liste aller IPv6-Firewall-Ereignisse. Die Einträge haben folgende Bedeutung:

- **Idx.**: Fortlaufender Index. Darüber lässt sich die Tabelle auch über SNMP abfragen.
- **System-Zeit**: System-Zeit in UTC-Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt).
- **Quell-Adresse**: Quell-Adresse des gefilterten Pakets.
- **Ziel-Adresse**: Ziel-Adresse des gefilterten Pakets.
- **Prot.**: Protokoll (TCP, UDP etc.) des gefilterten Pakets.
- **Quell-Port**: Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Ziel-Port**: Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Filterregel**: Name der Regel, die den Eintrag erzeugt hat.
- **Limit**: Bitfeld, das das überschrittene Limit beschreibt, durch das die Firewall den Filter angewendet hat. Es sind zur Zeit folgende Werte definiert:

- 0x01: Absolute Anzahl
- 0x02: Anzahl pro Sekunde
- 0x04: Anzahl pro Minute
- 0x08: Anzahl pro Stunde
- 0x10: globales Limit
- 0x20: Byte-Limit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit)
- 0x40: Limit gilt nur in Empfangsrichtung
- 0x80: Limit gilt nur in Senderichtung

- **Schwelle**: überschrittener Grenzwert des auslösenden Limits.
- **Aktion**: Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind zur Zeit folgende Werte definiert:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Aufbaufilter
  - 0x00000400: Internet-(Defaultrouten-)Filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Quell-Adresse sperren
  - 0x00020000: Ziel-Adresse und -Port sperren
  - 0x20000000: Sende Syslog-Benachrichtigung
  - 0x40000000: Sende SNMP-Trap
  - 0x80000000: Sende E-Mail

SNMP-ID:

1.77.9.1

Pfad Telnet:

Status > **IPv6** > **Firewall** > **Log-Tabelle**

5.8 Ergänzungen Kommandozeile

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*: `show dhcp6-server`
- *IPv6-DHCP*: `show dhcpv6-client`
- *IPv6-Route*: `show ipv6-route`

5.8.1 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 2: Bestandteile der Kommandozeilenausgabe `show ipv6-adresses:`

Ausgabe	Erläuterung
Interface	Der Name des Interfaces
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

5.8.2 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.

5.8.3 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 3: 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 ■ 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

5.8.4 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 4: 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

Ausgabe	Erläuterung
	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.

5.8.5 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.

5.8.6 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.

5.8.7 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.

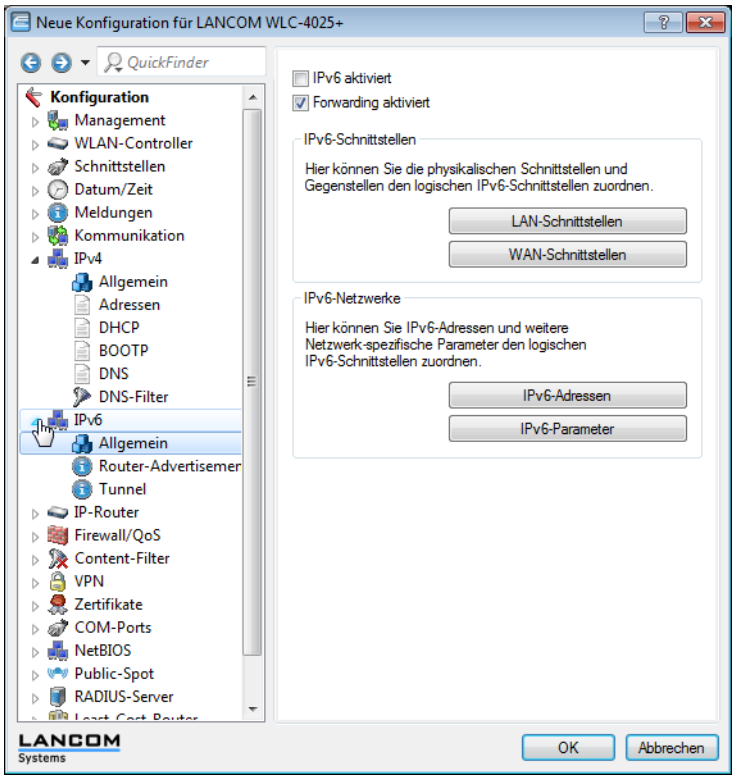
5.8.8 IPv6-Adressfreigabe

Befehl	Beschreibung
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. Der Platzhalter `*` wendet das Kommando auf alle Interfaces und Präfix-Delegationen an.

5.9 Ergänzungen in LANconfig

5.9.1 IPv6-Konfigurationsmenü

Im Gegensatz zu früheren Versionen, in denen es im Konfigurationsmenü die Konfigurationsmöglichkeit TCP/IP für IPv4 gab, finden Sie nun an dieser Stelle die Optionen **IPv4** und **IPv6**.



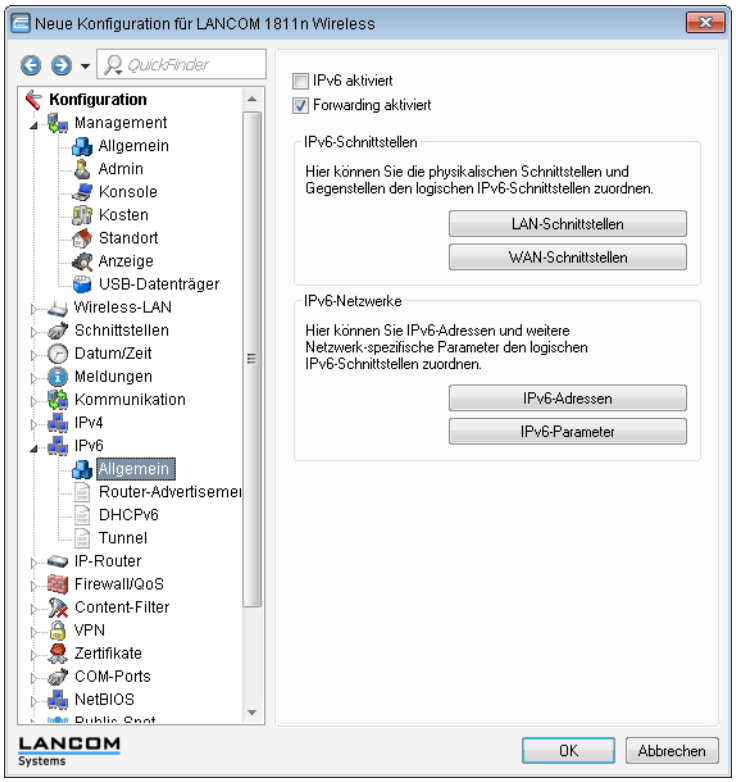
Klicken Sie auf **IPv6**, um die Einstellungen für dieses Protokoll vorzunehmen. Die Konfiguration **IPv6** ist unterteilt in die Optionen **Allgemein**, **Router- Advertisement** und **Tunnel**. Standardmäßig befinden Sie sich nach dem Klick auf **IPv6** in der Option *Allgemein*.

Allgemein

Hier nehmen Sie die Grundeinstellungen vor.

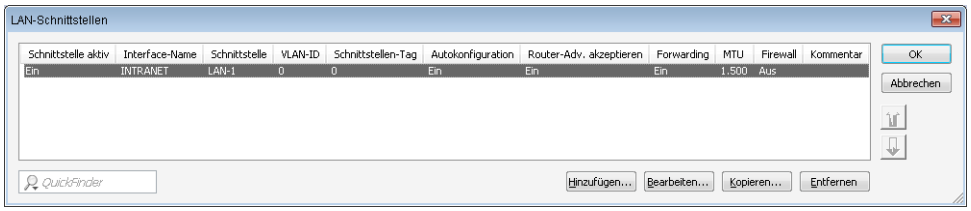
- **IPv6 aktiviert:** Sie haben die Möglichkeit, IPv6 im Gerät zu aktivieren oder zu deaktivieren.

- **Forwarding aktiviert:** Forwarding dient der Paketweiterleitung zwischen IPv6-Schnittstellen. Diese Option ist standardmäßig aktiviert.



- Über die Schaltflächen **LAN-Schnittstellen** und **WAN-Schnittstellen** gelangen Sie zu den Tabellen, die Ihnen die Möglichkeiten bieten, neue Schnittstellen hinzuzufügen sowie bestehende Schnittstellen zu konfigurieren oder zu löschen.

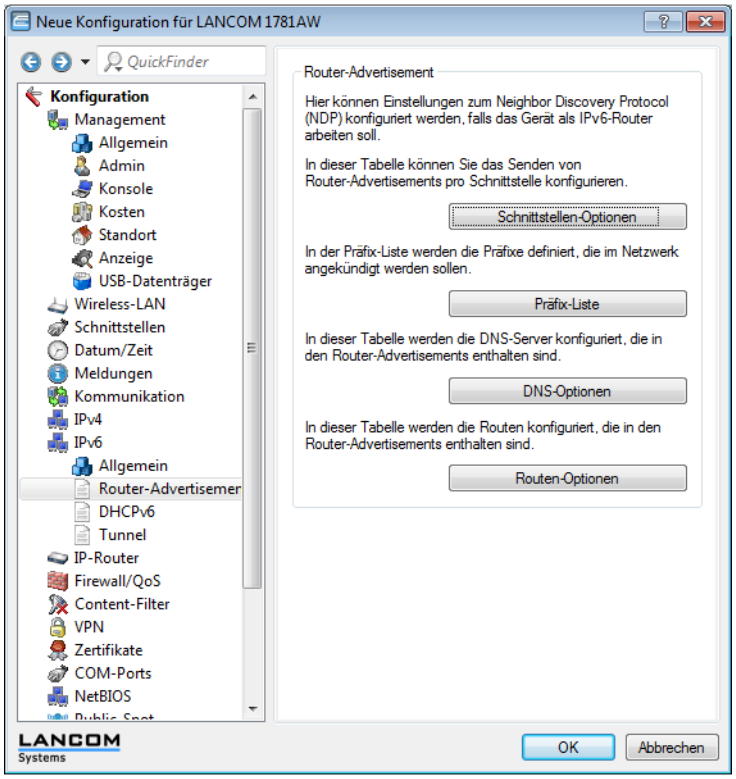
Das Beispiel zeigt die Tabelle mit einer LAN-Schnittstelle:



- Die Schaltflächen **IPv6-Adressen** und **IPv6-Parameter** dienen dazu, den Schnittstellen IPv6-Adressen zuzuordnen sowie die Parameter der Schnittstellen (Gateway-Adresse, erster und zweiter DNS) zu konfigurieren.

Router-Advertisement

In der Konfiguration **Router-Advertisement** bieten sich Ihnen 4 Schaltflächen mit Optionen zu Einstellungen des Neighbor Discovery Protocol (NDP), falls das Gerät als IPv6-Router arbeiten soll:



Die Schaltflächen öffnen jeweils Tabellen zur Einstellung der jeweiligen Funktionen:

- **Schnittstellen-Optionen:** Hier aktivieren oder deaktivieren Sie die folgenden Funktionen von Schnittstellen:
  - **Router Advertisement senden**: reguliert periodisches Senden von Router-Advertisements und das Antworten auf Router Solicitations.
  - **Managed-Flag**: wenn diese Funktion aktiv ist, konfiguriert ein Client, der dieses Router-Advertisement empfängt, Adressen durch Stateful Autoconfiguration (DHCPv6). Clients beziehen dann auch automatisch andere Informationen, wie z. B. DNS-Server.
  - **Other Flag**: wenn diese Funktion aktiv ist, bildet ein Client, der dieses Router-Advertisement empfängt, Adressen über die Autokonfiguration und bezieht zusätzliche Informationen, z. B. DNS-Server-Adressen, über DHCPv6.
  - **Standard-Router**: definiert das Verhalten, wie sich das Gerät als Standardgateway bzw. Router ankündigen soll.
  - **Router-Priorität**: definiert die Präferenz dieses Routers. Clients tragen diese Präferenz in ihre lokale Routing-Tabelle ein.

- **Präfix-Liste**: Setzen Sie die Präfix-Optionen verwendeter Schnittstellen. Möglich sind folgende Einstellungen:
  - **Präfix**: Tragen Sie hier ein Präfix ein, das in Router-Advertisements angekündigt wird, z. B. 2001:db8::/64. Die Präfixlänge muss immer exakt "/64" sein, da es sonst für Clients unmöglich ist, Adressen durch Hinzufügen ihrer Interface-Identifier (mit Länge 64 Bit) zu generieren. Soll ein vom Provider delegiertes Präfix automatisch weiter propagiert werden, so setzen Sie hier "::/64" und den Namen des entsprechenden WAN-Interfaces unter dem Parameter **Präfix beziehen von** ein.
  - **Subnetz-ID**. Tragen Sie hier die Subnetz-ID ein, die mit dem vom Provider delegierten Präfix kombiniert werden soll. Weist der Provider z. B. das Präfix "2001:db8:a::/48" zu und ist die Subnetz-ID "0001" oder kurz "1", so enthält das Router-Advertisement auf diesem Interface das Präfix "2001:db8:a:0001::/64". Die maximale

Subnetzlänge bei einem 48 Bit langen delegierten Präfix ist 16 Bit (65.536 Subnetze), d. h. mögliche Subnetz-IDs von "0000" bis "FFFF". Bei einem delegierten Präfix von "/56" ist die maximale Subnetzlänge 8 Bit (256 Subnetze), d. h. Subnetz-IDs von "00" bis "FF". In der Regel wird die Subnetz-ID "0" zur automatischen Bildung der WAN-IPv6-Adresse verwendet. Deshalb starten Subnetz-IDs für LANs bei "1". Die Default-Einstellung ist "1".

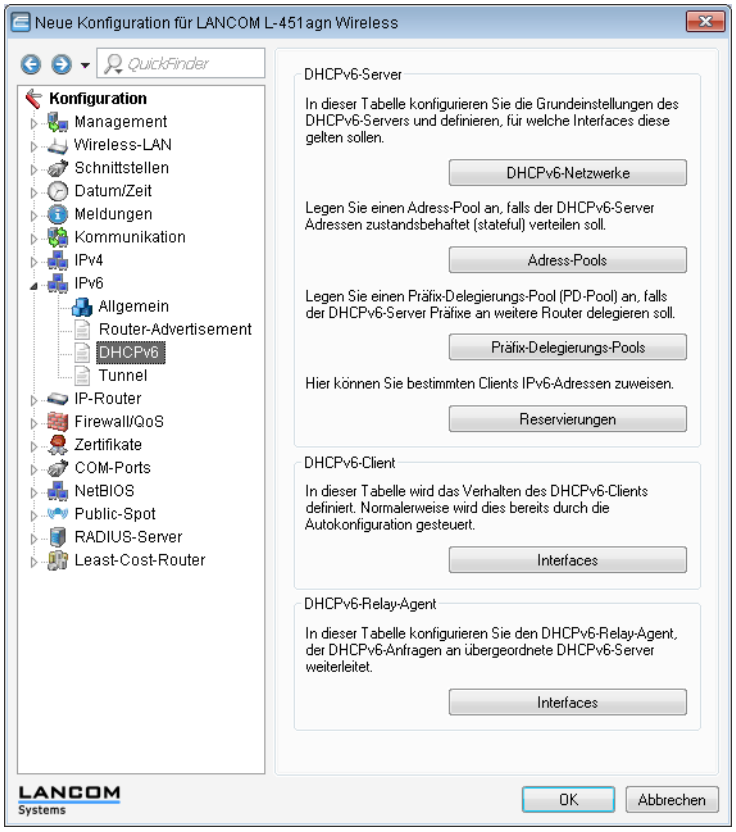
- **Autokonfiguration erlauben (SLAAC)**: Gibt an, ob der Client das Präfix für die Stateless Address Autoconfiguration (SLAAC) verwenden soll. Die Default-Einstellung ist "aktiviert".
- **Präfix beziehen von**: Definiert den Namen des Interfaces, auf dem ein Präfix über DHCPv6-Präfix-Delegation oder Tunnel empfangen wird. Aus diesem Präfix kann pro Interface ein Subnetz abgeleitet und propagiert werden.

- **DNS-Optionen**: Definiert die DNS-Informationen in Router-Advertisements nach RFC 6106. Möglich sind folgende Einstellungen:
  - **Interface-Name**: Name des Interfaces, auf dem der IPv6-DNS-Server Informationen in Router-Advertisements ankündigt.
  - **Erster DNS**: IPv6-Adresse des ersten IPv6-DNS-Servers (Recursive DNS-Server, RDNSS, nach RFC 6106) für dieses Interface.
  - **Zweiter DNS**: IPv6-Adresse des zweiten IPv6-DNS-Servers für dieses Interface.
  - **DNS-Suchliste vom internen DNS-Server importieren**: 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. Die Default-Einstellung ist "aktiviert".
  - **DNS-Suchliste vom WAN inportieren**: 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.

- **Routen-Optionen**: Definiert die Routen-Option in Router-Advertisements nach RFC 4191 (Route Information Option). Möglich sind folgende Einstellungen:
  - **Interface-Name**: Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements mit dieser Routen-Option gesendet werden sollen.
  - **Präfix**: Präfix der Routen-Option, z. B. "2001:db8::/32".
  - **Routen-Präferenz**: Präferenz der Route. Mögliche Werte sind "Hoch", "Mittel" (Default) und "Niedrig".

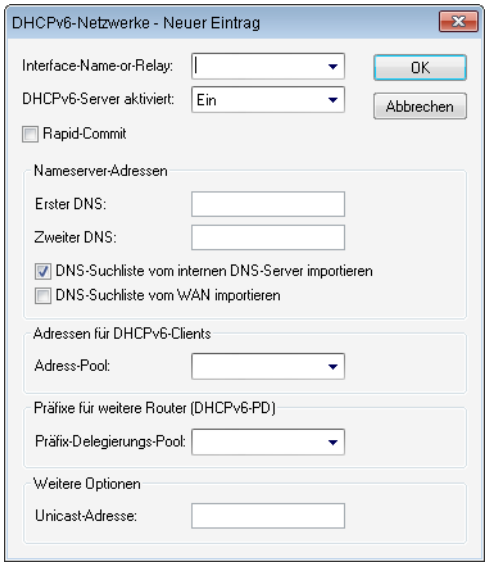
DHCPv6

Hier konfigurieren Sie DHCPv6-Server, den DHCPv6-Client und den DHCPv6-Relay-Agent.



DHCPv6-Server

Öffnen Sie mit den folgenden Schaltflächen die Tabellen zur Einstellung der jeweiligen Funktionen:



- **DHCPv6-Netzwerke:** In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.

- **Interface-Name-or-Relay**: Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ hinterlegen Sie hier die IPv6-Adresse des entfernten DHCPv6 Relay-Agenten.
- **DHCPv6-Server aktiviert**: Aktiviert bzw. deaktiviert den Eintrag.
- **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.

- **Erster DNS:** IPv6-Adresse des ersten DNS-Servers.
- **Zweiter DNS:** IPv6-Adresse des zweiten DNS-Servers.
- **DNS-Suchliste vom internen DNS-Server importieren**: 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. Die Default-Einstellung ist "aktiviert".
- **DNS-Suchliste vom WAN importieren**: Gibt an, ob die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Die Default-Einstellung ist "deaktiviert".
- **Adress-Pool**: Name des für dieses Interface verwendeten Adress-Pools.

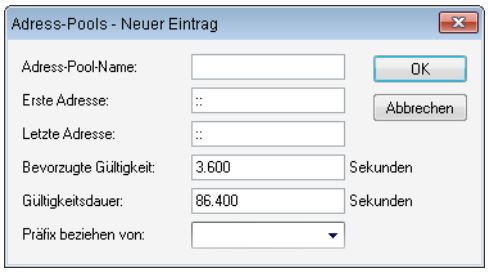
  Verteilt der DHCPv6-Server seine Adressen 'stateful', müssen Sie entsprechende Adressen in die Tabelle **Adress-Pools** eintragen.

- **Präfix-Delegierungs-Pool**: Name des Präfix-Pools, den der DHCPv6-Server verwenden soll.

  Soll der DHCPv6-Server Präfixe an weitere Router delegieren, müssen Sie entsprechende Präfixe in der Tabelle **Präfix-Delegierungs-Pools** eintragen.

- **Unicast-Adresse**: Standardmäßig reagiert der DHCPv6-Server ausschließlich auf Multicast-Anfragen. Wenn der DHCPv6-Server auf eine Unicast-Anfragen reagieren soll, so kann hier diese IPv6-Adresse konfiguriert werden. In der Regel reicht Multicast zur Kommunikation aus.

- **Adress-Pools**: In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll:



  - **Adress-Pool-Name**: Name des Adress-Pools
  - **Erste Adresse**: Erste Adresse des Pools, z. B. "2001:db8::1"
  - **Letzte Adresse**: Letzte Adresse des Pools, z. B. "2001:db8::9"
  - **Bevorzugte Gültigkeit**: 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'.
  - **Gültigkeitsdauer**: Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse 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.

  - **Präfix beziehen von**: Mit diesem Parameter können Sie den Netzwerk-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix "2001:db8::/64" zugewiesen,

dann können Sie beim Parameter **Erste Adresse** den Wert "::1" und bei **Letzte Adresse** den Wert "::9" eingeben. Zusammen mit dem vom Provider delegierten Präfix "2001:db8::/64" erhalten Clients dann Adressen aus dem Pool "2001:db8::1" bis "2001:db8::9".

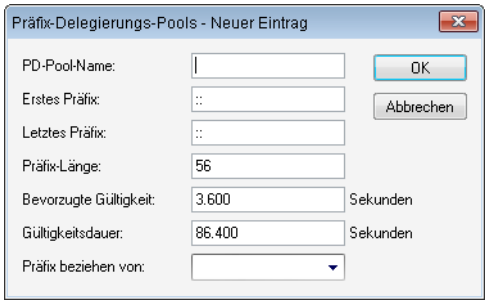
Ist das Provider-Präfix größer als "/64", z. B. "/48" oder "56", so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen.

Beispiel:

- Zugewiesenes Provider-Präfix: "2001:db8:abcd:aa::/56"
- "/64" als Präfix des logischen Netzwerks (Subnetzt-ID 1): "2001:db8:abcd:aa01::/64"
- Erste Adresse: "0:0:0:0001::1"
- Letzte Adresse: "0:0:0:0001::9"

Sie sollten diesen Mechanismus nur verwenden, wenn der Provider ein festes Präfix zuweist. Ansonsten kann es passieren, dass der Provider dem Router ein neues Präfix delegiert hat, aber der Client noch eine Adresse aus dem Pool mit dem alten Präfix besitzt. Dazu muss der Client seine Adresse beim Server aktualisieren.

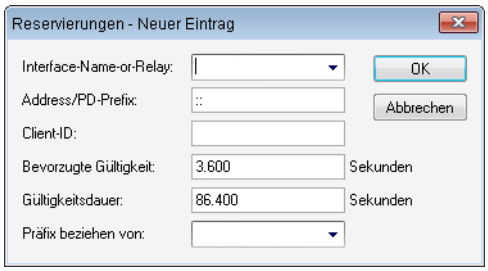
- **Präfix-Delegierungs-Pools**: In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll:



  - **PD-Pool-Name**: Name des PD-Pools
  - **Erstes Präfix**: Erstes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:1100::"
  - **Letztes Präfix**: Letztes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:FF00::"
  - **Präfix-Länge**: Länge der Präfixe im PD-Pool, z. B. "56" oder "60"
  - **Bevorzugte Gültigkeit**: 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'.
  - **Gültigkeitsdauer**: 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.
  - **Präfix beziehen von**: Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

- **Reservierungen**: Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, können Sie in dieser Tabelle pro Client eine Reservierung vornehmen:



  - **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.
  - **Adresse/PD-Präfix**: IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.
  - **Client-ID**: DHCPv6-Unique-Identifier (DUID) des Clients.

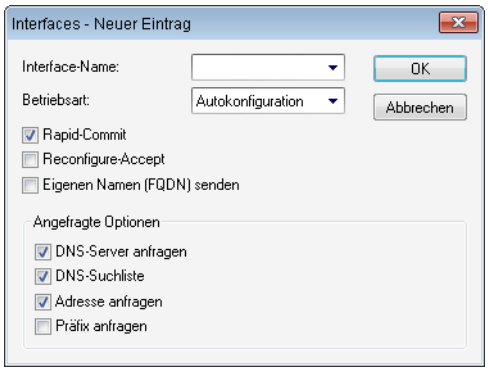
    Bei DHCPv6 lassen sich Clients nicht mehr wie bei DHCPv4 anhand ihrer MAC-Adresse, sondern anhand der DUID identifizieren. Die DUID lässt sich auf dem jeweiligen Client auslesen, unter Windows beispielsweise mit dem Kommandozeilen-Befehl `ipconfig /all`.
  - **Bevorzugte Gültigkeit**: Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.
  - **Gültigkeitsdauer**: Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse 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.
  - **Präfix beziehen von**: Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

DHCPv6-Client

Öffnen Sie mit den folgenden Schaltflächen die Tabellen zur Einstellung der jeweiligen Funktionen:

- **Interfaces**: Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Clients.



Normalerweise steuert bereits die Autokonfiguration das Client-Verhalten. Deshalb sind in dieser Tabelle nur Einträge nötig, falls Sie den Client 'Standalone' betreiben oder bestimmte Optionen, die von den Standard-Einstellungen abweichen, verwenden wollen.

  - **Interface-Name**: Name des Interfaces, auf dem der DHCPv6-Client arbeitet Dies können LAN-Interfaces oder WAN-Interfaces (Gegenstellen) sein, z. B. "INTRANET" oder "INTERNET".

- **Betriebsart**: Bestimmt, wie und ob das Gerät den Client aktiviert. Mögliche Werte sind:
  - "Autokonfiguration": 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. Dabei ignoriert das Gerät die Vorgaben aus Router-Advertisements.
  - "Nein:": Der DHCPv6-Client ist auf diesem Interface deaktiviert. Auch, wenn das Gerät Router-Advertisements empfängt, startet es den Client nicht.
- **Rapid-Comment**: 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.
- **Reconfigure-Accept**: Wenn der Client mit dem Server beim ersten Kontakt erfolgreich ein Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten 'Reconfigure Key' geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so vrewirft der Client diese Aufforderung zur Re-Konfiguration.

  Der Client unterstützt dazu das 'Reconfigure Key Authentication Protocol' nach RFC 3315 für die Optionen 'Renew' und 'Information-Request'.

  Für WAN-Interfaces ist diese Option standardmäßig aktiviert.
- **Eigenen Namen (FQDN) senden**: Der Client sendet den eigenen Hostnamen (Fully Qualified Domain Name). Diese Option ist standardmäßig auf LAN-Interfaces aktiv.
- **DNS-Server anfragen**: Legt fest, ob der Client beim DHCPv6-Server nach DNS-Servern fragen soll.

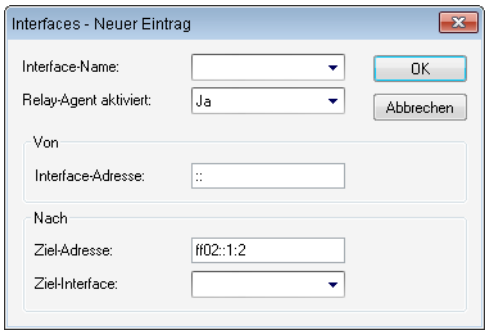
  Sie müssen diese Option aktivieren, damit das Gerät Informationen über einen DNS-Server erhält.
- **DNS-Suchliste**: Der Client fragt die DNS-Suchliste an.
- **Adresse anfragen**: Legt fest, ob der Client beim DHCPv6-Server nach einer IPv6-Adresse fragen soll.

  Diese Option sollten Sie nur dann aktivieren, wenn der DHCPv6-Server die Adressen über dieses Interface stateful, d. h. nicht durch 'SLAAC', verteilt.
- **Präfix anfragen**: Legt 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.

DHCPv6-Relay-Agent

Öffnen Sie mit den folgenden Schaltflächen die Tabellen zur Einstellung der jeweiligen Funktionen:

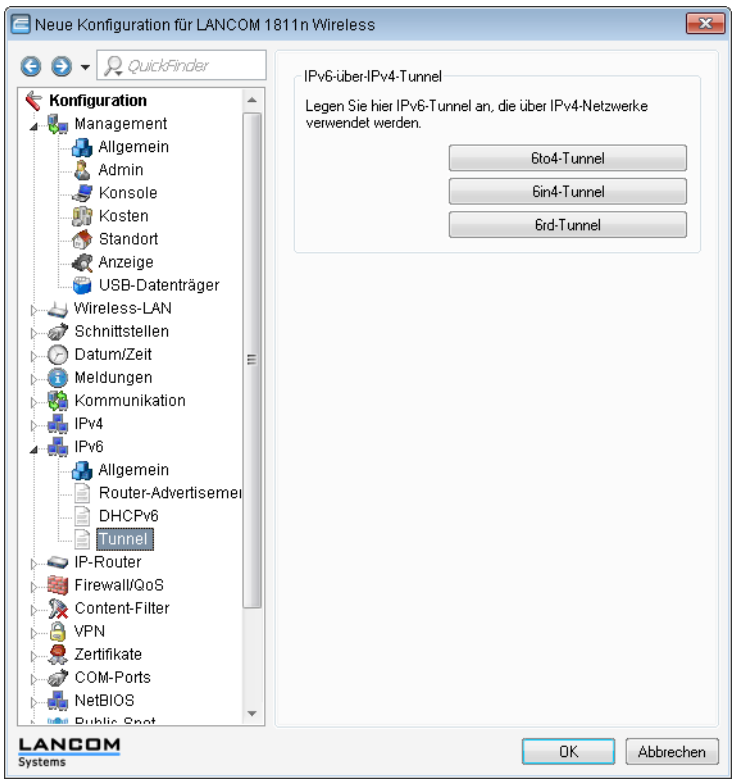
- **Interfaces**: Ein DHCPv6-Relay-Agent leitet DHCP-Nachrichten zwischen DHCPv6-Clients und DHCPv6-Servern weiter, die sich in unterschiedlichen Netzwerken befinden. Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Relay-Agents.



  - **Interface-Name**: Name des Interfaces, auf dem der Relay-Agent Anfragen von DHCPv6-Clients entgegennimmt, z. B. "INTRANET".
  - **Relay-Agent aktiviert**: Bestimmt, wie und ob das Gerät den Relay-Agent aktiviert. Mögliche Werte sind:
    - "Ja:" Relay-Agent ist aktiviert. Diese Option ist die Standardeinstellung.
    - "Nein:" Relay-Agent ist nicht aktiviert.
  - **Interface-Adresse**: 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.
  - **Ziel-Adresse**: 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.
  - **Ziel-Interface**: 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.

Tunnel

In der Konfiguration **Tunnel** legen Sie über 3 Schaltflächen IPv6-Tunnel an, die über IPv4-Netzwerke verwendet werden. Dies benötigen Sie, um den Zugang zum IPv6-Internet über eine IPv4-Verbindung herzustellen.



- **6to4-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6to4-Tunneln.

  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.

- **6in4-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6in4-Tunneln.

  6in4-Tunnel haben einen höheren administrativen Aufwand, stellen aber eine sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Möglichkeit ist auch für den professionellen Einsatz geeignet.

- **6rd-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6rd-Tunneln.

  6rd-Tunnel sind sowohl für Endanwender als auch für den professionellen Einsatz geeignet, da es nicht den Konfigurationsaufwand von 6in4-Tunneln erfordert, aber dennoch nicht die Sicherheitsrisiken von 6to4-Tunneln hat.

5.9.2 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Darüberhinaus können Sie festlegen, ob die Datenkommunikation über eine IPv4- oder eine IPv6-Verbindung erfolgen soll.

Zur Authentifizierung von Point-to-Point-Verbindungen im WAN wird häufig eines der Protokolle PAP, CHAP, MSCHAP oder MSCHAPv2 eingesetzt. Dabei haben die Protokolle untereinander eine „Hierarchie", d. h. MSCHAPv2 ist ein „höheres" Protokoll als, MSCHAP, CHAP und PAP (höhere Protokolle zeichnen sich durch höhere Sicherheit aus). Manche Einwahlrouter bei den Internetprovidern erlauben vordergründig die Authentifizierung über ein höheres Protokoll wie CHAP, unterstützen im weiteren Verlauf aber nur die Nutzung von PAP. Wenn im LANCOM das Protokoll für die Authentifizierung fest eingestellt ist, kommt die Verbindung ggf. nicht zustande, da kein gemeinsames Authentifizierungsprotokoll ausgehandelt werden kann.

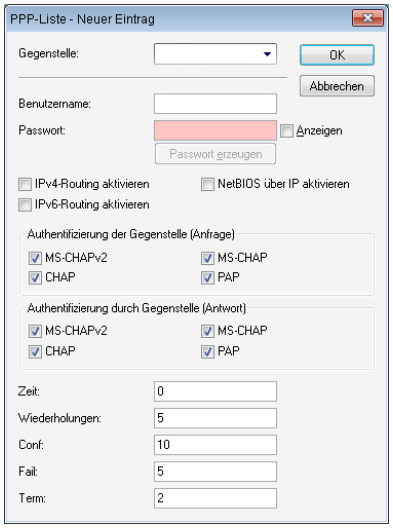
Prinzipiell ist es möglich, während der Verbindungsaushandlung eine erneute Authentifizierung durchzuführen und dafür ein anderes Protokoll auszuwählen, wenn dies zum Beispiel erst durch den Usernamen erkannt werden konnte. Diese erneute Aushandlung wird aber nicht in allen Szenarien unterstützt. Insbesondere bei der Einwahl über UMTS muss daher explizit vom Gerät der Wunsch von der Providerseite nach CHAP abgelehnt werden, um für eine Weiterleitung der Anfragen beim Provider PAP-Userdaten bereitstellen zu können.

Mit der flexiblen Einstellung der Authentifizierungsprotokolle im Gerät wird sichergestellt, dass die PPP-Verbindung wie gewünscht zustande kommt. Dazu können ein oder mehrere Protokolle definiert werden, die zur Authentifizierung von Gegenstellen im Gerät (eingehende Verbindungen) bzw. beim Login des Gerätes in andere Gegenstellen (ausgehende Verbindungen) akzeptiert werden.

- Das Gerät fordert beim Aufbau eingehender Verbindungen das niedrigste der zulässigen Protokolle, lässt aber je nach Möglichkeit der Gegenstelle auch eines der höheren (im Gerät aktivierten) Protokolle zu.
- Das Gerät bietet beim Aufbau ausgehender Verbindungen alle aktivierten Protokolle an, lässt aber auch nur eine Auswahl aus genau diesen Protokollen zu. Das Aushandeln eines der nicht aktivierten, evtl. höheren Protokolle ist nicht möglich.

Die Einstellung der PPP-Authentifizierungsprotokolle finden Sie in der PPP-Liste.

LANconfig: **Kommunikation** > **Protokolle** > **PPP-Liste**

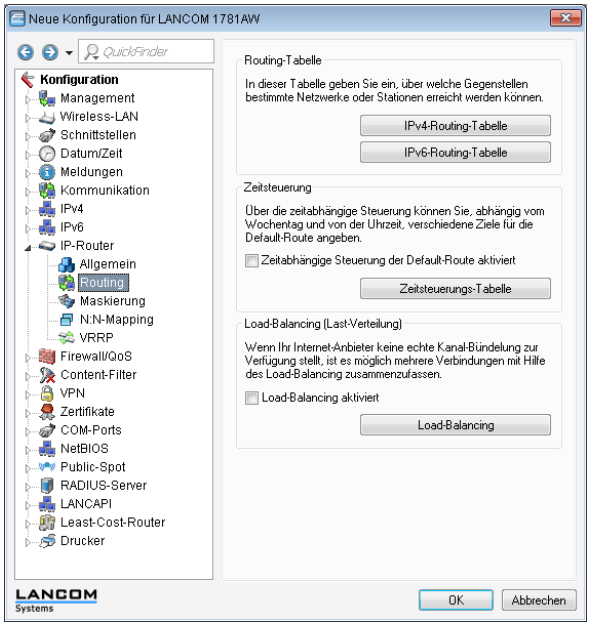


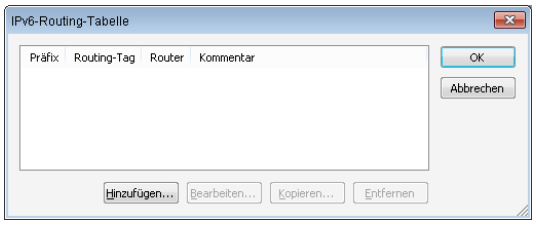
5.9.3 IP-Routing-Tabellen

Im Gegensatz zu früheren Versionen, in denen es im Konfigurationsmenü eine einzige IP-Routing-Tabelle gab, finden Sie nun an dieser Stelle die Möglichkeit, getrennte Routing-Tabellen für IPv4- und IPv6-Verbindungen zu konfigurieren.

Sie finden die neue Tabelle unter **IP-Router** > **Routing** > **IPv6-Routing-Tabelle**

Alle Einstellungen zu IPv4, die Sie zuvor in der Tabelle **IP-Routing-Tabelle** durchführen konnten, finden Sie nun in der Tabelle **IPv4-Routing-Tabelle**.





Die Tabelle enthält die Einträge für das Routing von Paketen mit IPv6-Adresse.

Präfix

Bestimmen Sie den Präfix des Netzbereiches, dessen Daten zur angegeben Gegenstelle geroutet werden sollen.

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.

Router

Wählen Sie hier die Gegenstelle für diese Route aus.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Die Eingabe eines Kommentars ist optional.

5.9.4 Getrennte Ansicht für IPv4- und IPv6-Firewall

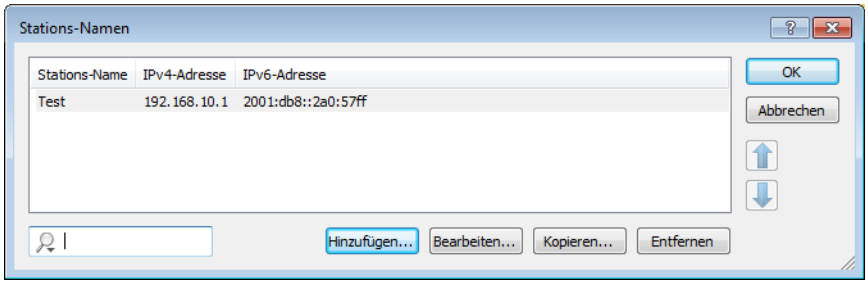
Ab LCOS-Version 8.80 können Sie die Regeln für die IPv4- und IPv6-Firewalls mit LANconfig jeweils in getrennten Ansichten konfigurieren.

Sie finden die jeweilige Konfigurationen nun unter **Firewall/QoS** > **IPv4-Regeln** bzw. **Firewall/QoS** > **IPv6-Regeln** .

5.9.5 IPv6 DNS-Hosts in DNS-Liste

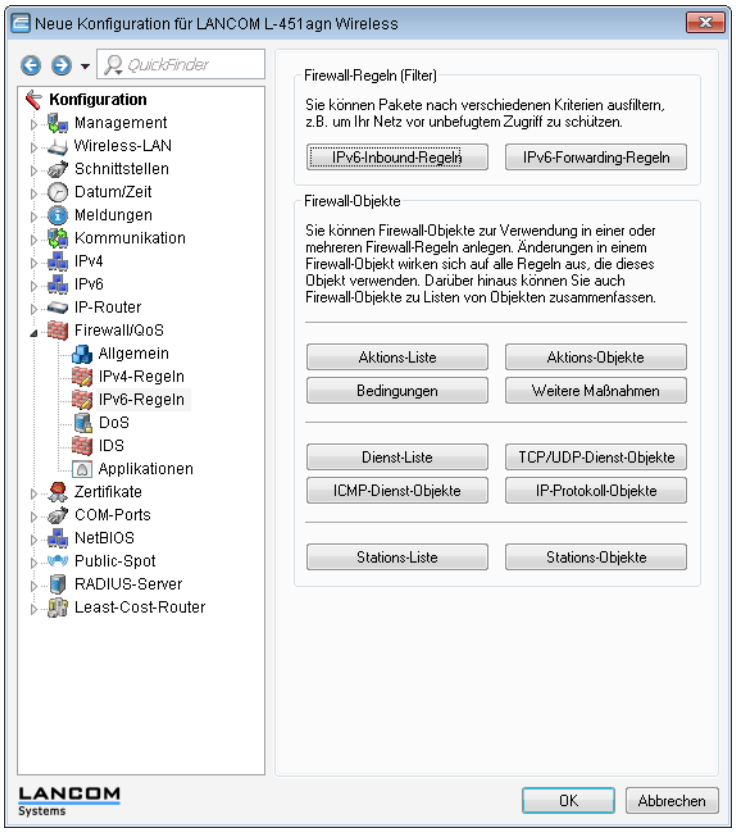
In der Liste der Stationsnamen erfassen Sie die IP-Adressen, mit denen der DNS-Servers Ihres Geräts die Anfragen nach einem Stationsnamen beantwortet. Zu jedem Stationsnamen definieren Sie dabei entweder die IPv4- oder die IPv6-Adresse, alternativ tragen Sie beide IP-Adressen ein.

Die Tabelle mit den definierten Stationsnamen und den zugeordneten IP-Adressen finden Sie in LANconfig unter **IPv4** > **DNS** > **Stations-Namen** .



5.9.6 Konfiguration der IPv6-Firewall-Regeln

Mit LANconfig können Sie die Firewall-Regeln unter **Firewall/QoS** > **IPv6-Regeln** festlegen.



Standardmäßig sind bereits einige Objekte und Listen für die wichtigsten Anwendungsfälle vorgegeben.

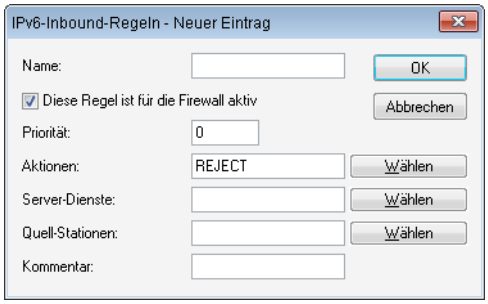
Sie können Listen oder Objekte nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

IPv6-Inbound-Regeln

Über die Schaltfläche **IPv6-Inbound-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den ankommenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

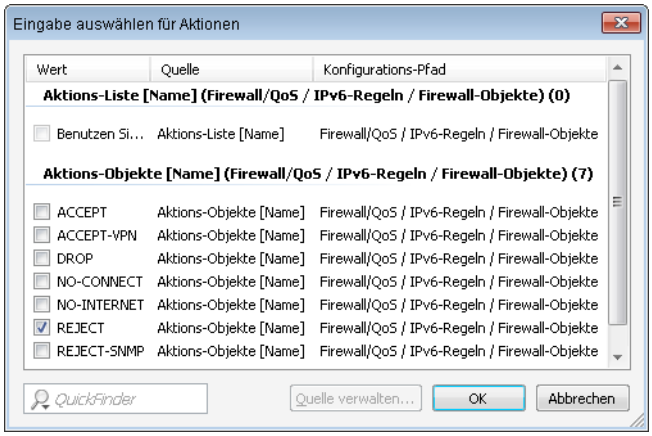
Aktiviert die Regel.

Priorität

Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Server-Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

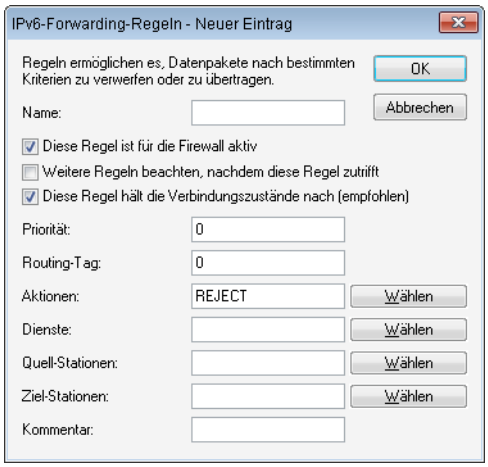
IPv6-Forwarding-Regeln

Über die Schaltfläche **IPv6-Inbound-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den weiterzuleitenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Um die Reihenfolge der Regeln zu ändern, markieren Sie in der Tabelle die entsprechende Regel und verschieben diese über einen Klick auf eine Pfeil-Schaltfläche nach oben oder unten in der Tabelle. Die Firewall wendet die Regel nacheinander von oben nach unten an.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

Aktiviert die Regel.

Weitere Regeln beachten, nachdem diese Regel zutrifft

Wenn Sie diese Option aktivieren, führt die Firewall zusätzlich die nachfolgenden Regeln der Liste aus. Das ist dann sinnvoll, wenn die Firewall z. B. zunächst eine Gruppen-Regel und anschließend jeweils eine Regel für die einzelnen Gruppen-Objekte anwenden soll.

Diese Regel hält die Verbindungszustände nach (empfohlen)

Aktivieren Sie diese Option, wenn die Regel die TCP-Verbindungszustände nachhalten soll.

Priorität

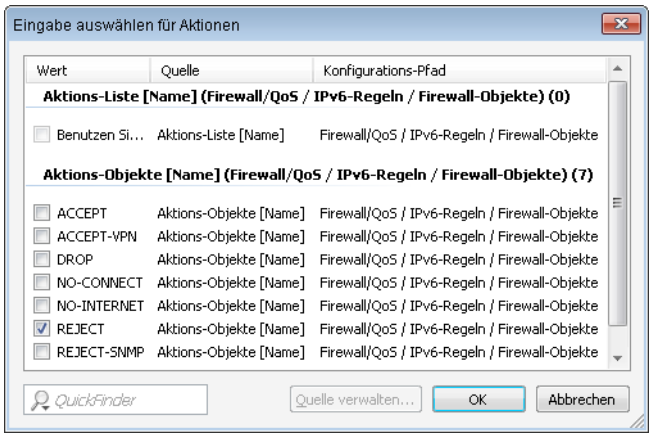
Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

Routing-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.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Server-Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Ziel-Stationen

Bestimmt die Ziel-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

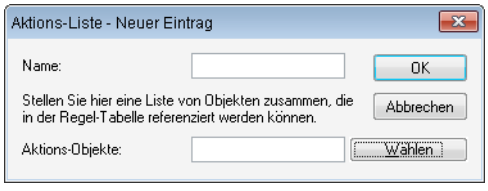
Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

Aktions-Liste

Über die Schaltfläche **Aktions-Liste** können Sie Aktionen zu Gruppen zusammenfassen. Die Aktionen definieren Sie vorher unter **Aktions-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



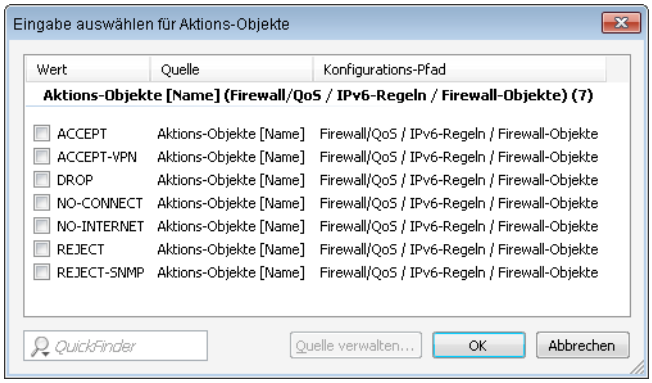
Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Aktions-Objekte

Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

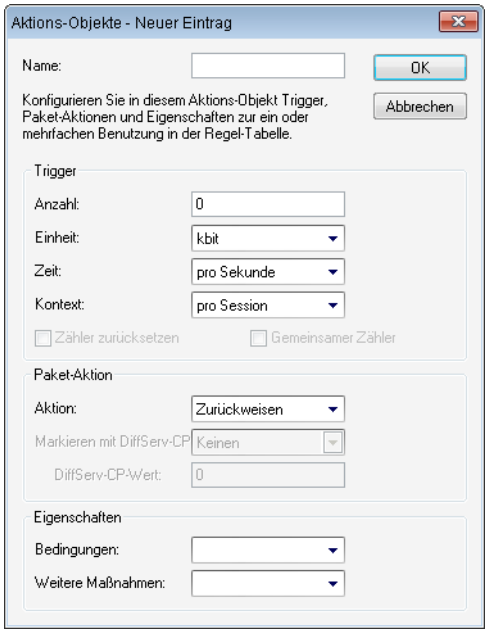


Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Aktions-Objekte

Über die Schaltfläche **Aktions-Objekte** definieren Sie Aktionen, die die IPv6-Firewall bei gültiger Filterregel ausführen kann.

Klicken Sie auf **Hinzufügen...**, um eine neue Aktion festzulegen.



Sie können die folgenden Eigenschaften des Objektes bestimmen:

Name

Bestimmt den Namen des Objektes.

Anzahl

Bestimmt das Limit, bei dessen Überschreiten die Firewall die Aktion ausführt.

Einheit

Bestimmt die Einheit des Limits. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zeit

Bestimmt, für welchen Messzeitraum die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Kontext

Bestimmt, in welchem Kontext die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zähler zurücksetzen

Wenn Sie diese Option aktivieren, setzt die Firewall den Zähler nach Ausführen der Aktion wieder zurück.

Diese Option können Sie nur aktivieren, wenn Sie unter **Zeit** den Wert "absolut" ausgewählt haben.

Gemeinsamer Zähler

Wenn Sie diese Option aktivieren, zählt die Firewall alle Aktions-Trigger gemeinsam.

Diese Option können Sie nur aktivieren, wenn Sie unter **Kontext** die Werte "pro Station" oder "global" ausgewählt haben.

Aktion

Bestimmt die Aktion, die die Firewall bei Erreichen des Limits ausführt.

Die folgende Auswahl ist möglich:

- **Zurückweisen**: Die Firewall weist das Datenpaket zurück und sendet einen entsprechenden Hinweis an den Absender.
- **Verwerfen**: Die Firewall verwirft das Datenpaket ohne Benachrichtigung.
- **Übertragen**: Die Firewall akzeptiert das Datenpaket.

Markieren mit DiffServ-CP

Bestimmt die Priorität der Datenpakete (Differentiated Services, DiffServ), mit der die Firewall die Datenpakete übertragen soll.

Diese Option können Sie nur festlegen, wenn Sie unter **Aktion** den Wert "Übertragen" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

Diese Option können Sie nur festlegen, wenn Sie unter **Markieren mit DiffServ-CP** den Wert "Wert" ausgewählt haben.

Bedingungen

Bestimmt, welche Bedingung zusätzlich zur Ausführung der Aktion erfüllt sein müssen. Die Bedingungen können Sie unter **Bedingungen** definieren.

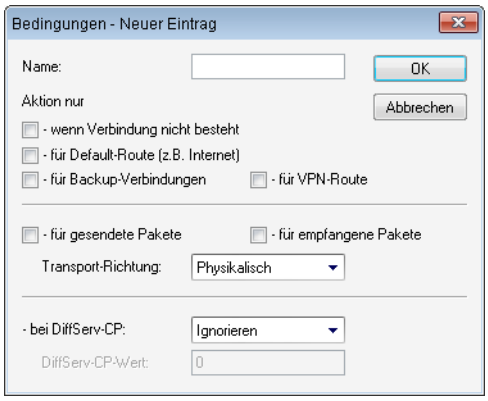
Weitere Maßnahmen

Bestimmt, welche Trigger-Aktionen die Firewall zusätzlich zur Filterung der Datenpakete starten soll. Die Trigger-Aktionen können Sie unter **Weitere Maßnahmen** definieren.

Bedingungen

Über die Schaltfläche **Bedingungen** definieren Sie Bedingungen, die zum Anwenden der Forwarding- und Inbound-Regeln erfüllt sein müssen.

Klicken Sie auf **Hinzufügen...**, um eine neue Bedingung festzulegen.



Sie können die folgenden Eigenschaften der Bedingung bestimmen:

Name

Bestimmt den Namen des Objektes.

Aktion nur - wenn Verbindung nicht besteht

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn keine Verbindung besteht.

Aktion nur - für Default-Route (z. B. Internet)

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn die Verbindung über die Default-Route besteht.

Aktion nur - für Backup-Verbindungen

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine Backup-Verbindung handelt.

Aktion nur - für VPN-Route

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine VPN-Verbindung handelt.

Aktion nur - für gesendete Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um gesendete Datenpakete handelt.

Aktion nur - für empfangene Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um empfangene Datenpakete handelt.

Transport-Richtung

Bestimmt, ob die Transportrichtung sich auf den logischen Verbindungsaufbau oder die physikalische Datenübertragung über das jeweilige Interface bezieht.

Aktion nur - bei DiffServ-CP

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”.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

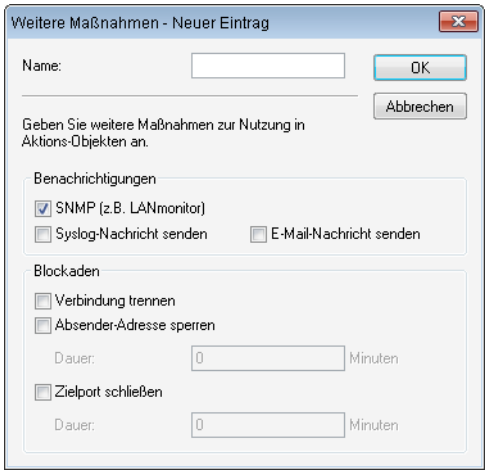
Geben Sie hier einen Wert ein, wenn Sie im Feld **- bei DiffServ-CP** die Option "Wert" ausgewählt haben.

Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Weitere Maßnahmen

Über die Schaltfläche **Weitere Maßnahmen** definieren Sie weitere Maßnahmen, die die Firewall nach Anwenden der Forwarding- und Inbound-Regeln ausführen kann.

Klicken Sie auf **Hinzufügen...**, um eine neue Maßnahme festzulegen.



Sie können die folgenden Eigenschaften der Trigger-Aktion bestimmen:

Name

Bestimmt den Namen des Objektes.

SNMP (z. B. LANmonitor)

Aktivieren Sie diese Option, wenn die Firewall eine Benachrichtigung über SNMP versenden soll. Diese Benachrichtigung können Sie z. B. mit LANmonitor empfangen.

Syslog-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine Syslog-Nachricht versenden soll.

Weitere Informationen zu SYSLOG finden Sie im Referenzhandbuch im Kapitel "Diagnose" im Abschnitt "SYSLOG".

E-Mail-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine E-Mail-Nachricht versenden soll.

Wenn Sie eine Benachrichtigung per E-Mail erhalten möchten, müssen Sie unter **Firewall/QoS** > **Allgemein** > **Administrator E-Mail** eine entsprechende E-Mail-Adresse angeben.

Verbindung trennen

Aktivieren Sie diese Option, wenn die Firewall die Verbindung trennen soll.

Absender-Adresse sperren

Aktivieren Sie diese Option, wenn die Firewall die Absender-Adresse sperren soll. Die Firewall trägt die gesperrte IP-Adresse, die Sperrzeit sowie die zugrunde liegende Regel in die **Hostsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

Dauer

Wenn die Firewall den Absender sperren soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert "0" deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Zielport schließen

Aktivieren Sie diese Option, wenn die Firewall den Ziel-Port sperren soll. 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.

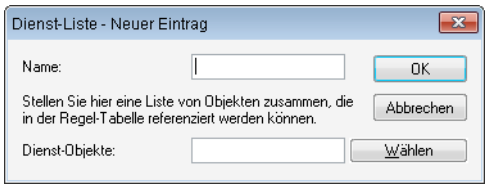
Dauer

Wenn die Firewall den Zielport schließen soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert "0" deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Dienst-Liste

Über die Schaltfläche **Dienst-Liste** können Sie Dienste zu Gruppen zusammenfassen. Die Dienste definieren Sie vorher unter **TCP/UDP-Dienst-Objekte**, **ICMP-Dienst-Objekte** und **IP-Protokoll-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Dienst-Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Dienst-Objekte

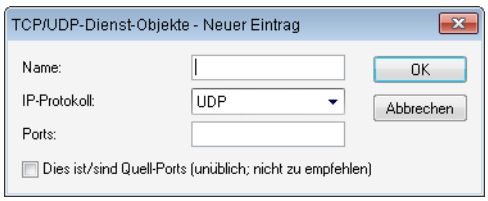
Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

TCP/UDP-Dienst-Objekte

Über die Schaltfläche **TCP/UDP-Dienst-Objekte** definieren Sie TCP/UDP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen...**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

IP-Protokoll

Bestimmt das Protokoll des Dienstes

Ports

Bestimmt 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*.

Dies ist/sind Quell-Ports

Bestimmt, ob es sich bei den angegebenen Ports um Quell-Ports handelt.

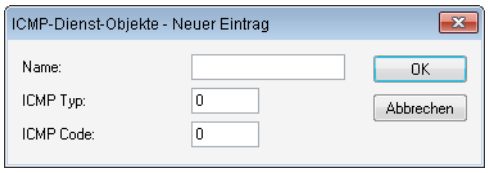
In bestimmten Szenarien kann es sinnvoll sein, einen Quell-Port anzugeben. Normalerweise ist es aber unüblich, so dass die Auswahl "nein" zu empfehlen ist.

ICMP-Dienst-Objekte

Über die Schaltfläche **ICMP-Dienst-Objekte** definieren Sie ICMP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen...**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

ICMP Typ

Bestimmt den Typ des ICMP-Dienstes.

ICMP Code

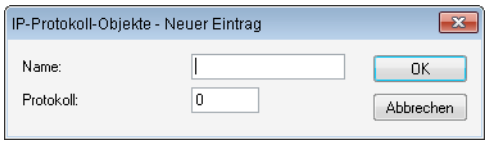
Bestimmt den Code des ICMP-Dienstes.

IP-Protokoll-Objekte

Über die Schaltfläche **IP-Protokoll-Objekte** definieren Sie Internet-Protokoll-Objekte, die die IPv6-Firewall für Filterregeln verwenden kann.

Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen...**, um ein neues Objekt festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

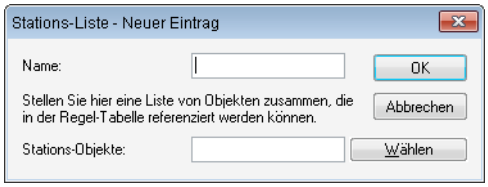
Protokoll

Bestimmt die Protokoll-Nummer.

Stations-Liste

Über die Schaltfläche **Stations-Liste** können Sie Stationen zu Gruppen zusammenfassen. Die Stationen definieren Sie vorher unter **Stations-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Stations-Objekte

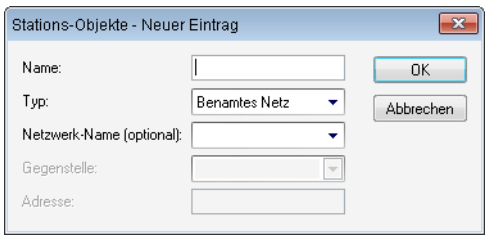
Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Stations-Objekte

Über die Schaltfläche **Stations-Objekte** definieren Sie Stationen, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen...**, um ein neues Objekt anzulegen.



Sie können die folgenden Eigenschaften der Objekte festlegen:

Name

Bestimmt den Namen des Objektes.

Typ

Bestimmt den Stationstyp.

Netzwerk-Name

Geben Sie hier den Namen des Netzwerkes ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Die Angabe eines Netzwerk-Namens ist optional.

Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Adresse

Geben Sie hier die Adresse der Gegenstelle ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

5.10 Tutorials

5.10.1 Einrichtung eines IPv6-Internetzugangs

Sie haben die Möglichkeit einen Zugang zu einem IPv6-Netz einrichten, wenn

- Sie ein IPv6-fähiges Gerät besitzen,
- eine Tunneltechnologie benutzen und
- Ihr Provider ein natives IPv6-Netz unterstützt oder Sie einen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

IPv6-Zugang über den Setup-Assistenten von LANconfig

Der Setup-Assistent unterstützt Sie bei der Konfiguration des IPv6-Zugangs für Ihre Geräte.

Folgende Optionen stehen Ihnen im Assistenten zur Verfügung:

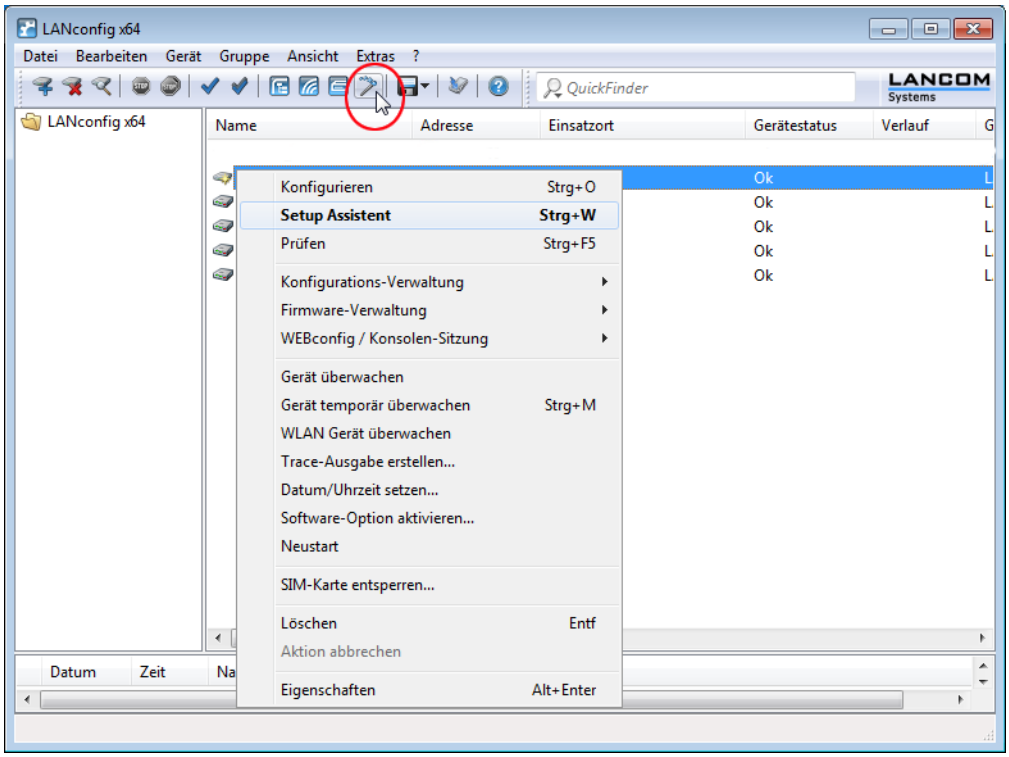
- *Den IPv6-Zugang bei einem neuen, unkonfigurierten Gerät einrichten.*
- *Bei einem bestehenden Gerät einen IPv6-Zugang zusätzlich zum bestehenden IPv4-Zugang einrichten.*

Setup-Assistent - IPv6 bei einem neuen Gerät einrichten

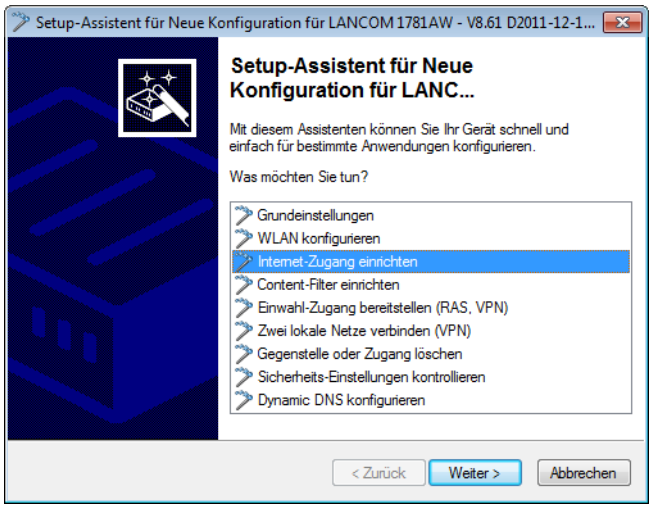
Wenn Sie ein neues Gerät angeschlossen, aber noch nicht konfiguriert haben, haben Sie die Möglichkeit per Setup-Assistent IPv4- und IPv6-Verbindungen herzustellen.

Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie nun entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste



2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**.

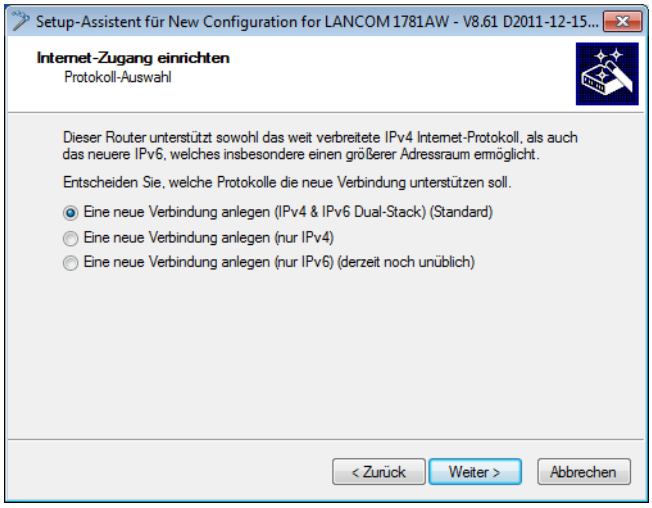


3. Sie haben die Möglichkeit, zwischen den folgenden Optionen zu wählen:

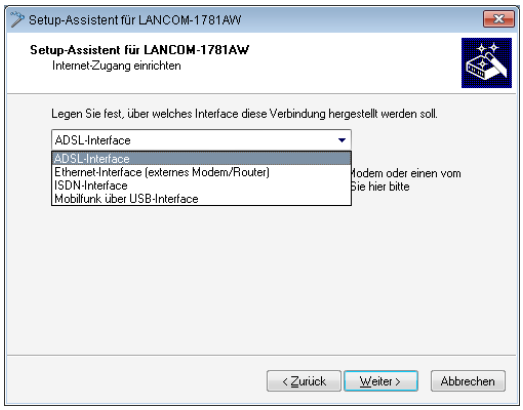
   - Eine Dual-Stack-Verbindung herstellen. Diese ist IPv4- und IPv6-tauglich und daher derzeit für ein neues Gerät die empfohlene Option.

- Eine reine IPv4-Verbindung herstellen.
- Eine reine IPv6-Verbindung herstellen.

Nachfolgend führen wir Sie durch die Einrichtung einer Dual-Stack-Verbindung. Aktivieren Sie die entsprechende Auswahl.



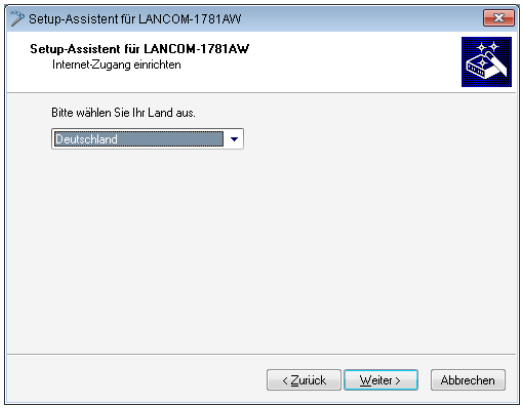
4. Bestimmen Sie das Interface, über das Sie die Verbindung herstellen möchten.



Sie haben folgende Einträge zur Auswahl:

- ADSL-Interface
- Ethernet-Interface (externes Modem/Router)
- ISDN-Interface
- Mobilfunk über USB-Interface

5. Wählen Sie aus der Liste Ihr Land aus.

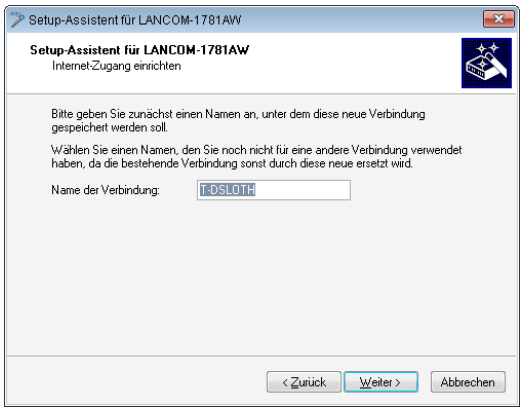


6. Wählen Sie Ihren Internet-Provider aus.

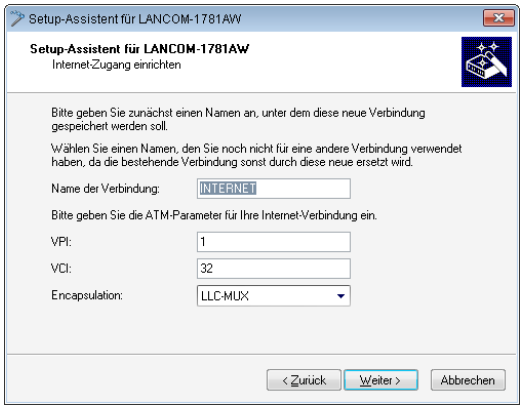
   Sie haben folgende Einträge zur Auswahl:

   - Eine Auswahl der wichtigsten Internet-Provider
   - Alternative Internet-Anbieter über T-DSL
   - Internet-Zugang über PPP over ATM (PPPoA)
   - Internet-Zugang über PPP over Ethernet (PPPoE, PPPoEoA)
   - Internet-Zugang über Plain IP (IPoA)
   - Internet-Zugang über Plain Ethernet (IPoE, IPoEoA)

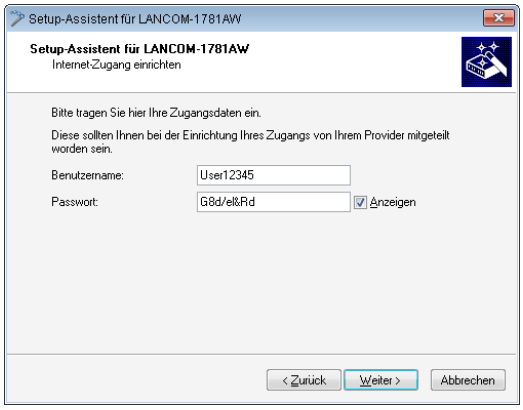
7. Definieren Sie einen Namen für diese Verbindung.



Wenn Sie den Internet-Zugang alternativ z. B. über eine PPPoE-Verbindung einrichten wollen, geben Sie zusätzlich noch die entsprechenden ATM-Parameter ein.

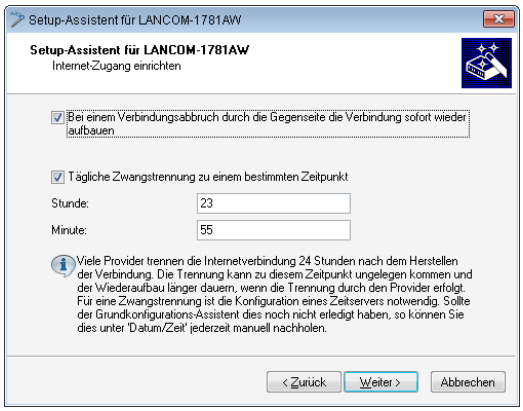


8. Tragen Sie die Zugangsdaten ein, die Ihnen Ihr Provider bei der Errichtung Ihres Internetzugangs mitgeteilt hat.

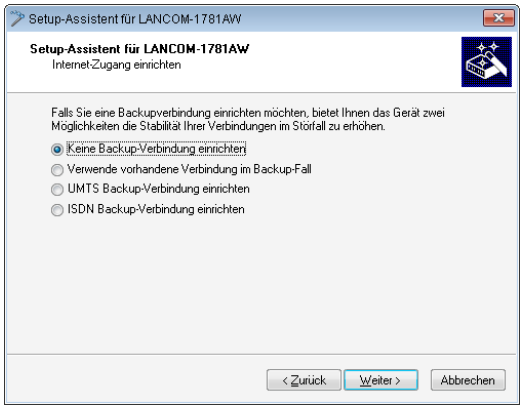


Je nach Provider können sich Art und Anzahl der Felder unterscheiden.

9. Legen Sie fest, wie sich das Gerät bei einem Verbindungsabbruch verhalten soll. Außerdem können Sie angeben, ob und wann das Gerät die Internetverbindung zwangsweise trennen soll.



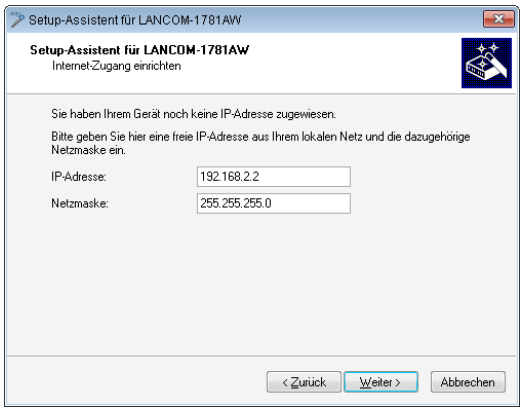
10. Definieren Sie die Art der Backup-Verbindung im Fall einer Verbindungsstörung.



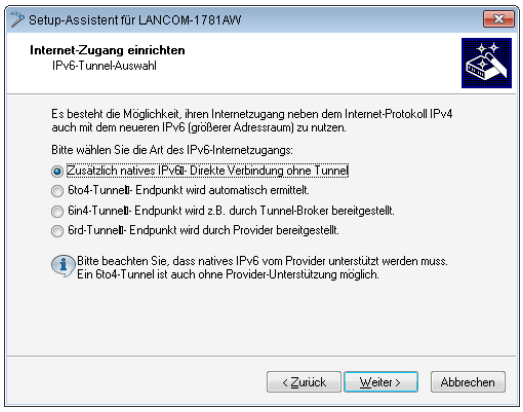
Sie haben folgende Optionen zur Auswahl:

- Keine Backup-Verbindung verwenden: Sie überspringen die Konfiguration einer Backup-Verbindung.
- Die bereits konfigurierte Verbindung im Backup-Fall verwenden: Wählen Sie im Folgedialog aus einer Liste ein bereits konfigurierte Verbindung aus.
- Eine Backup-Verbindung über UMTS einrichten: Richten Sie im Folgedialog eine neue UMTS-Verbindung ein. Sie benötigen dafür die Zugangsdaten Ihres UMTS-Providers.
- Eine Backup-Verbindung über ISDN einrichten: Richten Sie im Folgedialog eine neue ISDN-Verbindung. Sie benötigen dazu die Zugangsdaten Ihres ISDN-Providers.

11. Falls Ihr Gerät noch keine IP-Adresse besitzt, tragen Sie eine neue IP-Adresse sowie die entsprechende Netzmaske ein.



12. Wählen Sie die Art des IPv6-Internet-Zugangs.

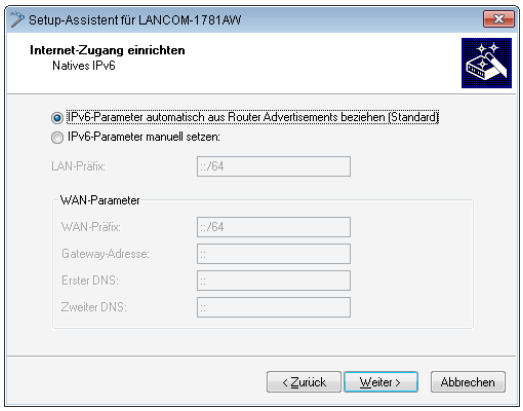


Sie haben folgende Optionen zur Auswahl:

- **Zusätzlich natives IPv6**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
- **6to4-Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-Tunnels.
- **6in4-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6in4-Tunnel.
- **6rd-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6rd-Tunnel.

Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

13. Übernehmen Sie die Default-Einstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



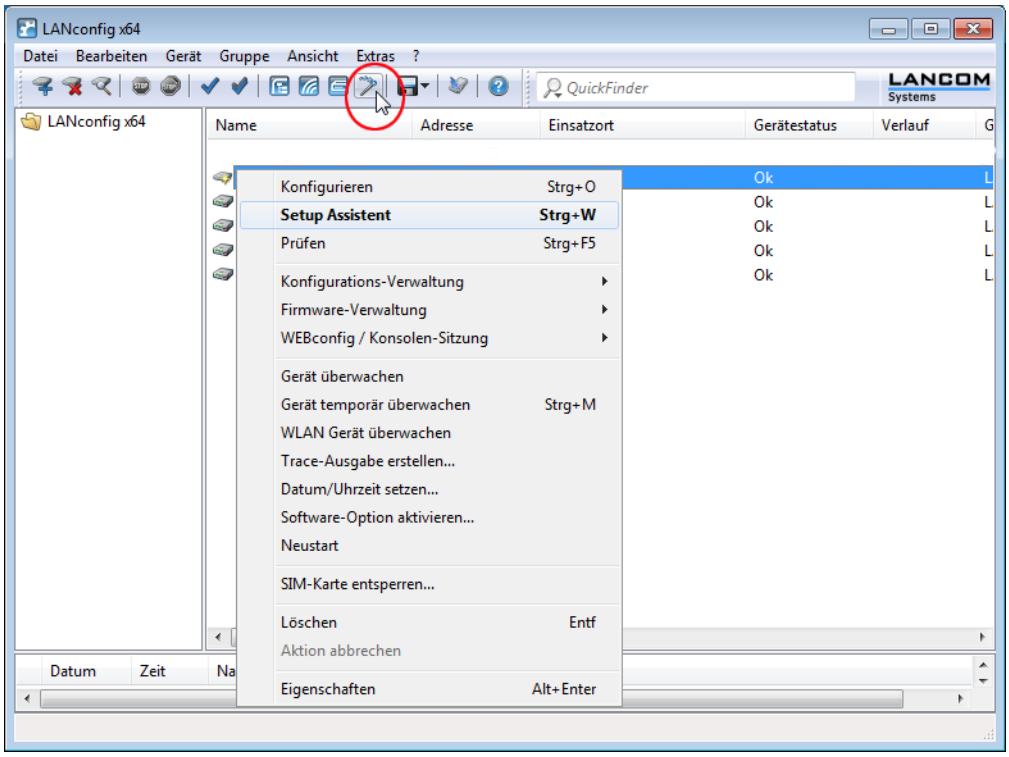
14. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

Setup-Assistent - IPv6 bei einem bestehenden Gerät einrichten

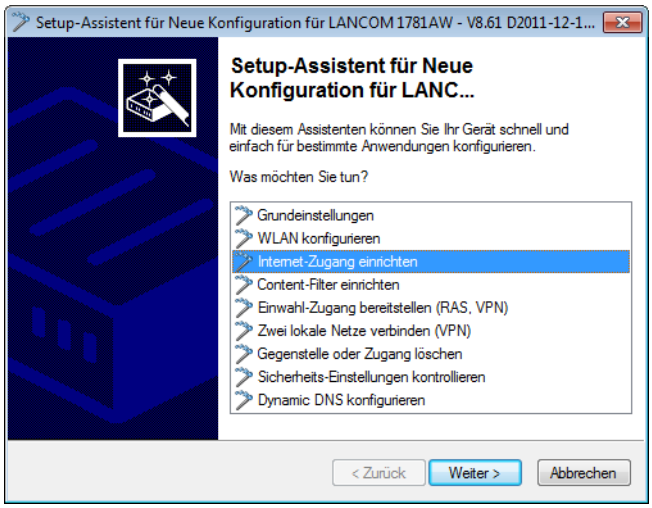
Wenn Sie ein Gerät für IPv4 konfiguriert haben und zusätzliche eine IPv6-Verbindung einrichten wollen, haben Sie die Möglichkeit, diese IPv6-Verbindungen über den Setup-Assistenten herzustellen.

Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

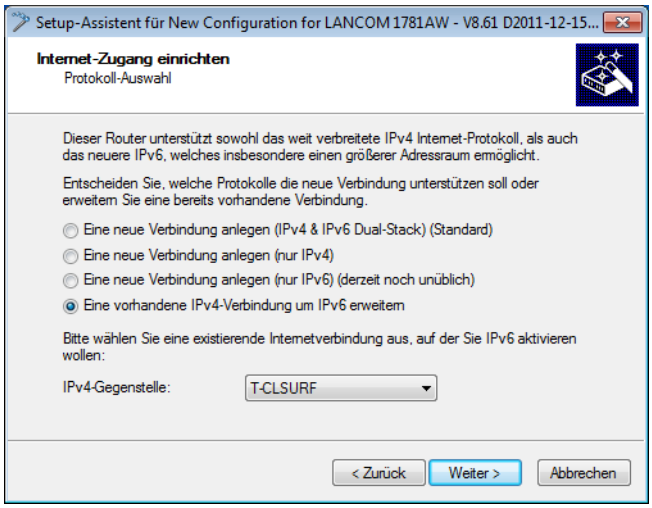
1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste



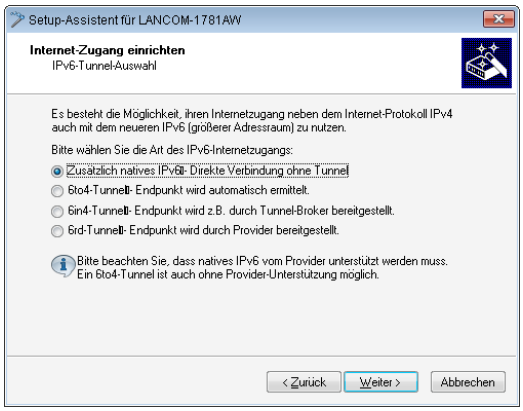
2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**. Klicken Sie anschließend auf **Weiter**.



3. Da ihr Gerät bereits für IPv4 beherrscht, bietet der Setup-Assistent Ihnen die Möglichkeit, diese existierende Einstellung um IPv6 zu erweitern. Wählen Sie diese Option und klicken Sie anschließend auf **Weiter**.



4. Wählen Sie die Art des IPv6-Internet-Zugangs.

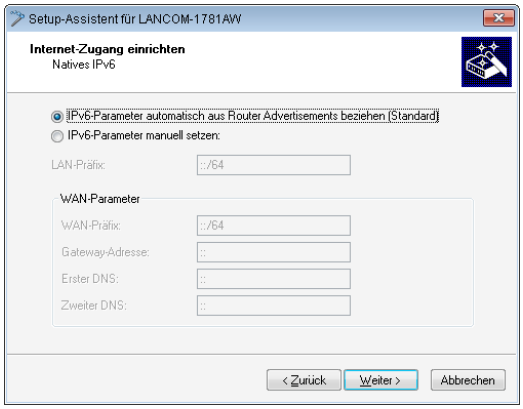


Sie haben folgende Optionen zur Auswahl:

- **Zusätzlich natives IPv6**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
- **6to4-Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-Tunnels.
- **6in4-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6in4-Tunnel.
- **6rd-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6rd-Tunnel.

Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

5. Übernehmen Sie die Default-Einstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



6. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

5.10.2 Einrichtung eines 6to4-Tunnels

Die Verwendung eines 6to4-Tunnels bietet sich an, wenn

- Ihr Gerät IPv6-fähig ist und Sie auf IPv6-Dienste zugreifen möchten,
- Ihr Provider jedoch kein natives IPv6-Netz unterstützt und
- Sie keinen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

Bei der Verwendung eines 6to4-Tunnels erhält das Gerät keine IPv6-Adresse bzw. kein IPv6-Präfix des Providers, da dieser keine IPv6-Funktionalität anbietet.

Das Gerät berechnet ein eigenes, eindeutiges Präfix aus "2002::/16" und der Hexadezimal-Darstellung der eigenen, öffentlichen IPv4-Adresse, die der Provider liefert. Diese Anwendung funktioniert daher ausschließlich dann, wenn das Gerät tatsächlich eine öffentliche IPv4-Adresse besitzt. Das Gerät erhält z. B. keine öffentlich gültige IPv4-Adresse, sondern nur eine IPv4-Adresse aus einem privaten Adressbereich, wenn es einen Internetzugang über UMTS herstellt und der Provider dafür nur private IP-Adressen zur Verfügung stellt, oder wenn das Gerät selbst nicht den Zugang zum Internet herstellt, sondern "hinter" einem anderen Router steht.

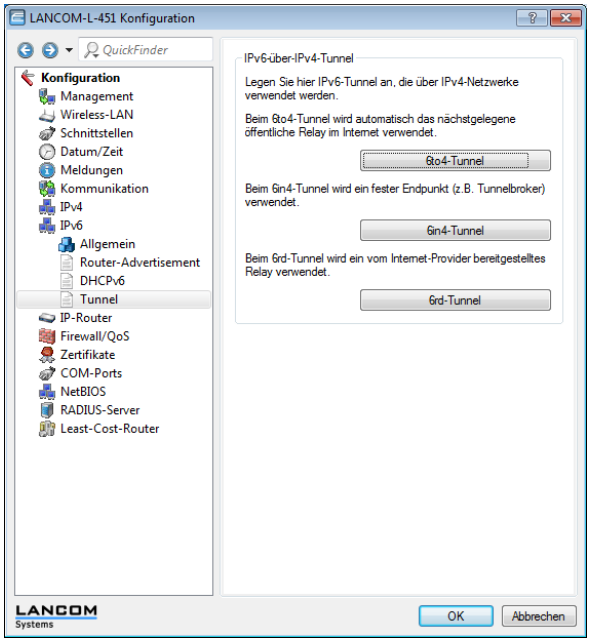
Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Geräts hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne das Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen 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.

Verwendung von LANconfig

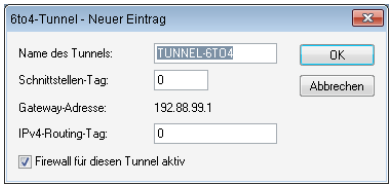
Um einen 6to4-Tunnel über LANconfig einzurichten, gehen Sie wie folgt vor:

1. Rufen Sie LANconfig z. B. aus der Windows-Startleiste auf mit **Start** > **Programme** > **LANCOM** > **LANconfig** auf. LANconfig sucht nun automatisch im lokalen Netz nach Geräten.
2. Wählen Sie das Gerät aus, für das Sie den 6to4-Tunnel einrichten wollen. Markieren Sie es mit einem Links-Klick und starten Sie die Konfiguration in der Menüleiste über **Gerät** > **Konfigurieren** .

3. Wechseln Sie im Konfigurationsdialog in die Ansicht **IPv6** > **Tunnel** und klicken Sie auf **6to4-Tunnel**.



4. Klicken Sie auf **Hinzufügen**, um einen neuen 6to4-Tunnel anzulegen.



5. Vergeben Sie den Namen des 6to4-Tunnels.
6. Tragen Sie als **Schnittstellen-Tag** einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, welche dieses 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.

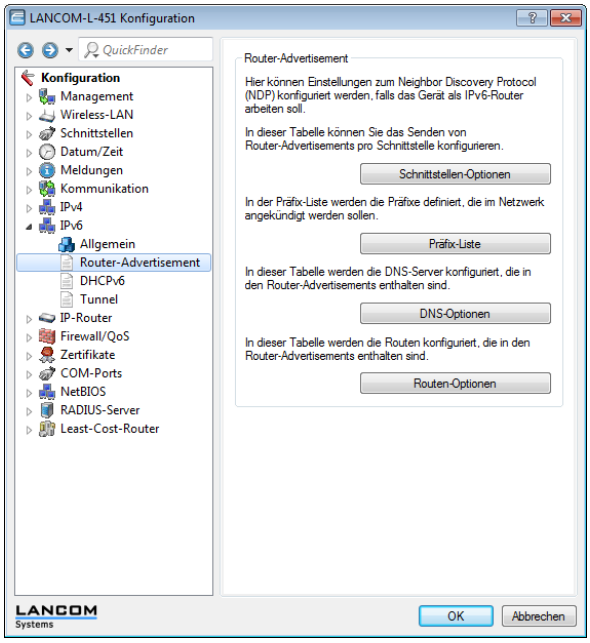
   In LCOS 8.61 Public Beta 2 noch ohne Funktion!

7. Die **Gateway-Adresse** ist per Default vorbelegt mit der Anycast-Adresse "192.88.99.1". Diese Adresse können Sie nur über WEBconfig bzw. Telnet ändern.
8. 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.
9. Als Default-Wert ist die Firewall dieses Tunnels aktiv.

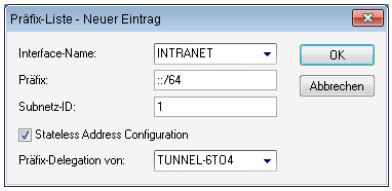
   Wenn Sie die globale Firewall deaktivieren, deaktivieren Sie ebenfalls die Firewall für den Tunnel.

10. Übernehmen Sie Ihre Eingaben mit **OK**.

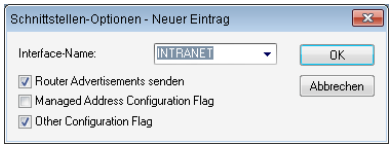
11. Wechseln Sie in das Verzeichnis **IPv6** > **Router-Advertisements** .



12. Öffnen Sie die **Präfix-Liste** und klicken Sie auf **Hinzufügen**.

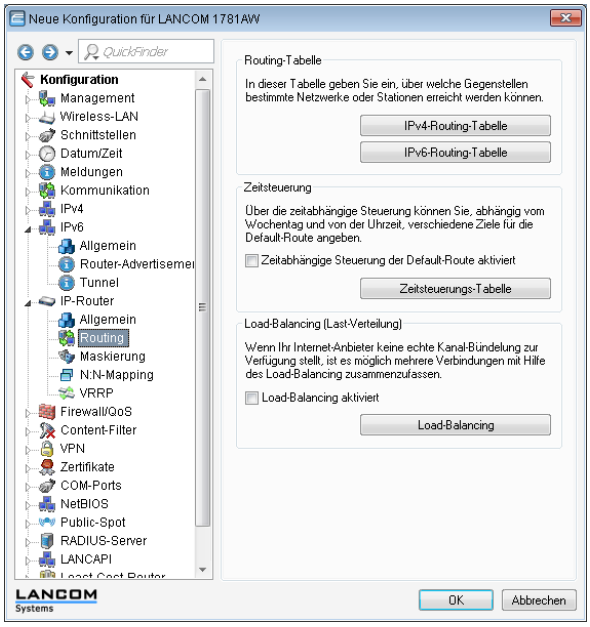


13. Vergeben Sie einen Namen für das Interface, das den 6to4-Tunnel verwenden wird, z. B. "INTRANET".
14. Bestimmen Sie als **Präfix** den Wert "::/64", um das vom Provider vergebene Präfix automatisch und in voller Länge zu übernehmen.
15. Übernehmen Sie die Default-Wert "1" für die **Subnetz-ID**.
16. Übernehmen Sie die aktivierte Option **Stateless Address Configuration**.
17. Übernehmen Sie im Feld **Präfix-Delegation von** aus der Liste den Namen des Tunnels, den Sie zuvor definiert haben, im Beispiel oben "TUNNEL-6TO4".
18. Übernehmen Sie Ihre Eingaben mit **OK**.
19. Im Verzeichnis **IPv6** > **Router-Advertisements** öffnen Sie die **Schnittstellen-Optionen** und klicken auf **Bearbeiten** für den Eintrag INTRANET.
20. Aktivieren Sie die Checkbox für **Router Advertisements senden**.

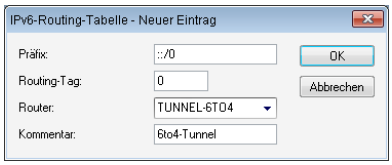


21. Übernehmen Sie alle weiteren Default-Werte unverändert.
22. Speichern Sie die Eingaben mit **OK**.

23. Wechseln Sie in das Verzeichnis **IP-Router** > **Routing** .



24. Öffnen Sie die **IPv6-Routing-Tabelle** und klicken auf **Hinzufügen**.



25. Vergeben Sie als **Präfix** den Wert "::/0".

26. Übernehmen Sie für **Routing-Tag** den Default-Wert "0".

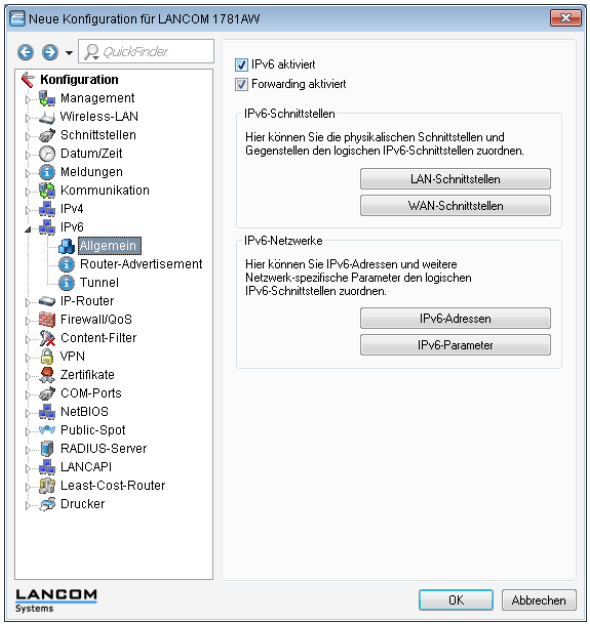
In LCOS 8.61 Public Beta 2 noch ohne Funktion!

27. Im Feld **Router** wählen Sie aus der Liste den Namen des Tunnels aus, den Sie definiert haben, im Beispiel oben "TUNNEL-6TO4".

28. Vergeben Sie einen aussagekräftigen **Kommentar** für diesen Eintrag.

29. Speichern Sie die Eingaben mit **OK**.

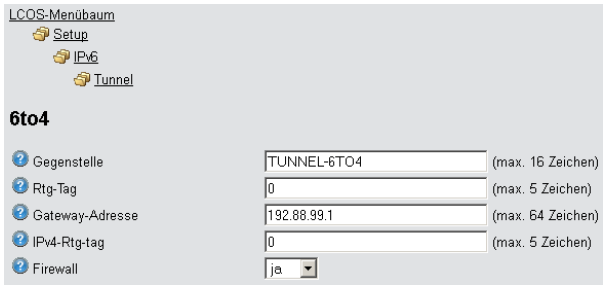
30. Wechseln Sie in das Verzeichnis **IPv6** > **Allgemein** und aktivieren Sie den IPv6-Stack.



Verwendung von WEBconfig

Um einen 6to4-Tunnel über WEBconfig einzurichten, gehen Sie wie folgt vor:

1. Geben Sie in der Adresszeile Ihres Browsers die Adresse des Gerätes ein, für das Sie den 6to4-Tunnel einrichten wollen.
2. Wechseln Sie in das Verzeichnis **LCOS-Menübaum** > **Setup** > **IPv6** > **Tunnel** > **6to4** und klicken Sie auf **Hinzufügen**.



3. Vergeben Sie den Namen der Gegenstelle, z. B. "TUNNEL-6TO4".
4. Das **Routing-Tag** lassen Sie unverändert auf dem Default-Wert "0".

   In LCOS 8.61 Public Beta 2 noch ohne Funktion!

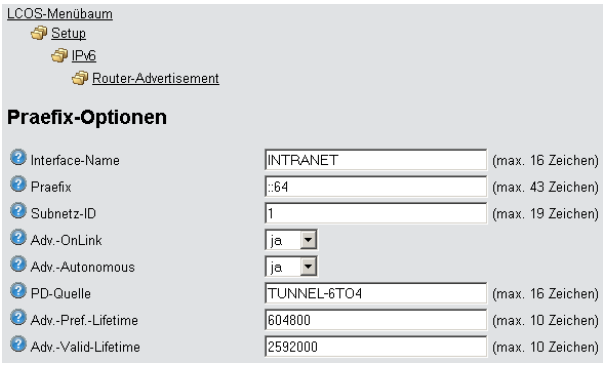
5. Als **Gateway-Adresse** können Sie den Default-Wert "192.88.99.1" übernehmen. Das ist die Standard-Anycast-Adresse für 6to4-Relays, mit denen sich Ihr Gerät verbindet.

   Diese Adresse ist der Grund dafür, dass ein 6to4-Tunnel instabil und unsicher ist. Weder ist sichergestellt, dass überhaupt ein 6to4-Relay verfügbar ist, noch können Sie jedem verfügbaren 6to4-Relay vertrauen. Es gibt keine Garantie dafür, dass das verbundene Relay keine Aufzeichnung Ihres Datenverkehrs vornimmt.

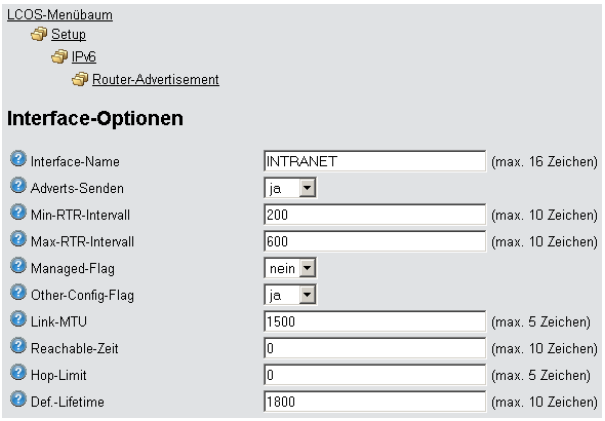
6. Übernehmen Sie im Feld **IPv4-Rtg-tag** den Default-Wert "0"
7. Aktivieren Sie die **Firewall** für diesen Tunnel.

   Wenn Sie die globale Firewall deaktivieren, deaktivieren Sie ebenfalls die Firewall für den Tunnel.

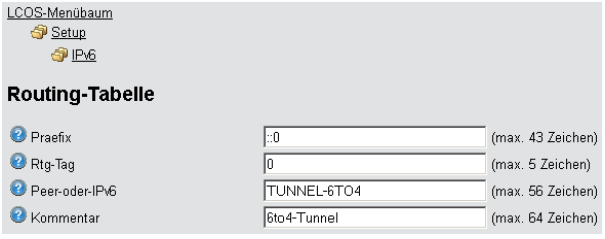
8. Speichern Sie die Eingaben mit **Setzen**.
9. Wechseln Sie in das Verzeichnis **LCOS-Menübaum** > **Setup** > **IPv6** > **Router-Advertisement** , öffnen Sie die Tabelle **Praefix-Optionen** und klicken Sie auf **Hinzufügen**.



10. Vergeben Sie einen Namen für das Interface, das den 6to4-Tunnel verwendet, z. B. "INTRANET".
11. Bestimmen Sie als **Präfix** den Wert "::/64", um das vom Provider vergebene Präfix automatisch und in voller Länge zu übernehmen.
12. Übernehmen Sie den Default-Wert "1" für die **Subnetz-ID**.
13. Vergeben Sie als **PD-Quelle** den Namen der Gegenstelle, den Sie zuvor definiert haben, im Beispiel oben "TUNNEL-6TO4".
14. Speichern Sie die Eingaben mit **Setzen**.
15. Wechseln Sie in das Verzeichnis **LCOS-Menübaum** > **Setup** > **IPv6** > **Router-Advertisement** , öffnen Sie die Tabelle **Interface-Optionen** und klicken Sie auf **Hinzufügen**.



16. Übernehmen Sie alle weiteren Default-Werte unverändert.
17. Speichern Sie die Eingaben mit **Setzen**.
18. Wechseln Sie in das Verzeichnis **LCOS-Menübaum** > **Setup** > **IPv6** , öffnen Sie die Tabelle **Routing-Tabelle** und klicken Sie auf **Hinzufügen**.

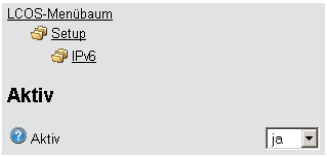


19. Vergeben Sie als **Praefix** den Wert "::/0".

20. Übernehmen Sie für **Rtg-Tag** den Default-Wert "0".

> In LCOS 8.61 Public Beta 2 noch ohne Funktion!

21. Im Feld **Peer-oder-IPv6** tragen Sie den Namen des Interfaces ein, das den 6to4-Tunnel verwenden wird, im Beispiel oben "TUNNEL-6TO4".
22. Vergeben Sie einen aussagekräftigen **Kommentar** für diesen Eintrag.
23. Speichern Sie die Eingaben mit **Setzen**.
24. Aktivieren Sie den IPv6-Stack, indem Sie unter **LCOS-Menübaum** > **Setup** > **IPv6** die Option **Aktiv** auf "ja" einstellen und mit **Setzen** speichern.



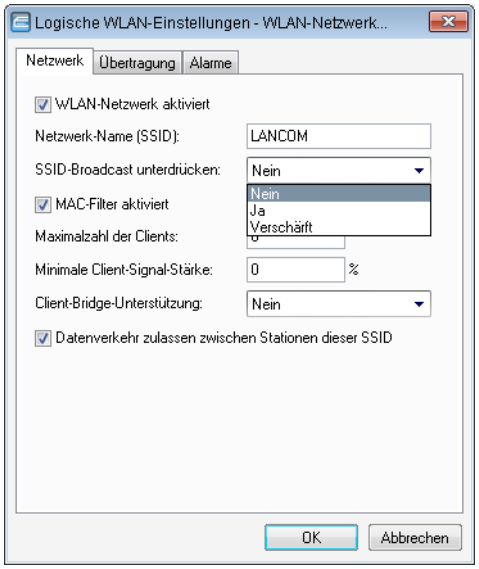
6 WLAN

6.1 Closed-Network-Funktion: SSID-Broadcast unterdrücken

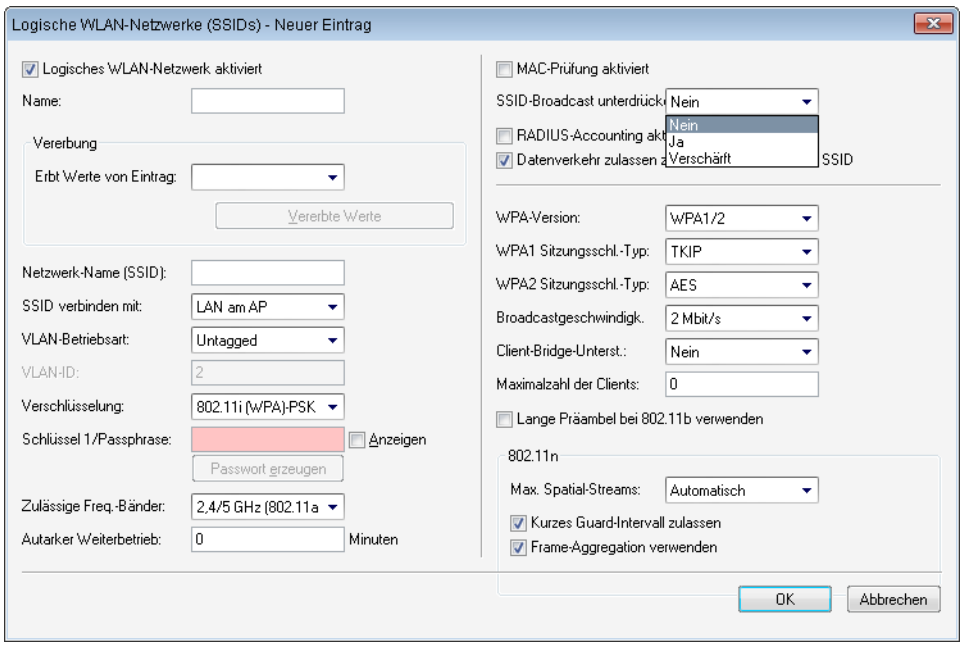
Nur mit der Kenntnis des Service Set Identifiers (SSID) kann sich ein WLAN-Client mit dem entsprechenden Funknetzwerk verbinden. In der Grundeinstellung erlauben viele drahtlose Netzwerke die Anmeldung mit der SSID "any" bzw. einer leeren SSID und ermöglichen so einem potenziellen Eindringling, das WLAN zu benutzen, ohne dessen SSID zu kennen. Die Closed-Network-Funktion verhindert, dass unbefugte WLAN-Clients sich am WLAN anmelden können. Der Access-Point verweigert dabei jeden Anmeldeversuch mit der SSID "any" bzw. einer leeren SSID. Jeder Benutzer muss die verwendete SSID genau kennen, um sich am WLAN anmelden zu können.

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.

LANconfig: Wireless-LAN > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen** > **Netzwerk** .



LANconfig: WLAN-Controller > Profile > Logische WLAN-Netzwerke (SSIDs)



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 das Gerät mit der SSID der Funkzelle (öffentlich sichtbares WLAN).
- **Ja**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer SSID, antwortet das Gerät ebenfalls mit einer leeren SSID. Der Client kann sich nicht an der Funkzelle anmelden.
- **Verschärft**: Der Access-Point veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe-Request mit leerer oder falscher SSID, antwortet das Gerät überhaupt nicht. Der Client kann sich nicht an der Funkzelle anmelden. Diese Einstellung reduziert zusätzlich die Netzlast, wenn sich in der Funkzelle viele WLAN-Clients befinden.

6.1.1 Ergänzungen im Menüsystem

Closed-Network (nur bei Standalone-Access-Points)

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.

SNMP-ID:

2.23.20.1.4

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Nein

Ja

Verschärft

Default:

Nein

SSID-Broadcast (nur bei WLAN-Controllern)

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 Access-Point 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 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 (öffentlich sichtbares WLAN).
- **Nein**: 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.

Die Funktion "Closed-Network" finden Sie im Access-Point unter **Setup** > **Schnittstellen** > **WLAN** > **Netzwerk** . Beachten Sie: Wenn Sie im WLAN-Controller bei **SSID-Broadcast** die Option "Nein" auswählen (Gerät veröffentlicht die SSID nicht), setzt der Access-Point bei **Closed-Network** die Einstellung auf "Ja" und umgekehrt. Nur die Logik bei der Einstellung "Verschärft" ist in beiden Geräten identisch.

SNMP-ID:

2.37.1.1.19

Pfad Telnet:

Pfad Telnet: Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Nein

Ja

Verschärft

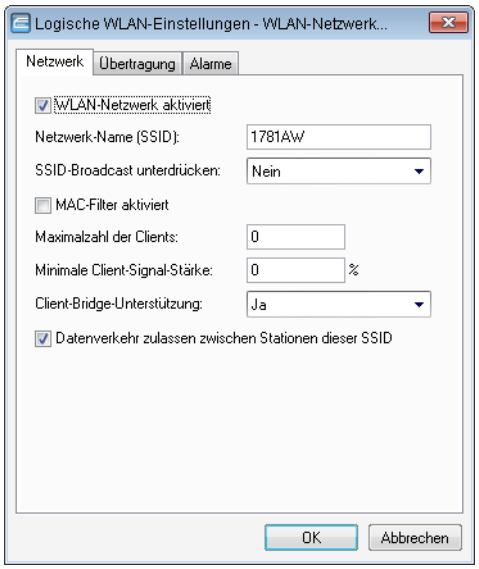
Default:

Ja

6.1.2 Ergänzungen in LANconfig

Netzwerkeinstellungen

LANconfig: Wireless-LAN > Allgemein > Logische WLAN-Einstellungen > Netzwerk



- **WLAN-Netzwerk aktiviert**

  Mit diesem Schalter aktivieren bzw. deaktivieren Sie das entsprechende logische WLAN.

- **Netzwerk-Name** (SSID)

  Bestimmen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen). Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

- **SSID-Broadcast unterdrücken**

  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.

- **MAC-Filter aktiviert**

  In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **Stationen**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem Access-Point einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

  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 beachtet der Access-Point daher immer die MAC-Filterliste, auch wenn Sie diese Option hier deaktivieren.

- **Maximale Client-Anzahl**

  Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access-Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der Access-Point ab.

- **Minimale Client-Signal-Stärke**

  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.

- **Client-Bridge-Unterstützung**

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

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

- **Datenverkehr zulassen zwischen Stationen dieser SSID**

  Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

6.2 Neuer Parameter für die Signalstärke von WLAN-CLients

Die LCOS-Version 8.62 wertet nun optional die Signalstärken beim Einbuchen von WLAN-Clients aus.

6.2.1 Ergänzungen im Menüsystem

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.

SNMP-ID:

2.23.20.1.16

Pfad Telnet:

Pfad Telnet: Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

0-100

Default:

0

6.3 Spectral Scan

Neben der Anbindung von Rechnern an das Internet nutzen professionelle Anwender das Wireless Local Area Network (WLAN) immer häufiger auch für geschäftsrelevante Prozesse. Als Beispiele seien hier der Zugriff auf Patientenakten, die Online-Überwachung einer Produktion oder die (idealerweise verzögerungsfreie) Übertragung von Video- und Audiodaten genannt. Die Zuverlässigkeit und die Leistungsfähigkeit eines WLAN-Systems nehmen daher kontinuierlich an Bedeutung zu.

Aufgrund der zunehmenden Nutzung und Bedeutung von WLAN für die Datenübertragung ergeben sich immer häufiger Situationen, in denen Geräte oder Systeme anderer Nutzer die WLAN-Frequenzbereiche zeitgleich nutzen. Dies können z. B. Mikrowellenherde, kabellose Telefone, Bluetooth-Geräte oder Video-Transmitter sein, wobei deren Signale sowohl kontinuierlich wie intermittierend auftreten können. Durch die zeitgleiche Nutzung eines Frequenzbandes bzw. Frequenzbereiches ergeben sich Interferenzen, die die Zuverlässigkeit und Leistungsfähigkeit eines WLANs stören oder beeinträchtigen können. Solche Störungen können zum Verlust von Datenpaketen oder zum Abbruch von Verbindungen führen. Ist die Überlagerung zu stark, kann es sogar zum vollständigen Ausfall des WLANs kommen.

Es ist daher zunehmend von Bedeutung, den aktuell verwendeten Frequenzbereich durch eine gezielte Analyse zu überprüfen. Dies dient einerseits dem Zweck, Interferenzen oder andere Störfaktoren zu erkennen und bei Bedarf Gegenmaßnahmen einzuleiten. Andererseits lässt sich so auch sicherstellen, dass das WLAN ordnungsgemäß und störungsfrei funktioniert.

Eine gezielte Analyse bietet die Möglichkeit, folgende Faktoren zu klären bzw. näher zu bestimmen:

- Ordnungsgemäßer und störungsfreier Betrieb des WLANs
- Vorhandensein einer Interferenz bzw. eines Störsignals
- Anzeige oder Nennung der gestörten Bänder
- Stärke des Störsignals
- Regelmäßigkeit bzw. Häufigkeit des Störsignals
- Art und ggf. Herkunft des Störsignals

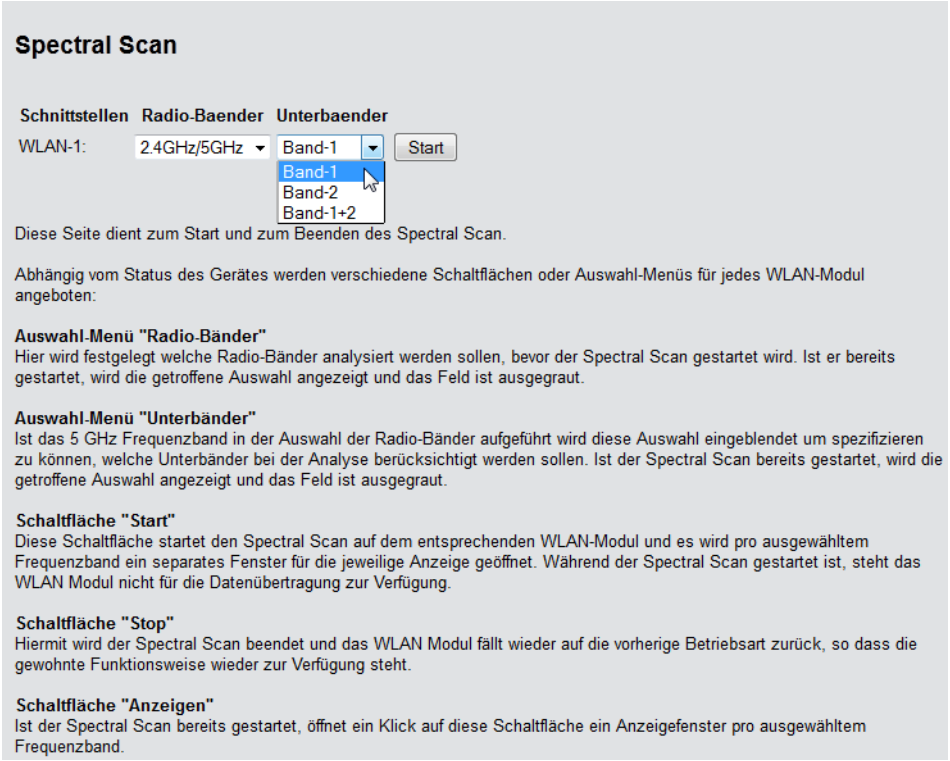
Die Untersuchung des für WLAN in Frage kommenden Frequenzbereiches findet auf der spektralen Ebene statt. Entsprechend hierzu werden die Ergebnisse grafisch wiedergeben, d. h. in Form von Echtzeit-Diagrammen oder Echtzeit-Übersichten, auf denen man Frequenzen und Störungen erkennen und ggf. ablesen kann. Hierbei ist zu bedenken, dass grafische Auswertungen eines spektralen Bereiches naturgemäß einen Interpretationsspielraum offen lassen und in manchen Fällen keine ganz eindeutigen Resultate ermöglichen. Ein Szenario wie das folgende wäre daher nicht ungewöhnlich: Sie stellen fest, dass Ihre aktuell verwendete Frequenz durch ein Signal gestört wird, das kontinuierlich auftritt und gleichbleibend stark ist. Sie können jedoch nicht eindeutig feststellen oder gar "ablesen", aus welchem Raum oder Gebäude das Signal kommt und welche Art von Gerät der Urheber des Störsignals ist.

6.3.1 Funktionen des Software-Moduls

Das Software-Modul "Spectral Scan" bietet Ihnen die Möglichkeit, eine Spektralanalyse direkt am Access Point durchzuführen. Sie müssen sich also keine zusätzliche Soft- oder Hardware anschaffen, sondern können auf die integrierte Funktionalität zurückgreifen, um die in Frage kommenden Frequenzbereiche und -bänder zu untersuchen. Somit können

Sie sich jederzeit einen grafischen Überblick über das Frequenzverhalten in Ihrem WLAN verschaffen, sei es nun zur Vorbeugung oder zur Aufdeckung von Störungen.

Ein Klick unter WEBconfig auf den Menüpunkt **Extras** > **Spectral Scan** öffnet den nachstehend abgebildeten Dialog:



Wenn das WLAN-Modul deaktiviert ist (**Setup** > **Schnittstellen** > **WLAN** > **Betriebs-Einstellungen**), erscheint ein entsprechender Hinweis, und der Spectral Scan lässt sich nicht starten. Konfigurieren Sie den Access Point für die Betriebsart "Basisstation" oder stellen Sie sicher, dass ein WLAN-Controller den Access Point konfiguriert.

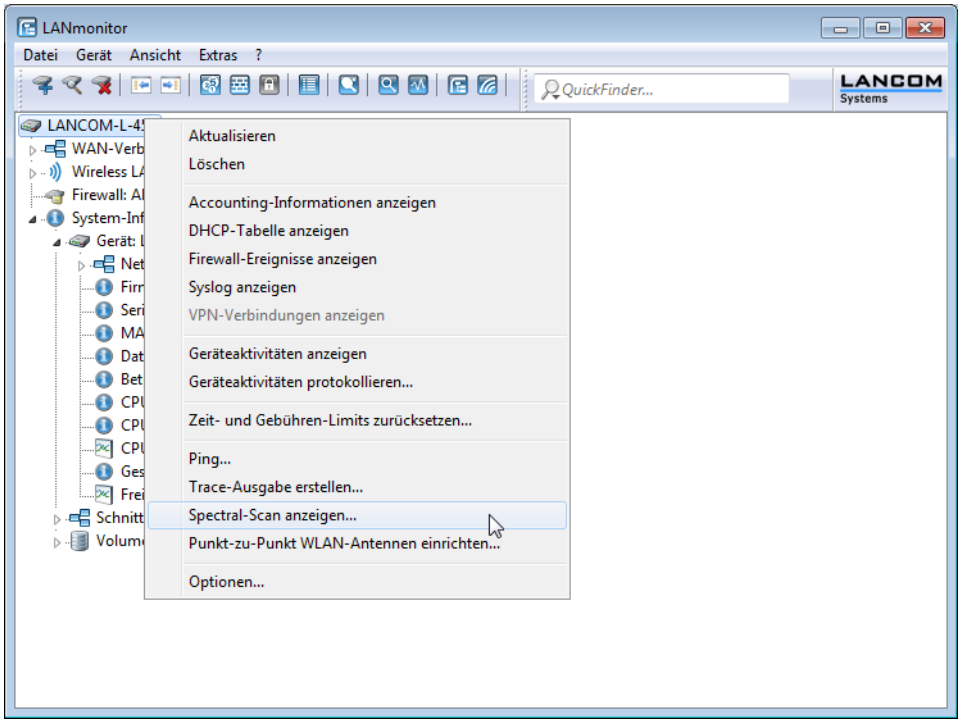
Hier stehen Ihnen folgende Einträge, Schaltflächen und Auswahl-Menüs zur Verfügung:

- **Schnittstellen**: Zeigt das ausgewählte, zu untersuchende WLAN-Modul an.
- **Radio-Baender**: Mit diesem Auswahl-Menü legen Sie fest, welches Frequenzband bzw. welche Frequenzbänder Sie untersuchen möchten. Wenn der Spectral Scan auf diesem Modul bereits gestartet ist, ist das betreffende Feld ausgegraut.
- **Unterbänder**: Dieses Auswahl-Menü ist nur aktiv, wenn Sie bei **Radio-Baender** entweder '5GHz' oder '2.4GHz/5Ghz' ausgewählt haben. Sie können dann festlegen, welche Unterbänder des 5GHz-Bandes bei der Analyse berücksichtigt werden sollen.
- **Start**: Ein Klick auf diese Schaltfläche startet die Analyse (den "Spectral Scan") auf dem entsprechenden WLAN-Modul. Dabei öffnet sich ein separates Fenster pro ausgewähltem Frequenzband.
- **Stop**: Mit dieser Schaltfläche beenden Sie die Analyse. Das WLAN-Modul kehrt dann in die vorherige Betriebsart zurück und steht wieder mit der gewohnten Funktionalität zur Verfügung.

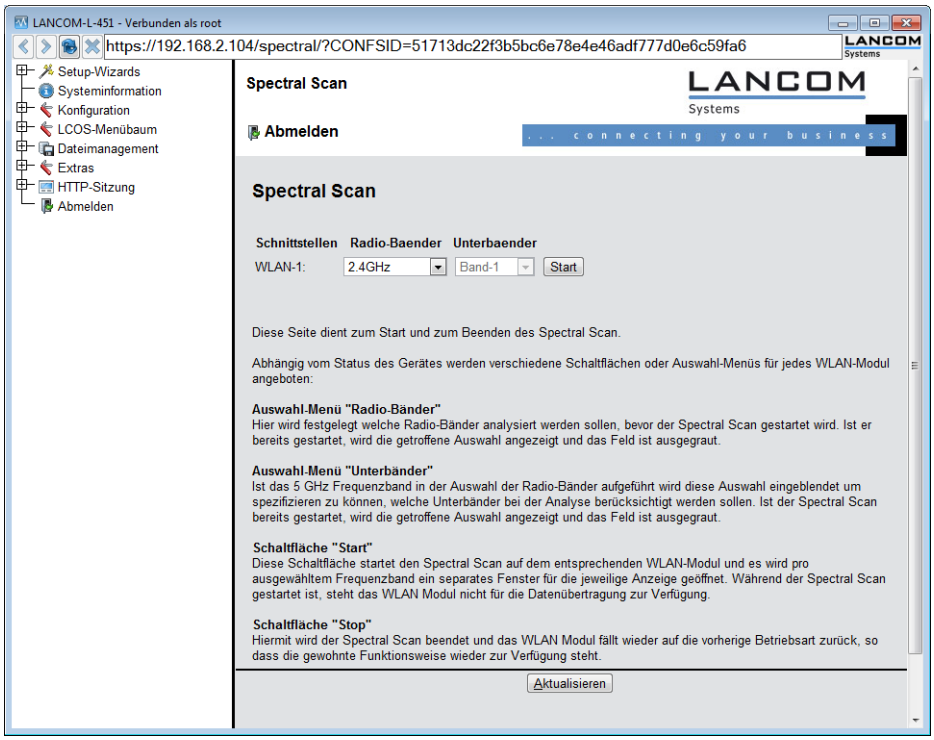
  Diese Schaltfläche erscheint erst nach dem Start des Moduls.

- **Anzeigen**: Sofern der Spectral Scan bereits gestartet ist, öffnen Sie mit einem Klick auf diese Schaltfläche ein Anzeigefenster pro ausgewähltem Frequenzband. Durch mehrfaches Betätigen der Schaltfläche können Sie mehrere Fenster öffnen.

Sie können den Spectral Scan auch aus dem LANmonitor heraus starten. Klicken Sie dazu das entsprechende Gerät in der Liste mit der rechten Maustaste an und wählen Sie im Kontextdialog den Punkt **Spectral Scan anzeigen**.



Es öffnet sich ein Browserfenster, in dem Ihnen alle Einträge, Schaltflächen und Auswahl-Menüs zur Verfügung stehen, wie Sie sie auch unter WEBconfig vorfinden.



Während des Analysevorgangs überträgt das untersuchte WLAN-Modul keine Daten und sendet keine SSID.

Nur LANCOM Access Points der Serie L-4xx, der Serie L-32x Serie sowie die Modelle 1781AW, 1781EW und 1780EW-3G unterstützen die Funktion "Spectral Scan".

6.3.2 Analyse-Fenster Spectral Scan

Die Anzeige des Spectral Scans erfolgt in einer Browser-Anwendung. Damit sie ordnungsgemäß funktioniert, muss Ihr Browser Websockets in der aktuellen Version das HTML5-Element `<canvas>` unterstützen. Der in LANmonitor integrierte Browser erfüllt alle Anforderungen.

Im separaten Analyse-Fenster des Spectral Scan haben Sie unterschiedliche Möglichkeiten, die jeweiligen Frequenzen bzw. Frequenzbereiche nebst möglichen Störungen darzustellen. Hierfür stehen Ihnen am oberen Rand des Fensters die folgenden Schaltflächen zur Verfügung:

- **Current**: Zeigt oder verbirgt die Kurve der aktuell gemessenen Werte.
- **Maximum**: Zeigt oder verbirgt die Maximalwerte des laufenden Spektrum-Scans, bezogen auf den aktuell eingestellten History-Bereich.
- **Average**: Zeigt oder verbirgt die Durchschnittswerte des laufenden Spektrum-Scan, bezogen auf den aktuell eingestellten History-Bereich.
- **History**: Zeigt oder verbirgt die zuletzt gemessenen Werte.
- **Number of history values**: Bestimmt die Anzahl der angezeigten, zuletzt gemessenen Ergebnisse. Sie können sich mindestens die letzten 5 und maximal die letzten 50 Messpunkte je Frequenz anzeigen lassen.
- **Last Channel**: Zeigt oder verbirgt den zuletzt benutzten Kanal.
- **Frequency**: Wechselt die Anzeige auf der x-Achse zwischen WLAN-Kanal und Frequenz.

Das Fenster enthält zwei grafische Darstellungen, die Ihnen die Messergebnisse unterschiedlich präsentieren. Das obere Diagramm zeigt auf der y-Achse die Signalstärke in dBm, auf der x-Achse entweder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz. Das untere Diagramm enthält den zeitlichen Verlauf der Analyse in Form eines Wasserfall-Diagramms, wobei die y-Achse die Zeit darstellt, während die x-Achse wieder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz zeigt. Diese Formen der Darstellung können sowohl andauernde als auch zeitlich variierende Störungen in den Frequenzen anschaulich machen, so dass Sie entsprechende Maßnahmen zur Verbesserung der Verbindung durchführen können (z. B. Wechsel des Kanals oder Identifizierung und Beseitigung der Störquelle). So weisen z. B. bestimmte Störquellen wie Mikrowellen-Geräte, DECT-Telefone (die im 2,4 GHz Frequenzbereich arbeiten) oder Audio-Video-Transmitter ganz typische Sendemuster auf, die in beiden Diagrammen deutlich hervortreten.

Am unteren Rand des Fensters sehen Sie einen mit **Time Slider** bezeichneten Schieberegler. Mit diesem können Sie für das Wasserfall-Diagramm den zu analysierenden Zeitraum der betreffenden Frequenz erweitern oder begrenzen. Alternativ können Sie über das Eingabefeld rechts neben dem Schieberegler auswählen, wie viele Messergebnisse Sie sich im Wasserfall-Diagramm anzeigen lassen möchten. 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.

Nachstehend sehen Sie einige exemplarische Analyse-Ergebnisse, die jeweils andere Einstellungen auf unterschiedliche Weise grafisch aufbereiten:

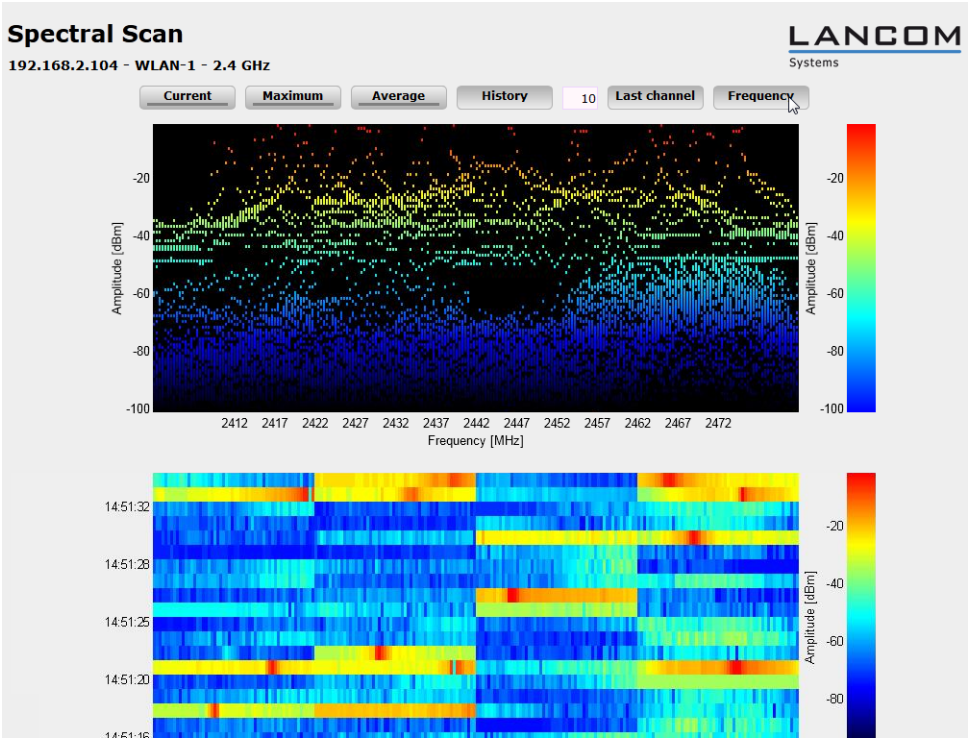


Abbildung 1: Spectral Scan, Frequenz-Anzeige der letzten 10 History-Werte

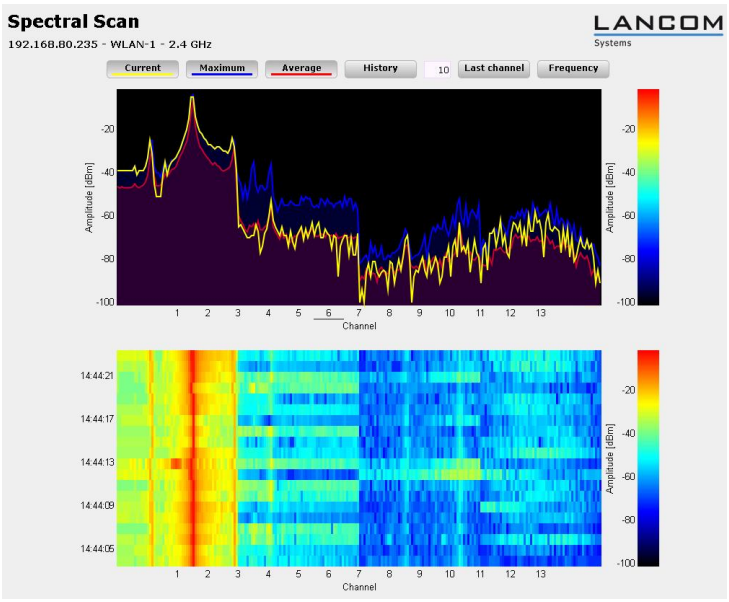


Abbildung 2: Spectral Scan, Kanal-Anzeige Current, Maximum, Average, Störung durch Funk-Kamera

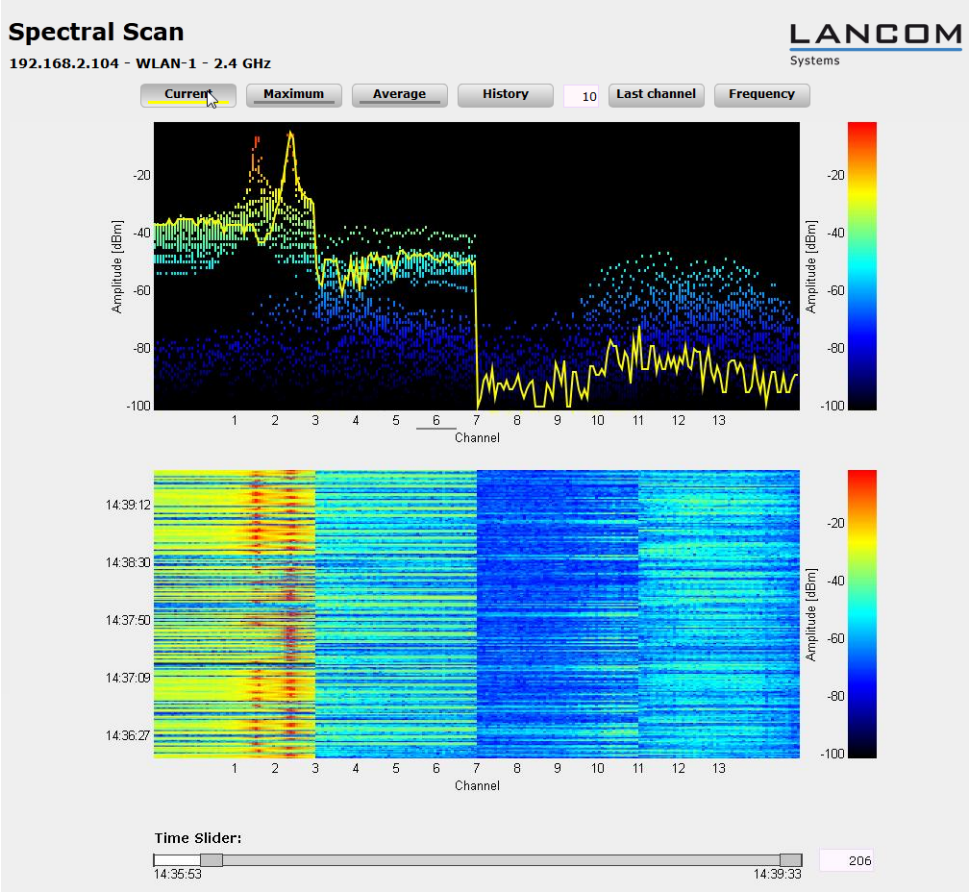


Abbildung 3: Spectral Scan, Kanal-Anzeige Current, letzte 10 History-Werte und "Time Slider", Störung durch Baby-Phone

6.3.3 Ergänzungen im LANmonitor

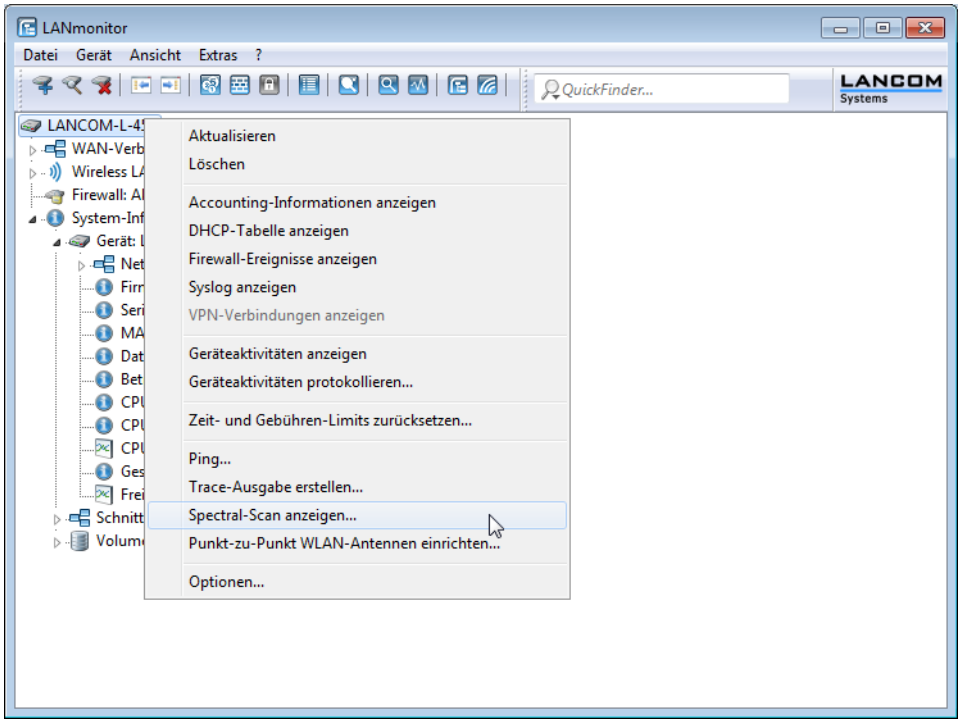
Anwendungskonzepte für den LANmonitor

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANmonitor, wie z. B. die Abfrage der CPU- und Speicherauslastung über SNMP oder die Durchführung eines Spektral Scans.

Spectral Scan

Das Software-Modul "Spectral Scan" bietet Ihnen die Möglichkeit, eine Spektralanalyse direkt am Access Point durchzuführen. Sie müssen sich also keine zusätzliche Soft- oder Hardware anschaffen, sondern können auf die integrierte Funktionalität zurückgreifen, um die in Frage kommenden Frequenzbereiche und -bänder zu untersuchen. Somit können Sie sich jederzeit einen grafischen Überblick über das Frequenzverhalten in Ihrem WLAN verschaffen, sei es nun zur Vorbeugung oder zur Aufdeckung von Störungen.

Klicken Sie das entsprechende Gerät in der Liste mit der rechten Maustaste an und wählen Sie im Kontextdialog den Punkt **Spectral Scan anzeigen**.



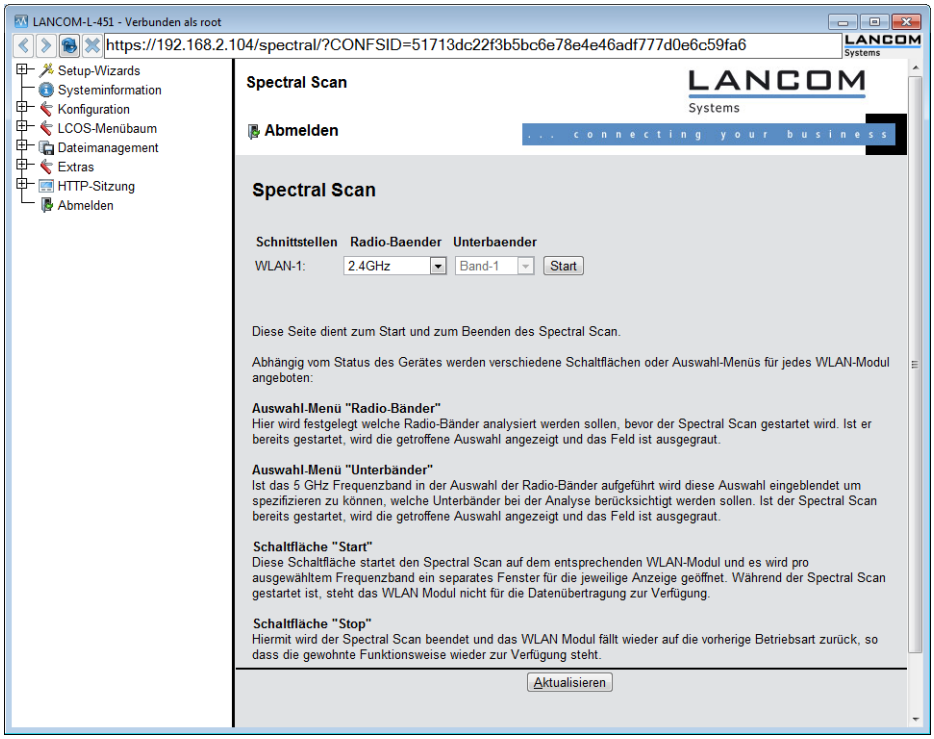
Hier stehen Ihnen folgende Einträge, Schaltflächen und Auswahl-Menüs zur Verfügung:

- **Schnittstellen**: Zeigt das ausgewählte, zu untersuchende WLAN-Modul an.
- **Radio-Baender**: Mit diesem Auswahl-Menü legen Sie fest, welches Frequenzband bzw. welche Frequenzbänder Sie untersuchen möchten. Wenn der Spectral Scan auf diesem Modul bereits gestartet ist, ist das betreffende Feld ausgegraut.
- **Unterbänder**: Dieses Auswahl-Menü ist nur aktiv, wenn Sie bei **Radio-Baender** entweder '5GHz' oder '2.4GHz/5Ghz' ausgewählt haben. Sie können dann festlegen, welche Unterbänder des 5GHz-Bandes bei der Analyse berücksichtigt werden sollen.
- **Start**: Ein Klick auf diese Schaltfläche startet die Analyse (den "Spectral Scan") auf dem entsprechenden WLAN-Modul. Dabei öffnet sich ein separates Fenster pro ausgewähltem Frequenzband.
- **Stop**: Mit dieser Schaltfläche beenden Sie die Analyse. Das WLAN-Modul kehrt dann in die vorherige Betriebsart zurück und steht wieder mit der gewohnten Funktionalität zur Verfügung.

  Diese Schaltfläche erscheint erst nach dem Start des Moduls.

- **Anzeigen**: Sofern der Spectral Scan bereits gestartet ist, öffnen Sie mit einem Klick auf diese Schaltfläche ein Anzeigefenster pro ausgewähltem Frequenzband. Durch mehrfaches Betätigen der Schaltfläche können Sie mehrere Fenster öffnen.

Weitere Informationen über die angezeigten Diagramme entnehmen Sie dem Abschnitt *Analyse-Fenster Spectral Scan*.



Während des Analysevorgangs überträgt das untersuchte WLAN-Modul keine Daten und sendet keine SSID.

Nur LANCOM Access Points der Serie L-4xx, der Serie L-32x Serie sowie die Modelle 1781AW, 1781EW und 1780EW-3G unterstützen die Funktion "Spectral Scan".

6.3.4 Ergänzungen im Setup-Menü

Betriebsart

LANCOM Wireless-Geräte können grundsätzlich in verschiedenen Betriebsarten arbeiten.

SNMP-ID:

2.23.20.7.3

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:

LANCOM Wireless Router: Access Point

LANCOM Access Points: Managed-AP

Probe-Einstellungen

In dieser Tabelle befinden sich die Einstellungen für den Spectral Scan.

In diesem Betriebsmodus kann das Gerät weder Daten senden noch empfangen.

SNMP-ID:

2.23.20.15

Pfad Telnet:

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

Ifc

Öffnet die Einstellungen für die physikalische WLAN-Schnittstelle.

SNMP-ID:

2.23.20.15.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Auswahl aus den verfügbaren physikalischen WLAN-Schnittstellen.

Radio-Baender

Hier können Sie auswählen, welche Frequenzbänder der Spectral Scan untersuchen soll.

SNMP-ID:

2.23.20.15.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

2,4GHz

5GHz

2,4GHz/5GHz

Default:

2,4GHz

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.

SNMP-ID:

2.23.20.15.3

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Band-1

Band-2

Band-1+2

Default:

Band-1

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.

SNMP-ID:

2.23.20.15.4

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max. 48 Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

1,5,9,13

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.

SNMP-ID:

2.23.20.15.5

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

Band-1

Band-2

Band-1+2

Default:

Band-1

Kanalliste-5GHz

In diesem Feld bestimmen Sie die Kanalliste für den Spectral Scan im 5GHz-Frequenzband. Trennen Sie die einzelnen Kanäle durch Kommas.

SNMP-ID:

2.23.20.15.6

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max. 48 Zeichen

aus ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789

Default:

leer

Kanal-Verweil-Zeit

Bestimmen Sie hier, wieviele 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.

SNMP-ID:

2.23.20.15.7

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Probe-Einstellungen**

Mögliche Werte:

max 10 Zeichen

von 0 bis 9

Default:

250

6.4 WLAN Band Steering

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

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

Für die gezielte Zuweisung gibt es mehrere, zum Teil sehr fortgeschrittene Kriterien. Eines dieser Kriterien betrifft die verwendeten Funkfrequenzbereiche, in denen Clients kommunizieren. So erwartet man von modernen Dual-Band-WLAN-Clients immer häufiger, dass diese den 5-GHz-Frequenzbereich gegenüber dem inzwischen überfüllten 2,4-GHz-Bereich bevorzugen. Weist man einem WLAN-Client ganz gezielt ein bestimmtes Frequenzband bzw. einen bestimmten Frequenzbereich zu, spricht man von Band Steering.

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

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

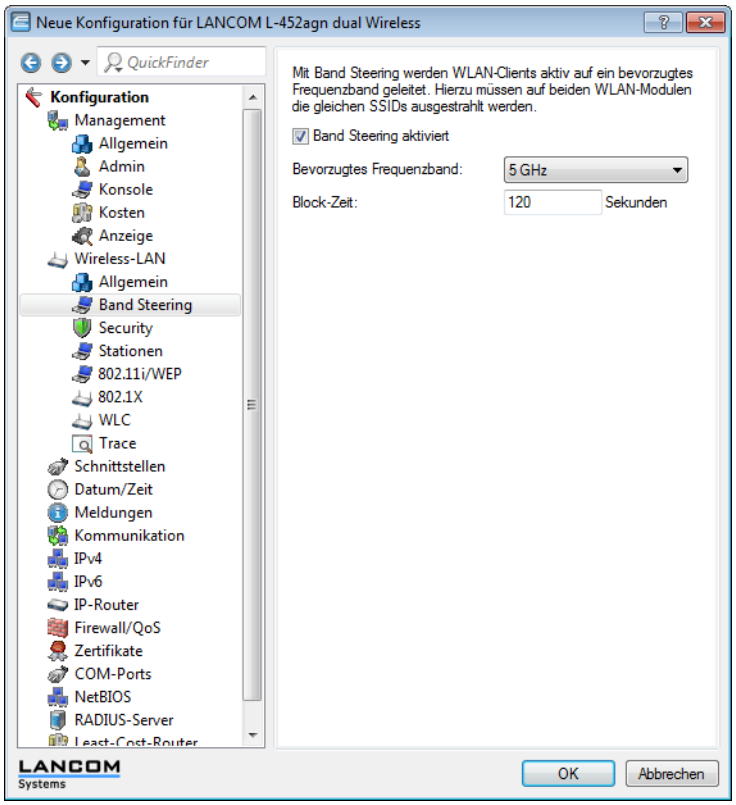
- **LANconfig: Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** > **Minimale Client-Signal-Stärke**
- **WEBconfig: Setup** > **Schnittstellen** > **WLAN** > **Netzwerk** > **Minimal-Stations-Staerke**

Sie können das Band-Steering des Access Points im LANconfig unter **Wireless-LAN** > **Band Steering** aktivieren und verwalten.

6.4.1 Ergänzungen in LANconfig

Band Steering

Dieser Dialog bietet Ihnen die Möglichkeit, die Einstellungen für das Band Steering in LANconfig vorzunehmen.



Unter **Wireless-LAN** > **Band Steering** stehen Ihnen folgende Funktionen zur Verfügung:

- **Band Steering aktiviert**: Aktiviert oder deaktiviert diese Funktion.
- **Bevorzugtes Frequenzband**: Gibt das Frequenzband vor, auf welches das Gerät WLAN-Clients leitet. Mögliche Werte sind:
  - **2,4GHz**: Das Gerät leitet Clients auf das Frequenzband 2,4GHz.
  - **5GHz**: Das Gerät leitet Clients auf das Frequenzband 5GHz.
- **Block-Zeit**: Der Zeitraum, während dessen der Access Point den WLAN-Client auf das bevorzugte Frequenzband leitet. Der Standardwert lautet 120 Sekunden.

6.4.2 Ergänzungen im Setup-Menü

Client-Steering

Hier bestimmen Sie die Einstellungen für das 'WLAN Band Steering' der am Access Point angemeldeten WLAN-Clients.

SNMP-ID:

2.12.87

Pfad Telnet:

Setup > **WLAN**

In-Betrieb

Mit dieser Option aktivieren Sie das 'Client steering' im Access Point.

SNMP-ID:

2.12.87.1

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

Kriterium

Bestimmen Sie hier, nach welchen Kriterien der Access Point den WLAN-Client steuern soll.

SNMP-ID:

2.12.87.2

Pfad Telnet:

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

Mögliche Werte:

Radio-Band

Default:

Radio-Band

Bevorzugtes-Band

Bestimmen Sie hier, in welches Frequenzband der Access Point den WLAN-Client bevorzugt leiten soll.

SNMP-ID:

2.12.87.3

Pfad Telnet:

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

Mögliche Werte:

5GHz

2,4GHz

Default:

5GHz

Proberequest-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 entsprechen niedrig ansetzen

SNMP-ID:

2.12.87.3

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

6.4.3 Ergänzungen im Status-Menü

Gesehene-Clients

SNMP-ID:

1.3.45

Pfad Telnet:

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

Diese Tabelle enthält folgende Status-Werte:

Anzahl-ProbeRsp-OK

Anzahl der Probe-Responses, die an diesen Client geschickt wurden und angekommen sind.

Anzahl-ProbeRsp-Fehler

Anzahl der Probe-Responses, die an diesen Client geschickt wurden nicht und angekommen sind (Tx-Fehler).

Anzahl-ProbeRsp-unterdrueckt

Anzahl der Probe-Responses, die an diesen Client geschickt wurden, weil entweder dessen Signalstärke unter dem Schwellwert lag oder das Band Steering den Response unterdrückt hat.

Band

Zeigt das WLAN-Band an, auf dem der Client zuletzt kommuniziert hat.

6.5 STBC/LDPC

6.5.1 Grundlagen

Datenübertragungen nach dem IEEE-802.11n-Standard erfolgt in der MIMO-Technik (multiple input, multiple output). Der Sender überträgt hierbei Datenpakete gleichzeitig über mehrere, räumlich voneinander getrennte Antennen, so dass Reflexionen und die dadurch entstehenden Interferenzen das Signal weniger stören können. Mit jeder weiteren Antenne wird jedoch der Gewinn an Datendurchsatz geringer, dafür wird der Aufwand für die Signalaufbereitung in den Geräten immer höher.

Low Density Parity Check (LDPC)

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 Datenübertragungsrate.

Space Time Block Coding (STBC)

Die Funktion 'STBC' (Space Time Block Coding) 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.

6.5.2 Ergänzungen im Setup-Menü

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.

SNMP-ID:

2.23.20.2.23

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)

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.

SNMP-ID:

2.23.20.2.24

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)

6.5.3 Ergänzungen im Status-Menü

Rx-STBC

Dieser Parameter zeigt an, ob und wie viele Datenströme die erkannte Gegenstelle im STBC-Verfahren empfangen kann.

SNMP-ID:

1.3.32.60

Pfad Telnet:

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

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob das ausgewählte WLAN-Interface die LDPC-Kodierung unterstützt.

SNMP-ID:

1.3.32.61

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Tx-STBC

Dieser Parameter zeigt an, ob die erkannte Gegenstelle fähig ist, mit STBC zu senden.

SNMP-ID:

1.3.34.38

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Rx-STBC

Dieser Parameter zeigt an, ob und wie viele Datenströme die erkannte Gegenstelle im STBC-Verfahren empfangen kann.

SNMP-ID:

1.3.34.39

Pfad Telnet:

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

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob die erkannte Gegenstelle LDPC-kodierte Datenpakete auswerten kann.

SNMP-ID:

1.3.34.41

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Rx-STBC

Dieser Parameter zeigt an, ob und wie viele Datenströme die erkannte Gegenstelle im STBC-Verfahren empfangen kann.

SNMP-ID:

1.3.36.1.41

Pfad Telnet:

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

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob das ausgewählte WLAN-Interface die LDPC-Kodierung unterstützt.

SNMP-ID:

1.3.36.1.42

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Rx-STBC

Dieser Parameter zeigt an, ob und wie viele Datenströme die erkannte Gegenstelle im STBC-Verfahren empfangen kann.

SNMP-ID:

1.3.43.51.38

Pfad Telnet:

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

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob das ausgewählte WLAN-Interface die LDPC-Kodierung unterstützt.

SNMP-ID:

1.3.43.51.39

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Tx-STBC

Dieser Parameter zeigt an, ob die erkannte Gegenstelle fähig ist, mit STBC zu senden.

SNMP-ID:

1.3.44.38

Pfad Telnet:

Status > **WLAN** > **Andere-Netzwerke**

Mögliche Werte:

Ja

Nein

Rx-STBC

Dieser Parameter zeigt an, ob und wieviele Datenströme die erkannte Gegenstelle im STBC-Verfahren empfangen kann.

SNMP-ID:

1.3.44.39

Pfad Telnet:

Status > **WLAN** > **Andere-Netzwerke**

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob die erkannte Gegenstelle LDPC-kodierte Datenpakete auswerten kann.

SNMP-ID:

1.3.44.41

Pfad Telnet:

Status > **WLAN** > **Andere-Netzwerke**

Mögliche Werte:

Ja

Nein

Rx-STBC

Dieser Parameter zeigt an, wie viele Datenströme das ausgewählte WLAN-Interface empfangen kann, wenn die Option **STBC** aktiviert ist.

Bei der Anzeige **0** bietet das WLAN-Interface keine STBC-Unterstützung.

SNMP-ID:

1.3.55.34

Pfad Telnet:

Status > **WLAN** > **WLAN-Parameter**

Mögliche Werte:

Keiner

Einer

Zwei

Drei

LDPC

Dieser Parameter zeigt an, ob das ausgewählte WLAN-Interface die LDPC-Kodierung unterstützt.

SNMP-ID:

1.3.55.35

Pfad Telnet:

Status > **WLAN** > **WLAN-Parameter**

Mögliche Werte:

Ja

Nein

6.6 LANCOM-spezifisches UUID-Info-Element für Access-Points

Ab LCOS-Version 8.80 überträgt der LANCOM Access-Point eine LANCOM-spezifische UUID-Gerätekennung.

6.6.1 UUID-Info-Element für LANCOM WLAN Access Points

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

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

Zur Netzwerk-Überwachung und -Planung ist es jedoch sinnvoll, die logischen Netzwerke den entsprechenden Geräten (bzw. Funkmodulen) zuordnen zu können.

LANCOM Access-Points unterstützen unter anderem ein Aironet-kompatibles Info-Element, das den vom Administrator vergebenen Namen des Gerätes beinhaltet. Die Übertragung dieser Information ist jedoch optional, wobei viele Anwender sie deaktivieren, weil sie z. B. aus Sicherheitsgründen so wenig Informationen wie möglich über den Access-Point im Netzwerk veröffentlichen möchten.

Bei der Überwachung des Netzwerkes taucht diese Information also entweder gar nicht auf, oder sie identifiziert das Gerät je nach Eingabe nicht zwingend als LANCOM Access-Point.

Darüber hinaus besitzen LANCOM Access-Points eine UUID (Universally Unique Identifier), die aus Geräte-Typ und Seriennummer errechnet wird und das Gerät eindeutig im Netzwerk identifizieren kann. Durch eine Verschlüsselung bei der UUID-Erzeugung ist jedoch ein Rückschluss auf Gerät oder Seriennummer nur mit hohem Aufwand (Brute-Force-Angriff über alle möglichen Geräte-Typen und Seriennummern) möglich.

Sie können die Übertragung der UUID je Funkmodul und logischem Netzwerk unabhängig voneinander ein- oder ausschalten.

Ergänzungen im Setup-Menü

UUID-Einschliessen

Hier bestimmen Sie, ob das entsprechende Funkmodul seine UUID übertragen soll.

SNMP-ID:

2.23.20.1.17

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja

6.7 DFS

Im Folgenden finden Sie Informationen zu DFS (Dynamic Frequency Selection).

6.7.1 DFS4

Ab LCOS-Version 8.80 unterstützen alle Geräte, die im 5GHz-WLAN funken, die Norm ETSI EN 301 893 V1.6.1 ("DFS4").

6.7.2 Entwicklungsgeschichte und Funktion

Beim für 5GHz-WLANs geforderten DFS-Verfahren (Dynamic Frequency Selection) wählt das Gerät automatisch eine freie Frequenz, z. B. um Radaranlagen nicht zu stören und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Die Signale von Wetter-Radarstationen waren jedoch manchmal nicht sicher zu erkennen.

Die europäische Kommission forderte daher in Ergänzung zu den Standards ETSI EN 301 893 V1.3.1 und ETSI EN 301 893 V1.4.1, im Unterband 2 des 5GHz-Bandes drei Kanäle (120, 124 und 128) auszusparen und solange nicht für die automatische Kanalwahl zu verwenden, bis Verfahren zur Erkennung der Wetter-Radar-Signaturen zur Verfügung stehen. Man bezeichnete die Version EN 301 893 V1.3 und EN 301 893 V1.4 kurz als "DFS2"

Mitte 2010 trat die neue Version ETSI EN 301 893 V1.5.1 in Kraft, die einige Veränderungen für die Nutzung von WLAN-Frequenzen in den Bereichen 5,25 - 5,35 GHz und 5,47 - 5,725 GHz mit sich brachte. Die neue Version 1.5.1 regelte das DFS-Verfahren für diese Frequenzbereiche, um Radarstationen vor dem Einfluss durch WLAN-Systeme zu schützen. Bei der Erkennung von bestimmten Mustern in den empfangenen Funksignalen können seitdem WLAN-Systeme mit Hilfe von DFS die Radarstationen erkennen und einen automatischen Wechsel der verwendeten Kanäle durchführen. Im Unterschied zu den bisherigen Regelungen bezeichnete man die aktualisierte DFS-Version nach EN 301 893-V1.5 kurz als "DFS3".

Generell bestimmen die Werte Pulsrate, Pulsbreite und Anzahl der Pulse ein Pulsmuster. Die bisherigen DFS-Verfahren gaben vor, nur feste Radarmuster zu prüfen, die durch definierte Kombinationen verschiedener Pulsraten und Pulsbreiten im WLAN-Gerät hinterlegt waren. Nach DFS3 konnte das Gerät nun auch Muster aus wechselnden Pulsraten und Pulsbreiten als Radarmuster erkennen. Außerdem konnten innerhalb eines Radarsignals zwei oder drei unterschiedliche Pulsraten verwendet werden.

Am 01.01.2013 endet die Gültigkeit der Version ETSI EN 301 893 V1.5.1 (DFS-3). Danach gilt die neue Version ETSI EN 301 893 V1.6.1 (kurz "DFS4"), die auch kürzere Radarimpulse erkennt.

Für die Erkennung von Wetterradaren (Kanäle 120, 124 und 128 im Frequenzbereich 5,6 - 5,65 MHz) gelten besondere Nutzungsbedingungen. Die DFS-Implementierung im LCOS unterstützt die verschärften Erkennungsbedingungen nicht. Deshalb werden diese drei Kanäle von neueren LCOS-Versionen ausgespart.

Ergänzungen im Setup-Menü

Bevorzugtes-DFS-Schema

Alle WLAN-Systeme, die nach Inkrafttreten der EN 301 893-V1.6 in Betrieb genommen werden, müssen im 5GHz-Band DFS4 verwenden.

Hier haben Sie die Möglichkeit zwischen DFS2 (EN 301 893-V1.3), DFS3 (EN 301 893-V1.5) und DFS4 (EN 301 893-V1.6) zu wählen.

SNMP-ID:

2.23.20.8.20

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

Default:

EN 301 893-V1.6

Bei einem Upgrade von einer Firmware vor LCOS-Version 8.80 auf eine LCOS-Version 8.80 oder höher, wird die vorherige Einstellung DFS3 (EN 301 893-V1.5) beibehalten.

6.8 PMK-Caching im WLAN-Client-Modus

Beim Verbindungsaufbau eines WLAN-Clients zu einem Access Point handeln die beiden Gegenstellen im Rahmen der 802.1x-Authentifizierung einen gemeinsamen Schlüssel für die nachfolgende Verschlüsselung aus, den Pairwise Master Key (PMK). Bei Anwendungen mit bewegten WLAN-Clients (Notebooks in größeren Büro-Umgebungen, bewegte Objekte mit WLAN-Anbindung im Industriebereich) wechseln die WLAN-Clients häufig den Access Point, bei dem sie sich in einem WLAN-Netz anmelden. Die WLAN-Clients roamen also zwischen verschiedenen, aber in der Regel immer den gleichen Access Points hin und her.

Access Points speichern üblicherweise einen ausgehandelten PMK für eine bestimmte Zeit. Auch ein WLAN-Gerät in der Betriebsart als WLAN-Client speichert den PMK. Sobald ein WLAN-Client einen Anmeldevorgang bei einem Access Point startet, zu dem zuvor schon einer Verbindung bestand, kann der WLAN-Client direkt den vorhandenen PMK zur Prüfung an den Access Point übermitteln. Die beiden Gegenstellen überspringen so die Phase der PMK-Aushandlung während des Verbindungsaufbaus, WLAN-Client und Access Point stellen die Verbindung deutlich schneller her.

6.8.1 Ergänzungen im Setup-Menü

PMK-Caching

Aktiviert das PMK-Caching im WLAN-Client-Modus

SNMP-ID:

2.23.20.3.15

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

PMK-Caching

Verwalten Sie hier das PMK-Caching.

SNMP-ID:

2.12.85

Pfad Telnet:

Setup > **WLAN** > **PMK-Caching**

Vorgabe-Lebenszeit

Definiert die Dauer in Sekunden, für die der PMK gültig ist.

SNMP-ID:

2.12.85.1

Pfad Telnet:

Setup > **WLAN** > **PMK-Caching** > **Vorgabe-Lebenszeit**

Mögliche Werte:

max. Zeichen aus 0123456789

Besondere Werte:

0:

Default:

0

6.8.2 Ergänzungen im Status-Menü

PMK-Caching

Dieses Verzeichnis enthält den Status des PMK-Caches.

SNMP-ID:

1.3.60

Pfad Telnet:

Status > **WLAN** > **PMK-Caching**

Inhalt

Dieses Tabelle enthält alle Einträge des PMK-Caches.

SNMP-ID:

1.3.60.1

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Authenticator

Dieser Eintrag enthält die MAC-Adresse des authentifizierenden Access-Points.

SNMP-ID:

1.3.60.1.1

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Supplicant

Dieser Eintrag enthält die MAC-Adresse des sich authentifizierenden WLAN-Clients.

SNMP-ID:

1.3.60.1.2

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Benutzername

Dieser Eintrag enthält den Benutzernamen, den der RADIUS-Server bei Zugangsgenehmigung an den Access-Point sendet.

Übermittelt der RADIUS-Server keinen Benutzernamen, bleibt dieses Feld leer.

SNMP-ID:

1.3.60.1.4

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

VLAN-Id

Dieser Eintrag enthält die VLAN-Id, die der RADIUS-Server bei Zugangsgenehmigung an den Access-Point sendet.

Übermittelt der RADIUS-Server keinen VLAN-Id, bleibt dieses Feld leer.

SNMP-ID:

1.3.60.1.4

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Lebenszeit

Dieser Eintrag enthält die Lebenszeit des PMKs in Sekunden. Sie berechnet sich aus der Gültigkeit der Sitzung, die der RADIUS-Server in der Zugangsgenehmigung übermittelt.

Die Wert beträgt 0 Sekunden, wenn der RADIUS keine Dauer überträgt bzw. der PMK keinen Gültigkeitszeitraum besitzt.

SNMP-ID:

1.3.60.1.5

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Lebenszeit

Dieser Eintrag zeigt, ob ein PMK abgelaufen ist. Ist das der Fall, akzeptiert der Access-Point keine PMK-Caching- oder Authentifizierungs-Versuche mit diesem PMK mehr. Stattdessen startet er eine neue 802.1x-Authentifizierung.

SNMP-ID:

1.3.60.1.6

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

Quelle

Dieser Eintrag zeigt an, auf welchem Weg der WLAN-Client den PMK bezogen hat:

- **Unbekannt**: Die Quelle ist unbekannt. Dieser Eintrag sollte im normalen Betrieb nicht vorkommen.
- **Authentifizierung**: Der PMK ist das Ergebnis einer normalen 802.1x-Authentifizierung zwischen WLAN-Client und Access-Point.
- **Prä-Authentifizierung**: Der PMK ist das Ergebnis einer 802.1x-Prä-Authentifizierung zwischen WLAN-Client und einem weiteren Access-Point.

SNMP-ID:

1.3.60.1.7

Pfad Telnet:

Status > **WLAN** > **PMK-Caching** > **Inhalt**

6.9 Prä-Authentifizierung im WLAN-Client-Modus

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

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

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

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

Client-seitig ist die Anzahl gleichzeitiger Prä-Authentifizierungen auf vier begrenzt, um in Netzwerk-Umgebungen mit vielen Access-Points die Netzlast für den zentralen RADIUS-Server gering zu halten.

6.9.1 Ergänzungen im Setup-Menü

Prae-Authentisierung

Aktiviert die Prä-Authentifizierung für das entsprechende WLAN.

Um Prä-Authentifizierung nutzen zu können, muss das PMK-Caching aktiviert sein.

SNMP-ID:

2.23.20.3.16

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Nein

6.10 Zeitversetztes Roaming für Dual-Radio-Client WLAN-Module

Wechselt ein Dual-Radio-Client von einer WLAN-Funkzelle in eine benachbarte Funkzelle, sorgt Multi-Radio-Handover-Koordinierung dafür, dass immer ein WLAN-Modul mit dem aktuellen Access-Point verbunden bleibt, bis das andere WLAN-Modul sich erfolgreich in der neuen WLAN-Funkzelle angemeldet hat.

Ist die Funktion aktiviert und befinden sich ein oder mehrere WLAN-Module in der Registrierungsphase, sperrt der WLAN-Client die Registrierung des WLAN-Moduls mit bestehender Verbindung, damit sich nicht beide Module gleichzeitig in einer neuen Funkzelle anzumelden versuchen und infolgedessen kurzzeitig keines der beiden WLAN Module über eine Verbindung verfügt.

Sollte das gesperrte WLAN-Modul die Verbindung verlieren, bevor eines der anderen Module eine neue Verbindung ausgehandelt hat, gibt der Client dieses Modul wieder zur Aushandlung einer neuen Verbindung frei.

Hat sich ein WLAN-Modul erfolgreich in der neuen WLAN-Funkzelle angemeldet, bleibt diese Verbindung für eine Mindestdauer bestehen, damit der Access-Point der neuen Funkzelle genügend Zeit hat, seine Netzwerkeinträge zu aktualisieren.

6.10.1 Ergänzungen im Menüsystem

Dual-Roaming

Verwalten Sie hier das Roaming-Verhalten von Geräten mit mehreren WLAN-Modulen.

SNMP-ID:

2.12.80

Pfad Telnet:

Setup > **WLAN** > **Dual-Roaming**

Gruppe

Bestimmt, ob alle WLAN-Module am Dual-Roaming teilnehmen.

SNMP-ID:

2.12.80.1

Pfad Telnet:

Setup > **WLAN** > **Dual-Roaming**

Mögliche Werte:

Aus

WLAN-1 + WLAN-2

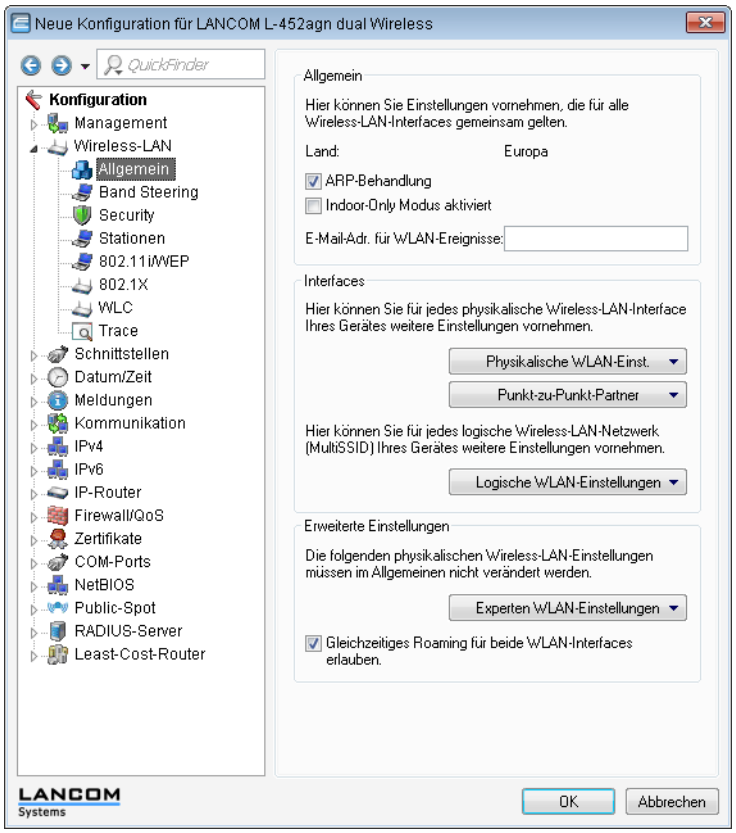
Default:

Aus

6.10.2 Ergänzungen in LANconfig

Zeitversetztes Roaming für Dual-Radio-Client WLAN-Module

Das zeitversetzte Roaming aktivieren Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen** > **Gleichzeitiges Roaming für beide WLAN-Interfaces erlauben** .



6.11 Greenfield-Modus für Access Points mit IEEE 802.11n

Bei Access Points nach dem Standard IEEE 802.11n haben Sie in den physikalischen WLAN-Einstellungen die Möglichkeit, die Datenübertragung nach den Standards IEEE 802.11a/b/g/n gezielt zu erlauben oder einzuschränken.

Neben der Auswahl der einzelnen Standards a/b/g und verschiedenen gemischten Betriebsarten erlauben die Access Points auch die Auswahl des Greenfield-Modus. Wenn Sie in den physikalischen WLAN-Einstellungen einer WLAN-Schnittstelle den Greenfield-Modus aktivieren, können sich nur WLAN-Clients in die zugehörigen logischen WLANs

(SSIDs) einbuchen, die ihrerseits den Standard IEEE 802.11n unterstützen. Andere WLAN-Clients, die ausschließlich nach den Standards IEEE 802.11a/b/g arbeiten, können sich nicht in diese WLANs einwählen.

Der Standard IEEE 802.11n erlaubt nur Verschlüsselungen nach WPA2/AES und unverschlüsselte Verbindungen. WEP- und TKIP-basierte Verschlüsselungen sind in IEEE 802.11n nicht erlaubt. Bitte beachten Sie je nach Einstellungen der physikalischen und logischen WLAN-Einstellungen die folgenden Einschränkungen:

- Wenn Sie in den physikalischen Einstellungen einen gemischten Modus mit Unterstützung für den Standard IEEE 802.11n aktivieren ist und einzelne WLAN-Clients in einem logischen Netzwerk nur WEP-Verschüsselung erlauben, reduziert der Access Point die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit WEP nicht erlaubt sind.
- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs neben AES auch andere Sitzungsschlüssel nach TKIP erlauben, verwendet der Access Point für dieses WLAN ausschließlich den Sitzungsschlüssel nach AES, weil TKIP nach IEEE 802.11n nicht erlaubt ist.
- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs ausschließlich Sitzungsschlüssel nach TKIP erlauben, reduziert der Access Point die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit TKIP nicht erlaubt sind

6.12 Separate RADIUS-Server pro SSID

Wenn Sie RADIUS zur zentralen Verwaltung von Konto- und Zugangsinformationen in Ihren WLANs einsetzen, übernimmt standardmäßig der Access Point zentral das Weiterleiten der Anfragen für die Authorisierung und das Accounting an den RADIUS-Server. Sofern Sie für die Verwaltung der Access Points einen WLAN-Controller einsetzen, kann auch der WLAN-Controller die RADIUS-Anfragen von allen angeschlossenen Access Points an den entsprechenden RADIUS-Server weiterleiten.

In manchen Anwendungsfällen möchte der Betreiber von Access Points oder WLAN-Controllern jedoch unterschiedliche RADIUS-Server für einzelnen logischen WLANs (SSIDs) einsetzen. Das ist z.B. dann der Fall, wenn mehrere Kunden die technische WLAN-Infrastruktur gemeinsam nutzen, dabei jedoch eigene Systeme zur Authentifizierung einsetzen (zum Beispiel bei Wireless as a Service - WaaS).

In diesen Fällen haben Sie die Möglichkeit, für jedes logische WLAN (also jede SSID) ein separates RADIUS-Profil zu wählen. Das RADIUS-Profil enthält alle notwendigen Angaben zur Nutzung der entsprechenden RADIUS-Server inklusive der optionalen Backup-Lösung.

6.12.1 Ergänzungen im Menüsystem

RADIUS-Server-Profiles

Standardmäßig übernimmt Ihr WLAN-Controller die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung zum RADIUS-Server. Damit die Access Points den entsprechenden RADIUS- Server direkt ansprechen können, definieren sie in dieser Tabelle die nötigen RADIUS-Profile. Bei der Definition der logischen WLANs (SSISs) haben Sie die Möglichkeit, pro SSID ein separates RADIUS-Profil zu wählen.

SNMP-ID: 2.37.35

Pfad Telnet: /Setup/WLAN-Management

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

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 Access Point die entsprechenden RADIUS-Anfragen an den WLAN Controller.

SNMP-ID: 2.37.35.7

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

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

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

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

Access-Protokoll

Protokoll für die Kommunikation zwischen dem Access Point 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

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 Access Point die entsprechenden RADIUS-Anfragen an den WLAN Controller.

SNMP-ID: 2.37.35.2

Pfad Telnet: /Setup/WLAN-Management/RADIUS-Server-Profiles

Mögliche Werte:

- Gültige IP-Adresse.

Default: 0.0.0.0

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

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

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

Account-Protokoll

Protokoll für die Kommunikation zwischen dem Access Point 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

Backup

Name des Backup-RADIUS-Profils. Unter diesem Namen referenzieren Sie das Backup-RADIUS-Profil aus den logischen WLAN-Einstellungen. Der WLAN-Controller 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

Netzwerkprofile

Hier definieren Sie die logischen WLAN-Netzwerke, die auf den angemeldeten Access-Points (APs) aktiviert und betrieben werden können.

SNMP-ID: 2.37.1.1

Pfad Telnet: /Setup/WLAN-Management/AP-Konfiguration

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:

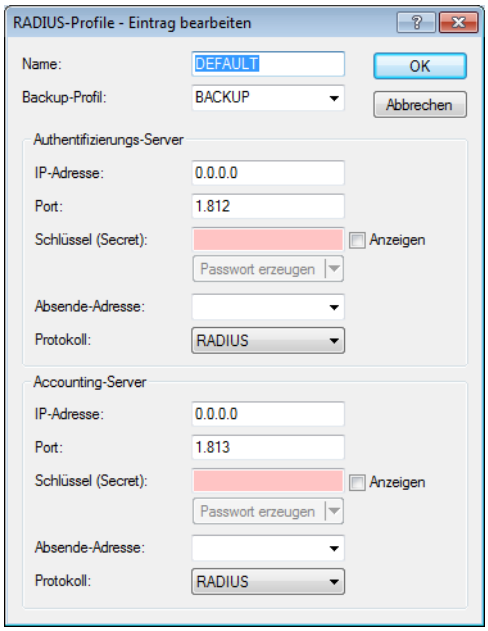
- max. 16 Zeichen

Default: leer

6.12.2 Ergänzungen in LANconfig

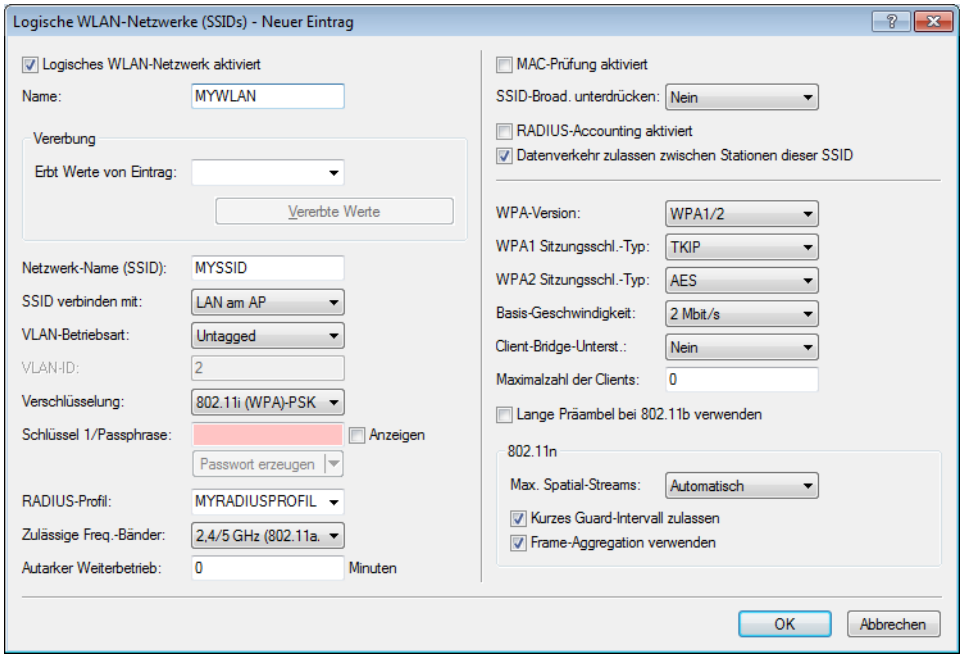
Einstellung der RADIUS-Profile

Die Einstellungen für die RADIUS-Profile im WLAN-Controller finden Sie in LANconfig unter **WLAN-Controller** > **Profile** > **RADIUS-Profile** .



Auswahl eines RADIUS-Profils für ein logisches WLAN

Die Auswahl des RADIUS-Profils für ein logisches WLAN im WLAN-Controller finden Sie in LANconfig unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** .



7 Public Spot

7.1 Verwaltung von Public-Spot-Nutzern über das Web-API

Über die Eingabe einer speziellen URL in der Adresszeile haben Sie die Möglichkeit, Public-Spot-Benutzer direkt statt über den Setup-Assistenten anzuzeigen, neu anzulegen oder zu löschen.

7.1.1 Hinzufügen eines Public-Spot-Benutzers

Über die folgende URL registrieren Sie einen neuen Public-Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`comment`

Kommentar zum registrierten Benutzer

Sind für einen Public-Spot-Benutzer mehrere Kommentare möglich, geben Sie die Kommentare und die entsprechenden Kommentarfeld-Namen wie folgt an:

```
&comment=<Inhalt1>:<Feldname1>;<Inhalt2>:<Feldname1>;
   ...;<Inhalt5>:<Feldname5>
```

Existiert ausschließlich ein Kommentarfeld pro Benutzer, genügt die Angabe des Kommentars:

```
&comment=<Kommentar>
```

Deutsche Umlaute werden nicht unterstützt.

Die maximale Zeichenanzahl des Kommentar-Parameters beträgt 191 Zeichen.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche, über die Sie den Voucher ausdrucken können.

`printcomment`

Kommentar auf den Voucher drucken.

Fehlt dieser Parameter, erscheint der Kommentar nicht auf dem Voucher (Default-Einstellung).

`nbguests`

Anzahl der anzulegenden Public-Spot-Benutzer.

Fehlt dieser Parameter, legt der Assistent ausschließlich einen Benutzer an (Default-Einstellung).

`defaults`

Default-Werte verwenden

Der Assistent ersetzt fehlende oder falsche Parameter durch Default-Werte.

`expiretype`

Kombinierte Angabe von Ablauf-Typ und Verfalls-Dauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expiretype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ (absolut, relativ, absolute und relativ, none)
- `Wert2`: Verfallsdauer des Vouchers

Fehlt dieser Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`ssid`

Netzwerk-Name

Fehlt dieser Parameter, verwendet der Assistent den Standard-Netzwerk-Namen (Default-Einstellung).

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`multilogin`

Mehrfach-Login

Wenn Sie diesen Parameter angeben, kann sich der Benutzer mehrfach mit seinem Benutzer-Account anmelden. Fehlt dieser Parameter, ist der Mehrfach-Login defaultmäßig deaktiviert.

Sind für fehlende Parameter in der Public-Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesen die fehlenden Werte ein.

7.2 Public-Spot-Benutzer-Verwaltung

Die Setup-Wizards unterstützen Sie auch bei der einfachen Verwaltung von Public-Spot-Benutzern.

7.2.1 Neue Public-Spot-Benutzer mit einem Klick hinzufügen

Registrieren Sie neue Public-Spot-Benutzer über WEBconfig mit dem Setup-Wizard **Public-Spot-Benutzer einrichten.**. Der Wizard ist mit Standard-Werten voreingestellt, so dass Sie mit einem Klick auf **Speichern & Drucken** einen neuen

Benutzer einrichten. Bei einem Klick auf **Speichern & CSV-Export** stellt Ihnen der Assistent die Voucherdaten als CSV-Datei zum Download zur Verfügung.

Die folgenden Einstellungen sind nach Bedarf konfigurierbar:

- **Startzeitpunkt des Zugangs:** Legt fest, ab wann der Voucher gültig ist. Mögliche Werte sind:
  - **erster Login (Default)**: Zugang gilt ab Erstanmeldung des Benutzers
  - **sofort:** Zugang gilt ab Anlegen des Benutzers
- **Gültigkeitsdauer des Vouchers:** Geben Sie die Dauer an, nach der der Voucher ungültig wird.

  Es ist unmöglich eine Gültigkeitsdauer einzutragen, wenn der Zugang ab sofort gültig ist.
- **Dauer des Zugangs:** Wählen Sie die Dauer aus, für die dieser Zugang ab Registrierung oder Erstanmeldung gültig ist.
- **SSID (Netzwerkname):** Wählen Sie aus, für welches WLAN-Netz der Zugang gilt. Der Standard-Netzwerkname ist bereits markiert. Die hier aufgelisteten SSIDs verwalten Sie in der SSID-Tabelle.

  Drücken Sie die "Strg"-Taste, um mehrere Einträge auszuwählen.
- **Anzahl Voucher:** Geben Sie an, wie viele Vouchers Sie gleichzeitig erstellen möchten (Default: 1).
- **Zeit-Budget (Minuten):** Geben Sie an, nach welcher Online-Zeit der Public-Spot-Zugang schließt.

  Je nach gewählter Ablauf-Methode bestimmt entweder dieses Zeit-Budget (inkrementell) oder die eingestellte Voucher-Zugangsdauer (absolut) die Frist für den Zugang.
- **Volumen-Budget (MByte):** Geben Sie an, nach welcher übertragenen Datenmenge der Zugang schließt.
- **Kommentar (optional):** Fügen Sie einen Kommentar ein.
- **Drucke Kommentar auf Voucher:** Aktivieren Sie diese Option, damit der Kommentar auf dem Voucher erscheint.
- **Drucken:** Aktivieren Sie diese Option, damit Sie beim Speichern gleichzeitig die registrierten Vouchers ausdrucken (Default: an).

  Wenn Sie diese Option deaktiviert haben, zeigt Ihnen der Assistent nach der Registrierung eine Übersicht der neuen Public-Spot-Benutzer. Sie erhalten dann noch einmal die Gelegenheit, die Vouchers auszudrucken.
- **Mehrfach-Logins:** Aktivieren Sie diese Option, damit sich ein Benutzer mehrfach mit seinem Benutzer-Account am Public-Spot anmelden kann (Default: aus).

Konfigurieren Sie die Default-Werte für die Einrichtung neuer Public-Spot-Zugänge in folgenden Menüs:

- LANconfig: **Public-Spot** > **Public-Spot Assistent**
- WEBconfig: **LCOS-Menübaum** > **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

7.3 Groß-/Klein-Schreibung beim Benutzernamen einstellen

Sie können festlegen, ob RADIUS-Server und Benutzer-Assistent die korrekte Groß-/Kleinschreibung des Benutzernamens prüfen sollen.

7.3.1 RADIUS-Server

In der Benutzer-Tabelle des RADIUS-Servers ist bei jedem Benutzer die Option gespeichert, ob der RADIUS-Server bei Benutzer-Anmeldung auf Groß- und Kleinschreibung achten soll. Das kann je nach Einstellung dazu führen, dass Benutzereinträge nicht eindeutig sind.

Beispielsweise können in der Benutzertabelle drei am Public-Spot registrierte Benutzer mit jeweils gültiger Options-Einstellung **Case-sensitiv** existieren:

- Benutzer 1: `Testuser`, Case-sensitiv: `ja`
- Benutzer 2: `testuser`, Case-sensitiv: `nein`
- Benutzer 3: `TESTUSER`, Case-sensitiv: `nein`

Bei der Anfrage eines Benutzers `Testuser` muss der RADIUS-Server entscheiden können, welcher Benutzer sich gerade anmelden möchte. Er wählt den Benutzer aus der Tabelle nach der folgenden Prioritätenliste:

1. Einträge mit aktivierter Groß-/Kleinschreibung (Case-sensitiv: ja) haben die höchste Priorität.
2. Danach überprüft der RADIUS-Server die Einträge für die Stations-ID-Masken in der jeweiligen Benutzereinstellung (**Setup** > **RADIUS** > **Server** > **Benutzer**) in dieser Reihenfolge:
   a. **Rufende-Station-Id-Maske**: Ein Eintrag ohne Wildcards ('?' oder '*') hat eine höhere Priorität als ein Eintrag mit Wildcards. Eine leere Maske gilt als Wildcard-Ausdruck ('*')
   b. **Gerufene-Station-Id-Maske**: Ein Eintrag ohne Wildcards ('?' oder '*') hat eine höhere Priorität als ein Eintrag mit Wildcards. Eine leere Maske gilt als Wildcard-Ausdruck ('*')
3. Sollten sich danach noch Konflikte ergeben, wählt der RADIUS-Server den obersten Eintrag in der Tabelle.

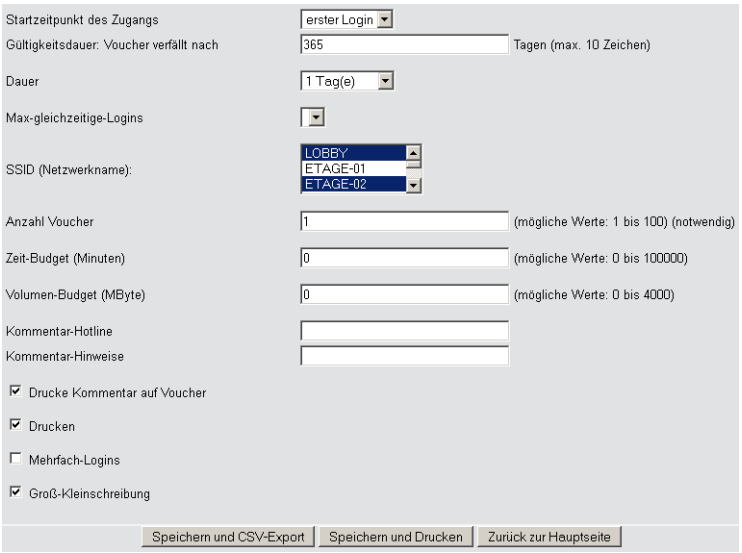
Unter **Setup** > **RADIUS** > **Server** > **Benutzer** > **Case-Sensitiv** können Sie festlegen, ob der RADIUS-Server die Groß-/Kleinschreibung des ausgewählten Benutzernamens beachten soll.

7.3.2 Public-Spot-Assistent

Bei der Registrierung eines neuen Public-Spot-Benutzers hinterlegt der Public-Spot-Assistent im jeweiligen Benutzerprofil, ob die Groß-/Kleinschreibung bei der Anmeldung erforderlich ist.

Unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** können die folgenden Einstellungen für den Public-Spot-Assistenten festlegen:

- **Groß-Kleinschreibung**: Hier bestimmen Sie, ob der Assistent die Beachtung der Groß-/Kleinschreibung für neu registrierte Benutzer vorschreibt. Der Standardwert ist "ja".
- **Groß-Kleinschreibung-Schalter-verstecken**: Falls der Public-Spot-Administrator die Einstellung für Groß-/Kleinschreibung beim Ausführen des Assistenten nicht mehr ändern soll, können Sie hier das Auswahlkästchen im Public-Spot-Assistenten ausblenden. Der Standardwert ist "ja".



7.3.3 Ergänzungen im Setup-Menü

Case-Sensitiv

Mit dieser Einstellung bestimmen Sie, ob der RADIUS-Server die Groß-/Kleinschreibung des Benutzernamens beachtet.

SNMP-ID:

2.25.10.7.17

Pfad Telnet:

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

Mögliche Werte:

Ja

Nein

Default:

Ja

Groß-Kleinschreibung

Mit dieser Einstellung bestimmen Sie, ob der Assistent für das Anlegen eines neuen Public-Spot-Benutzers die Groß-/Kleinschreibung des Benutzernamens beachtet.

SNMP-ID:

2.24.19.12

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Ja

Nein

Default:

Ja

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.

SNMP-ID:

2.24.19.13

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Ja

Nein

Default:

Ja

7.4 Selbständige Benutzeranmeldung für Public Spot

Geräte mit Public Spot bieten Anwendern einen zeitlich begrenzten Zugang zu drahtlosen Netzwerken. Für das Anlegen eines solchen Zugangs war bisher ein Administrations-Account auf dem Gerät mit Public Spot erforderlich. Für die Mitarbeiter an der Rezeption in einem Hotel legen Sie dazu z. B. einen speziellen Administrations-Account an, der ausschließlich über die Funktionsrechte zum Anlegen von Public-Spot-Benutzern verfügt. Mit wenigen Mausklicks kann der Mitarbeiter dann den Hotelgästen einen Voucher für den Zugang zum drahtlosen Netzwerk ausdrucken.

Allerdings erfordert auch die komfortable Lösung mit Vouchers immer die Aktivität eines Administrators. Alternativ können Sie den Nutzern die Möglichkeit einräumen, auf der Startseite des Public Spot selbst Zugangsdaten zum drahtlosen Netzwerk zu generieren und sich die Zugangsdaten per E-Mail oder SMS zusenden zu lassen. Für die Zusendung der SMS nutzt das Gerät dabei einen externen SMS-Dienstanbieter, der je nach Wunsch die Gebühren der SMS dem Nutzer belastet.

7.4.1 Ergänzungen im Setup-Menü

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 zwei Möglichkeiten:

- Die Anmeldung erfolgt mit Benutzername und Passwort oder zusätzlich mit der physikalischen bzw. MAC-Adresse. In diesem Fall teilt der Adminstrator den Benutzers die Zugangsdaten z.B. mt einem Ausdruck mit.
- Alternativ erfolgt der Versand der Zugangsdaten bei erstmaliger Anmeldung automatisch entweder per E-Mail oder per SMS.

SNMP-ID:

2.24.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Modus**

Mögliche Werte:

keine

Benutzer+Passwort

MAC+Benutzer+Passwort

Email

Email2SMS

Default:

Email2SMS

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.

SNMP-ID:

2.24.41

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module**

EMail-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.

SNMP-ID:

2.24.41.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung**

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 leere Domain-List als Black-List alle Domains ablehnt.

SNMP-ID:

2.24.41.1.9

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Domain-List**

Mögliche Werte:

Gültige E-Mail-Domänen (z. B. @web.de) mit maximal 150 Zeichen.

Default:

leer

Benutzer-Muss-AGBs-Akzeptieren

Mit diesem Parameter legen Sie fest, ob ein Benutzer Ihre AGBs akzeptieren muss, um den Zugriff auf das Netzwerk zu nutzen.

SNMP-ID:

2.24.41.1.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Benutzer-Muss-AGBs-Akzeptieren**

Mögliche Werte:

ja

nein

Default:

ja

Betreffzeile

Geben Sie hier den in der versendeten E-Mail angezeigten Betreff ein.

SNMP-ID:

2.24.41.1.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Max. 250 Zeichen

Default:

Your Public Spot Account

Black-White-Domain-List

In diesem Menü haben Sie die Möglichkeit, eine von Ihnen erstellte Liste mit Dömanen von E-Mail-Anbietern als "Blacklist" oder als "Whitelist" zu definieren. Stellen Sie das Auswahlmenü auf "Blacklist", wenn Sie die aufgeführten Anbieter generell sperren möchten. Verwenden Sie "Whitelist", um die aufgeführten Anbieter generell zuzulassen.

SNMP-ID:

2.24.41.1.8

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Black-White-Domain-List**

Mögliche Werte:

Blacklist

Whitelist

Default:

Blacklist

EMail-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.

SNMP-ID:

2.24.41.1.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **EMail-pro-Stunde-Limit**

Mögliche Werte:

Max. 5 Ziffern

Default:

100

Lokale-EMail-Adresse

Geben Sie hier die in der versendeten E-Mail angezeigte Absenderadresse ein.

SNMP-ID:

2.24.41.1.6

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Lokale-EMail-Adresse**

Mögliche Werte:

Gültige E-Mail-Adresse mit maximale 150 Zeichen.

Default:

leer

Max-Request-Versuche

Mit diesem Parameter legen Sie fest, wieviele verschiedene Zugangsdaten Sie innerhalb eines Tages für eine MAC-Adresse bereitstellen.

SNMP-ID:

2.24.41.1.5

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Max-Request-Versuche**

Mögliche Werte:

Max. 5 Ziffern

Default:

3

Name

Geben Sie hier den in der versendeten E-Mail angezeigten Absendernamen ein.

SNMP-ID:

2.24.41.1.7

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Name**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

Textinhalt

Mit diesem Parameter legen Sie den Inhalt der versendeten E-Mail fest, wobei $PSpotPasswd die Variable für das generierte Passwort ist.

SNMP-ID:

2.24.41.1.4

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Max. 500 Zeichen

Default:

Your Password for LANCOM Public Spot is $PSpotPasswd.

EMail2Sms-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.

SNMP-ID:

2.24.41.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung**

Erlaubte-Landesvorwahlen

Mit dieser Liste können Sie zulässige Landesvorwahlen für die Anwahl ausländischer Telefonnummern festlegen, um z. B. den Anruf in bestimmte Länder auszuschließen.

SNMP-ID:

2.24.41.2.11

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Erlaubte-Landesvorwahlen**

Mögliche Werte:

Ländername und zugehörige Landesvorwahl in der Schreibweise ohne Plus-Zeichen und ohne führende Nullen.

Default:

leer

Benutzer-muss-AGBs-akzeptieren

Mit diesem Parameter legen Sie fest, ob ein Benutzer Ihre AGBs akzeptieren muss, um den Zugriff auf das Netzwerk zu nutzen.

SNMP-ID:

2.24.41.2.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Benutzer-muss-AGBs-akzeptieren**

Mögliche Werte:

ja

nein

Default:

ja

Betreffzeile

Geben Sie hier den in der versendeten E-Mail angezeigten Betreff 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:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers
- `$PSpotPasswd` für das vom Public-Spot generierte Password des Benutzers

SNMP-ID:

2.24.41.2.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Betreffzeile**

Mögliche Werte:

Max. 250 Zeichen

Default:

Your Password for LANCOM Public Spot is `$PSpotPasswd`.

EMail-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.

SNMP-ID:

2.24.41.2.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **EMail-pro-Stunde-Limit**

Mögliche Werte:

Max. 5 Ziffern

Default:

100

Gateway-EMail-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:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers
- `$PSpotPasswd` für das vom Public-Spot generierte Password des Benutzers

SNMP-ID:

2.24.41.2.13

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Gateway-EMail-Adresse**

Mögliche Werte:

Gültige E-Mail-Adresse eines Gateways mit max. 150 Zeichen. .

Default:

leer

Lokale-EMail-Adresse

Geben Sie hier die in der versendeten E-Mail angezeigte Absenderadresse ein.

SNMP-ID:

2.24.41.2.5

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Lokale-EMail-Adresse**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

Max-Request-Versuche

Mit diesem Parameter legen Sie fest, wie viele verschiedene Zugangsdaten Sie innerhalb eines Tages für eine MAC-Adresse bereitstellen.

SNMP-ID:

2.24.41.2.4

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Max-Request-Versuche**

Mögliche Werte:

Max. 5 Ziffern

Default:

3

Name

Geben Sie hier den in der versendeten SMS angezeigten Absendernamen ein.

SNMP-ID:

2.24.41.2.6

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Name**

Mögliche Werte:

Max. 150 Zeichen

Default:

leer

Textinhalt

Mit diesem Parameter legen Sie den Inhalt der versendeten E-Mail fest. 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:

- `$PSpotUserMobileNr` für die Mobilfunknummer des Benutzers
- `$PSpotPasswd` für das vom Public-Spot generierte Password des Benutzers

SNMP-ID:

2.24.41.2.12

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **EMail2Sms-Authentifizierung** > **Textinhalt**

Mögliche Werte:

Max. 512 Zeichen

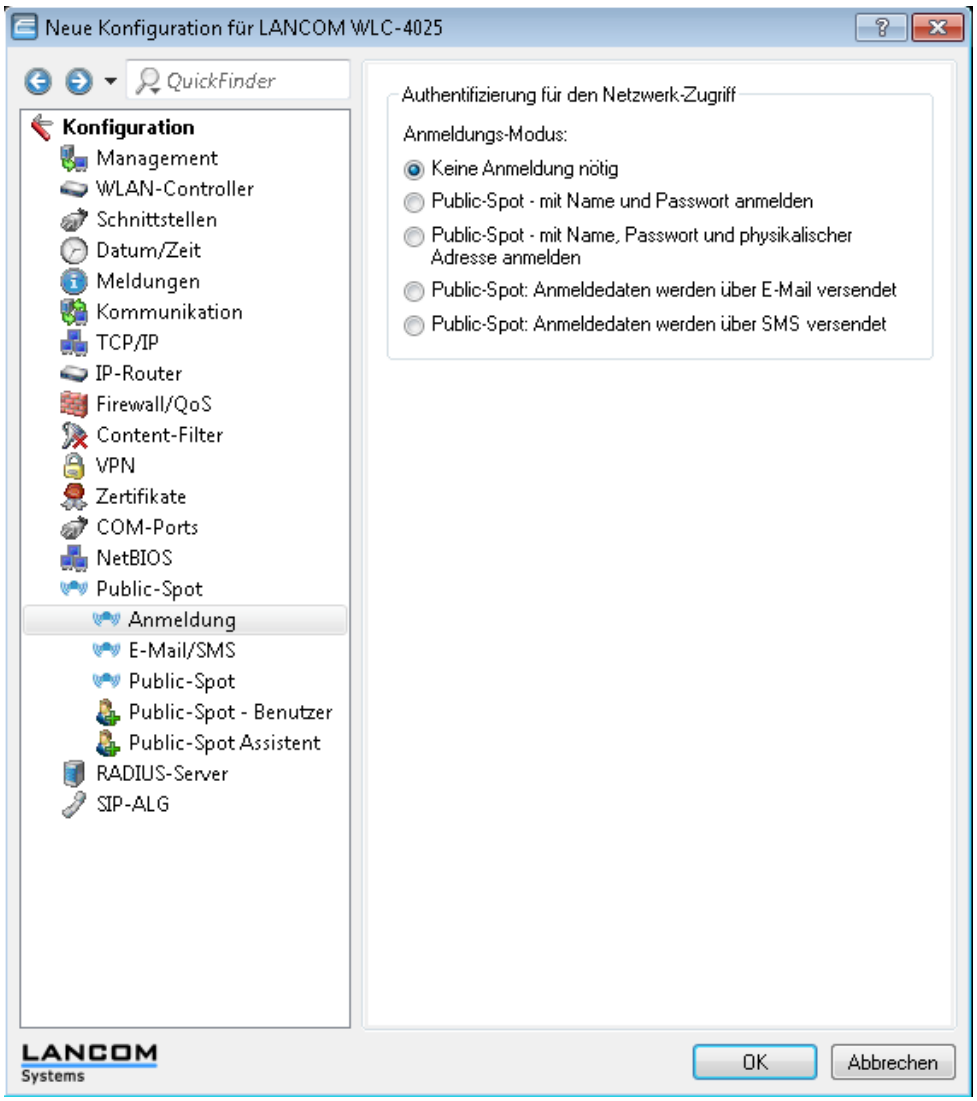
Default:

#Key#Route#From#

7.4.2 Ergänzungen in LANconfig

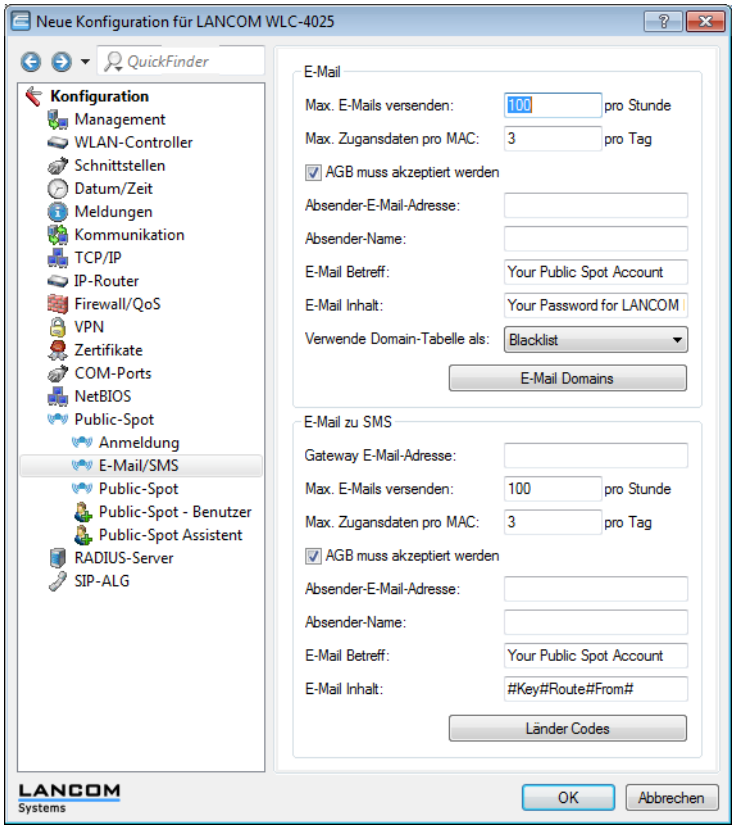
Anmeldung

In diesem Dialog legen Sie die Einstellungen für die Authentifizierung am Netzwerk und den Versand der Anmeldedaten fest.



E-Mail/SMS

In diesem Dialog definieren Sie die Einstellungen für den Versand der Anmeldedaten über E-Mail oder SMS.



7.5 DNS-Snooping

Sie können den Public-Spot-Benutzern gestatten, Webseiten, Webserver oder ganze Netze auch ohne Registrierung bzw. Anmeldung am Public-Spot zu benutzen. Die entsprechenden Adressen erfassen Sie hier:

- LANconfig: **Public-Spot** > **Public-Spot** > **Zugriff ohne Anmeldung ermöglichen** > **Freie-Netze**
- WEBconfig: **Setup** > **Public-Spot-Modul** > **Freie-Netze**

Webdienste mit hohen Nutzerzahlen verteilen die Datenanfragen zur besseren Auslastung auf mehrere Server. So kommt es, dass zwei DNS-Anfragen für denselben Hostnamen (z. B. "www.google.de") zu zwei unterschiedlichen IP-Adressen führen können.

Bei Eingabe eines Hostnamens erhält der Public-Spot vom zuständigen DNS-Server unter Umständen mehrere gültige IP-Adressen, speichert allerdings davon nur eine für zukünftige Anfragen von Public-Spot-Benutzern. Bekommt der Benutzer jedoch bei einer weiteren Anfrage für denselben Hostnamen die IP-Adresse eines anderen Servers zugeteilt, sperrt der Public-Spot diese Verbindung, weil er diese IP-Adresse nicht als zugangsberechtigt gespeichert hat.

Damit Public-Spot-Benutzer sich trotz wechselnder IP-Adressen mit dem angefragten Host verbinden können, analysiert der Public-Spot die DNS-Anfragen der Benutzer und speichert die jeweils zurückgegebene IP-Adresse zusammen mit dem Hostnamen, der Gültigkeitsdauer (TTL: "Time to Live"), dem Alter und der Datenquelle fortan als freie Zieladresse in der Tabelle **Status** > **Public-Spot** > **Freie-Hosts** .

Die Einträge in dieser Tabelle verfallen nach der in der DNS-Antwort übertragenen Gültigkeitsdauer (TTL). Um bei sehr niedrigen Werten (z. B. 5 Sekunden) den Public-Spot-Benutzer nicht sofort nach einer Anfrage wieder auszusperren, können Sie unter **Setup** > **Public-Spot-Modul** > **Freie-Hosts-Minimal-TTL** eine Mindest-Gültigkeitsdauer festlegen.

7.5.1 Ergänzungen im Setup-Menü

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').

SNMP-ID:

2.24.32

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

7.5.2 Ergänzungen im Status-Menü

Freie-Netzwerke

Die Tabelle **Freie-Netzwerke** unter **Status** > **Public-Spot** entfällt ab LCOS-Version 8.80. Die Liste der für den Public-Spot-Benutzer frei verfügbaren Hosts, Sub-Netzwerke und IP-Adressen finden Sie nun in den Tabellen **Status** > **Public-Spot** > **Freie-Hosts** und **Status** > **Public-Spot** > **Freie-Netze** .

Freie-Netze

Diese Tabelle enthält eine Liste aller aktuell von Public-Spot-Benutzern verwendeten Netzwerken (mit **Adresse** und **Maske**), die im Setup unter **Setup** > **Public-Spot-Modul** > **Freie-Netze** freigegeben sind und die ein komplettes Sub-Netzwerk beschreiben (also eine andere Netzmaske als '255.255.255.255' besitzen).

SNMP-ID:

1.44.31

Pfad Telnet:

Status > **Public-Spot**

Freie-Hosts

Diese Tabelle enthält eine Liste aller aktuell von Public-Spot-Benutzern verwendeten Netzwerken. Sie zeigt sowohl "statische" als auch "dynamische" Einträge an:

- statisch: Die statischen Einträge sind aktuell verwendete Hosts, die in der Setup-Tabelle **Setup** > **Public-Spot-Modul** > **Freie-Netze** mit IP-Adresse und einer Netzwerk-Maske von '255.255.255.255' gespeichert sind. Wenn Sie den entsprechenden Eintrag in der Setup-Tabelle löschen, löschen Sie damit auch den Eintrag in dieser Statustabelle.
- dynamisch: Die dynamischen Einträge sind die Ergebnisse der Analyse einer DNS-Antwort.

SNMP-ID:

1.44.32

Pfad Telnet:

Status > **Public-Spot**

7.6 XML-Interface

Um eine Vielzahl von Public-Spot-Szenarios abdecken zu können, ist die Standard-Authentifizierungsmethode des Public-Spots alleine über Name und Passwort nicht ausreichend. Zugriffs- und Abrechnungsmodelle über Key-Cards, Dongles oder Prepaid-Kreditkarten erfordern oft zusätzliche Zugriffsdaten, die der Public-Spot in dieser Form nicht verwalten kann.

Die implementierte XML-Schnittstelle verbindet den Public-Spot und ein externes Gateway. Sie leitet dabei die Daten des Benutzers nur an das Gateway weiter, das anschließend die Authentifizierung und Abrechnung übernimmt und dem Public-Spot nur Informationen über Dauer und Limitierungen des Benutzerzugangs mitteilt.

Der Public-Spot übernimmt also dabei nur die folgenden Aufgaben:

- Weiterleiten der Benutzeranfragen
- Einschränken von unerlaubten Zugangsversuchen
- Annahme der Gateway-Kommandos zum Starten und Beenden einer Sitzung
- ggf. Abrechnen der Sitzungen

Da es nicht sinnvoll ist, alle vorhandenen, teilweise sehr speziellen Szenarios mit den zugehörigen Gateway-Befehlen im Public-Spot zu implementieren, ist die XML-Schnittstelle universal und flexibel aufgebaut.

7.6 Funktion

Die Kommunikation zwischen XML-Interface und externem Gateway läuft ab wie folgt:

1. Der Benutzer meldet sich am Public-Spot an, öffnet die Anmeldemaske des externen Gateways und meldet sich dort mit seinen Benutzerdaten an.

   Damit der Benutzer diese Anmeldemaske öffnen kann, muss sich das externe Gateway entweder in einem frei zugänglichen Netz oder die Adresse des externen Gateways in der Liste der freien Hosts befinden.

   Das externe Gateway erhält die MAC-Adresse des anfragenden Public-Spot-Clients dabei in der Weiterleitung durch den Public-Spot. Unter **Public-Spot-Modul** > **Seitentabelle** wählen Sie dazu bei der entsprechenden Seite den **Typ** "Redirect" aus und ergänzen die **URL** um den Parameter `?myvar=%m`.

   Beispiel: `http://192.168.1.1/?myvar=%m`

   Hierbei ist `myvar` eine beliebig wählbare Variable. Entscheidend ist die Variable `%m`, die der Public-Spot beim Weiterleiten der Anfrage durch die MAC-Adresse des Public-Spot-Clients ersetzt.

2. Das Gateway prüft die Anmeldedaten des Benutzers und sendet anschließend eine XML-Datei mit den Benutzerdaten an das XML-Interface des Public-Spots. Das externe Hotspot-Gateway muss das Gerät mit Public-Spot-XML-Schnittstelle über die URL `http://<Geräte-URL>/xmlauth` ansprechen.

Der Schnittstellen-Parser analysiert diese Datei und veranlasst den Public-Spot zu den betreffenden Aktionen. Gleichzeitig bestätigt die XML-Schnittstelle die Anfrage, indem sie eine entsprechende XML-Datei an das Gateway sendet. Der Public-Spot speichert die Zugangsdaten außerdem in seinen Benutzertabellen.

Damit der Public-Spot die Anweisungen der XML-Datei verarbeiten kann, muss im Gerät ein spezieller Administrator eingerichtet sein, der das Funktionsrecht "Public-Spot-XML-Schnittstelle" besitzt. Über dieses Admin-Konto meldet sich das Gateway am Public-Spot an.

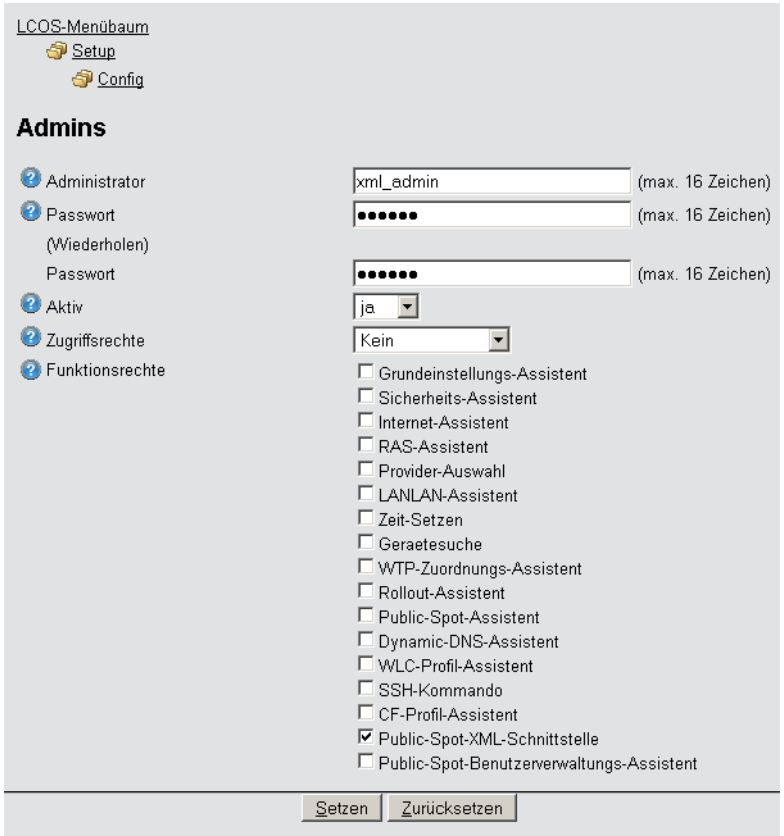
3. Während der Benutzer am Public-Spot angemeldet ist, können XML-Schnittstelle und Gateway Statusinformationen in Form von XML-Dateien über die aktuelle Session austauschen.
4. Hat der Benutzer sein Online-Kontingent ausgeschöpft, sendet das Gateway einen Stop-Befehl an das XML-Interface, woraufhin der Public-Spot dem Benutzer den weiteren Zugang sperrt.
   Auch die Sperrung des Zugangs bestätigt das XML-Interface wieder mit einer entsprechenden XML-Datei an das Gateway.

7.6 Einrichtung des XML-Interfaces über WEBconfig

Der folgende Abschnitt beschreibt die Einrichtung des XML-Interfaces.

Sie benötigen das Zugriffsrecht "Supervisor", um einen weiteren Administrator anlegen zu können.

1. Melden Sie sich auf der Startseite von WEBconfig als Administrator an.
2. Wechseln Sie in die Tabelle **LCOS-Menübaum** > **Setup** > **Config** > **Admins** und klicken Sie auf **Hinzufügen**.
3. Erstellen Sie einen neuen Administrator mit dem Funktionsrecht "Public-Spot-XML-Schnittstelle". Speichern Sie die Eingabe mit **Setzen**.



Über dieses Administrator-Konto sendet das Gateway später die XML-Dateien an die XML-Schnittstelle des Public-Spots.

4. Wechseln Sie in die Ansicht **LCOS-Menübaum** > **Setup** > **Public-Spot-Modul** > **XML-Schnittstelle** und aktivieren Sie die XML-Schnittstelle und ggf. die RADIUS-Authentifizierung.
5. Wechseln Sie in die Ansicht **LCOS-Menübaum** > **Setup** > **Public-Spot-Modul** > **Freie-Netze** und klicken Sie auf **Hinzufügen**.
6. Geben Sie den Host-Namen bzw. die IP-Adresse der Anmeldeseite des Gateways ein, dessen Dienste die Public-Spot-Benutzer nutzen dürfen. Als Netzmaske geben Sie "255.255.255.255" ein. Speichern Sie die Eingaben mit Klick auf **Setzen**.
   Durch die Speicherung als freies Netz können die Benutzer ohne Anmeldung am Public-Spot direkt auf die Anmeldeseite des Gateways zugreifen.
7. Konfigurieren Sie das Gateway so, dass es die Sitzungsdaten des Benutzers als XML-Datei an die XML-Schnittstelle des Public-Spots sendet.
   Kontaktieren Sie bei Fragen zur Konfiguration des Gateways den zuständigen Service-Provider.

7.6.1 Befehle

Das XML-Interface kann je drei Arten von Anfragen und Antworten verarbeiten:

- Login
- Logout
- Status

Dabei kann eine XML-Datei auch mehrere Anfragen bzw. Antworten enthalten.

Login

Sendet das externe Gateway in einer XML-Datei einen "Login"-Request, schaltet der Public-Spot den Online-Zugriff für den entsprechenden Benutzer frei. Ein "Login"-Request enthält das Attribut `COMMAND="RADIUS_LOGIN"`.

Verwendet der Public-Spot keinen RADIUS-Server, speichert er bei einem "Login"-Request den Benutzer inkl. seiner MAC-Adresse direkt in der internen Statustabelle. Dadurch kann er den Benutzer zukünftig sofort authentifizieren und muss ihm nicht erst eine Login-Seite anzeigen, auf der er Benutzername und Passwort eingeben muss.

Bei Verwendung eines RADIUS-Servers ist eine erfolgreiche Ausführung des "Login"-Request nur dann möglich, wenn die Anmeldedaten des entsprechende Benutzers schon im RADIUS-Server vorliegen.

Über das Web-API des Public-Spots können Sie komfortabel neue Public-Spot-Benutzer im internen RADIUS-Server des LANCOMs anlegen. Weitere Informationen dazu finden Sie im Referenzhandbuch im Kapitel "Public-Spot".

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_PASSWORD`

Benutzerpasswort

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Das XML-Interface sendet dem Gateway daraufhin eine "Login"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- RADIUS_LOGIN_ACCEPT: Login erfolgreich
- RADIUS_LOGIN_REJECT: Login wird zurückgewiesen

SUB_MAC_ADDR

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Login-Request

Das externe Gateway sendet die Daten für den Start einer Sitzung an den Public-Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Der Public-Spot aktiviert den Benutzer 'user2350' in der internen Status-Tabelle.

Login-Response:

Das XML-Interface sendet eine Bestätigung über den Start einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout

Sendet das externe Gateway in einer XML-Datei einen "Logout"-Request, sperrt der Public-Spot den Online-Zugriff für den entsprechenden Benutzer. Ein "Logout"-Request enthält das Attribut COMMAND="RADIUS_LOGOUT".

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

SUB_USER_NAME

Benutzername

Bekommt der LANCOM diesen Request und stellt das PublicSpot Modul fest, dass dieser User mit den passenden MAC online ist, loggt der LANCOM diesen aus.

SUB_MAC_ADDR

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für das Abmelden des Benutzers

Das XML-Interface sendet dem Gateway daraufhin eine "Logout"-Response, die die folgenden XML-Elemente enthalten kann:

SUB_USER_NAME

Benutzername

SUB_STATUS

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_LOGOUT_DONE`: Logout erfolgreich
- `RADIUS_LOGOUT_REJECT`: Logout wird zurückgewiesen

SUB_MAC_ADDR

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Grund für die Sperrung des Zugangs

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Logout-Request

Das externe Gateway sendet den Befehl für die Beendigung einer Sitzung an den Public-Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout-Response:

Das XML-Interface sendet eine Bestätigung über den Stopp einer Sitzung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
```

```
   <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>

    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status

Mit einem "Status"-Request erfragt das externe Gateway beim Public-Spot den aktuellen Status eines Benutzers. Ein "Status"-Request enthält das Attribut `COMMAND="RADIUS_Status"`.

Das XML-Interface kann die folgenden XML-Elemente einer Anfrage verarbeiten:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Das XML-Interface sendet dem Gateway daraufhin eine "Status"-Response, die die folgenden XML-Elemente enthalten kann:

`SUB_USER_NAME`

Benutzername

`SUB_MAC_ADDR`

MAC-Adresse des Benutzer-Gerätes. Mögliche Formate sind:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`SUB_STATUS`

Der aktuelle Benutzerstatus. Folgende Werte sind möglich:

- `RADIUS_STATUS_DONE`: Status Anfrage erfolgreich
- `RADIUS_STATUS_REJECT`: Status Anfrage zurückgewiesen, z.B. unbekannter User oder MAC Adresse

`SESSION_TXBYTES`

Aktuell gesendete Datenmenge

`SESSION_RXBYTES`

Aktuell empfangene Datenmenge

`SESSION_TXPACKETS`

Anzahl der bisher gesendeten Datenpakete

`SESSION_RXPACKETS`

Anzahl der bisher empfangenen Datenpakete

SESSION_STATE

Aktueller Status der Sitzung

SESSION_ACTUAL_TIME

Aktuelle Uhrzeit

Im Folgenden finden Sie einige Beispiele für XML-Dateien:

Status-Request

Das externe Gateway sendet den Befehl für die Statusabfrage an den Public-Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status-Response:

Das XML-Interface sendet eine Statusmeldung an das externe Gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <SESSION_ID>2</SESSION_ID>
     <SESSION_TXBYTES>0</SESSION_TXBYTES>
     <SESSION_RXBYTES>0</SESSION_RXBYTES>
     <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
     <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
     <SESSION_STATE>Authenticated</SESSION_STATE>
     <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

7.6 Analyse des XML-Interfaces mit cURL

Der folgende Abschnitt beschreibt die Analyse des XML-Interfaces mit der Open-Source-Software cURL.

cURL (Client for URL) ist eine Kommandozeilen-Anwendung, mit der man Dateien ohne den Einsatz von Web-Browsern oder FTP-Clients in einem Netzwerk übertragen kann. Auf der Seite *http://curl.haxx.se/* steht die Software für eine Vielzahl von Betriebssystemen zum Download bereit.

Um das XML-Interface mit cURL analysieren zu können, benötigen Sie im Public-Spot einen Administrator mit dem Funktionsrecht "Public-Spot-XML-Schnittstelle".

1. Laden Sie zunächst cURL herunter und installieren bzw. entpacken Sie es.
2. Starten Sie cURL mit der Befehlszeile `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`
   Die Parameter haben folgende Bedeutung:
   @filename

   Pfad und Name der lokalen XML-Datei, z. B. der Login-Request aus den *Beispielen*.

user

Benutzername mit Funktionsrecht "Public-Spot-XML-Schnittstelle". Ohne diese Authentifizierung funktioniert das XML-Feature nicht.

pass

Passwort des Benutzers

myhost

IP-Adresse bzw. DNS-Name des LANCOMs mit Public-Spot-XML-Schnittstelle

3. Über Telnet können Sie mit dem Befehl `trace # XML-Interface-PbSpot` einen Trace aktivieren, um zu überprüfen, ob XML-Anfragen erfolgreich waren bzw. Fehlermeldungen erhalten.

7.6.2 Ergänzungen im Setup-Menü

XML-Interface

Hier konfigurieren Sie das XML-Interface.

SNMP-ID:

2.24.40

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

Aktiv

Hier aktivieren Sie das XML-Interface.

SNMP-ID:

2.24..40.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

Mögliche Werte:

Ja

Nein

Default:

Nein

Radius-Authentifizierung

Hier aktivieren bzw. deaktivieren Sie die Authentifizierung über einen Radius-Server.

SNMP-ID:

2.24.40.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **XML-Interface**

Mögliche Werte:

Ja

Nein

Default:

Ja

7.7 Mehrfach-Logins

Sie haben jetzt die Möglichkeit, den Public-Spot-Benutzern zu gestatten, sich mit mehreren Geräten gleichzeitig auf einem Account bzw. ins WLAN einzuloggen. Dies könnte dann erforderlich sein, wenn eine Gruppe von zusammengehörigen Personen (wie eine Familie) mehrere Geräte besitzt und diese zur gleichen Zeit für den Zugang ins Netz nutzen möchte.

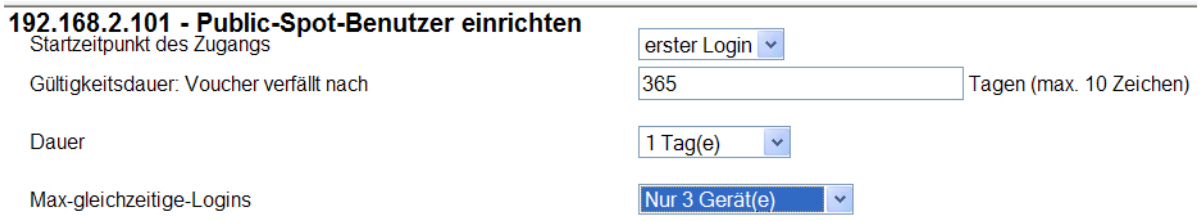
Um diese Funktion zu aktivieren, definieren Sie im ersten Schritt die mögliche Anzahl gleichzeitig zu nutzender Geräte in der Tabelle **Max-gleichzeitige-Logins-Tabelle**. Hier können Sie mehrere Werte eintragen, die Sie im zweiten Schritt mit Hilfe des Assistenten **Public-Spot-Benutzer einrichten** in dem analog zur Tabelle benannten Auswahlmenü bestätigen.

Beachten Sie, dass es für die Aktivierung dieser Funktion erforderlich ist, dass bei der Konfiguration über Telnet der Parameter **Verbiete-Mehrfach-Logins** auf **nein** gesetzt ist. Unter LANconfig finden Sie diesen Parameter unter **Public-Spot** > **Public-Spot - Benutzer** > **Mehrfachanmeldungen zulassen** .

7.7.1 Auswahl der Mehrfach-Logins im Public-Spot-Assistenten

Wenn Sie den Assistenten Assistenten **Public-Spot-Benutzer einrichten** aufrufen, finden Sie das Auswahlmenü **Max-gleichzeitige-Logins** vor. Die hier angezeigten Werte entsprechen den Zahlen, die Sie zuvor in der analog benannten Tabelle festgelegt haben. Die Zahlen werden innerhalb der Phrase "Nur...Gerät(e)" wiedergegeben.

Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf den Account bzw. auf das WLAN zugreifen dürfen.



7.7.2 Ergänzungen im Setup-Menü

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.

SNMP-ID:

2.24.19.14

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**

Mögliche Werte:

Max. 5 Ziffern

Default:

leer

7.8 Assistent zur Basis-Konfiguration eines Public-Spots

Ab LCOS-Version 8.80 unterstützt Sie ein spezieller Public-Spot-Assistent bei der einfachen Erstinbetriebnahme eines Public-Spots für einfache Einsatzszenarien.

7.8.1 Grundeinstellungen

Die Anleitung der Grundkonfiguration ist in drei separate Abschnitte aufgeteilt:

- Der erste Abschnitt beschreibt die Einrichtung eines Public-Spots mit lokaler Benutzerverwaltung – dabei registrieren Sie die Benutzer manuell in der lokalen Benutzerverwaltung über LANconfig bzw. WEBconfig.

  Um einen Public-Spot für ein einfaches Anwendungsszenario einzurichten, können Sie einen entsprechenden Assistenten starten, der Sie bei der Inbetriebnahme des Public-Spots unterstützt.
- Der zweite Abschnitt zeigt die Nutzung der Public-Spot-Assistenten, mit denen auch Mitarbeiter ohne weitere Administrator-Rechte neue Public-Spot-Benutzer sehr komfortabel anlegen können.
- Der dritte Teil beschreibt die zentrale Verwaltung der Benutzerdaten auf einem externen RADIUS-Server.

Die Abschnitte bauen teilweise aufeinander auf, Sie sollten also idealerweise diese Informationen in der entsprechenden Reihenfolge bearbeiten.

7.8.2 Tutorials zur Einrichtung und Verwendung des Public-Spots

Die folgenden Tutorials beschreiben beispielhaft, wie Sie die Public-Spot-Option sinnvoll einsetzen können.

Basis-Installation eines Public-Spots für einfache Einsatz-Szenarien

Dieses Tutorial beschreibt, wie Sie mit dem Public-Spot-Assistenten die Basis-Installation eines Public-Spots vornehmen können.

Einrichtung über LANconfig

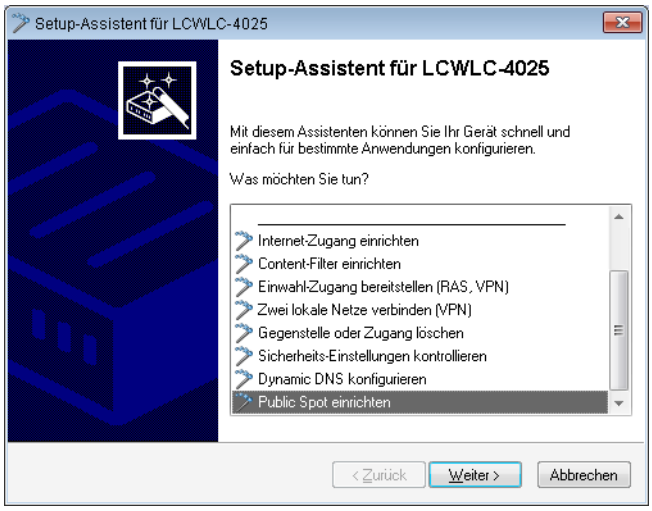
Der folgende Abschnitt beschreibt die Basis-Installation eines Public-Spots über LANconfig.

Sie benötigen das Zugriffsrecht "Supervisor", um einem Mitarbeiter die Public-Spot-Verwaltung übertragen zu können.

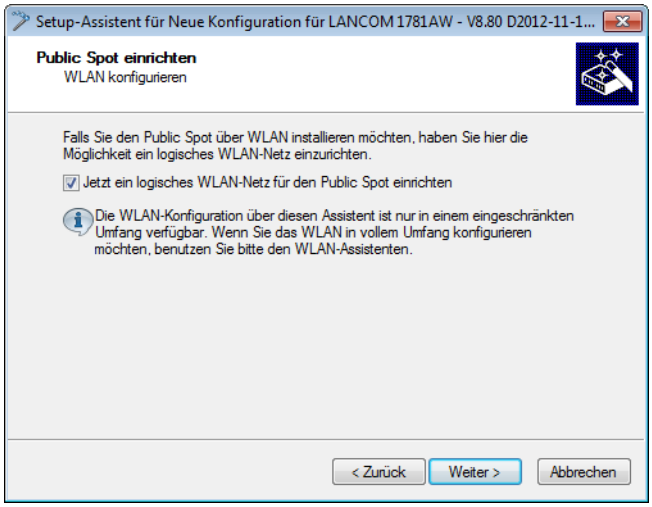
Der Assistent für die Basis-Konfiguration des Public-Spots zeigt je nach Gerätetyp und Verlauf verschiedene Dialoge. Dieses Tutorial stellt nur ein mögliches Beispiel dar.

1. Rufen Sie LANconfig z. B. aus der Windows-Startleiste auf mit **Start** > **Programme** > **LANCOM** > **LANconfig** .
2. Markieren Sie das Gerät, für das Sie einen Public-Spot einrichten wollen.

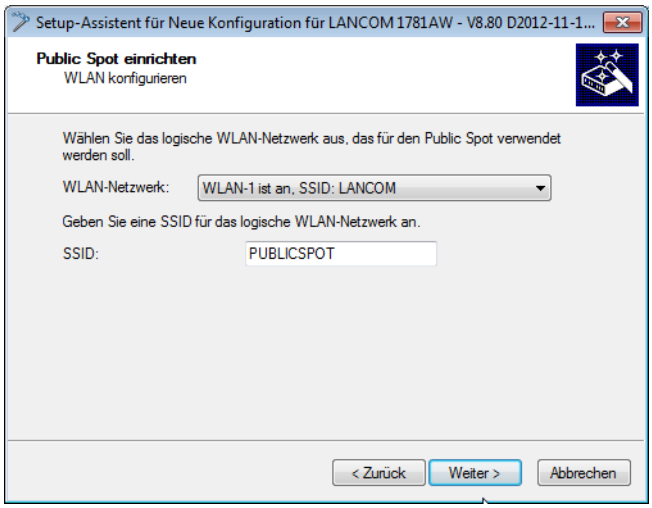
3. Starten Sie den Setup-Assistenten über **Gerät** > **Setup-Assistent** , wählen Sie die Aktion **Public-Spot einrichten** und klicken Sie anschließend auf **Weiter**.



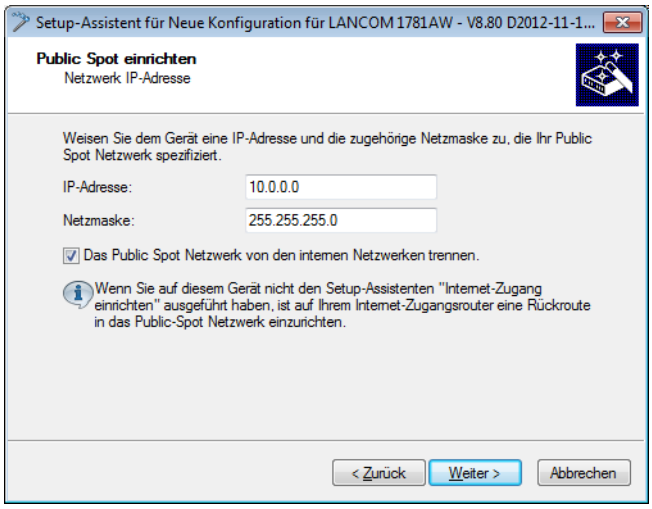
4. Falls Sie die Nutzung des Public-Spots über WLAN einrichten möchten, aktivieren Sie die entsprechende Option und klicken Sie auf **Weiter**.



5. Wählen Sie das logische WLAN-Netzwerk für den Public-Spot und geben Sie die gewünschte SSID ein. Klicken Sie auf **Weiter**.



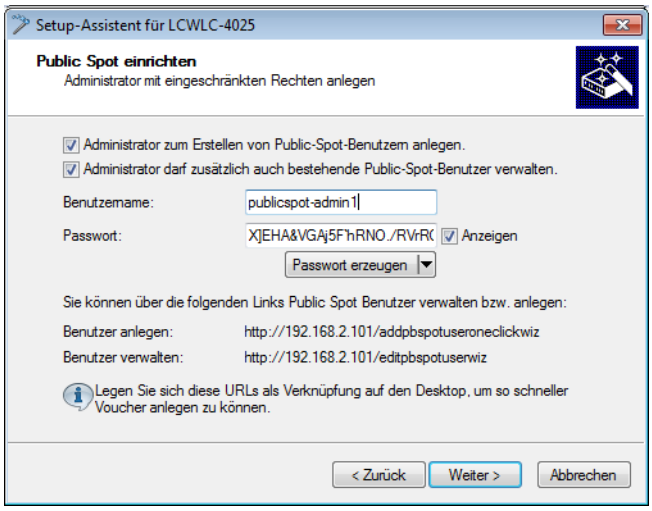
6. Geben Sie die IP-Adresse sowie die Netzmaske ein und klicken Sie auf **Weiter**.



Wählen Sie dazu in der Drop-Down-Liste das entsprechende Interface aus, und vergeben Sie dafür eine IP-Adresse und eine Netzmaske.

Wenn Sie das Public-Spot-Netzwerk aus Sicherheitsgründen von den internen Netzwerken trennen möchten, aktivieren Sie die entsprechende Option.

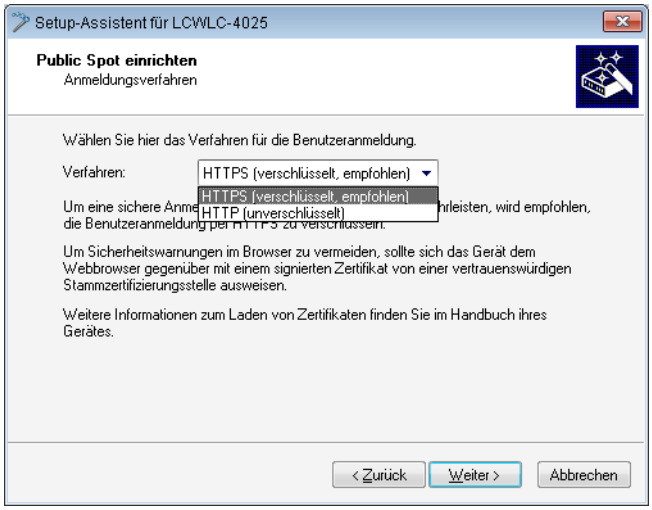
7. Erstellen Sie ggf. einen Public-Spot-Administrator, der die Public-Spot-Benutzer verwalten darf. Klicken Sie anschließend auf **Weiter**.



Sie können auswählen, ob der Administrator nur vorhandene Benutzer verwalten oder auch neue Benutzer anlegen darf.

Achten Sie bei der Vergabe eines Passwortes darauf, dass es sicher ist. Der Setup-Assistent prüft während der Eingabe die Qualität des Passwortes. Bei unsicheren Passworten erscheint das Eingabefeld rot, bei erhöhter Sicherheit wechselt es zu orange, und bei sehr sicheren Passworten erhält es einen weißen Hintergrund.

8. Wählen Sie das Verfahren für die Benutzer-Anmeldung.



Sie können in der Drop-Down-Liste zwischen **HTTPS** und **HTTP** wählen, wobei Sie mit einer Verbindung über HTTPS die Sicherheit für die Public-Spot-Benutzer gewährleisten.

9. Klicken Sie abschließend auf **Weiter** und **Fertig stellen**, um die Basis-Installation des Public-Spots abzuschließen. Der Setup-Assistent sendet nun die Einstellungen an das Gerät.

7.9 Getrennte Funktionsrechte

Beim Anlegen eines neuen Administrators können Sie jetzt festlegen, ob der Administrator neue Public-Spot-Benutzer lediglich anlegen oder zusätzlich auch verwalten kann. Diese Einstellungen nehmen Sie vor, indem Sie die entsprechenden Funktionsrechte im Menü **Admins** einzeln oder gemeinsam zuweisen.

7.9.1 Ergänzungen im Setup-Menü

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.

SNMP-ID:

2.11.21.3

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.

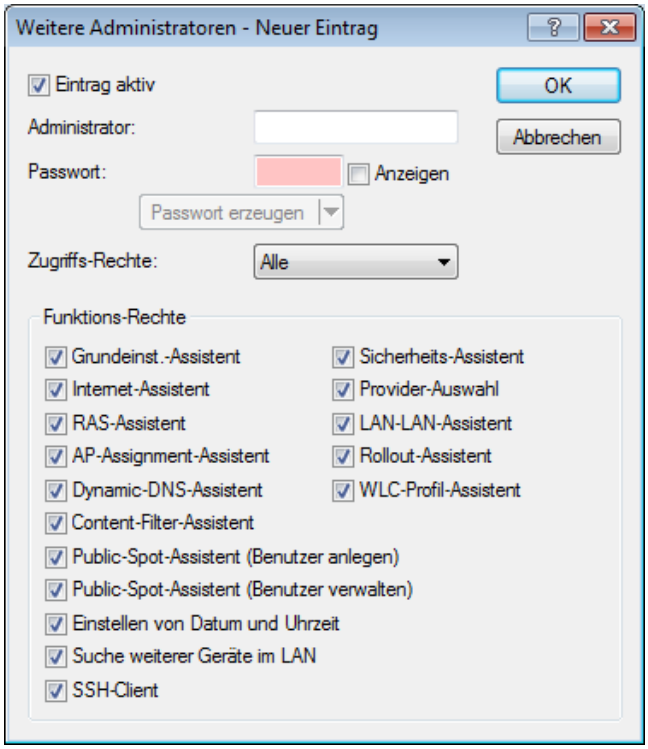
Default:

leer

7.9.2 Ergänzungen in LANconfig

Funktionsrechte neuer Administratoren spezifizieren

Wenn Sie einen neuen Administrator einrichten möchten, können Sie über die Schaltfläche **Weitere Administratoren** des Dialogs **Admin** festlegen, ob der einzurichtende Administrator über den Public-Spot-Assistenten neue Benutzer lediglich anlegen oder auch verwalten kann. Für diese Einstellungen finden Sie im Rahmen "Funktions-Rechte" zwei Kästchen, die jeweils mit "Public-Spot-Assistent (...)" bezeichnet sind.



7.10 Ergänzungen im Setup-Menü

7.10.1 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.

SNMP-ID:

2.24.31

Pfad Telnet:

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

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.

SNMP-ID:

2.24.31.1

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

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.

SNMP-ID:

2.24.31.2

Pfad Telnet:

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

Mögliche Werte:

Max. 15 Zeichen

Default:

0.0.0.0

8 Routing und WAN-Verbindungen

8.1 Default-Mode im DSLoL-Interface

Ab LCOS-Version 8.80 ist das DSLoL-Interface auf den Default-Modus 'Exclusive' eingestellt.

8.1.1 Ergänzungen im Setup-Menü

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.

SNMP-ID:

2.23.4.6

Pfad Telnet:

Setup > **Schnittstellen** > **DSLoL-Interface**

Mögliche Werte:

Auto

Exclusiv

Default:

Exclusiv

9 Diagnose

9.1 SYSLOG-Accounting in der Standard-Einstellung deaktiviert

In der Tabelle der Syslog-Server definieren Sie, welche Systeminformationen das Gerät mit welchem Syslog-Level an die definierten Syslog-Server schickt. In der Standard-Einstellung umfasst diese Tabelle 8 Einträge für die Ziel-IP-Adresse `127.0.0.1`, welche den internen Syslog-Speicher des Geräts repräsentiert.

```
root@:/Setup/SYSLOG/Server
> l

Idx.  IP-Address       Source  Level   Loopback-Addr.
-----------------------------------------------------
0001  127.0.0.1        04      00      INTRANET
0002  127.0.0.1        01      1f      INTRANET
0003  127.0.0.1        10      02      INTRANET
0004  127.0.0.1        40      08      INTRANET
0005  127.0.0.1        02      0a      INTRANET
0006  127.0.0.1        08      08      INTRANET
0007  127.0.0.1        20      00      INTRANET
0008  127.0.0.1        80      01      INTRANET
```

Für die Quellen 04 (Systemzeit) und 20 (Accounting) versendet das Gerät in der Standardeinstellung keine Syslog-Nachrichten an den internen Syslog-Speicher.

9.2 SYSLOG, Eventlog und Bootlog bootpersistent

Ab LCOS-Version 8.80 haben die Geräte die Möglichkeit, SYSLOG-, Eventlog- und Bootlog-Nachrichten so zu speichern, dass sie auch nach einem Neustart des Geräts verfügbar sind (bootpersistent).

9.2.1 Ergänzungen im Setup-Menü

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

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

Maximales-Nachrichtenalter

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.

SNMP-ID: 2.22.9

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- 1 bis 99

Default: 24

Alte-Nachrichten-Entfernen

Dieser Parameter aktiviert das Löschen der SYSLOG-Nachrichten im Gerät nach der unter *Maximales-Nachrichtenalter* definierten Zeit.

SNMP-ID: 2.22.10

Pfad Telnet: /Setup/SYSLOG

Mögliche Werte:

- Ja
- Nein

Default: Nein

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.

Bei Bedarf löschen Sie den persistenten Bootlog-Speicher mit dem Kommandozeilen-Befehl `deletebootlog`.

SNMP-ID: 2.11.71

Pfad Telnet: /Setup/Config

Mögliche Werte:

- ja
- nein

Default: ja

9.2.2 Ergänzungen der Kommandozeilenbefehle

Bootlog löschen

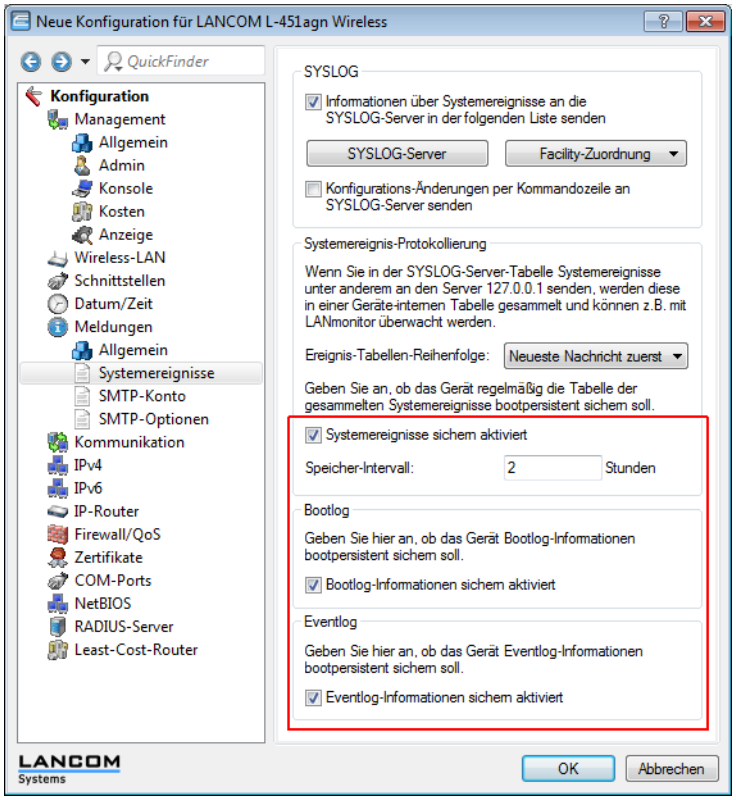
Der Bootlog speichert die Informationen über die Boot-Vorgänge des Gerätes. Mit dem Parameter *Bootlog-sichern* aktivieren Sie optional das persistente Speichern des Bootlogs.

Durch Eingabe des Befehls `deletebootlog` an einer beliebigen Stelle auf der Kommandozeile löschen Sie bei Bedarf den Inhalt des persistenten Bootlog-Speichers.

9.2.3 Ergänzungen in LANconfig

SYSLOG, Eventlog und Bootlog bootpersistent

Die Einstellungen für das bootpersistente Speichern von Syslog-, Eventlog- und Bootlog-Nachrichten finden Sie in LANconfig unter **Meldungen** > **Systemereignisse** .



9.3 Protokollieren der Konfigurationsänderungen über Kommandozeile

Um erhöhte Sicherheitsanforderungen an die Infrastruktur von Netzwerken zu erfüllen, haben die Geräte die Möglichkeit, alle Änderungen der Konfiguration über die Kommandozeile im Syslog-Speicher zu protokollieren. Als Konfigurationsänderungen gelten dabei alle Änderungen an den Konfigurationsparametern, das Ausführen von Aktionen sowie das Hochladen von Dateien wie z.B. Zertifikaten.

Folgende Informationen schreiben die Geräte dabei in den Syslog-Speicher:

- Benutzername
- Name des geänderten Menüeintrags bzw. der ausgeführten Aktion
- Neuer Wert (bzw. der Hinweis, dass die Änderung nicht erfolgreich war, z.B. aufgrund fehlender Berechtigung)

9.3.1 Ergänzungen im Setup-Menü

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

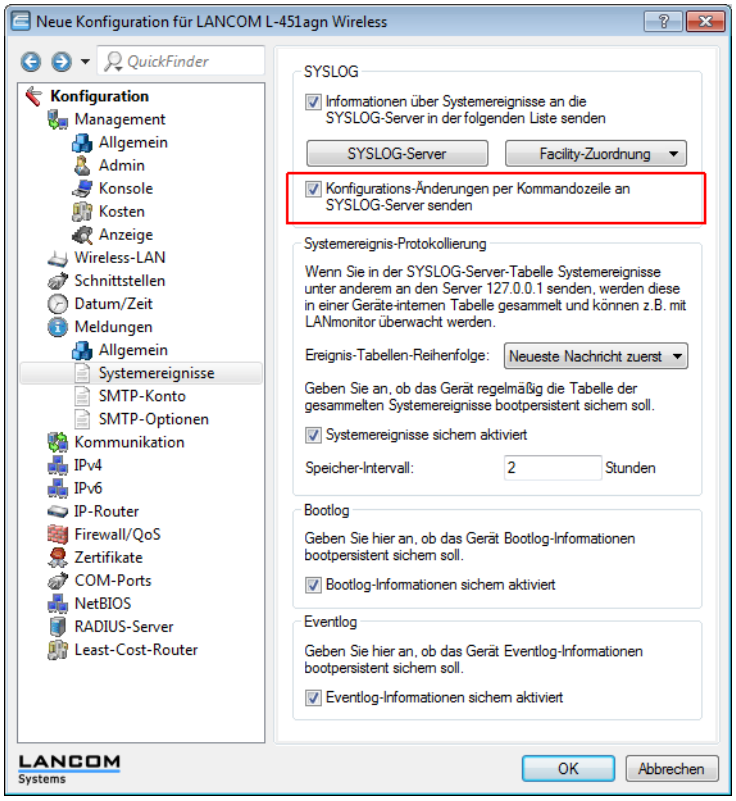
Default: Nein

9.3.2 Ergänzungen in LANconfig

Konfigurationsänderungen per Kommandozeile an Syslog-Server senden

Die Einstellung für das Protokollieren der Konfigurationsänderungen über Kommandozeile finden Sie in LANconfig unter **Meldungen** > **Systemereignisse** .

Diese Protokollierung umfasst ausschließlich die an der Kommandozeile ausgeführten Befehle. Konfigurationsänderungen und Aktionen über LANconfig oder Webconfig sind davon nicht erfasst.



9.4 SYSLOG: Änderung der Default-Reihenfolge

Ab LCOS-Version 8.80 zeigen die Geräte die neuesten Nachrichten in der SYSLOG-Tabelle standardmäßig in den obersten Positionen. Auf Wunsch können Sie die Sortierung umgekehrt einstellen.

9.4.1 Ergänzungen im Setup-Menü

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:

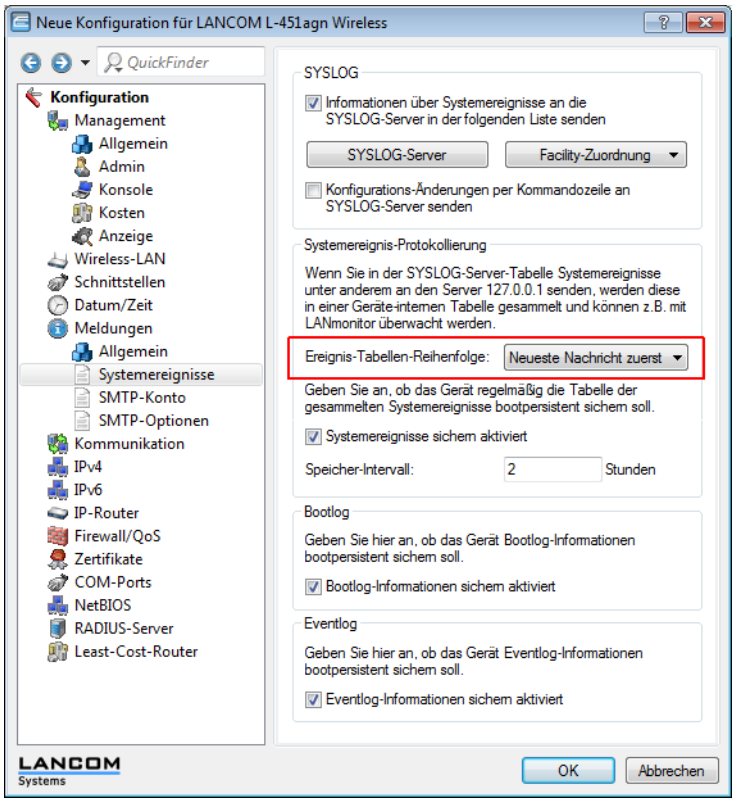
- oldest on top
- newest-on-top

Default: newest-on-top

9.4.2 Ergänzungen in LANconfig

Reihenfolge der Systemereignisse

Die Einstellung für die Anzeige-Reihenfolge der Systemereignisse finden Sie in LANconfig unter **Meldungen** > **Systemereignisse** .



9.5 Paket-Capturing

Um Datenpakete zwecks Analyse von Störungen oder Problemen aufzuzeichnen, besteht seit der LCOS-Version 8.60 die Möglichkeit, über ein Kommandozeilen-Tool den Befehl **lcoscap** auszuführen. Dieser Befehl aktiviert die Aufzeichnung der Pakete und schreibt die Ergebnisse in eine Datei, die Sie mit einem Tool wie Wireshark öffnen und analysieren können.

Seit der LCOS-Version 8.80 steht Ihnen eine zusätzliche, deutlich komfortablere Methode zur Verfügung: Über einen neuen Menüpunkt in Webconfig können Sie unterschiedliche Parameter definieren und auf diese Weise Datenpakete ausgewählter Schnittstellen aufzeichnen und mittels einer Ergebnisdatei analysieren.

Diese Methode bietet Ihnen mehrere Vorteile:

- Sie sind auf keine spezielle Software angewiesen, da Sie Webconfig auf beliebigen Web-Browsern ausführen können.
- Die Eingabe von Kommandozeilenbefehlen entfällt. Stattdessen stehen Ihnen komfortable Menü-Elemente zur Verfügung.
- Wenn Sie Webconfig über HTTPS betreiben, ist die Vertraulichkeit und Sicherheit des aufgezeichneten Datenverkehrs gewährleistet.

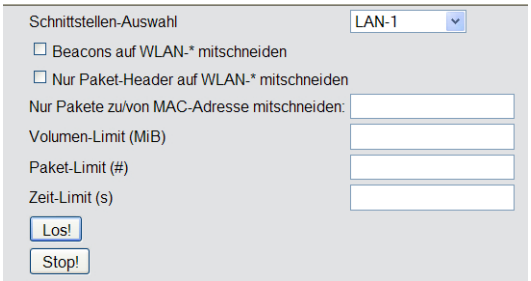
Das neue Feature finden Sie unter **Extras** > **Paket-Capturing** . Nach dem Festlegen der Parameter und einem Klick auf **Los!** erzeugen Sie eine extern zu speichernde Datei, die Sie z. B. mit Wireshark öffnen können.

9.5.1 Ergänzungen in Webconfig

Paket-Capturing

Der Dialog **Extras** > **Paket-Capturing** bietet Ihnen eine einfache Möglichkeit, Datenpakete von unterschiedlichen Schnittstellen aufzuzeichnen und anschließend zu analysieren. Beachten Sie, dass die Einstellmöglichkeiten je nach Gerätetyp variieren können. So haben Sie etwa bei WLAN-Geräten mehr Einstellmöglichkeiten als bei Geräten ohne WLAN-Funktionalität.

Die nachstehende Abbildung zeigt den entsprechenden Dialog bei einem WLAN-Gerät. Der Dialog enthält somit zwei zusätzliche, WLAN-spezifische Parameter.



Für die Spezifizierung der Ausgabe-Datei stehen Ihnen folgende allgemeine Menüpunkte zur Verfügung:

- **Schnittstellen-Auswahl**: Mit diesem Auswahlmenü bestimmen Sie die Schnittstelle, deren Datenpakete aufgezeichnet werden.
- **Nur Pakete zu/von MAC-Adresse mitschneiden:**: Wenn Sie nur Datenpakete einer bestimmten physikalischen Adresse innerhalb der ausgewählten Schnittstelle aufzeichnen wollen, können Sie diese hier festlegen.
- **Volumen-Limit (MiB)**: Geben Sie hier das maximale Volumen der aufgezeichneten Pakete in Mebibytes an.
- **Paket-Limit (#)**: Hier können Sie eine maximale Anzahl aufzuzeichnender Pakete festlegen.
- **Zeit-Limit (s)**: Geben Sie hier eine maximale Zeit in Sekunden an, nach welcher die Aufzeichnung endet.

Klicken Sie jetzt auf **Los!**, um den Aufzeichnungsvorgang zu starten. Nach einiger Zeit (abhängig von der Verbindungsgeschwindigkeit) öffnet sich ein Dialog, der Sie zum Speichern der erzeugten Datei auffordert. Sie können die Datei mit der Endung .cap jetzt lokal speichern. Standardmäßig erhält die Datei einen Namen, welcher die Bezeichnung und die zugehörige Schnittstelle des Gerätes enthält, dessen Datenpakete Sie aufgezeichnet haben (z. B. LCWLC-4025-LAN-2.cap). Sie können den voreingestellten Dateinamen jedoch während des Speichervorgangs oder auch nachträglich ändern.

Eine laufende Aufzeichnung können Sie jederzeit durch einen Klick auf **Stop!** beenden. Dies kann beispielsweise dann sinnvoll sein, wenn Sie zunächst eingegebene Parameter korrigieren bzw. anpassen wollen.

Wenn Sie Aufzeichnung ohne Angabe von Limts starten, zeichnet das Gerät die Pakete solange auf, bis Sie den Vorgang mit einem Klick auf **Stop** manuell beenden.

9.6 Trace-Ausgabe für das XML-Interface

Ab LCOS-Version 8.80 können Sie mit dem Befehl `trace # XML-Interface-PbSpot` einen Trace aktivieren, um zu überprüfen, ob XML-Anfragen erfolgreich waren bzw. Fehlermeldungen erhalten.

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
XML-Interface-PbSpot	Meldungen des Public-Spot-XML-Interfaces

9.7 Ping Befehl für IPv6

Ab LCOS-Version 8.80 können Sie mit dem Kommando `ping -6` (oder mit dem Alias `ping6`) "ICMP-Echo-Requests" an einen Host in einem IPv6-Netzwerk senden.

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 Netzwerk "INTRANET" zu erreichen ist.

`ping -6 2001:db8::1`

Ping auf die globale IPv6-Adresse "2001:db8::1".

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

Parameter	Bedeutung
-6 <IPv6-Adresse>%<Scope>	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus.

10 LCMS

10.1 Ergänzungen in LANconfig

10.1.1 Interner Browser in LANconfig

Bisher startete LANconfig zur Geräte-Konfiguration über WEBconfig den im System eingestellten Standardbrowser. Ab LCOS-Version 8.80 haben Sie die Möglichkeit, alternativ einen LANconfig-internen Browser zu starten.

Ergänzungen in LANconfig

Die Menüstruktur in LANconfig

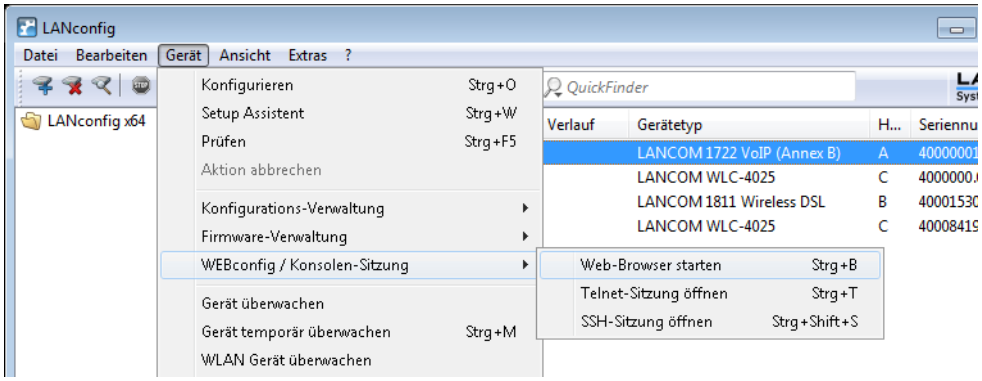
Über die Menüleiste können Sie Geräte und deren Konfigurationen verwalten sowie das Aussehen und die Funktionsweise von LANconfig anpassen.

Gerät

Unter dem Menüpunkt **Gerät** können Sie die Konfiguration von am Netzwerk angeschlossenen Geräten bearbeiten, Firmware-Updates verwalten und Geräteverbindungen überwachen.

Die Funktionen im Menü **Gerät** können Sie nur auswählen, wenn Sie mindestens ein Gerät in der Geräteliste markiert haben. Dieses Menü können Sie ebenfalls über die rechte Maustaste für ein markiertes Gerät aufrufen.

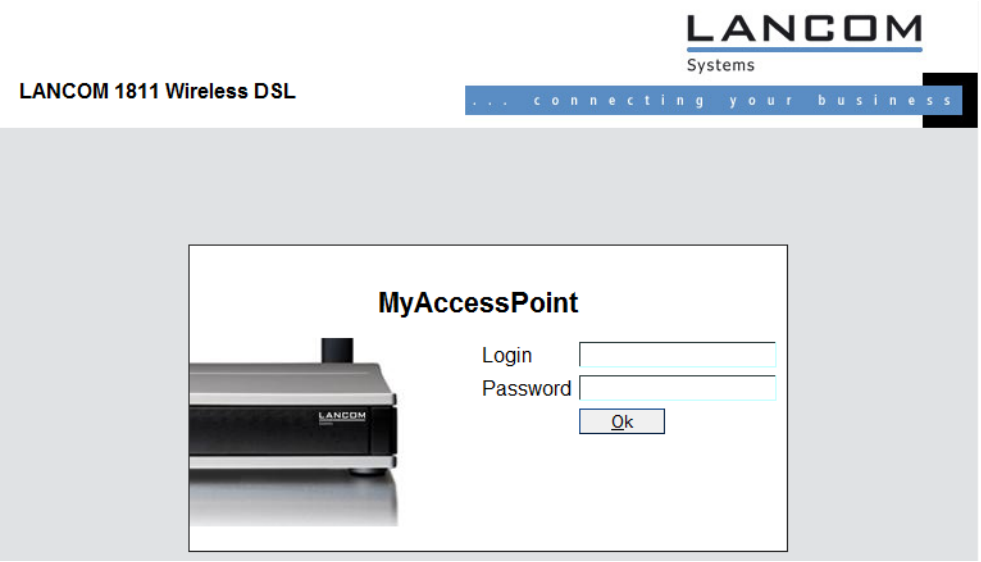
WEBconfig / Konsolen-Sitzung



Unter **Gerät** > **WEBconfig / Konsolen-Sitzung** können Sie die folgenden Aktionen wählen:

Web-Browser starten

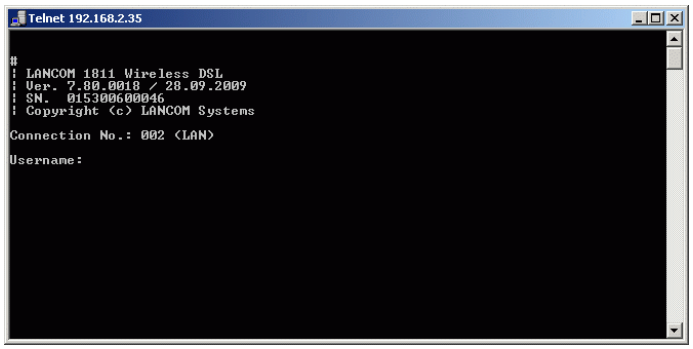
Öffnet den Web-Browser für das markierte Gerät.



Unter **Extras** > **Optionen** > **Extras** > **Browser zur Darstellung von WEBconfig** können Sie auswählen, ob LANconfig zur Anzeige den Standardbrowser des Systems oder den internen Browser verwenden soll.

Telnet-Sitzung öffnen

Öffnet die Telnet-Sitzung.



SSH-Sitzung öffnen

Öffnet eine Konfigurationssitzung im SSH-Client.

Sie müssen unter **Extras** > **Optionen** > **Extras** > **Externe Programme** für Telnet- bzw. SSH-Verbindungen jeweils ein Programm festlegen, das LANconfig zum Verbindungsaufbau zum Gerät nutzen soll.

Extras

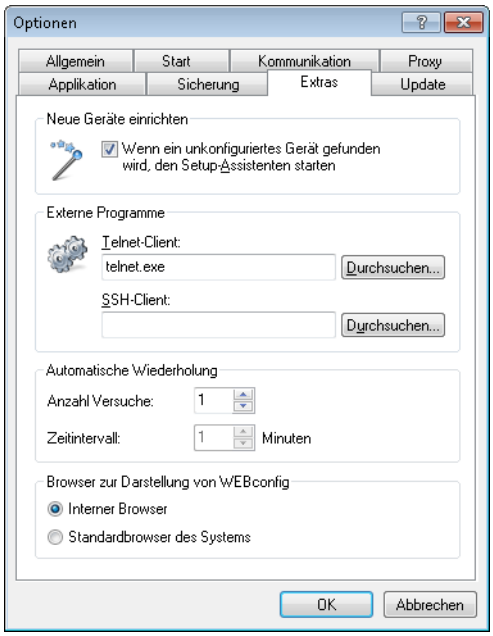
Wenn Sie in der Menüleiste auf **Extras** > **Optionen** klicken, öffnet sich die Dialogbox für weitere Einstellungsmöglichkeiten. (Sie erreichen diese Dialogbox auch, indem Sie F7 drücken.)

Optionen

Unter dem Menüpunkt **Optionen** können Sie zusätzliche Funktionen von LANconfig aufrufen, z. B. für die Kommunikation mit angeschlossenen Geräten, den Aufruf externer Anwendungen oder die automatische Suche nach Firmware-Updates.

Extras

In diesem Dialog können Sie **zusätzliche Einstellungen** vornehmen.



Neue Geräte einrichten

Wenn diese Option markiert ist, startet LANconfig bei jedem gefundenen, aber noch nicht konfigurierten Gerät den Setup-Assistenten.

Externe Programme

Bestimmen Sie hier jeweils die Programmdatei des Telnet-Clients und des SSH-Clients, die LANconfig für Verbindungen zu den Geräten benutzen soll.

Automatische Wiederholung

Anzahl Versuche

Geben Sie hier die Anzahl der Versuche für einen Firmware- oder Konfigurations-Upload an.

Die Anzahl können Sie im Bereich von 1 bis 9999 einstellen. Einen Verbindungsversuch führt LANconfig immer durch. Schlägt dieser fehl, erfolgt eine Wiederholung der Aktion nach abgelaufener Intervall-Zeit. Es erfolgen so viele Wiederholungen, bis LANconfig entweder die eingestellte Anzahl von Versuchen durchgeführt hat oder die Aktion erfolgreich war. Es ist jedoch auch möglich, dass LANconfig die Wiederholungen vorzeitig abbricht, wenn eine Situation eintritt, die voraussichtlich nicht ohne weitere Einflussnahme zum Erfolg führt. Dies kann z. B. eine Datei sein, die das Gerät nicht öffnen kann.

Zeitintervall

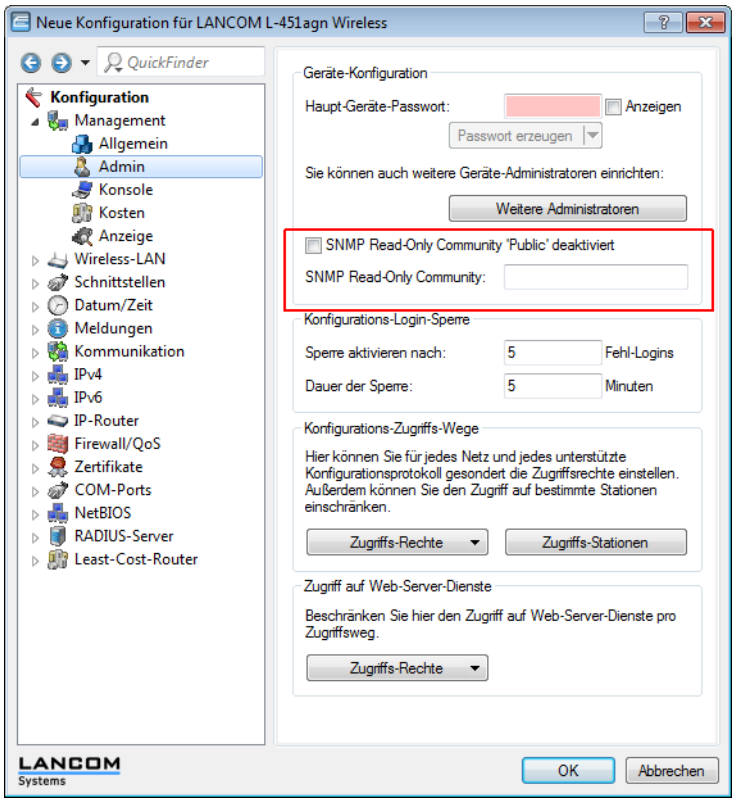
Geben Sie hier die Intervalldauer in Minuten an, die zwischen zwei Firmware- oder Konfigurations-Upload-Versuchen verstreichen soll. Die Intervalldauer können Sie im Bereich von 1 bis 9999 einstellen.

Browser zur Darstellung von WEBconfig

Bestimmen Sie hier, welchen Browser LANconfig standardmäßig für die Anzeige von WEBconfig verwenden soll. Zur Auswahl stehen der Standard-Browser des Betriebssystems und der LANconfig-interne Browser LCCEF (LANCOM Chromium Embedded Framework).

10.2 Einstellung der SNMP Read-Only Community 'Public'

Die Einstellung für die SNMP Read-Only Community 'Public' finden Sie im LANconfig unter **Management** > **Admin** .

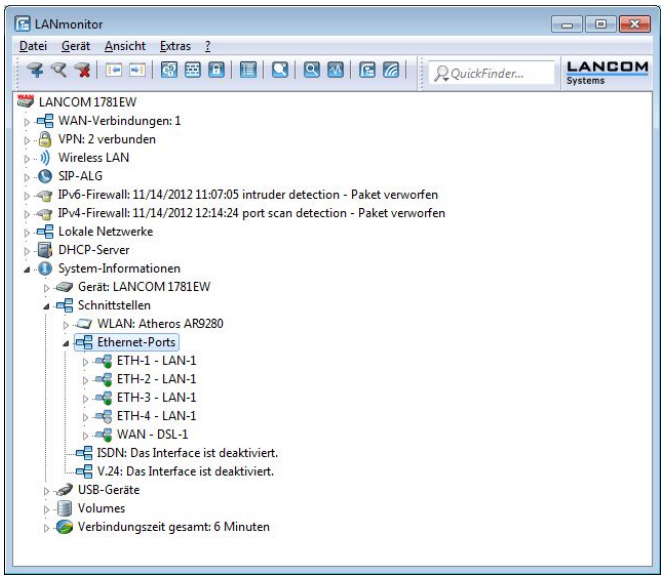


10.3 Ergänzungen im LANmonitor

10.3.1 Anzeige der aktiven Ethernet-Ports

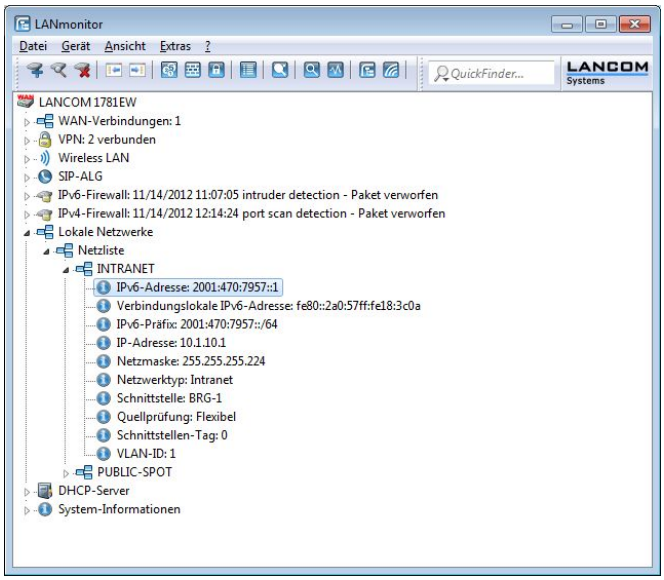
LANmonitor bietet Ihnen ab LCOS-Version 8.80 die Möglichkeit, sich den Betriebszustand der Ethernet-Ports anzeigen zu lassen.

Der Menüpunkt **System-Informationen** > **Schnittstellen** > **Ethernet-Ports** zeigt Ihnen zum einen an, ob der jeweilige Port in Betrieb ist. Zum anderen sehen Sie anhand der Port-Überschrift, welchem Netz dieser Port zugeordnet ist (z. B. LAN-1).



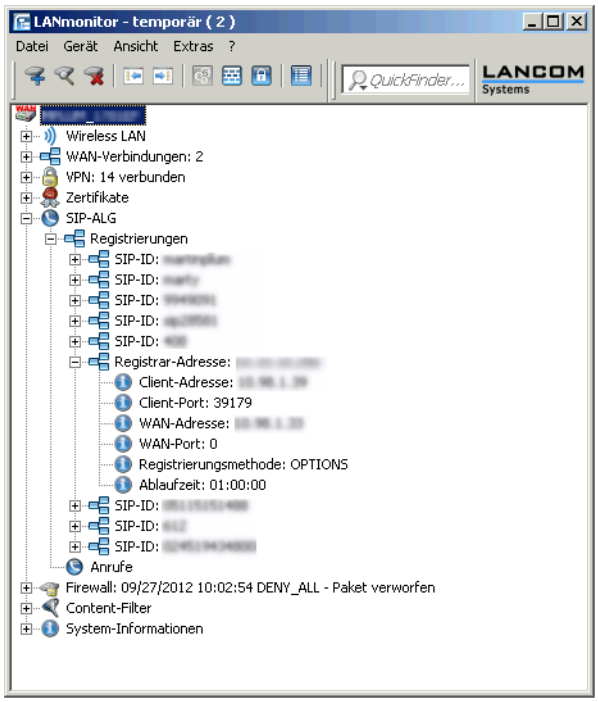
10.3.2 Anzeige lokaler IPv6-Adressen

Ab LCOS-Version 8.80 haben Sie die Möglichkeit, sich per LANmonitor die IPv6-Adressen lokaler Netzwerke anzeigen zu lassen. Diese Anzeigefunktion steht Ihnen an mehreren Stellen innerhalb des Menüs zur Verfügung.



10.3.3 Anzeige von PBX-Leitungen im SIP-ALG

LANmonitor zeigt ab LCOS-Version 8.80 im Bereich **SIP-ALG** > **Registrierungen** die PBX-Leitungen separat mit der Registrierungsmethode **Options** an.



11 Virtual Private Networks - VPN

11.1 Default-Proposals für IKE und IPSec

Die Proposals für IKE und IPSec unterstützen nun in den Default-Einstellungen eine Schlüssellänge von 256 Bit.

Ein Firmware-Upgrade aktiviert diese Änderung zunächst nicht, um bestehende Installationen nicht zu gefährden. Um die Änderungen zu übernehmen, müssen Sie einen Reset des Gerätes oder einen Reset der Tabellen durchführen. Bei Neugeräten, die LCOS 8.62 oder neuer enthalten, sind die neuen Defaults bereits aktiv.

11.2 Replay-Detection

Mit der Replay-Detection beinhaltet der IPsec-Standard eine Möglichkeit, sogenannte Replay-Attacken zu erkennen. Bei einer Replay-Attacke sendet eine Station die zuvor unberechtigt protokollierten Daten an eine Gegenstelle, um eine andere als die eigene Identität vorzutäuschen.

Die Idee der Replay-Detection besteht darin, eine bestimmte Anzahl von aufeinander folgenden Paketen zu definieren (ein "Fenster" mit der Länge "n"). Da der IPSec-Standard die Pakete mit einer fortlaufenden Sequenznummer versieht kann das empfangene VPN-Gerät feststellen, ob ein Paket eine Sequenznummer aus dem zulässigen Fensters trägt. Wenn z.B. die aktuell höchste empfangene Sequenznummer 10.000 lautet bei einer Fensterbreite von 100, dann liegt die Sequenznummer 9.888 außerhalb des erlaubten Fensters.

Die Replay-Detection verwirft emfpangene Paketedann, wenn sie entweder:

- eine Sequenznummer vor dem aktuellen Fenster tragen, in diesem Fall betrachtet die Replay-Detection als zu alt, oder
- eine Sequenznummer tragen,, welche das VPN-Gerät zuvor schon einmal empfangen hat, in diesem Fall wertet die Replay-Detection dieses Paket als Teil einer Replay-Attacke

Bitte beachten Sie bei der Konfiguration des Fensters für die Replay-Detection folgende Aspekte:

- wenn Sie das Fenster zu groß wählen, übersieht die Replay-Detection möglicherweise eine aktuell von einem Angreifer ausgeführte Replay-Attacke
- wenn Sie das Fenster zu klein wählen, verwirft die Replay-Detection aufgrund einer während der Datenübertragung geänderten Paketreihenfolge möglicherweise rechtmäßige Pakete und erzeugt so Störungen in der VPN-Verbindung

Wägen Sie den Einsatz der Replay-Detection in Ihrem speziellen Anwendungsfall ab. Aktivieren Sie die Replay-Detection nur dann, wenn Sie die Sicherheit der VPN-Verbindung höher bewerten als die störungsfreie Datenübertragung.

11.2.1 Ergänzungen im Menüsystem

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.

SNMP-ID:

2.19.30

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 5 Ziffern

Default:

0

Besondere Werte:

Der Wert 0 deaktiviert die Replay-Detection.

11.3 myVPN

Mit der LANCOM myVPN App können Sie sehr komfortabel einen VPN-Zugang zu Ihrem Firmennetzwerk auf Ihrem iPhone, iPad oder iPod (allgemein: iOS-Gerät) einrichten. LANCOM myVPN bietet die folgenden Funktionen:

- Hochsichere, mobile VPN-Verbindungen
- Übernimmt die komplexe VPN-Konfiguration des in iOS-Geräten integrierten VPN-Clients und des LANCOM Routers
- PIN-Verfahren zur Authentisierung beim VPN-Tunnelaufbau
- Zugriffskontrolle durch einstellbare Firewall-Regeln auf den LANCOM VPN-Gateways
- LANCOM myVPN-Benutzermanagement und automatische Erkennung myVPN-aktivierter LANCOM Gateways
- Für iOS-Geräte ab Version 4.1 geeignet

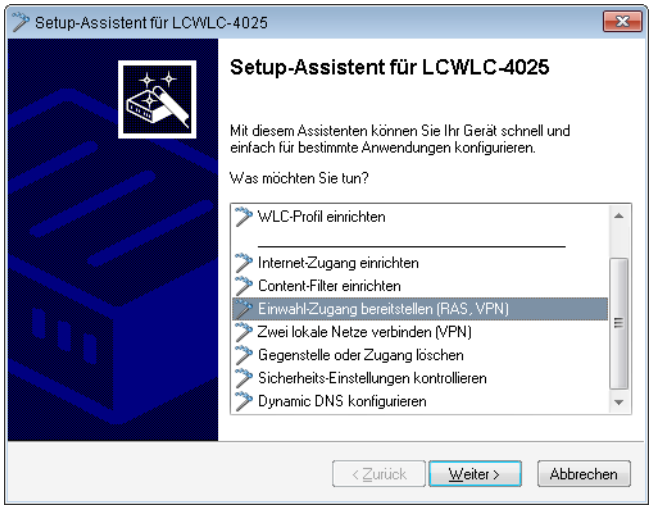
Nach der Installation von LANCOM myVPN bezieht die App ein VPN-Profil von Ihrem LANCOM VPN-Gerät und konfiguriert automatisch alle erforderlichen Einstellungen im iOS-Gerät. Anschließend können Sie über die betriebssystem-internen Funktionen des iOS mit wenigen Schritten eine VPN-Verbindung zum Firmennetzwerk aufbauen.

11.3 VPN-Profil für die LANCOM myVPN App mit dem Setup-Assistenten von LANconfig einrichten

So konfigurieren Sie mit dem Setup-Assistenten einen Zugang für einen VPN-Client auf einem iOS-Gerät:

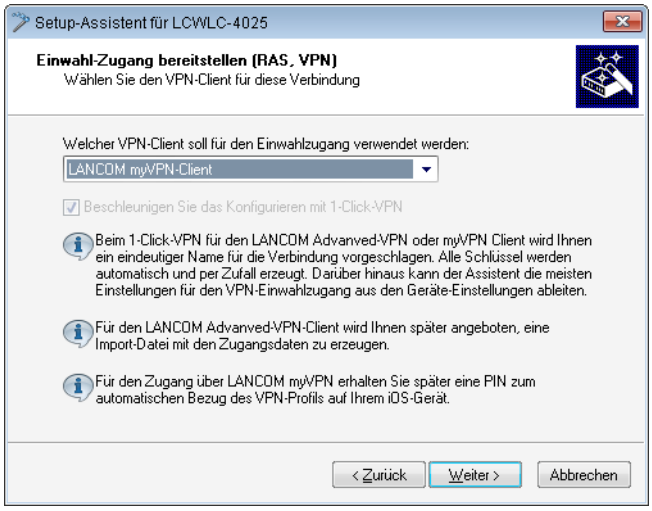
1. Rufen Sie LANconfig z. B. aus der Windows-Startleiste auf mit **Start** > **Programme** > **LANCOM** > **LANconfig** . LANconfig sucht nun automatisch im lokalen Netz nach Geräten.
2. Markieren Sie das gewünschte Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent** .

3. Wählen Sie den Punkt **Einwahl-Zugang bereitstellen (RAS, VPN)** und klicken Sie auf **Weiter**.

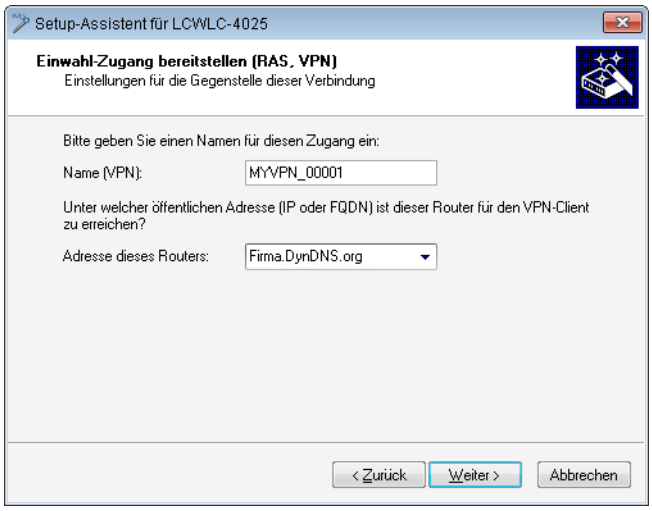


Sie können das nächste Informations-Fenster mit **Weiter** überspringen.

4. Wählen Sie aus der Auswahlliste die Option **LANCOM myVPN-Client** und klicken Sie auf **Weiter**.

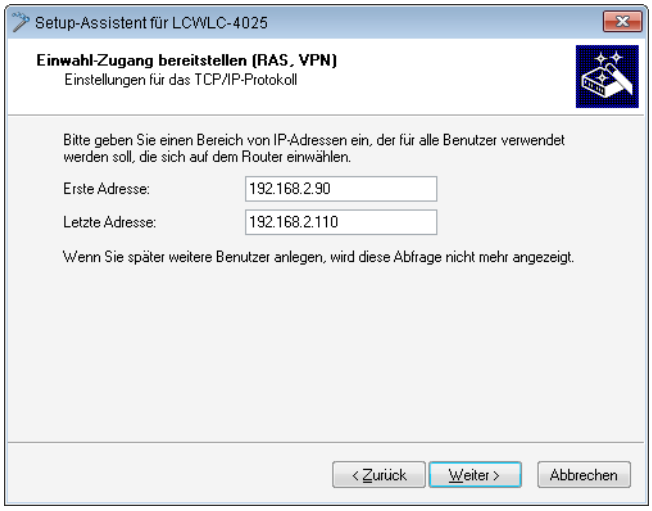


5. Vergeben Sie einen Namen für diesen Zugang und bestimmen Sie die Adresse, über die der Router für den VPN-Client auf dem iOS-Gerät zu erreichen ist. Klicken Sie anschließend auf **Weiter**.



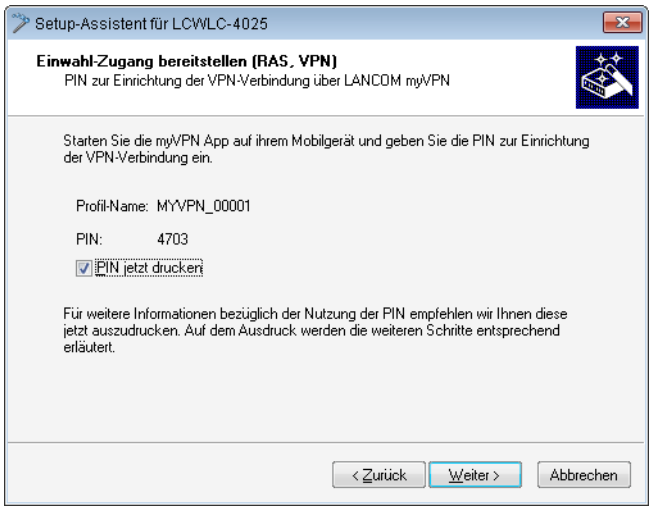
Der Setup-Assistent schlägt Ihnen einen Namen vor, den Sie übernehmen können.

6. Wenn in dem VPN-Gerät bisher noch kein Pool für die Zuweisung von IP-Adressen für die einwählenden VPN-Clients konfiguriert wurde, fordert Sie der Assistent im folgenden Dialog auf, einmalig einen Bereich von IP-Adressen als Pool anzugeben. Bei der Einwahl weist das VPN-Gerät dem iOS-Gerät dann automatisch eine freie IP-Aresse aus diesem Pool zu.



Wenn in dem VPN-Gerät zuvor schon ein Pool für die Zuweisung von IP-Adressen für die einwählenden VPN-Clients konfiguriert wurde, so nutzt das VPN-Gerät automatisch die Adressen aus diesem Adress-Pool, der Assistent überspringt den hier abgebildeten Dialog.

7. Der Setup-Assistent zeigt Ihnen den Profil-Namen sowie die automatisch generierte PIN für den VPN-Client an. Wenn Sie die PIN zum Abschluss ausdrucken möchten, markieren Sie die Option **PIN jetzt drucken**. Klicken Sie auf **Weiter**.



8. Mit einem Klick auf **Fertig stellen** speichert der Setup-Assistent alle Einstellungen auf dem entsprechenden VPN-Gerät. Ggf. startet er anschließend den Ausdruck der myVPN-PIN.
   Das myVPN-Modul ist auf dem gewählten VPN-Gerät nun aktiviert. Sie können nun die myVPN-App auf Ihrem iOS-Gerät starten und mit Eingabe der PIN das VPN-Profil beziehen.

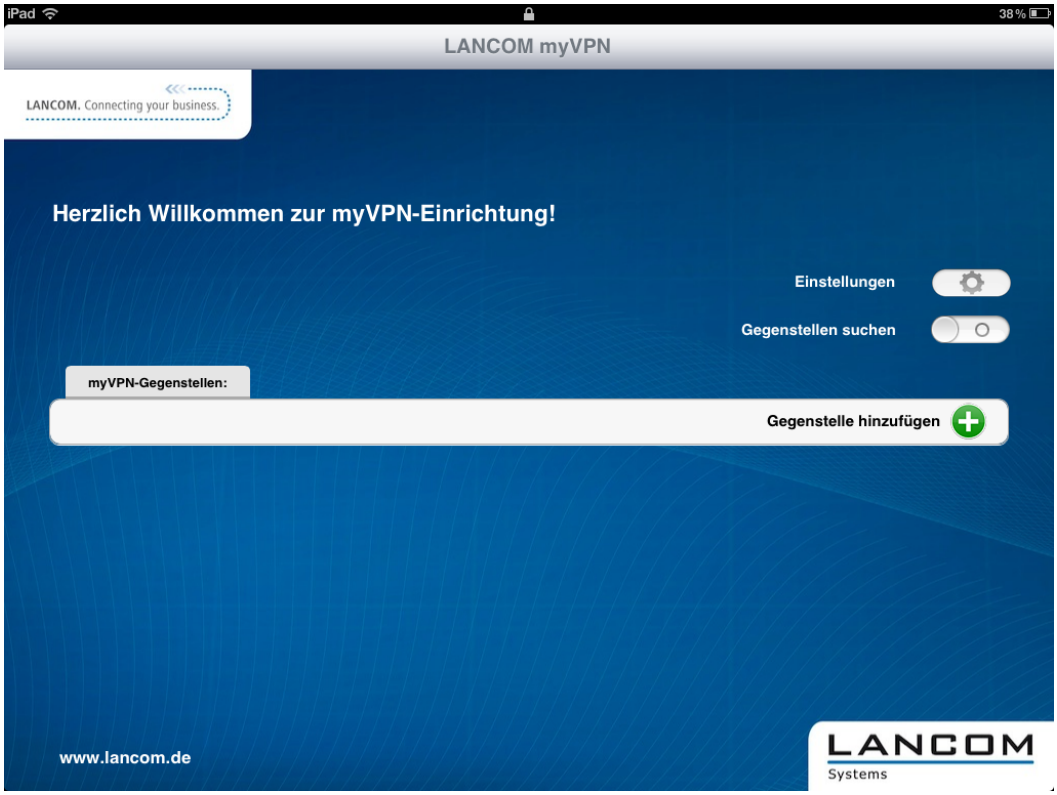
11.3 VPN-Profil mit der LANCOM myVPN App beziehen

So beziehen Sie auf Ihrem iOS-Gerät mit Hilfe der LANCOM myVPN App ein VPN-Profil von einem LANCOM VPN-Gerät:

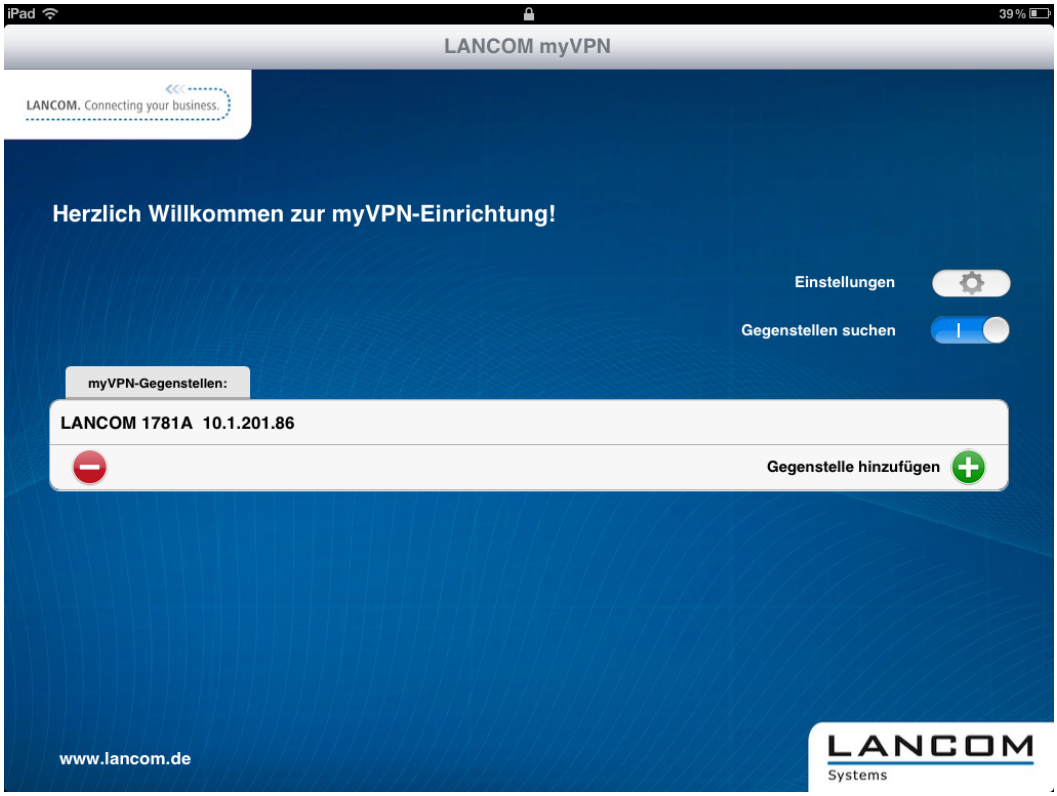
Die LANCOM myVPN App hat ausschließlich die Aufgabe, die korrekten Einstellungen für den im iOS-Gerät vorhandenen VPN-Client schnell und komfortabel einzurichten. Das Aufbau der VPN-Verbindung zum Firmennetzwerk selbst erfolgt direkt über den VPN-Client im iOS-Gerät.

1. Laden Sie die LANCOM myVPN App aus dem Apple-App-Store.

2. Öffnen Sie die App auf Ihrem iPhone oder iPad.

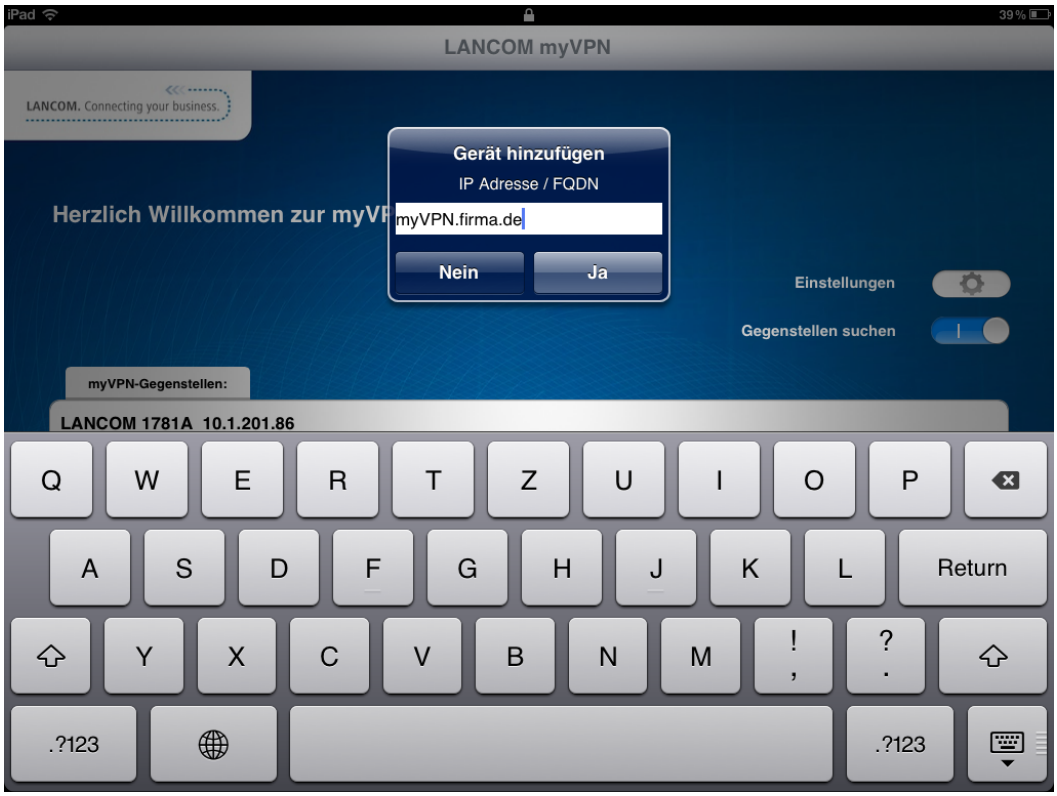


3. Optional: Aktivieren Sie die Option **Gegenstellen suchen**, um VPN-Geräte mit aktiviertem LANCOM myVPN Modul zu finden, welche das iOS-Gerät über WLAN erreichen kann.

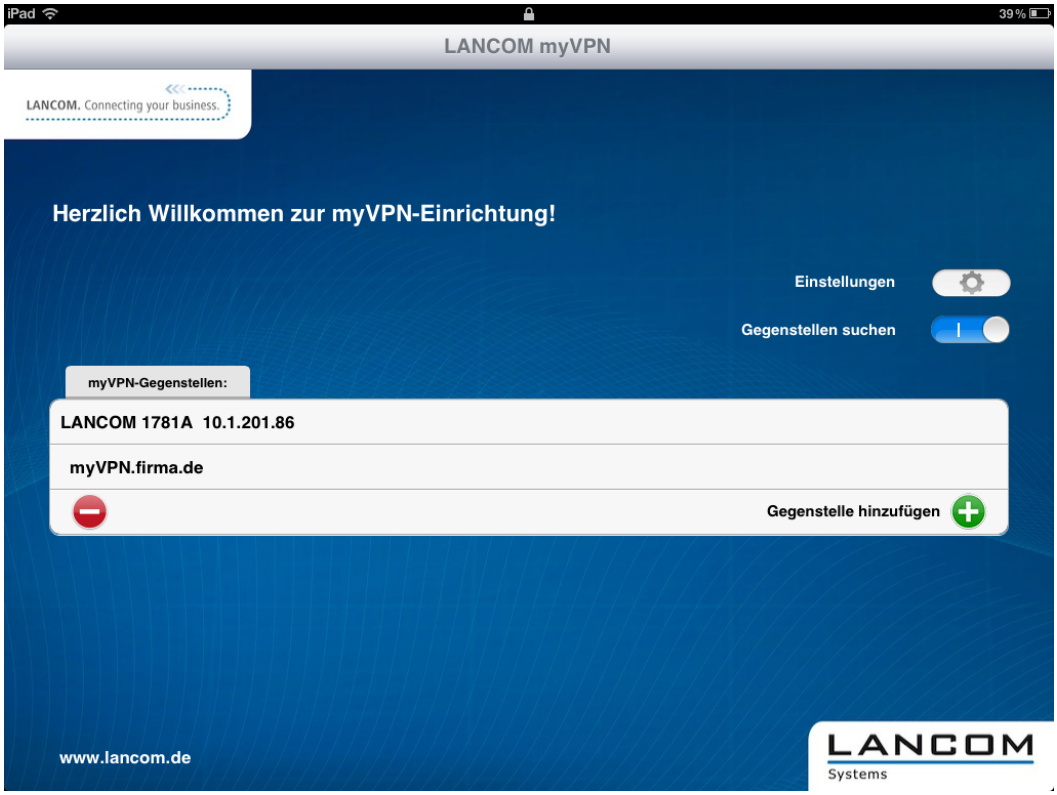


Das iOS-Gerät listet nun alle über WLAN erreichbaren VPN-Geräte mit aktiviertem LANCOM myVPN Modul auf. Ein Eintrag in dieser Liste bedeutet dabei nicht, dass Ihr iOS-Gerät von diesem VPN-Gerät auch ein LANCOM myVPN-Profil beziehen kann.

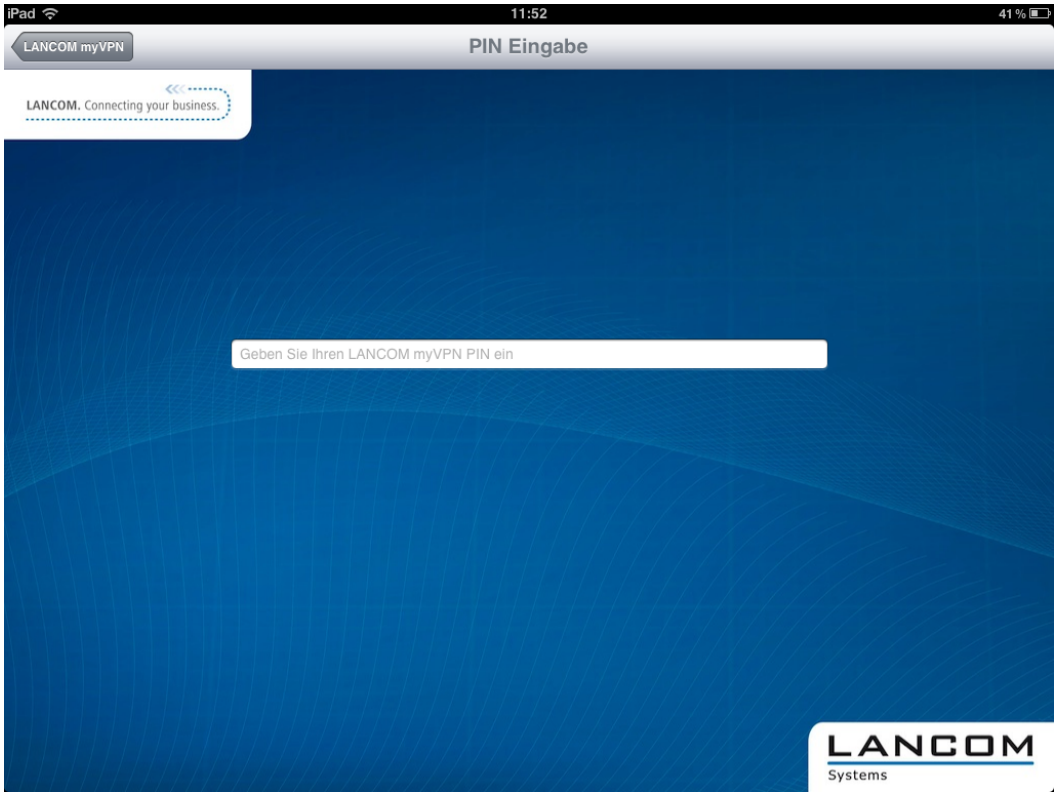
4. Optional: Wählen Sie die Option **Gerät manuell hinzufügen**, um die IP-Adresse oder den Namen von VPN-Geräten einzugeben, welche das iOS-Gerät über eine Internet-Verbindung (3G oder WLAN) erreichen kann. Geben Sie im folgenden Dialog die IP-Adresse oder den Namen des VPN-Gerätes ein und bestätigen Sie mit **Ja**.



5. Die App zeigt nun alle VPN-Geräte, welche Profile für die LANCOM myVPN App anbieten.



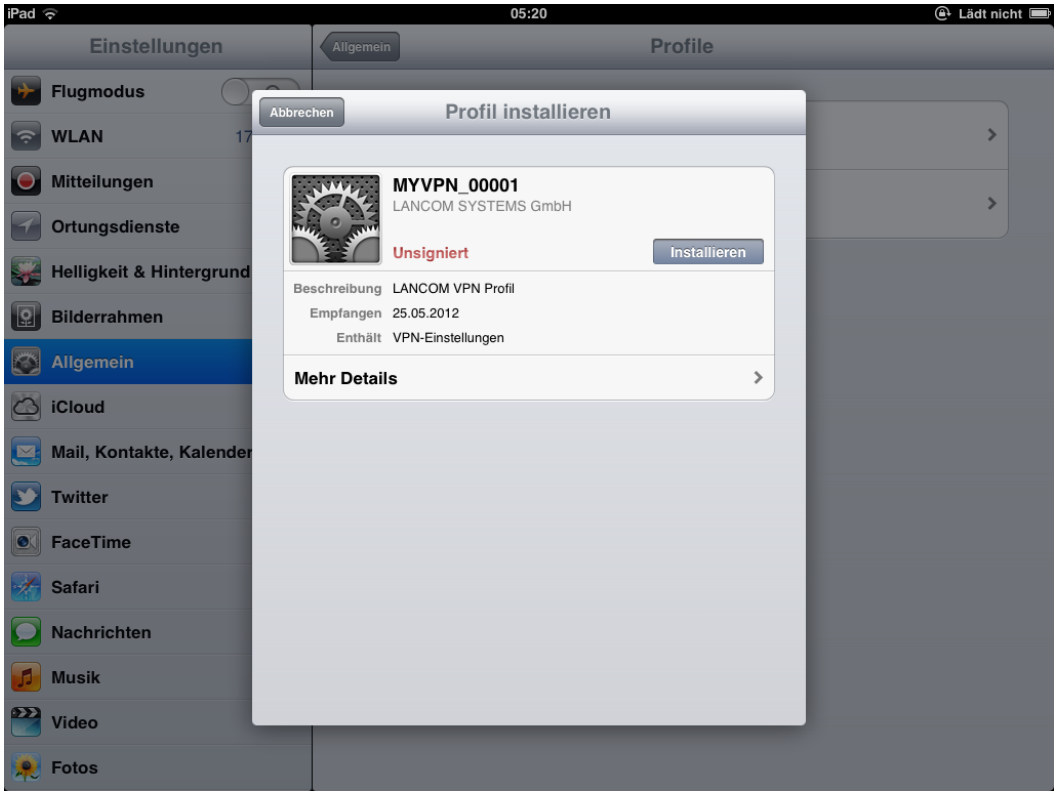
6. Wählen Sie durch Antippen das gewünschte VPN-Gerät aus der Liste aus und geben Sie im folgenden Dialog die PIN für den Bezug des VPN-Profils ein.



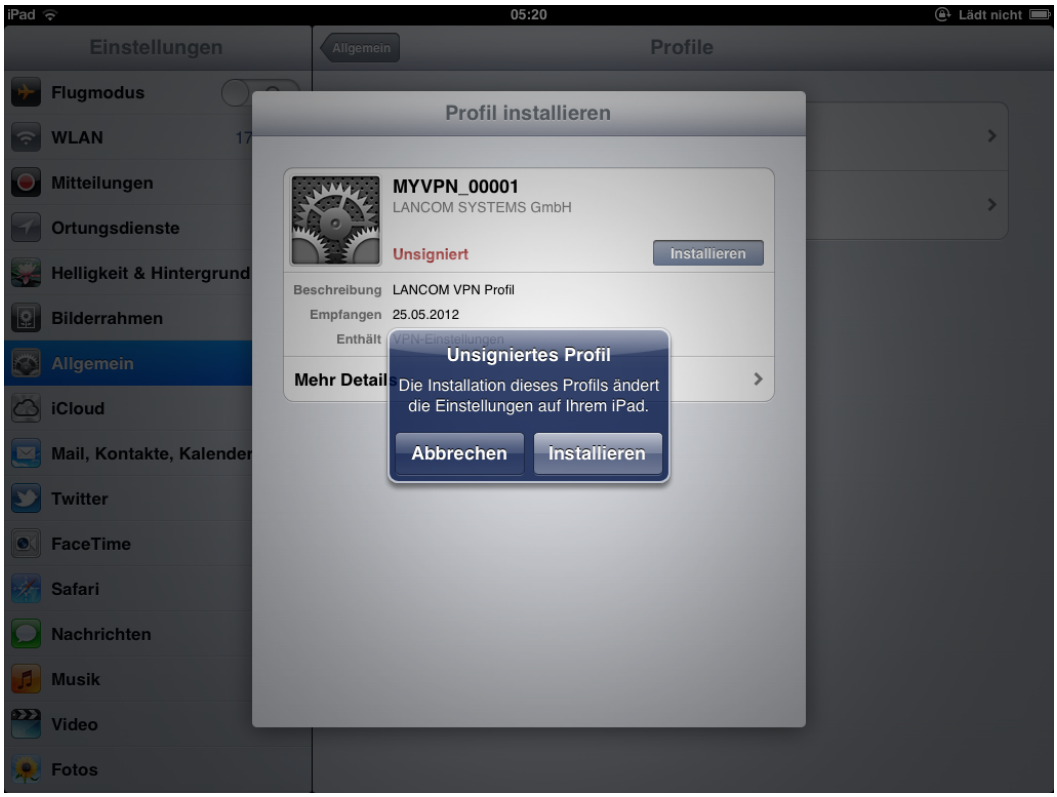
Wenn Sie die PIN 5 Mal falsch eingeben, wird das myVPN-Modul auf dem LANCOM VPN-Gerät komplett für eine bestimmte Zeit gesperrt. VPN-Verbindungen von iOS-Geräten mit zuvor erfolgreich eingerichteten VPN-Zugängen sind in diesem Zustand weiter möglich. Allerdings können iOS-Geräte von diesem VPN-Gerät für die Dauer der Sperrung keine neuen myVPN-Profile beziehen. Ein Administrator kann die Sperrung im myVPN-Modul wieder aufheben.

7. Bestätigen Sie im nächsten Dialog den Hinweis auf ein evtl. nicht signiertes Zertifikat mit der Schaltfläche **Ja**.

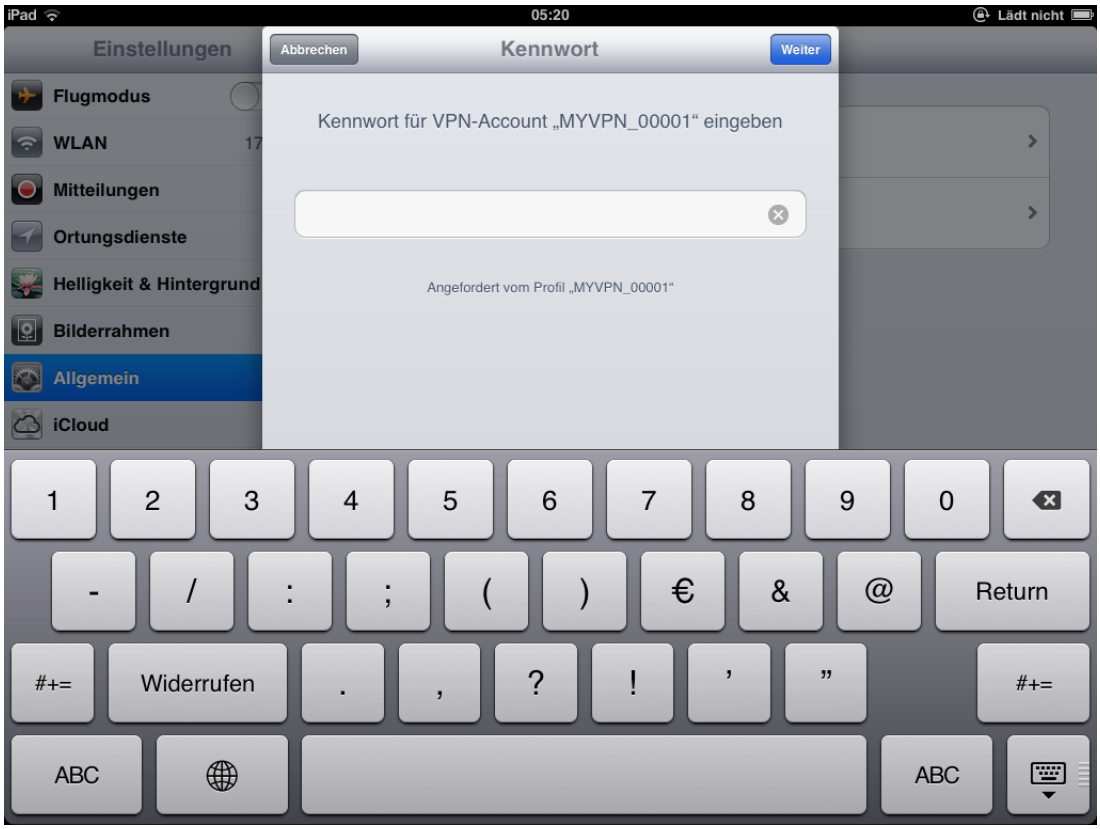
8. Bestätigen Sie im nächsten Dialog die Aufforderung zur Installation des Profils mit der Schaltfläche **Installieren**.



Bestätigen Sie auch die notwendigen Änderungen der Einstellungen auf Ihrem iOS-Gerät.

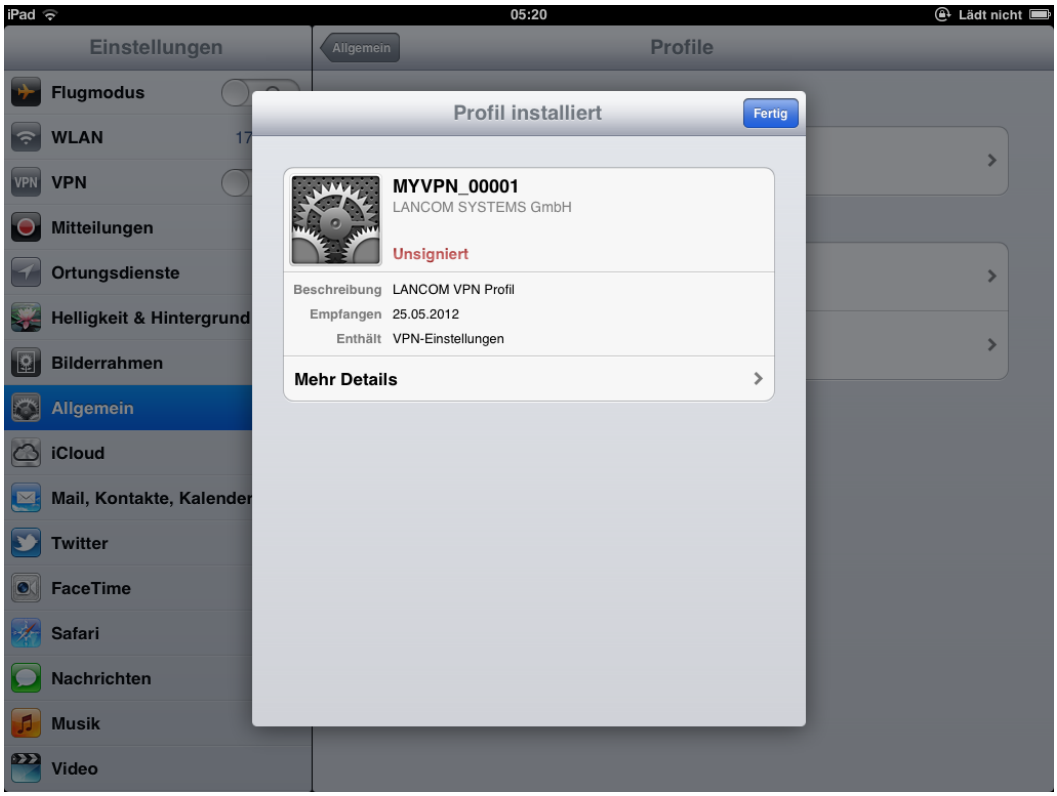


9. Die Installations-Routine fordert Sie im nächsten Schritt zur Eingabe des Kennworts für den VPN-Zugang auf. Das VPN-Kennwort entspricht standardmäßig der PIN für das myVPN-Profil. Wenn Sie das Kennwort für den VPN-Zugang hier eingeben, kann das iOS-Gerät anschließend ohne weitere Kennworteingabe eine VPN-Verbindung zu Ihrem Firmennetzwerk aufbauen. Lassen Sie das Feld für das VPN-Kennwort frei, damit das iOS-Gerät Sie bei jedem Verbindungsaufbau erneut zur Eingabe des VPN-Kennworts auffordert. Bestätigen Sie Ihre Auswahl mit der Schaltfläche **Weiter**.

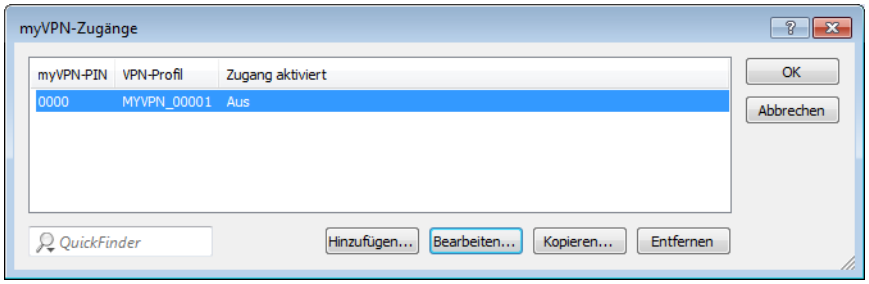


Wir empfehlen aus Sicherheitsgründen, das Kennwort für den VPN-Zugang **nicht** auf dem Gerät zu speichern, sondern sie bei jedem Verbindungsaufbau einzugeben.

10. Das VPN-Profil ist nun vollständig auf Ihrem iOS-Gerät installiert und bereit für den Aufbau einer VPN-Verbindung in Ihr Firmennetzwerk. Bestätigen Sie den Abschluss der Installation mit der Schaltfläche **Fertig**.



Sobald das myVPN-Profil von einem iOS-Gerät bezogen wurde, deaktiviert die Installationsroutine dieses myVPN-Profil auf dem LANCOM VPN-Gerät. Sie können diesen Zustand z. B. über LANconfig im Konfigurationsbereich **VPN** > **myVPN** in der Liste **myVPN-Zugänge** überprüfen:



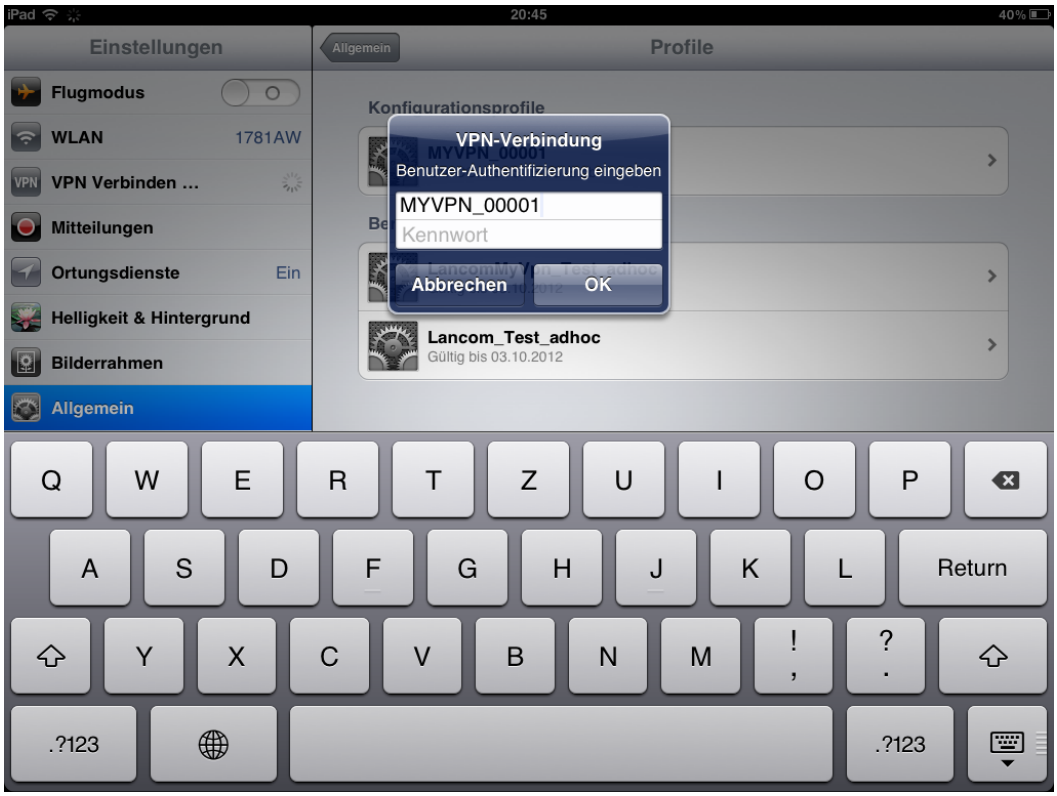
Das Deaktivieren des myVPN-Profils verhindert ausschließlich, dass ein weiteres iOS-Gerät das gleiche myVPN-Profil noch einmal installiert und somit die gleichen Einstellungen für den VPN-Zugang verwendet. Das Deaktivieren des myVPN-Profils hat hingegen keine Auswirkung auf den VPN-Zugang selbst.

11.3 VPN-Verbindung auf dem iOS-Gerät herstellen und beenden

Nachdem Sie das VPN-Profil mit der LANCOM myVPN App auf Ihrem iOS-Gerät installiert haben, stellen Sie wie folgt die VPN-Verbindung zu Ihrem Firmennetzwerk her oder beenden diese:

1. Aktivieren Sie den VPN-Tunnel im Konfigurationsbereich **Einstellungen** über die Option **VPN**.

2. Im folgenden Dialog ist der Benutzername aus dem myVPN-Profil bereits eingetragen. Geben Sie das Kennwort für die VPN-Verbindung ein und bestätigen Sie mit **OK**.



Standardmäßig entspricht das Kennwort für die VPN-Verbindung der PIN für das myVPN-Profil.

Das Kennwort ist bereits eingetragen, wenn Sie das Kennwort für die VPN-Verbindung bei der Installation des myVPN-Profils eingegeben haben. In diesem Fall erscheint dieses Fenster nicht, die Verbindung wird direkt hergestellt.

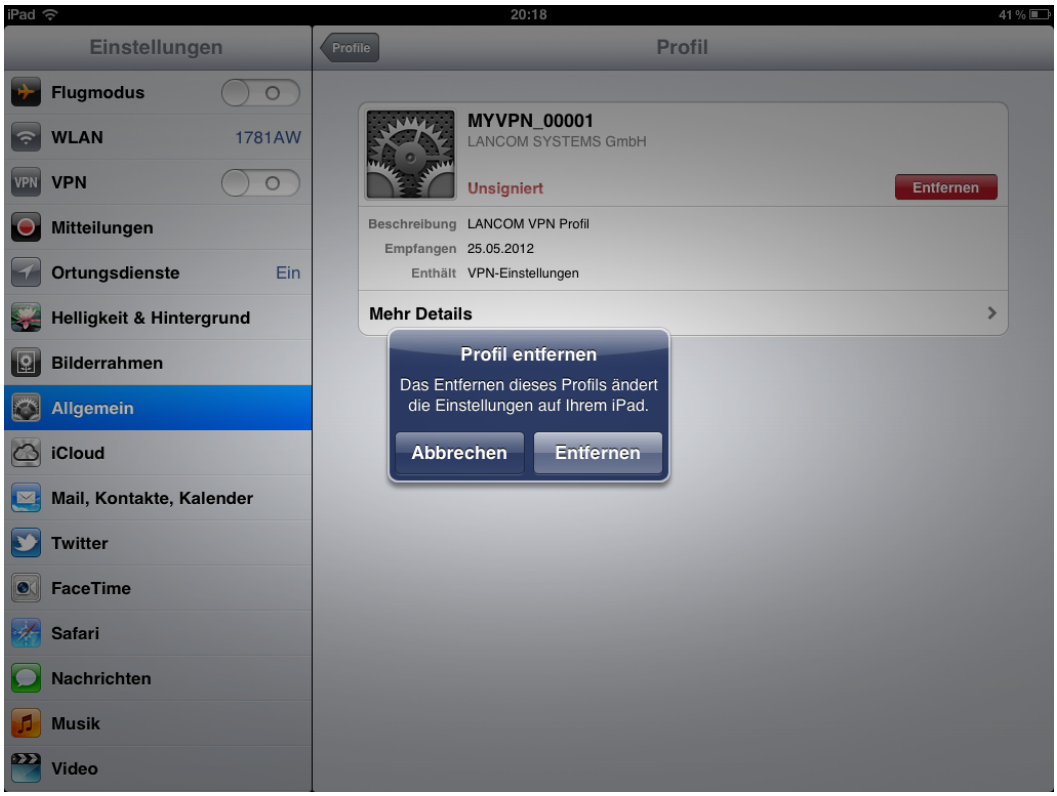
3. Beenden Sie die VPN-Verbindung auf Ihrem iOS-Gerät im Konfigurationsbereich **Einstellungen** über die Option **VPN**.

11.3 VPN-Profil auf dem iOS-Gerät löschen

So löschen Sie das VPN-Profil wieder von Ihrem iOS-Gerät:

1. Wechseln Sie mit **Einstellungen** > **Allgemein** > **Profile** in die Liste der verfügbaren Profile Ihres iOS-Gerätes.

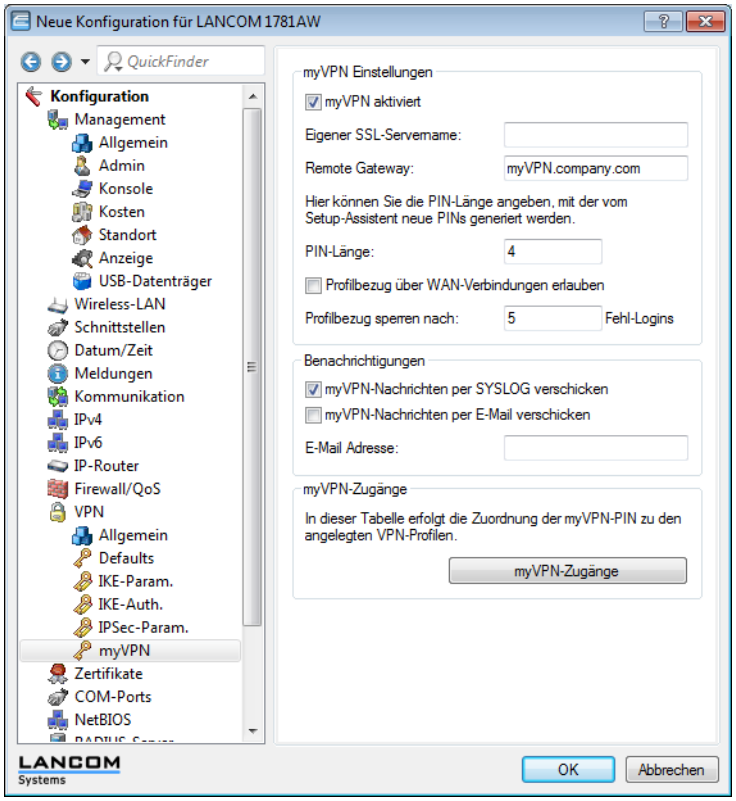
2. Wählen Sie das gewünschte Profil aus, klicken Sie auf **Entfernen** und bestätigen Sie im nächsten Dialog die Aktion noch einmal mit **Entfernen**.



11.3.1 Ergänzungen in LANconfig

Konfiguration der LANCOM myVPN App

Unter **VPN** > **myVPN** können Sie die Einstellungen für die LANCOM myVPN App manuell festlegen.



Markieren Sie **myVPN aktiviert**, um der LANCOM myVPN App zu ermöglichen, ein VPN-Profil zu laden.

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.

Bestimmen Sie im Feld **Remote-Gateway** die WAN-Adresse oder den über öffentliche DNS-Server auflösbaren Namen dieses Routers. Geben Sie dieses Remote-Gateway in der LANCOM myVPN App an, sofern die App das Gateway nicht über die automatische Suche findet.

Bestimmen Sie die **PIN-Länge**, mit der der Setup-Assistent neue PINs generiert (Default = 4).

Aktivieren Sie die Option **myVPN-Nachrichten per SYSLOG verschicken**, um Nachrichten der LANCOM myVPN App an SYSLOG zu versenden.

Aktivieren Sie die Option **myVPN-Nachrichten per E-Mail verschicken**, um Nachrichten der LANCOM myVPN App an eine bestimmte E-Mail-Adresse zu versenden.

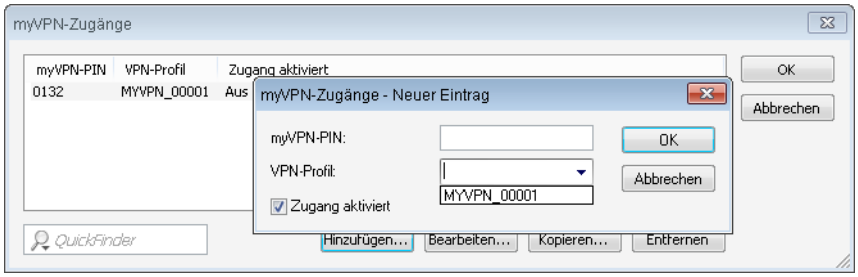
Diese Nachrichten umfassen:

- Erfolgreicher Profilbezug
- Auftreten einer Loginsperre für die LANCOM myVPN App aufgrund zu vieler Fehlversuche
- Aufhebung der Loginsperre (wobei nicht berücksichtigt wird, ob sie durch den Ablauf der vorgegebenen Zeitspanne oder manuell erfolgt ist)

Bestimmen Sie die **E-Mail-Adresse**, an welche die LANCOM myVPN App Nachrichten versenden soll.

Der Versand von E-Mails muss auf dem VPN-Gerät dazu konfiguriert sein.

Über **myVPN-Zugänge** erfolgt die Zuordnung der myVPN-PIN zu den angelegten VPN-Profilen.



Bestimmen Sie hier das **VPN-Profil**, dessen Daten die LANCOM myVPN App beim Profilbezug laden soll.

Vergeben Sie hier die myVPN-PIN zum Profilbezug der LANCOM myVPN App.

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 fünf Fehlversuchen sperrt das Gerät den Profilbezug für 15 Minuten. Fünf weitere Fehlversuche sperren den Profilbezug für einen Tag. 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.

Aktivieren Sie das Profil, indem Sie die Option **Zugang aktiviert** markieren.

Nach einem erfolgreichen Profilbezug deaktiviert das Gerät das entsprechende Profil automatisch, um den wiederholten Download von einem anderen Gerät zu vermeiden.

Sobald Sie diese Einstellungen im Gerät speichern, ist das myVPN-Modul auf dem gewählten VPN-Gerät aktiviert. Sie können nun die LANCOM myVPN App auf Ihrem iOS-Gerät starten und mit Eingabe der PIN das VPN-Profil beziehen.

11.3.2 Ergänzungen im Menüsystem

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*.

SNMP-ID:

2.19.28

Pfad Telnet:

Pfad Telnet: Setup > Vpn > myVPN

Aktiv

Mit diesem Schalter können Sie myVPN für dieses Gerät aktivieren.

SNMP-ID:

2.19.28.1

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Ja

Nein

Default:

Nein

PIN-Laenge

Hier können Sie die PIN-Länge angeben, mit der der Setup-Assistent neue PINs generiert.

SNMP-ID:

2.19.28.2

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Maximale Länge: 12

Minimale Länge: 4

Default:

4

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.

SNMP-ID:

2.19.28.3

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 31 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

leer

Mapping

In dieser Tabelle erfolgt die Zuordnung der myVPN-PIN zu den angelegten VPN-Profilen.

SNMP-ID:

2.19.28.4

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

PIN

Hinterlegen Sie hier die PIN zum Profilbezug der myVPN-App.

Der myVPN-Setup-Assisstent 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.

SNMP-ID:

2.19.28.4.1

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

max. 12 Ziffern aus 1234567890

Default:

leer

VPN-Profil

Bestimmen Sie hier das VPN-Profil, dessen Daten die myVPN-App beim Profilbezug laden soll.

SNMP-ID:

2.19.28.4.2

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

16 Zeichen aus

0-9

a-z

A-Z

@{|}~!$%&'()+-,/:;<=>?[\]^_.

Default:

leer

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.

SNMP-ID:

2.19.28.4.3

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN** > **Mapping**

Mögliche Werte:

Nein

Ja

Default:

Nein

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.

SNMP-ID:

2.19.28.5

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

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)

SNMP-ID:

2.19.28.6

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

E-Mail-Adresse

Bestimmen Sie hier die E-Mail-Adresse, an die die myVPN-App Nachrichten versenden soll.

SNMP-ID:

2.19.28.7

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

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

Default:

leer

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)

SNMP-ID:

2.19.28.8

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

Nein

Ja

Default:

Nein

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.

SNMP-ID:

2.19.28.9

Pfad Telnet:

Pfad Telnet: Setup > **Vpn** > **myVPN**

Mögliche Werte:

max. 63 Zeichen aus

0-9

a-z

A-Z

#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

leer

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 zwiten Überschreitung für 24 Stunden.

Der Konsolenbefehl `Loginsperre-aufheben` hebt diese Sperrung wieder auf (siehe *Loginsperre-aufheben*).

SNMP-ID:

2.19.28.10

Pfad Telnet:

Setup > **Vpn** > **myVPN**

Mögliche Werte:

5-30

Default:

5

Zugriff-vom-WAN-erlauben

Dieser Parameter erlaubt oder unterbindet das Laden des myVPN App-Profils durch den Benutzer vom WAN aus.

SNMP-ID:

2.19.28.11

Pfad Telnet:

Setup > **Vpn** > **myVPN**

Mögliche Werte:

ja

nein

Default:

ja

12 Voice over IP - VoIP

12.1 Default-Wert für die WAN-Anmeldung eines SIP-Benutzers

Der Default-Wert für die WAN-Anmeldung eines SIP-Benutzers hat sich geändert von 'Ja' zu 'Nein'.

12.1.1 Ergänzungen im Menüsystem

Zugriff von WAN

Bestimmen Sie hier, ob und wie sich SIP-Clients über eine WAN-Verbindung mit dem entsprechenden Benutzerdaten anmelden können.

SNMP-ID:

2.33.3.1.1.8

Pfad Telnet:

Setup > **Voice-Call-Manager** > **User** > **SIP-User** > **User**

Mögliche Werte:

ja

nein

VPN

Default:

Nein

Index