Benutzerhandbuch
Digitalisierungsbox Standard

Erweiterte Konfiguration

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

bintec elmeg GmbH gibt keinerlei Gewährleistung auf die in dieser Bedienungsanleitung enthaltenen Informationen. bintec elmeg GmbH übernimmt keine Haftung für mittelbare, unmittelbare, Neben-, Folge- oder andere Schäden, die mit der Auslieferung, Bereitstellung oder Benutzung dieser Bedienungsanleitung im Zusammenhang stehen.

Open Source Software in diesem Produkt

Dieses Produkt enthält neben anderen Komponenten Open-Source-Software, die von Drittanbietern entwickelt wurde und unter einer Open-Source-Softwarelizenz lizenziert ist. Diese Open-Source-Softwaredateien unterliegen dem Copyright. Eine aktuelle Liste der in diesem Produkt enthaltenen Open-Source-Softwareprogramme und die Open-Source-Softwarelizenzen finden Sie unter *www.bintec-elmeg.com* .

GEMA

Dieses Produkt verwendet interne Wartemusik, für deren Verwendung eine Genehmigung durch die GEMA (Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte) nicht erforderlich ist. Dies hat die GEMA mit Freistellungsbescheinigung bestätigt. Die Freistellungsbescheinigung kann unter folgender Internet-Adresse eingesehen werden: *www.bintec-elmeg.com* . Wartemelodien des Systems: elmeg Song, Hold the line.

Inhaltsverzeichnis

Kapitel 1 Zweck dieses Handbuchs

Dieses Handbuch beschreibt zum einen die Inbetriebnahme Ihrer **Digitalisierungsbox** von einem technischen Standpunkt aus, zum andern beschreibt es diejenigen Menüs, die in der Benutzeroberfläche über den Link **Mehr anzeigen** zugänglich sind und die Einrichtung erweiterter Funktionen erlauben. Die Einrichtung mittels der **Assistenten** ist im Handbuch "Bedienungsanleitung" beschrieben. Sie finden es im Downloadbereich Ihrer **Digitalisierungsbox**. Beide Einrichtungsansätze werden von der Online-Hilfe Ihres Geräts unterstützt.

Kapitel 2 Inbetriebnahme

2.1 Digitalisierungsbox Standard

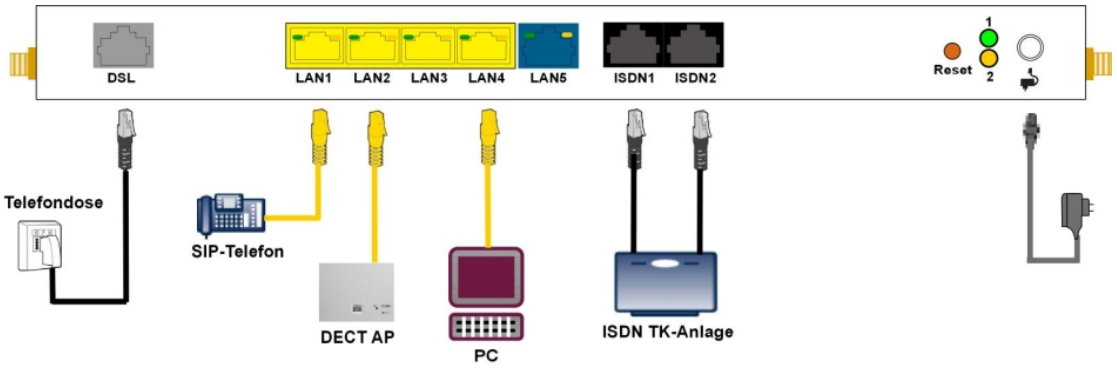
In diesem Kapitel erfahren Sie, wie Sie Ihr Gerät aufstellen, anschließen und in wenigen Minuten in Betrieb nehmen.

Der Weg zu einer weiterführenden Konfiguration wird Ihnen anschließend Schritt für Schritt erläutert. Tiefergehende Kenntnisse über Telefonanlagen und Router sind dabei nicht erforderlich. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

Die PDF-Version dieses Dokuments enthält eine schlanke Version des Handbuchs. Sie beinhaltet alle Informationen zur Installation und Montage sowie die Beschreibung der Konfigurationsparameter, aber keine Screenshots. Eine HTML-basierte Version mit Screenshots ist im Downloadbereich Ihres Gerätes als ZIP-Datei verfügbar. Entpacken Sie die ZIP-Datei in einen Ordner Ihrer Wahl und rufen Sie die Datei "start.html" in einem Webbrowser auf.

2.1.1 Aufstellen und Anschließen

Die **Digitalisierungsbox Standard** wird an einem reinen IP-Anschluss betrieben. Sie telefonieren ausschließlich über VoIP, sind aber beim Anschluss Ihrer Endgeräte nicht eingeschränkt: Sie können SIP-Endgeräte, eine ISDN-Telefonanlage sowie PCs anschließen.



Achtung

Vor Installation und Inbetriebnahme Ihres Geräts lesen Sie bitte aufmerksam die beiliegenden Sicherheitshinweise.

Achtung

Die Verwendung eines falschen Steckernetzgeräts kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich das mitgelieferte Steckernetzgerät!

Gehen Sie beim Aufstellen und Anschließen in der folgenden Reihenfolge vor:

(1) Montage
Um einen störungsfreien Betrieb zu gewährleisten, sollte die **Digitalisierungsbox Standard** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein (lesen Sie bitte aufmerksam das Kapitel *Montage* auf Seite 7).

(2) Netzanschluss
Schließen Sie den Netzanschluss des Geräts mit dem mitgelieferten Steckernetzgerät an eine 230 V~ Steckdose an.

(3) Antennen
Schrauben Sie die mitgelieferten Antennen auf die dafür vorgesehenen Anschlüsse.

(4) DSL

Verbinden Sie den Anschluss **DSL** über das graue Kabel an die TAE-Buchse der Telefondose an.

(5) ISDN-Telefonanlage
Schließen Sie eine ISDN-Telefonanlage an den internen ISDN-Anschluss der **Digitalisierungsbox Standard** an. Die Up0-Schnittstelle wird nicht unterstützt.

(6) SIP-Telefone
Schliessen Sie Ihre SIP-Telefone an die 10/100/1000 Base-T Ethernet-Schnittstellen an. Einen letzten Schritt müssen Sie am PC ausführen.

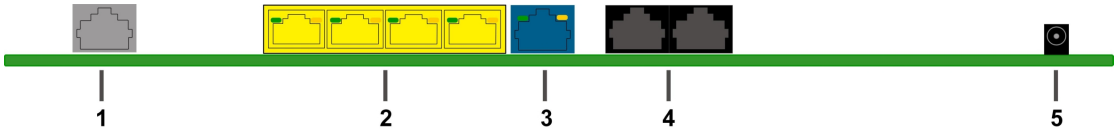
(7) PC
Schließen Sie einen geeigneten PC über ein Ethernet-Kabel an eine der Ethernet-Schnittstellen der **Digitalisierungsbox Standard** an. Sollten Probleme bei der Verbindung zwischen PC und der **Digitalisierungsbox Standard** auftreten, lesen Sie bitte die entsprechenden Kapitel zur Grundkonfiguration.

(8) VoIP
Für einen reinen IP-Anschluss ohne ISDN verwenden Sie die vom Provider bereitgestellte Anleitung.

Hinweis

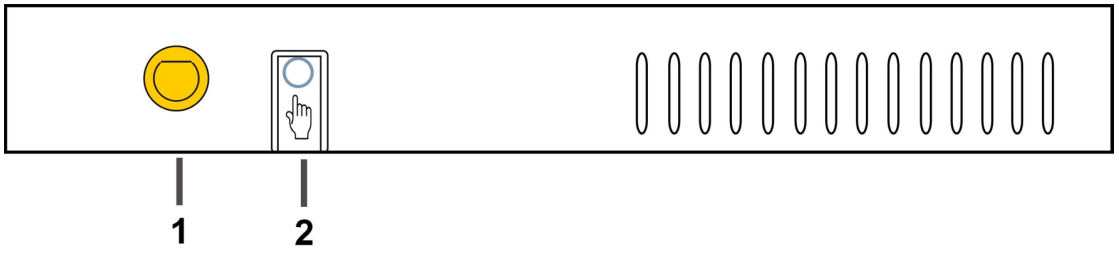
Mit der **"Automatischen Konfiguration"** der Telekom wird Ihr Gerät automatisch eingerichtet (siehe *Automatische Konfiguration* auf Seite 10).

2.1.2 Anschlüsse



1	DSL-Schnittstelle Annex B/J
2	10/100/1000 Base-T Ethernet-Schnittstellen (LAN 1 - LAN4)
3	Ethernet-WAN-Schnittstelle (LAN5)
4	Schnittstelle für ISDN TK-Anlagen (ISDN1, ISDN2)
5	Buchse für das Steckernetzteil

2.1.3 Anschlüsse (seitlich)



1	Antennenanschluss
2	Funktionstaste

2.1.4 Montagewinkel

Aufgrund der Platzierung der Geräte im Netzwerkschrank, empfiehlt es sich auf abgesetzte Antennen zurückzugreifen. Montieren Sie die Montagewinkel mit den im Set beiliegenden Schrauben am Gehäuse. Die Montagewinkel und die Schrauben sind als Zubehör erhältlich (Artikelnummer MN40285514).

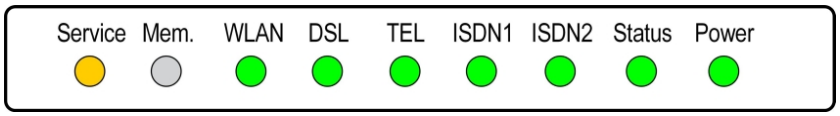
Hinweis

Bei Betrieb im Netzwerkschrank darf die Umgebungstemperatur 40 °C nicht übersteigen!

2.1.5 LEDs

Anhand der LEDs können Sie den Status Ihres Geräts ablesen.

Die LEDs der **Digitalisierungsbox Standard** sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
Service	Gelb	an	Automatische Wartung aktiv
		aus	Automatische Wartung inaktiv
Mem.			ohne Funktion
WLAN		aus	WLAN oder alle zugeordneten Drahtlosnetzwerk deaktiviert
	Grün	langsam blinkend	Drahtlosnetzwerk ist aktiv, kein Client ist angemeldet
	Grün	schnell blinkend	Drahtlosnetzwerk ist aktiv, mindestens ein Client ist angemeldet
	Grün	flackernd	Drahtlosnetzwerk ist aktiv, mindestens ein Client ist angemeldet, es besteht Datenverkehr
DSL	Grün	an	Verbindung hergestellt
	Grün	langsam blinkend	Synchronisation läuft
		aus	Keine Synchronisation
	Grün	flackernd	Datentransfer
TEL	Grün	an	Telefonie am IP-Anschluss (Voice over IP) bereit
		aus	Telefonie nicht eingerichtet
ISDN1 / ISDN 2	Grün	an	ISDN-Endgeräte angeschlossen
		aus	Ruhezustand oder außer Betrieb
Status	Grün	an	Nach dem Einschalten: Gerät wird gestartet während des Betriebs: Fehler
	Grün	langsam blinkend	Gerät ist aktiv
Power	Grün	an	Stromversorgung ist angeschlossen
		aus	Keine Stromversorgung

Die LEDs der Ethernet-Buchsen LAN 1-4 (LAN) und LAN 5 (WAN) zeigen folgende Statusinformationen an:

Ethernet-LEDs

LED	Farbe	Status	Information
LAN 1 bis 4 (Link/Act)	Grün	an	Ethernet -Verbindung hergestellt
LAN 1 bis 4 (Link/Act)	Grün	blinkend	Datenübertragung über Ethernet
LAN 1 bis 4 (Link/Act)		aus	Keine Ethernet-Verbindung

LED	Farbe	Status	Information
LAN 1 bis 4 (Speedt)	Grün	an	1000 Mbit/s Übertragungsrate
LAN 1 bis 4 (Speedt)	Orange	an	100 Mbit/s Übertragungsrate
LAN 1 bis 4 (Speedt)		aus	10 Mbit/s Übertragungsrate
LAN 5 (Link/Act)	Grün	an	WAN- Ethernet -Verbindung hergestellt
LAN 5 (Link/Act)	Grün	blinkend	Daten über ETH 5 senden/ empfangen
LAN 5 (Link/Act)		aus	Keine Ethernet-Verbindung
LAN 5 (Speedt)	Grün	an	1000 Mbit/s Übertragungsrate
LAN 5 (Speedt)	Orange	an	100 Mbit/s Übertragungsrate
LAN 5 (Speedt)		aus	10 Mbit/s Übertragungsrate

2.1.6 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Produktname	Kabelsätze/Sonstiges	Dokumentation
Digitalisierungsbox Standard	ein Ethernet LAN-Kabel (gelb) ein Ethernet WAN-Kabel (blau) ein DSL-Kabel (grau) ein Netzteil zwei WiFi-Antennen	Installationsposter Sicherheitshinweise

2.1.7 Allgemeine Produktmerkmale

Die allgemeinen Produktmerkmale umfassen die Leistungsmerkmale und die technischen Voraussetzungen für Installation und Betrieb Ihres Geräts.

Allgemeine Produktmerkmale Digitalisierungsbox Standard

Eigenschaft	
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	328 x 193 x 44 mm
Gewicht	ca. 900 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1800 g
Speicher	128 MB SDRAM
LEDs	19 (8 x Funktion, 1 x Service, 5x2 Ethernet)
Leistungsaufnahme Gerät	max. 24 W 12 V DC
Spannungsversorgung	12 V DC 2 A
Umweltanforderungen:	
Lagertemperatur	-20 °C bis +70 °C

Eigenschaft	
Betriebstemperatur	+5 °C bis +40 °C
Relative Luftfeuchtigkeit	max. 85 %
Raumklassifizierung	Nur in trockenen Räumen betreiben
Verfügbare Schnittstellen:	
DSL-Schnittstelle	Internes DSL-Modem
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
ISDN-Schnittstellen	2 interne ISDN-Schnittstellen, ISDN-Terminierung
Vorhandene Buchsen:	
WLAN Antennen	R-SMA-Buchsen
Ethernet-Schnittstellen 1 - 4 (LAN)	RJ45-Buchse
Ethernet-Schnittstelle 5 (WAN)	RJ45-Buchse
ISDN-Schnittstelle (ISDN1, ISDN2)	RJ45-Buchse
DSL-Schnittstelle	RJ45-Buchse
Hohlsteckerbuchse für Stromversorgung	

2.2 Reset

Der Reset wird über den Reset-Knopf an der Anschlussseite des Systems durchgeführt.

Bei einem kurzen Tastendruck (ca. eine Sekunde) wird das Gerät neu gestartet. Dieser Tastendruck entspricht einer Unterbrechung der Stromversorgung. Die gespeicherten Daten bleiben erhalten, aber alle Verbindungen werden unterbrochen.

Drücken Sie die Reset-Taste für ca. 30 bis 40 Sekunden, führt das Gerät einen Factory Reset durch. Dies bedeutet, dass das Gerät in den Auslieferungszustand zurückversetzt wird. Die Verbindungsdaten ein und ausgehender Anrufe werden dabei nicht gelöscht. Die Konfiguration wird gelöscht und alle Passwörter werden zurückgesetzt. Der Reset ist beendet, wenn nach 30 bis 40 Sekunden die Status-LED gleichmäßig blinkt.

2.3 Support-Information

Ergänzende Beratung zu Ihrer Digitalisierungsbox erhalten Sie während der üblichen Geschäftszeiten unter der kostenfreien Rufnummer 0800 330 1300 oder unter 0800 330 2870 (für Großkunden). Weitere Hinweise finden Sie auch im Internet unter *http://hilfe.telekom.de*. Vermuten Sie eine Störung Ihres Anschlusses, wenden Sie sich bitte unter der entsprechenden Nummer an den Technischen Kundendienst oder informieren Sie sich unter *http://hilfe.telekom.de*.

Kapitel 3 Montage

Warnung

Zur Vermeidung eines Elektroschocks ist Vorsicht beim Anschließen von Telekommunikationsnetzen (TNV-Stromkreisen) geboten. LAN-Ports verwenden ebenfalls RJ-Steckverbinder.

Achtung

Um einen störungsfreien Betrieb zu gewährleisten, sollte die **Digitalisierungsbox Standard** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein. Das Gerät darf keiner direkten Sonneneinstrahlung oder anderen Wärmequellen ausgesetzt sein. Beachten Sie auch die einzuhaltenden Abstände (siehe *Wandmontage* auf Seite 7).

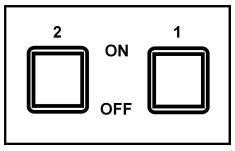
3.1 Anschluss von Endgeräten

3.1.1 Interner ISDN-Anschluss

Der interne ISDN-Anschluss der **Digitalisierungsbox Standard** stellt an jedem internen ISDN-Anschluss 2,5 Watt Speiseleistung für den Anschluss von maximal zwei ungespeisten ISDN-Endgeräten zur Verfügung. Der interne ISDN-Anschluss ist im Auslieferungszustand als "Kurzer passiver Bus" ("S0-Bus") eingerichtet. Es ist die einfache Bus-Verkabelung eines ISDN-Systems mit einer Länge von bis zu 120 m.

3.1.2 Terminierung der ISDN-Schnittstellen

Die Schalter für die Terminierung der ISDN-Schnittstellen befinden sich im Boden/Unterschale des Geräts. Im Auslieferungszustand sind beide Schalter auf ON gestellt. Damit ist die Terminierung aktiv und das Gerät für alle gängigen Anwendungen vorkonfiguriert.



3.2 Reset Taster

An der Anschlussseite des Geräts befindet sich der Reset-Taster, mit dem Sie einen Neustart des Geräts erzwingen oder den Auslieferungszustand wieder herstellen können (siehe *Reset* auf Seite 6).

3.3 Wandmontage

In diesem Abschnitt werden die Abläufe der Montage beschrieben. Halten Sie sich bitte an diesen Ablauf.

(1) Suchen Sie einen Montageort aus, der max. 1,5 Meter von einer 230 V ~ Netzsteckdose und 2,5 Meter vom Übergabepunkt des Netzbetreibers entfernt ist.

(2) Um eine gegenseitige Beeinträchtigung auszuschließen, montieren Sie das Gerät nicht in unmittelbarer Nähe von elektronischen Geräten wie z. B. HiFi-Geräten, Bürogeräten oder Mikrowellengeräten. Vermeiden Sie auch einen Aufstellort in der Nähe von Wärmequellen, z. B. Heizkörpern oder in feuchten Räumen.

(3) Halten Sie die Abstände ein, die auf der Rückseite des Geräts eingeprägt sind.

(4) Markieren Sie die Bohrlöcher an der Wand.

(5) Überprüfen Sie die feste Auflage aller Befestigungspunkte der **Digitalisierungsbox Standard** an der Wand. Vergewissern Sie sich, dass im Bereich der markierten Bohrlöcher keine Versorgungsleitungen, Kabel o. ä. verlegt sind.

(6) Bohren Sie die Befestigungslöcher an den markierten Stellen (bei Montage mit den Dübeln verwenden Sie einen 5 mm Steinbohrer). Setzen Sie die Dübel ein.

(7) Schrauben Sie die beiden Schrauben so ein, dass zwischen Schraubenkopf und Wand noch ein Abstand von ca. 5 mm verbleibt.

(8) Hängen Sie die **Digitalisierungsbox Standard** mit den rückseitigen Halterungen von oben hinter den Schraubenköpfen ein.

(9) Installieren Sie, wenn erforderlich, die Anschlussdosen für die Endgeräte. Verbinden Sie die Installation der Anschlussdosen mit der des Geräts. Die Anschlussdosen dienen der festen Installation, beispielsweise im Flur. Wenn diese installiert sind, werden die Anschlusskabel mit den Anschlüssen des Geräts verbunden.

(10) Stecken Sie die Anschlüsse der Endgeräte in die Anschlussdosen.

(11) Verbinden Sie die **Digitalisierungsbox Standard** mit dem externen Anschluss. Sie können dazu so verfahren, wie auf dem beigelegten Installationsposter beschrieben.

(12) Stecken Sie das Steckernetzgerät in die 230 V~ Steckdose.

(13) Stecken Sie den Hohlstecker des Steckernetzgeräts in die entsprechende Buchse an Ihrem Gerät.

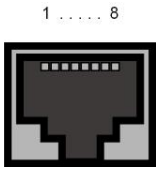
(14) Sie können das Gerät in Betrieb nehmen.

3.4 Pin-Belegungen

3.4.1 Ethernet-Schnittstellen

Die Geräte verfügen über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (LAN1 - LAN4) sowie über eine weitere Ethernet-Schnittstelle zum Anschluss einer WAN-Verbindung oder eines Servers..

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Der Anschluss erfolgt über RJ45-Buchsen.



Die Pin-Zuordnung für die Ethernet 10/100/1000 Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

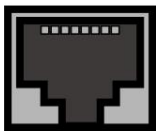
RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	Pair 0 +
2	Pair 0 -
3	Pair 1 +
4	Pair 2 +
5	Pair 2 -
6	Pair 1 -
7	Pair 3 +
8	Pair 3 -

3.4.2 ISDN-Schnittstelle

Der Anschluss erfolgt über eine RJ45-Buchse:

1 8



Die Pin-Zuordnung für die ISDN-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für ISDN-Anschluss

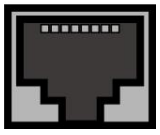
Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Senden (+)
4	Empfangen (+)
5	Empfangen (-)
6	Senden (-)
7	Nicht genutzt
8	Nicht genutzt

3.4.3 xDSL-Schnittstelle

Die **Digitalisierungsbox Standard** verfügt über eine xDSL-Schnittstelle. Die xDSL-Schnittstelle wird mittels eines RJ45-Steckers vergebunden.

Nur die inneren zwei Pins werden für die xDSL-Verbindung verwendet.

1 8



Die Pin-Zuordnung für die xDSL-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für xDSL-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Nicht genutzt
4	Leitung 1a
5	Leitung 1b
6	Nicht genutzt
7	Nicht genutzt
8	Nicht genutzt

Kapitel 4 Grundkonfiguration

Der Weg zur Basiskonfiguration ohne eine Automatische Konfiguration wird Ihnen im Folgenden Schritt für Schritt erläutert. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

4.1 Vorbereitungen

Ihr Gerät ist werksseitig als DHCP-Server eingerichtet, es übermittelt also PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie den PC, mit dem Sie die Grundkonfiguration durchführen wollen, für den automatischen Bezug einer IP-Konfiguration einrichten, ist in *PC einrichten* auf Seite 12 beschrieben.

Hinweis

Sollten Sie in Ihrem LAN bereits einen DHCP-Server betreiben, empfiehlt sich die Konfiguration des Geräts an einem Einzel-PC, der nicht in Ihr LAN integriert ist. Schließen Sie diesen PC allein an Ihrer **Digitalisierungsbox Standard** an, so dass zur Konfiguration ein eigenes Netz entsteht.

4.1.1 Automatische Konfiguration

Die Automatische Konfiguration ist ein Service für Kunden der Telekom, den Sie mit Ihrer **Digitalisierungsbox Standard** nutzen können.

Verbinden Sie die **Digitalisierungsbox Standard** mit dem Stromnetz. Schließen Sie die Kabel an die dafür vorgesehenen Dosen/Buchsen an. Warten Sie, bis die Service-LED nicht mehr leuchtet.

Starten Sie einen Internet-Browser, geben Sie *www.telekom.de* in die Adresszeile ein und bestätigen Sie mit der Eingabetaste. Sie werden auf die Autokonfigurationsseite der Telekom weitergeleitet.

Geben Sie Ihre Zugangskennung und Ihr Passwort ein und klicken Sie auf **Konfiguration starten**. Während der Konfiguration leuchtet die Service-LED. Warten Sie, bis Sie die Bestätigung angezeigt bekommen, dass die Konfiguration erfolgreich war. Die Service-LED ist nun aus.

4.1.2 Systemsoftware

Das Gerät wird mit der zum Zeitpunkt der Produktion aktuellen Systemsoftwareversion betrieben. Die Systemsoftware wird fortwährend weiterentwickelt, um die Sicherheit und Funktionsvielfalt des Geräts zu erhöhen. Dank der **"Automatischen Konfiguration"** der Telekom wird die Systemsoftware Ihres Gerätes auf dem neuesten Stand gehalten (siehe *Automatische Konfiguration* auf Seite 10).

Alternativ können Sie einen Software-Aktualisierung im Menü **Wartung**->**Software &Konfiguration**->**Optionen** vornehmen. Eine Beschreibung der Vorgehensweise finden Sie in *Softwareaktualisierung Digitalisierungsbox Standard* auf Seite 14.

4.1.3 System-Voraussetzungen

Für die Konfiguration des Geräts müssen auf Ihrem PC folgende Systemvoraussetzungen erfüllt sein:

- geeignetes Betriebssystem (Windows, Linux, MAC OS)
- ein Web-Broweser (internet Explorer, Firefox, Chrome) in der jeweils aktuellen Version
- installierte Netzwerkkarte (Ethernet)
- installiertes TCP/IP-Protokoll
- hohe Farbanzeige für die korrekte Darstellung der Grafiken

4.1.4 Daten sammeln

Die wesentlichen Daten für die Konfiguration mit der Konfigurationsoberfläche haben Sie schnell gesammelt.

Bevor Sie mit der Konfiguration beginnen, sollten Sie die Daten für folgende Zwecke bereitlegen:

- Netzwerkeinstellungen (nur falls Sie Ihr Gerät in eine bestehende Netzinfrastruktur integrieren wollen)
- SIP-Provider
- Internetzugang

In den folgenden Tabellen haben wir jeweils Beispiele für die Werte der benötigten Zugangsdaten angegeben. Unter der Rubrik "Ihre Werte" können Sie Ihre persönlichen Daten ergänzen. Dann haben Sie diese bei Bedarf griffbereit.

Grundkonfiguration

Für eine Grundkonfiguration Ihres Geräts benötigen Sie Informationen, die Ihre Netzwerkumgebung betreffen:

Netzwerkeinstellungen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	*192.168.2.1*	
Netzmaske Ihres Gateways	*255.255.255.0*	

SIP-Provider

Zugangsdaten	Beispielwert	Ihre Werte
Beschreibung	Geben Sie den Namen Ihres SIP-Providers an, z.B. *Telekom*.	
Authentifizierungsname/Benutzername	Geben Sie Ihre ID ein, z.B. Ihre Email-Adresse	
Passwort	Geben Sie Ihr Passwort ein, das Sie vom SIP-Provider erhalten haben.	
Registrar	Geben Sie den entsprechenden Registrar ein, z. B. *tel.t-online.de*.	
Rufnummer	z. B. *123456*	

Daten für den Internetzugang über xDSL

Zugangsdaten	Beispielwert	Ihre Werte
Provider-Name	*GoInternet*	
Protokoll	*PPP over Ethernet (PPPoE)*	
Enkapsulierung	*LCC Bridged no FCS*	
VPI (Virtual Path Identifier)	*1*	
VCI (Virtual Circuit Identifier)	*32*	
Anschlusskennung (12-stellig)	*000123456789*	
T-Online-Nummer (meist 12-stellig)	*06112345678*	
Mitbenutzerkennung	*0001*	
Passwort	*TopSecret*	

4.1.5 PC einrichten

Um Ihr Gerät über das Netzwerk erreichen und eine Konfiguration vornehmen zu können, müssen auf dem PC, von dem aus die Konfiguration durchgeführt wird, einige Voraussetzungen erfüllt sein.

- Stellen Sie sicher, dass das TCP/IP-Protokoll auf dem PC installiert ist

TCP/IP-Protokoll prüfen

Um zu prüfen, ob Sie das Protokoll installiert haben, gehen Sie folgendermaßen vor:

(1) Klicken Sie im Startmenü auf **Einstellungen** -> **Systemsteuerung** -> **Netzwerkverbindungen** (Windows XP) bzw. **Systemsteuerung** -> **Netzwerk- und Freigabecenter** -> **Adaptereinstellungen ändern** (Windows 7).

(2) Klicken Sie auf **LAN-Verbindung**.

(3) Klicken Sie im Statusfenster auf **Eigenschaften**.

(4) Suchen Sie in der Liste der Netzwerkkomponenten den Eintrag **Internetprotokoll (TCP/IP)**.

TCP/IP-Protokoll installieren

Wenn Sie den Eintrag **Internetprotokoll (TCP/IP)** nicht finden, installieren Sie das TCP/IP-Protokoll wie folgt:

(1) Klicken Sie im Statusfenster der **LAN-Verbindung** zunächst auf **Eigenschaften**, dann auf **Installieren**.

(2) Wählen Sie den Eintrag **Protokoll**.

(3) Klicken Sie auf **Hinzufügen**.

(4) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **OK**.

(5) Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluss den Rechner neu.

Windows PC als DHCP-Client konfigurieren

Lassen Sie Ihrem PC wie folgt eine IP-Adresse zuweisen:

(1) Gehen Sie zunächst vor, wie oben beschrieben, um die Netzwerkeigenschaften anzuzeigen.

(2) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.

(3) Wählen Sie **IP-Adresse automatisch beziehen**.

(4) Wählen Sie ebenfalls **DNS-Serveradresse automatisch beziehen**.

(5) Schließen Sie alle Fenster mit **OK**.

Ihr PC sollte nun alle Voraussetzungen zur Konfiguration Ihres Geräts erfüllen.

Hinweis

Zur Konfiguration können Sie nun die Konfigurationsoberfläche aufrufen, indem Sie in einem unterstützten Browser die vorkonfigurierte IP-Adresse Ihres Gerätes eingeben (192.168.2.1) und sich mit den voreingestellten Anmeldedaten (**User**: `admin`, **Password**: `admin`) anmelden.

4.2 Konfiguration des Systems

4.2.1 Systempasswort ändern

Alle Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Nach dem ersten Login werden Sie daher aufgefordert, ein sicheres Passwort einzugeben. Bitte beachten Sie folgende Regeln für sichere Passwörter:

- Das Passwort muss mindestens acht Zeichen lang sein.
- Nehmen Sie Zeichen aus mindestens drei der folgenden vier Zeichengruppen:

  - Kleinbuchstaben [a-z]

  - Großbuchstaben [A-Z]

  - Zahlen [0-9]

  - Sonderzeichen.

Hinweis

Drücken Sie am Ende des Konfigurationsvorgangs die Schaltfläche **Konfiguration speichern**! Ansonsten geht auch das neue sichere Passwort nach einem Neustart verloren.

4.2.2 Netzwerkeinstellung (LAN)

Falls Sie Ihr Gerät in eine bestehende Netzinfrastruktur integrieren wollen, wählen Sie für die Netzwerkeinstellungen das Menü **Assistenten**->**Erste Schritte**->**Grundeinstellungen**. Für die LAN-IP-Konfiguration ist der **Adressmodus** standardmäßig auf **Statisch** gesetzt, da Ihr System werksseitig mit einer festen IP ausgeliefert wird. Geben Sie die gewünschte **IP-Adresse** Ihres Geräts in Ihrem LAN und die dazugehörige **Netzmaske** ein. Belassen Sie alle weiteren Einstellungen und klicken Sie **OK**. Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

4.2.3 SIP-Provider eintragen

Sie haben optional die Möglichkeit, für Telefonverbindungen nach extern SIP-Provider einzutragen. Bitte beachten Sie dazu die Beschreibung in der Online-Hilfe für das Menü **VoIP**->**Einstellungen**->**SIP-Konten**->**Neu**.

4.3 Internetverbindung einrichten

Sie können mit Ihrem Gerät eine Internetverbindung aufbauen.

4.3.1 Internetverbindung über das interne VDSL-Modem

Zur einfachen Konfiguration eines VDSL-Internetzugangs verfügt die Konfigurationsoberfläche über einen Assistenten, mit dem Sie die Verbindung unkompliziert und schnell einrichten können.

(1) Gehen Sie in der Benutzeroberfläche in das Menü **Assistenten**->**Internetzugang**.

(2) Legen Sie mit **Neu** einen neuen Eintrag an und übernehmen Sie den **Verbindungstyp** `Internes ADSL-Modem`.

(3) Folgen Sie den Schritten, die der Assistent vorgibt. Der Assistent verfügt über eine eigene Online-Hilfe, die Ihnen ggf. notwendige Informationen vermittelt.

(4) Nachdem Sie den Assistenten beendet haben, speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

4.3.2 Andere Internetverbindungen

Neben einem VDSL-Anschluss über das interne VDSL-Modem können Sie Ihr Gerät noch über weitere Verbindungsarten mit dem Internet verbinden, so etwa über WAN oder über ein externes Gateway / Kabelmodem. Bei dieser Art der Konfiguration unterstützt Sie ebenfalls der Assistent **Internetzugang** in der Konfigurationsoberfläche.

4.3.3 Konfiguration prüfen

Wenn Sie die Konfiguration Ihres Geräts abgeschlossen haben, können Sie die Verbindung in Ihrem LAN sowie zum Internet testen.

Führen Sie folgende Schritte aus, um Ihr Gerät zu testen:

(1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. *`192.168.2.1`*). Es erscheint ein Fenster mit dem Hinweis `"Antwort von..."`.

(2) Testen Sie den Internetzugang, indem Sie im Internet Browser *http://www.telekom.de* eingeben.

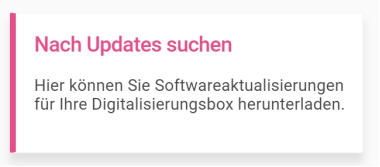
Hinweis

Durch eine Fehlkonfiguration von Endgeräten kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob das Gerät Verbindungen nur zu gewollten Zeiten aufbaut! Beobachten Sie die Leuchtanzeigen Ihres Geräts.

4.4 Softwareaktualisierung Digitalisierungsbox Standard

Die Funktionsvielfalt der **Digitalisierungsbox Standard** wird permanent erweitert. Dank der **"Automatischen Konfiguration"** der Telekom wird die Systemsoftware Ihres Gerätes auf dem neuesten Stand gehalten (siehe *Automatische Konfiguration* auf Seite 10).

Alternativ kann die Softwareaktualisierung über das **GUI** vorgenommen werden. Voraussetzung für ein automatisches Update ist eine bestehende Internetverbindung. Auf dem Home Screen befindet sich folgende Karte:



Bei einem Klick auf diese Karte verbindet sich Ihr Gerät mit dem Download-Server der Deutschen Telekom und überprüft, ob eine aktualisierte Version der Systemsoftware verfügbar ist. Ist dies der Fall, wird die Aktualisierung Ihres Geräts angeboten. Nach der Installation der neuen Software werden Sie zum Neustart des Geräts aufgefordert.

Achtung

Die Aktualisierung kann nach dem Bestätigen mit **Start** nicht abgebrochen werden. Sollte es zu einem Fehler bei der Aktualisierung kommen, starten Sie das Gerät nicht neu und wenden Sie sich an den Support.

Kapitel 5 Assistenten

Das Menü **Assistenten** bietet Schritt-für-Schritt-Anleitungen für grundlegende Konfigurationsaufgaben.

Wählen Sie die entsprechende Aufgabe aus der Navigation aus und folgen Sie den Anweisungen und Erläuterungen auf den einzelnen Assistentenseiten.

Kapitel 6 Home

6.1 Systemverwaltung

Das Menü **Systemverwaltung** enthält allgemeine Systeminformationen und -Einstellungen.

Sie erhalten eine System-Status-Übersicht. Weiterhin werden globale Systemparameter wie z. B. Systemname, Datum / Zeit, Passwörter und Lizenzen verwaltet sowie die Zugangs- und Authentifizierungsmethoden konfiguriert.

6.1.1 Globale Einstellungen

Im Menü **Globale Einstellungen** werden grundlegende Systemparameter verwaltet.

6.1.1.1 System (Media Gateway)

Im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** werden die grundlegenden Systemdaten Ihres Systems eingetragen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Möglich ist eine Zeichenkette mit max. 255 Zeichen. Als Standardwert ist der Gerätetyp voreingestellt.
Standort	Geben Sie an, wo sich Ihr Gerät befindet.
Kontakt	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Möglich ist eine Zeichenkette mit max. 255 Zeichen. Der Standardwert ist *Telekom Deutschland*.
Maximale Anzahl der Syslog-Protokolleinträge	Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind *0* bis *1000*. Der Standardwert ist *50*. Sie können die gespeicherten Meldungen in **Monitoring**->**Internes Protokoll** anzeigen lassen.
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Wählen Sie die Priorität der Systemmeldungen aus, ab der protokolliert werden soll. Nur Systemmeldungen mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass bei der Priorität *Debug* sämtliche erzeugten Meldungen aufgezeichnet werden. Mögliche Werte: • *Notfall*: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet. • *Alarm*: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet.

Feld	Wert
	• *Kritisch*: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet. • *Fehler*: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet. • *Warnung*: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet. • *Benachrichtigung*: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet. • *Information* (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet. • *Debug*: Es werden alle Meldungen aufgezeichnet.
Maximale Anzahl der Accounting-Protokolleinträge	Geben Sie die maximale Anzahl an Einträgen an, die für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind *0* bis *1000*. Der Standardwert ist *20*.
Herstellernamen anzeigen	Hier könne Sie die Anzeige des Herstellers in der MAC-Adresse ein- oder ausschalten. Für den Herstellernamen (meist eine Abkürzung desselben) werden bis zu acht Zeichen am Anfang der MAC-Adresse verwendet. Statt *00:a0:f9:37:12:c9* wird mit Herstelleranzeige zum Beispiel *BintecCo_37:12:c9* angezeigt.
Konfiguration der automatischen Speicherung	Hier können Sie festlegen, ob Änderungen der Konfiguration automatisch gespeichert werden sollen. Standardmäßig ist die Option aktiv. Eine genauere Beschreibung finden Sie unter dieser Tabelle.

Konfiguration der automatischen Speicherung

Nimmt man über das GUI eine Änderung an der Konfiguration vor und bestätigt diese auf der GUI-Seite (mit der entsprechenden Schaltfläche, also z. B. **OK**), so wird die Änderung wie bisher sofort aktiv. Zusätzlich wird die Änderung des Zustands der Konfiguration registriert. Sobald nach Erreichen dieses Zustands ein erneuter HTTP(S)-Verkehr zwischen dem Browser und dem GUI stattfindet, wird die Änderung des Zustands bestätigt und zur Speicherung freigegeben.

Sobald dieser Zustand erreicht ist und die Konfigurationssitzung über den Browser beendet wird, ohne dass die Konfiguration aktiv gespeichert wird, so nimmt das Gerät nach Ablauf der HTTP(S) Session eine automatische Speicherung vor.

Sollte man sich durch einen Konfigurationsfehler selbst vom Zugriff auf das GUI ausgesperrt haben, findet die Bestätigung der Änderung nicht statt und sie wird nach Ablauf der Session nicht gespeichert. Durch einen Neustart des Geräts lässt sich die Änderung dann rückgängig machen.

6.1.1.2 Passwörter (Media Gateway)

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

Hinweis

Alle Geräte werden mit gleichem Benutzernamen und Passwort und den gleichen PINs ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter bzw. PINs nicht geändert wurden.

Wenn Sie sich das erste Mal auf Ihrem Gerät einloggen, werden Sie aufgefordert, das Passwort zu ändern. Sie müssen das Systemadministrator-Passwort ändern, um Ihr Gerät

konfigurieren zu können.

Ändern Sie unbedingt alle Passwörter und PINs, um unberechtigten Zugriff auf das Gerät zu verhindern.

Das Menü **Systemverwaltung**->**Globale Einstellungen**->**Passwörter** besteht aus folgenden Feldern:

Felder im Menü Systempasswort

Feld	Wert
Systemadministrator-Kennwort	Geben Sie das Passwort für den Benutzernamen `admin` an. Das Standard-Passwort ist *admin*. Dieses Passwort wird bei SNMPv3 auch für Authentifizierung (MD5) und Verschlüsselung (DES) verwendet.
Systemadministrator-Kennwort bestätigen	Bestätigen Sie das Passwort, indem Sie es erneut eingeben.

Feld im Menü Globale Passwortoptionen

Feld	Wert
Passwörter und Schlüssel als Klartext anzeigen	Wählen Sie aus, ob die Passwörter im Klartext angezeigt werden sollen. Mit *Anzeigen* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv. Wenn Sie die Funktion aktivieren, werden alle Passwörter und Schlüssel in allen Menüs als Klartext angezeigt und können in Klartext bearbeitet werden. Eine Ausnahme bilden die IPSec-Schlüssel. Diese können nur im Klartext eingegeben werden. Nach Anklicken von **OK** oder erneutem Aufruf des Menüs werden sie als Sternchen angezeigt.

6.1.1.3 Datum und Uhrzeit

Die Systemzeit benötigen Sie u. a. für korrekte Zeitstempel bei Systemmeldungen oder Gebührenerfassung.

Für die Ermittlung der Systemzeit (lokale Zeit) haben Sie folgende Möglichkeiten:

Manuell

Die Umschaltung der Uhrzeit von Sommer- auf Winterzeit (und zurück) erfolgt automatisch. Die Umschaltung erfolgt unabhängig von der Zeit der Vermittlungsstelle oder von einem ntp-Server. Die Sommerzeit beginnt am letzten Sonntag im März durch die Umschaltung von 2 Uhr auf 3 Uhr. Die in der fehlenden Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt. Die Winterzeit beginnt am letzten Sonntag im Oktober durch die Umschaltung von 3 Uhr auf 2 Uhr. Die in der zusätzlichen Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt.

Zeitserver

Sie können die Systemzeit auch automatisch über verschiedene Zeitserver beziehen. Um sicherzustellen, dass das Gerät die gewünschte aktuelle Zeit verwendet, sollten Sie einen oder mehrere Zeitserver konfigurieren.

Hinweis

Wenn auf dem Gerät eine Methode zum automatischen Beziehen der Zeit festgelegt ist, haben die auf diese Weise erhaltenen Werte die höhere Priorität. Eine evtl. manuell eingegebene Systemzeit wird überschrieben.

Das Menü **Systemverwaltung**->**Globale Einstellungen**->**Datum und Uhrzeit** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Zeitzone	Wählen Sie die Zeitzone aus, in der Ihr Gerät installiert ist. Möglich ist die Auswahl der Universal Time Coordinated (UTC) plus oder minus der Abweichung davon in Stunden oder ein vordefinierter Ort. Der Standardwert ist *Europe/Berlin*.
Aktuelle Ortszeit	Hier werden das aktuelle Datum und die aktuelle Systemzeit angezeigt. Der Eintrag kann nicht verändert werden.

Felder im Menü Manuelle Zeiteinstellung

Feld	Beschreibung
Datum einstellen	Wenn Sie auf das Eingabefeld für das Datum klicken, öffnet sich ein Standardkalender in Monatsansicht. Ein Klick auf das gewünschte Datum überträgt es in die Konfigurationsoberfläche.
Zeit einstellen	Geben Sie eine neue Uhrzeit ein. Format: • **Stunde**: hh • **Minute**: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	Nur für Geräte mit ISDN-Schnittstelle. Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll. Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeitserver empfangen wurde. Für den Zeitraum, in dem die Zeit über einen Zeitserver ermittelt wird, wird die Aktualisierung über ISDN außer Kraft gesetzt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Erster Zeitserver	Geben Sie den ersten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37.

Feld	Beschreibung
	• *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zweiter Zeitserver	Geben Sie den zweiten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Dritter Zeitserver	Geben Sie den dritten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird. Der Standardwert ist *1440*.
Zeitaktualisierungsrichtlinie	Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen. Mögliche Werte: • *Normal* (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • *Aggressiv*: Zehn Minuten lang wird versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • *Endlos*: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. Bei der Verwendung von Zertifikaten für die Verschlüsselung des Datenverkehrs in einem VPN ist es von zentraler Bedeutung, dass auf dem Gerät die korrekte Zeit eingestellt ist. Um dies sicherzustellen, wählen Sie für **Zeitaktualisierungsrichtlinie** den Wert *Endlos*.

Feld	Beschreibung
System als Zeitserver	Wählen Sie aus, ob der interne Zeitserver verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Zeitanfragen eines Clients werden mit der aktuellen Systemzeit beantwortet. Diese wird als GMT ohne Offset angegeben. Standardmäßig ist die Funktion aktiv. Zeitanfragen der Clients im LAN werden beantwortet.

6.1.1.4 Systemlizenzen

In diesem Kapitel werden die im Auslieferungsstand aktivierten Software-Lizenzen angezeigt.

Die Optionen zum Bearbeiten, Neueintragen und Wiederherstellen werden in der Regel nicht benötigt.

Mögliche Werte für Status

Lizenz	Bedeutung
OK	Subsystem ist freigeschaltet.
Nicht OK	Subsystem ist nicht freigeschaltet.
Nicht unterstützt	Sie haben eine Lizenz für ein Subsystem angegeben, das Ihr System nicht unterstützt.

Außerdem wird die **Systemlizenz-ID** oberhalb der Liste angezeigt.

Hinweis

Um die Standardlizenzen eines Geräts wiederherzustellen, klicken Sie auf die Schaltfläche **Standardlizenzen**.

6.1.1.4.1 Bearbeiten oder Neu

Wähle Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Lizenzen einzutragen.

Das Menü **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Wert
Lizenzseriennummer	Geben Sie die Lizenzseriennummer ein, die Sie beim Kauf der Lizenz erhalten haben.
Lizenzschlüssel	Geben Sie den Lizenzschlüssel ein, den Sie per E-Mail erhalten haben.

Hinweis

Wenn als Status *Nicht OK* angezeigt wird:

- Geben Sie die Lizenzdaten erneut ein.
- Überprüfen Sie gegebenenfalls Ihre Hardware-Seriennummer.

Wenn der Lizenzstatus *Nicht unterstützt* angezeigt wird, haben Sie eine Lizenz für ein Subsystem angegeben, das Ihr Gerät nicht unterstützt. Sie werden die Funktionen dieser Lizenz nicht nutzen können.

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

(1) Gehen Sie zu **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**.

(2) Betätigen Sie das -Symbol in der Zeile, in der die zu löschende Lizenz steht.

(3) Bestätigen Sie mit **OK**.

Die Lizenz ist ausgeschaltet. Sie können Ihre Zusatzlizenz jederzeit durch Eingabe des gültigen Lizenzschlüssels und der Lizenzseriennummer wieder aktivieren.

6.1.2 Schnittstellenmodus / Bridge-Gruppen

In diesem Menü legen Sie den Betriebsmodus der Schnittstellen Ihres Geräts fest.

Routing versus Bridging

Mit Bridging werden gleichartige Netze verbunden. Im Gegensatz zu Routern arbeiten Bridges auf Schicht 2 (Sicherungsschicht) des OSI-Modells, sind von höheren Protokollen unabhängig und übertragen Datenpakete anhand von MAC-Adressen. Die Datenübertragung ist transparent, d. h. die Informationen der Datenpakete werden nicht interpretiert.

Mit Routing werden unterschiedliche Netze auf Schicht 3 (Netzwerkschicht) des OSI-Modells verbunden und Informationen von einem Netz in das andere weitergeleitet (routen).

Konventionen für die Port-/Schnittstellennamen

Verfügt Ihr Gerät über einen Funk-Port, erhält dieser den Schnittstellennamen WLAN. Sind mehrere Funkmodule vorhanden, setzen sich die Namen der Funk-Ports in der Benutzeroberfläche Ihres Geräts aus den folgenden Bestandteilen zusammen:

(a) WLAN

(b) Nummer des physischen Ports (1 oder 2)

Beispiel: *WLAN1*

Der Name des Ethernet-Ports setzt sich aus den folgenden Bestandteilen zusammen:

(a) ETH

(b) Nummer des Ports

Beispiel: *ETH1*

Der Name der Schnittstelle, die an einen Ethernet-Port gebunden ist, setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp, dabei steht *en* für Ethernet

(b) Nummer des Ethernet-Ports

(c) Nummer der Schnittstelle

Beispiel: *en1-0* (erste Schnittstelle am ersten Ethernet-Port)

Der Name der Bridge-Gruppe setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp, dabei steht *br* für Bridge-Gruppe

(b) Nummer der Bridge-Gruppe

Beispiel: *br0* (erste Bridge-Gruppe)

Der Name des Drahtlosnetzwerks (VSS) setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp, dabei steht *vss* für Drahtlosnetzwerk

(b) Nummer des Funkmoduls

(c) Nummer der Schnittstelle

Beispiel: *vss1-0* (erstes Drahtlosnetzwerk auf dem ersten Funkmodul)

Der Name der virtuellen Schnittstelle, die an einen Ethernet-Port gebunden ist, setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Ethernet-Ports

(c) Nummer der Schnittstelle, die an den Ethernet-Port gebunden ist

(d) Nummer der virtuellen Schnittstelle

Beispiel: *en1-0-1* (erste virtuelle Schnittstelle basierend auf der ersten Schnittstelle am ersten Ethernet-Port)

6.1.2.1 Schnittstellen

Sie definieren für jede Schnittstelle separat, ob diese im Routing- oder im Bridging-Modus arbeiten soll.

Wenn Sie den Bridging-Modus setzen wollen, können Sie zwischen bestehenden Bridge-Gruppen und dem Erstellen einer neuen Bridge-Gruppe wählen.

Das Menü **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschreibung	Zeigt den Namen der Schnittstelle an.
Modus / Bridge-Gruppe	Wählen Sie aus, ob Sie die Schnittstelle im *Routing-Modus* betreiben möchten oder ordnen Sie die Schnittstelle einer bestehenden (*br0*, *br1* usw.) oder neuen Bridge-Gruppe (*Neue Bridge-Gruppe*) zu. Bei Auswahl von *Neue Bridge-Gruppe* wird nach Anklicken des **OK**-Buttons automatisch eine neue Bridge-Gruppe erzeugt.
Konfigurationsschnittstelle	Wählen Sie aus, über welche Schnittstelle die Konfiguration durchgeführt wird. Mögliche Werte: • *Eine auswählen* (Standardwert): Einstellung im Auslieferungszustand. Die richtige Konfigurationsschnittstelle muss aus den anderen Optionen ausgewählt werden. • *Nicht beachten*: Keine Schnittstelle wird als Konfigurationsschnittstelle definiert. • *<Schnittstellenname>*: Legen Sie die Schnittstelle fest, die zur Konfiguration benutzt wird. Wenn diese Schnittstelle Mitglied einer Bridge-Gruppe ist, übernimmt sie deren IP-Adresse, wenn sie aus der Bridge-Gruppe herausgenommen wird.

6.1.2.1.1 Hinzufügen

Wählen Sie die **Hinzufügen**-Schaltfläche um den Modus von PPP-Schnittstellen zu bearbeiten.

Das Menü **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**->**Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, deren Modus Sie verändern wollen.

6.1.3 Administrativer Zugriff

In diesem Menü können Sie den administrativen Zugang zum Gerät konfigurieren.

6.1.3.1 Zugriff

Im Menü **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff** wird eine Liste aller IP-fähigen Schnittstellen angezeigt.

Für eine Ethernet-Schnittstelle sind die Zugangsparameter *HTTP*, *HTTPS*, *Ping* und für die ISDN-Schnittstellen *ISDN-Login* auswählbar.

Weiterhin können Sie Ihr Gerät für Wartungsarbeiten durch den Telekom-Kundenservice freischalten. Hierzu aktivieren Sie je nach angeforderter Service-Leistung die Option **Service Call Ticket (SSH Web-Access)** oder **Automatische Konfiguration (TR-069)** und wählen die Schaltfläche **OK**. Folgen Sie den Anweisungen des Telekom-Kundenservice!

Service Call Ticket (SSH Web-Access) ist standardmäßig nicht aktiv, **Automatische Konfiguration (TR-069)** ist standardmäßig aktiv.

6.1.3.1.1 Hinzufügen

Das Menü **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff**->**Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Zugriff

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die der administrative Zugriff konfiguriert werden soll.

6.1.4 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

6.1.4.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) ist ein Dienst, der es ermöglicht, Authentifizierungs- und Konfigurationsinformationen zwischen Ihrem Gerät und einem RADIUS-Server auszutauschen. Der RADIUS-Server verwaltet eine Datenbank mit Informationen zur Benutzerauthentifizierung, zur Konfiguration und für die statistische Erfassung von Verbindungsdaten.

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

Bei einer eingehenden Verbindung sendet Ihr Gerät eine Anforderung mit Benutzername und Passwort an den RADIUS-Server, woraufhin dieser seine Datenbank abfragt. Wenn der Benutzer gefunden wurde und authentifiziert werden kann, sendet der RADIUS-Server eine entsprechende Bestätigung zu Ihrem Gerät. Diese Bestätigung enthält auch Parameter (sog. RADIUS-Attribute), die Ihr Gerät als WAN-Verbindungsparameter verwendet.

Wenn der RADIUS-Server für Gebührenerfassung verwendet wird, sendet Ihr Gerät eine Accounting-Meldung am Anfang der Verbindung und eine Meldung am Ende der Verbindung. Diese Anfangs- und Endmeldungen enthalten zudem statistische Informationen zur Verbindung (IP-Adresse, Benutzername, Durchsatz, Kosten).

RADIUS Pakete

Folgende Pakettypen werden zwischen RADIUS-Server und Ihrem Gerät (Client) versendet:

Pakettypen

Feld	Wert
ACCESS_REQUEST	Client -> Server Wenn ein Verbindungs-Request auf Ihrem Gerät empfangen wird, wird beim RADIUS-Server angefragt, falls in Ihrem Gerät kein entsprechender Verbindungspartner gefunden wurde.
ACCESS_ACCEPT	Server -> Client Wenn der RADIUS-Server die im ACCESS_REQUEST enthaltenen Informationen authentifiziert hat, sendet er ein ACCESS_ACCEPT zu Ihrem Gerät mit den für den Verbindungsaufbau zu verwendenden Parametern.
ACCESS_REJECT	Server -> Client Wenn die im ACCESS_REQUEST enthaltenen Informationen nicht den Informationen in der Benutzerdatenbank des RADIUS-Servers entsprechen, sendet er ein ACCESS_REJECT zur Ablehnung der Verbindung.
ACCOUNTING_START	Client -> Server Wenn ein RADIUS-Server für Gebührenerfassung verwendet wird, sendet Ihr Gerät eine Accounting- Meldung am Anfang jeder Verbindung zum RADIUS-Server.
ACCOUNTING_STOP	Client -> Server Wenn ein RADIUS-Server für Gebührenerfassung verwendet wird, sendet Ihr Gerät eine Accounting- Meldung am Ende jeder Verbindung zum RADIUS-Server.

Im Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS** wird eine Liste aller eingetragenen RADIUS-Server angezeigt.

6.1.4.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere RADIUS-Server einzutragen.

Das Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Wert
Authentifizierungstyp	Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll. Mögliche Werte: • *PPP-Authentifizierung* (Standardwert, nur für PPP-Verbindungen): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. • *Accounting* (nur für PPP-Verbindungen): Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet. • *Login-Authentifizierung*: Der RADIUS-Server wird verwendet, um den Zugang zu Ihrem Gerät zu kontrollieren. • *IPSec-Authentifizierung*: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln.

Feld	Wert
	• *WLAN (802.1x)*: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln. • *XAUTH*: Der RADIUS-Server wird verwendet, um IPSec-Peers über XAuth zu authentisieren.
Betreibermodus	Nur für **Authentifizierungstyp** = *Accounting* In Standardanwendungen belassen Sie den Wert bei *Standard*. Mögliche Werte: • *France Telecom*: Für Anwendungen der France Telecom
Server-IP-Adresse	Geben Sie die IP-Adresse des RADIUS-Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
Standard-Benutzerpasswort	Einige RADIUS-Server benötigen für jede RADIUS-Anfrage ein Benutzerpasswort. Geben Sie daher das Passwort hier ein, das Ihr Gerät als Standard-Benutzerpasswort in der Anfrage für die Dialout-Routen an den RADIUS-Server mitsendet.
Priorität	Wenn mehrere RADIUS-Server-Einträge angelegt wurden, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächstniedrigeren Priorität verwendet usw. Mögliche Werte von *0* (höchste Priorität) bis *7* (niedrigste Priorität). Der Standardwert ist *0*. Siehe auch **Richtlinie** unter **Server-Optionen**.
Eintrag aktiv	Wählen Sie aus, ob der in diesem Eintrag konfigurierte RADIUS-Server verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Gruppenbeschreibung	Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der **Priorität** und der **Richtlinie** abgefragt. Mögliche Werte: • *Neu* (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein. • *Standardgruppe 0*: Wählen Sie diesen Eintrag für spezielle Anwendungen aus. • *<Gruppenname>*: Wählen Sie aus der Liste eine schon definierte Gruppe aus.

Das Menü **Server-Optionen** besteht aus folgenden Feldern:

Felder im Menü Server-Optionen

Feld	Wert
Richtlinie	Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.

Feld	Wert
	Mögliche Werte: • *Verbindlich* (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • *Nicht verbindlich*: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.
UDP-Port	Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein. Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älterne RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist. Der Standardwert ist *1812*.
Server Timeout	Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein. Nach Ablauf dieser Zeit wird die Anfrage gemäß **Wiederholungen** wiederholt bzw. der nächste konfigurierte RADIUS-Server angefragt. Mögliche Werte sind ganze Zahlen zwischen *50* und *50000*. Der Standardwert ist *1000* (1 Sekunde).
Erreichbarkeitsprüfung	Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im **Status** *Inaktiv*. Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check durchgeführt, in dem ein ACCESS_REQUEST an die IP-Adresse des RADIUS-Servers gesendet wird. Bei erneuter Erreichbarkeit wird der **Status** wieder auf *aktiv* gesetzt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Wiederholungen	Geben Sie die Anzahl der Wiederholungen für den Fall ein, dass eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der **Status** auf *inaktiv* gesetzt. Bei **Erreichbarkeitsprüfung** = *Aktiviert* versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird **Status** wieder auf *aktiv* zurückgesetzt. Mögliche Werte sind ganze Zahlen zwischen *0* und *10*. Der Standardwert ist *1*. Um zu verhindern, dass **Status** auf *inaktiv* gesetzt wird, setzen Sie diesen Wert auf *0*.
RADIUS-Dialout	Nur für **Authentifizierungstyp** = *PPP-Authentifizierung* und *IP-Sec-Authentifizierung*. Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
	Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben: • *Neulade-Intervall*: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. Standardmäßig ist hier *0* eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.

6.1.4.2 Optionen

Aufgrund der hier möglichen Einstellung führt Ihr Gerät bei eingehenden Rufen eine Authentifizierungsverhandlung aus, wenn es die Calling Party Number nicht identifiziert (z. B. weil die Gegenstelle keine Calling Party Number signalisiert). Wenn die mit Hilfe des ausgeführten Authentifizierungsprotokolls erhaltenen Daten (Passwort, Partner PPP ID) mit den Daten einer eingetragenen Gegenstelle oder eines RADIUS-Benutzers übereinstimmen, akzeptiert Ihr Gerät den ankommenden Ruf.

Das Menü **Systemverwaltung**->**Remote Authentifizierung**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale RADIUS-Optionen

Feld	Beschreibung
Authentifizierung für PPP-Einwahl	Standardmäßig wird folgende Reihenfolge bei der Authentisierung für eingehende Verbindungen unter Berücksichtigung von RADIUS angewendet: zunächst CLID, danach PPP und daraufhin PPP mit RADIUS. Optionen: • *Inband*: Nur Inband-RADIUS-Anfragen (PAP, CHAP, MS-CHAP V1 & V2) (d. h. PPP-Anfragen ohne Rufnummernidentifizierung) werden zum in **Server-IP-Adresse** definierten RADIUS-Server geschickt. • *Outband (CLID)*: Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummernidentifizierung) werden zum RADIUS-Server geschickt (CLID = Calling Line Identification). Standardmäßig ist *Inband* aktiviert, *Outband (CLID)* deaktiviert.

6.1.5 Konfigurationszugriff

Im Menü **Konfigurationszugriff** können Sie Benutzerprofile konfigurieren.

Sie legen dazu Zugriffsprofile und Benutzer an und weisen jedem Benutzer mindestens ein Zugriffsprofil zu. Ein Zugriffsprofil stellt denjenigen Teil des GUI zur Verfügung, den ein Benutzer für seine Aufgaben benötigt. Nicht benötigte Teile des GUI sind gesperrt.

6.1.5.1 Zugriffsprofile

Im Menü **Systemverwaltung**->**Konfigurationszugriff**->**Zugriffsprofile** wird eine Liste aller konfigurierten Zugriffsprofile angezeigt. Vorhandene Einträge können Sie mithilfe des Symbols löschen.

Für Telefonanlagen sind standardmäßig einige Zugriffsprofile bereits angelegt. Diese können Sie mithilfe des Symbols ändern sowie über das Symbol auf die Standardeinstellungen zurücksetzen.

6.1.5.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Zugriffsprofile anzulegen.

Um ein Zugriffsprofil zu erzeugen, können Sie alle Einträge in der Navigationsleiste des GUI sowie **Konfiguration speichern** verwenden. Sie können maximal 29 Zugriffsprofile anlegen.

Das Menü **Systemverwaltung**->**Konfigurationszugriff**->**Zugriffsprofile**->**Neu** besteht aus folgenden

Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine eindeutige Bezeichnung für das Zugriffsprofil ein.
Level Nr.	Das System vergibt automatisch eine laufende Nummer an das Zugriffsprofil. Diese kann nicht editiert werden.

Felder im Menü Schaltflächen

Feld	Beschreibung
Konfiguration speichern	Wenn Sie die Schaltfläche **Konfiguration speichern** aktivieren, darf der Benutzer Konfigurationen speichern. **Hinweis** Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können. Aktivieren oder deaktivieren Sie **Konfiguration speichern**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Navigationseinträge

Feld	Beschreibung
Menüs	Sie sehen alle Menüs aus der Navigationsleiste des GUI. Menüs, die mindestens ein Untermenü enthalten, sind mit bzw. gekennzeichnet. Das Symbol kennzeichnet Seiten. Wenn Sie ein neues Zugriffsprofil anlegen, sind noch keine Elemente zugewiesen, d.h. alle verfügbaren Menüs, Untermenüs und Seiten sind mit dem Symbol gekennzeichnet. Jedes Element in der Navigationsleiste kann drei Werte annehmen. Klicken Sie in der gewünschten Zeile auf das Symbol , um diese drei Werte anzeigen zu lassen. Mögliche Werte: • *Verweigern*: Das Menü und alle untergeordneten Menüs sind gesperrt. • *Zulassen*: Das Menü ist freigegeben. Untergeordenete Menüs müssen gegebenenfalls gesondert freigegeben werden. • *Alle zulassen*: Das Menü und alle untergeordneten Menüs sind freigegeben. Sie können in der entsprechenden Zeile *Zulassen* bzw. *Alle zulassen* wählen, um dem aktuellen Zugriffsprofil Elemente zuzuweisen. Elemente, die dem aktuellen Zugriffsprofil zugewiesen sind, sind mit dem Symbol gekennzeichnet. kennzeichnet ein Menü, das gesperrt ist, das aber mindestens über ein freigegebenes Untermenü verfügt.

6.1.5.2 Benutzer

Im Menü **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer** wird eine Liste aller konfigurierten Benutzer angezeigt. Die vorhandenen Einträge können Sie mithilfe des Symbols löschen.

Durch Klicken auf die Schaltfläche werden die Details zum konfigurierten Benutzer angezeigt. Sie sehen, welche Felder und welche Menüs dem Benutzer zugewiesen sind.

Das Symbol bedeutet, dass **Nur lesen** erlaubt ist. Ist eine Zeile mit dem Symbol kennzeichnet, so sind die Informationen zum Lesen und Schreiben freigegeben. Das Symbol kennzeichnet gesperrte Einträge.

6.1.5.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Benutzer einzutragen.

Das Menü **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Benutzer	Geben Sie eine eindeutige Bezeichnung für den Benutzer ein.
Passwort	Geben Sie ein Passwort für den Benutzer ein.
Benutzer muss das Passwort ändern	Mit der Option **Benutzer muss das Passwort ändern** kann der Administrator bestimmen, dass der Benutzer beim ersten Login ein eigenes Passwort vergeben muss. Dazu muss die Option **Konfiguration speichern** im Menü **Zugriffsprofile** aktiv sein. Ist diese Option nicht aktiv, so wird ein Warnhinweis angezeigt. Aktivieren oder deaktivieren Sie **Benutzer muss das Passwort ändern**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zugangs-Level	Mit **Hinzufügen** weisen Sie dem Benutzer mindestens ein Zugriffsprofil zu. Mit der Auswahl von **Nur lesen** wird festgelegt, dass der Benutzer die Parameter des Zugriffsprofils ansehen, aber nicht ändern kann. Werden einem Benutzer sich überschneidende Zugriffsprofile zugeordnet, so hat Lesen und Schreiben eine höhere Priorität als **Nur lesen**. Schaltflächen können nicht auf die Einstellung **Nur lesen** gesetzt werden.

6.1.6 Zertifikate

Ein asymmetrisches Kryptosystem dient dazu, Daten, die in einem Netzwerk transportiert werden sollen, zu verschlüsseln, digitale Signaturen zu erzeugen oder zu prüfen und Benutzer zu authentifizieren oder zu authentisieren. Zur Ver- und Entschlüsselung der Daten wird ein Schlüsselpaar verwendet, das aus einem öffentlichen und einem privaten Schlüssel besteht.

Für die Verschlüsselung benötigt der Sender den öffentlichen Schlüssel des Empfängers. Der Empfänger entschlüsselt die Daten mit seinem privaten Schlüssel. Um sicherzustellen, dass der öffentliche Schlüssel der echte Schlüssel des Empfängers und keine Fälschung ist, wird ein Nachweis, ein sogenanntes digitales Zertifikat benötigt.

Ein digitales Zertifikat bestätigt u. a. die Echtheit und den Eigentümer eines öffentlichen Schlüssels. Es ist vergleichbar mit einem amtlichen Ausweis, in dem bestätigt wird, dass der Eigentümer des Ausweises bestimmte Merkmale aufweist, wie z. B. das angegebene Geschlecht und Alter, und dass die Unter-

schrift auf dem Ausweis echt ist. Da es für Zertifikate nicht nur eine einzige Ausgabestelle gibt, wie z. B. das Passamt für einen Ausweis, sondern Zertifikate von vielen verschiedenen Stellen und in unterschiedlicher Qualität ausgegeben werden, kommt der Vertrauenswürdigkeit der Ausgabestelle eine zentrale Bedeutung zu. Die Qualität eines Zertifikats regelt das deutsche Signaturgesetz bzw. die entsprechende EU-Richtlinie.

Die Zertifizierungsstellen, die sogenannte qualifizierte Zertifikate ausstellen, sind hierarchisch organisiert mit der Bundesnetzagentur als oberster Zertifizierungsinstanz. Struktur und Inhalt eines Zertifikats werden durch den verwendeten Standard vorgegeben. X.509 ist der wichtigste und am weitesten verbreitete Standard für digitale Zertifikate. Qualifizierte Zertifikate sind personenbezogen und besonders vertrauenswürdig.

Digitale Zertifikate sind Teil einer sogenannten Public Key Infrastruktur (PKI). Als PKI bezeichnet man ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

Zertifikate werden für einen bestimmten Zeitraum, meist ein Jahr, ausgestellt, d.h. ihre Gültigkeitsdauer ist begrenzt.

Ihr Gerät ist für die Verwendung von Zertifikaten für VPN-Verbindungen und für Sprachverbindungen über Voice over IP ausgestattet.

6.1.6.1 Zertifikatsliste

Im Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** wird eine Liste aller vorhandenen Zertifikate angezeigt.

6.1.6.1.1 Bearbeiten

Klicken Sie auf das -Symbol, um den Inhalt des gewählten Objekts (Schlüssel, Zertifikat oder Anforderung) einzusehen.

Die Zertifikate und Schlüssel an sich können nicht verändert werden, jedoch können - je nach Typ des gewählten Eintrags - einige externe Attribute verändert werden.

Das Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**-> besteht aus folgenden Feldern:

Felder im Menü Parameter bearbeiten

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
Zertifikat ist ein CA-Zertifikat	Markieren Sie das Zertifikat als Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA). Zertifikate, die von dieser CA ausgestellt wurden, werden bei der Authentifizierung akzeptiert. Mit *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Überprüfung anhand einer Zertifikatsperrliste (CRL)	Nur für **Zertifikat ist ein CA-Zertifikat** = *Wahr* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Einstellungen: • *Deaktiviert*: keine Überprüfung von CRLs. • *Immer*: CRLs werden grundsätzlich überprüft. • *Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist* (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im

Feld	Beschreibung
	Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • *Einstellungen des übergeordneten Zertifikates benutzen*: Es werden die Einstellungen des übergeordneten Zertifikates verwendet, falls eines vorhanden ist. Falls nicht, wird genauso verfahren, wie unter "Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist" beschrieben.
Vertrauenswürdigkeit des Zertifikats erzwingen	Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll. Mit *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Achtung

Es ist von zentraler Wichtigkeit für die Sicherheit eines VPN, dass die Integrität aller manuell als vertrauenswürdig markierten Zertifikate (Zertifizierungsstellen- und Benutzerzertifikate), sichergestellt ist. Die angezeigten "Fingerprints" können zur Überprüfung dieser Integrität herangezogen werden: Vergleichen Sie die angezeigten Werte mit den Fingerprints, die der Aussteller des Zertifikats (z. B. im Internet) angegeben hat. Dabei reicht die Überprüfung eines der beiden Werte aus.

6.1.6.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

Bei der Verwendung von SCEP (Simple Certificate Enrollment Protocol) unterstützt Ihr Gerät auch separate Registration-Authority-Zertifikate.

Registration-Authority-Zertifikate werden von manchen Certificate Authorities (CAs) verwendet, um bestimmte Aufgaben (Signatur und Verschlüsselung) bei der SCEP Kommunikation mit separaten Schlüsseln abzuwickeln, und den Vorgang ggf. an separate Registration Authorities zu delegieren.

Beim automatischen Download eines Zertifikats, also wenn **CA-Zertifikat** = *-- Download --* ausgewählt ist, werden alle für den Vorgang notwendigen Zertifikate automatisch geladen.

Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, können diese auch manuell ausgewählt werden.

Wählen Sie die Schaltfläche **Zertifikatsanforderung**, um weitere Zertifikate zu beantragen oder zu importieren.

Das Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->**Zertifikatsanforderung** besteht aus folgenden Feldern:

Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
Zertifikatsanforderungsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Modus	Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen. Zur Verfügung stehen: • *Manuell* (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PKCS#10-Datei, die direkt im Browser hochgeladen oder im -Menü über das Feld **Details anzeigen** kopiert werden kann. Diese Datei muss der CA zugestellt und das erhaltene Zertifikat anschließend manuell auf Ihr Gerät importiert werden.

Feld	Beschreibung
	• *SCEP*: Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt.
Privaten Schlüssel generieren	Nur für **Modus** = *Manuell* Wählen Sie einen Algorithmus für die Schlüsselerstellung aus. Zur Verfügung stehen *RSA* (Standardwert) und *DSA*. Wählen Sie weiterhin die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Beachten Sie, dass ein Schlüssel mit der Länge 512 Bit als unsicher eingestuft werden könnte, während ein Schlüssel mit 4096 Bit nicht nur viel Zeit zur Erzeugung erfordert, sondern während der IPSec-Verarbeitung einen wesentlichen Teil der Ressourcen belegt. Ein Wert von 768 oder mehr wird jedoch empfohlen, als Standardwert ist 1024 Bit vorgegeben.
SCEP-URL	Nur für **Modus** = *SCEP* Geben Sie die URL des SCEP-Servers ein, z. B. http://scep.beispiel.com:8080/scep/scep.dll Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
CA-Zertifikat	Nur für **Modus** = *SCEP* Wählen Sie das CA-Zertifikat aus. • *-- Download --*: Geben Sie in **CA-Name** den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows*. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator. Falls keine CA-Zertifikate zur Verfügung stehen, wird Ihr Gerät zuerst das CA-Zertifikat der betroffenen CA herunterladen. Es fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü **Zertifikatsanforderung generieren** zurück. Falls das CA-Zertifikat keine CRL-Verteilstelle (Certificate Revocation List, CRL) enthält und auf Ihrem Gerät kein Zertifikatsserver konfiguriert ist, werden Zertifikate von dieser CA nicht auf ihre Gültigkeit überprüft. • <Name eines vorhandenen Zertifikats>: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.
RA-Signierungszertifikat	Nur für **Modus** = *SCEP* Nur für **CA-Zertifikat** nicht = *-- Download --* Wählen Sie ein Zertifikat für die Signierung der SCEP-Kommunikation aus. Der Standardwert ist *-- CA-Zertifikat verwenden --*, d. h. es wird das CA-Zertifikat verwendet.
RA-Verschlüsselungszertifikat	Nur für **Modus** = *SCEP* Nur wenn **RA-Signierungszertifikat** nicht = *-- CA-Zertifikat verwenden --*

Feld	Beschreibung
	Wenn Sie ein eigenes Zertifikat zur Signierung der Kommunikation mit der RA verwenden, haben Sie hier die Möglichkeit, ein weiteres zur Verschlüsselung der Kommunikation auszuwählen. Der Standardwert ist *-- RA-Signierungszertifikat verwenden --*, d. h. es wird dasselbe Zertifikat wie zur Signierung verwendet.
Passwort	Nur für **Modus** = *SCEP* Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.

Felder im Menü Subjektname

Feld	Beschreibung
Benutzerdefiniert	Wählen Sie aus, ob Sie die Namenskomponenten des Subjektnamens einzeln laut Vorgabe durch die CA oder einen speziellen Subjektnamen eingeben wollen. Wenn *Aktiviert* ausgewählt ist, kann in **Zusammenfassend** ein Subjektname mit Attributen, die nicht in der Auflistung angeboten werden, angegeben werden. Beispiel: "CN=VPNServer, DC=mydomain, DC=com, c=DE". Ist das Feld nicht markiert, geben Sie die Namenskomponenten in **Allgemeiner Name**, **E-Mail**, **Organisationseinheit**, **Organisation**, **Ort**, **Staat/Provinz** und **Land** ein. Standardmäßig ist die Funktion nicht aktiv.
Zusammenfassend	Nur für **Benutzerdefiniert** = aktiviert. Geben Sie einen Subjektnamen mit Attributen ein, die nicht in der Auflistung angeboten werden. Beispiel: "CN=VPNServer, DC=mydomain, DC=com, c=DE".
Allgemeiner Name	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie den Namen laut CA ein.
E-Mail	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie die E-Mail-Adresse laut CA ein.
Organisationseinheit	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie die Organisationseinheit laut CA ein.
Organisation	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie die Organisation laut CA ein.
Ort	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie den Standort laut CA ein.
Staat/Provinz	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie den Staat/das Bundesland laut CA ein.
Land	Nur für **Benutzerdefiniert** = deaktiviert.

Feld	Beschreibung
	Geben Sie das Land laut CA ein.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Subjekt-Alternativnamen

Feld	Beschreibung
#1, **#2**, **#3**	Definieren Sie zu jedem Eintrag den Typ des Namens und geben Sie zusätzliche Subjektnamen ein. Mögliche Werte: • *Keiner* (Standardwert): Es wird kein zusätzlicher Name eingegeben. • *IP*: Es wird eine IP-Adresse eingetragen. • *DNS*: Es wird ein DNS-Name eingetragen. • *E-Mail*: Es wird eine E-Mail-Adresse eingetragen. • *URI*: Es wird ein Uniform Resource Identifier eingetragen. • *DN*: Es wird ein Distinguished Name (DN) eingetragen. • *RID*: Es wird eine Registered Identity (RID) eingetragen.

Feld im Menü Optionen

Feld	Beschreibung
Autospeichermodus	Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

6.1.6.1.3 Importieren

Wählen Sie die Schaltfläche **Importieren**, um Zertifikate zu importieren.

Das Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->**Importieren** besteht aus folgenden Feldern:

Felder im Menü Importieren

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen des Zertifikats ein, welches importiert werden soll oder wählen Sie die Datei mit **Datei auswählen** über den Dateibrowser aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann. Mögliche Werte: • *Auto* (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung.

Feld	Beschreibung
	• *Base64* • *Binär*
Passwort	Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort. Tragen Sie das Passwort hier ein.

6.1.6.2 CRLs

Im Menü **Systemverwaltung**->**Zertifikate**->**CRLs** wird eine Liste aller CRLs (Certificate Revocation List) angezeigt.

Wenn ein Schlüssel nicht mehr verwendet werden darf, z. B. weil er in falsche Hände geraten oder verloren gegangen ist, wird das zugehörige Zertifikat für ungültig erklärt. Die Zertifizierungsstelle widerruft das Zertifikat, sie gibt Zertifikatsperrlisten, sogenannte CRLs, heraus. Nutzer von Zertifikaten sollten durch einen Abgleich mit diesen Listen stets prüfen, ob das verwendete Zertifikat aktuell gültig ist. Dieser Prüfvorgang kann über einen Browser automatisiert werden.

Das Simple Certificate Enrollment Protocol (SCEP) unterstützt die Ausgabe und den Widerruf von Zertifikaten in Netzwerken.

6.1.6.2.1 Importieren

Wählen Sie die Schaltfläche **Importieren**, um CRLs zu importieren.

Das Menü **Systemverwaltung**->**Zertifikate**->**CRLs**->**Importieren** besteht aus folgenden Feldern:

Felder im Menü CRL-Import

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen der CRL ein, welche importiert werden soll oder wählen Sie die Datei mit **Datei auswählen** über den Dateibrowser aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für die CRL ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät die CRL decodieren kann. Mögliche Werte: • *Auto* (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der CRL-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • *Base64* • *Binär*
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

6.1.6.3 Zertifikatsserver

Im Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsserver** wird eine Liste aller Zertifikatsserver angezeigt.

Eine Zertifizierungsstelle (Zertifizierungsdiensteanbieter, Certificate Authority, CA) stellt ihre Zertifikate den Clients, die ein Zertifikat beantragen, über einen Zertifikatsserver zur Verfügung. Der Zertifikatsserver stellt auch die privaten Schlüssel aus und hält Zertifikatsperrlisten (CRL) bereit, die zur Prüfung von Zertifikaten entweder per LDAP oder HTTP vom Gerät abgefragt werden.

6.1.6.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um einen Zertifikatsserver einzurichten.

Das Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsserver**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den Zertifikatsserver ein.
LDAP-URL-Pfad	Geben Sie die LDAP-URL oder die HTTP-URL des Servers ein.

6.2 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

6.2.1 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (beispielsweise Aktivierung bzw. Deaktivierung von Schnittstellen) durchgeführt werden können. Außerdem ist jede vorhandene MIB-Variable mit jedem beliebigen Wert konfigurierbar.

Sie legen die gewünschten **Aktionen** fest und definieren die **Auslöser**, die steuern, wann bzw. unter welchen Bedingungen die **Aktionen** durchgeführt werden sollen. Ein **Auslöser** kann ein einzelnes Ereignis sein oder eine Folge von Ereignissen, die in einer **Ereignisliste** zusammengefasst sind. Für ein einzelnes Ereignis legen Sie ebenfalls eine **Ereignisliste** an, die jedoch nur ein Element enthält.

Es ist möglich, zeitgesteuert Aktionen auszulösen. Außerdem kann der Status oder die Erreichbarkeit von Schnittstellen oder deren Datenverkehr zur Ausführung der konfigurierten Aktionen führen, oder aber auch die Gültigkeit von Lizenzen. Auch hier ist es möglich, jede beliebige MIB-Variable mit jedem beliebigen Wert als Auslöser einzurichten.

Um den Aufgabenplaner in Betrieb zu nehmen, aktivieren Sie das **Schedule-Intervall** unter **Optionen**. Dieses Intervall gibt den Zeitabstand vor, in dem das System prüft, ob mindestens ein Ereignis eingetreten ist. Dieses Ereignis dient als Auslöser für eine konfigurierte Aktion.

Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der **Digitalisierungsbox**. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

Hinweis

Voraussetzung für den Betrieb des Aufgabenplaners ist ein auf Ihrem Gerät eingestelltes Datum ab dem 1.1.2000.

6.2.1.1 Auslöser

Im Menü **Lokale Dienste**->**Scheduling**->**Auslöser** werden alle konfigurierten Ereignislisten angezeigt. Jede Ereignisliste enthält mindestens ein Ereignis, das als Auslöser für eine Aktion vorgesehen ist.

6.2.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Ereignislisten anzulegen.

Das Menü **Lokale Dienste**->**Scheduling**->**Auslöser**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ereignisliste	Mit *Neu* (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit **Beschreibung** geben Sie dieser Liste einen Namen. Mit Hilfe der übrigen Parameter legen Sie das erste Ereignis in der Liste an. Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu. Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereignisse werden in derseben Reihenfolge abgearbeitet wie sie in der Liste angelegt sind.
Beschreibung	Nur für **Ereignisliste** = *Neu* Geben Sie eine beliebige Bezeichnung für die **Ereignisliste** ein.
Ereignistyp	Wählen Sie den Typ des Ereignisses aus. Mögliche Werte: • *Zeit* (Standardwert): Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • *MIB/SNMP*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen. • *Schnittstellenstatus*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen. • *Schnittstellenverkehr*: Die in **Aktionen** konfigurierten und zugewiesenenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet. • *Ping-Test*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist. • *Lebensdauer eines Zertifikats*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist. • *Funktionstaste* Mit der Option *Funktionstaste* legen Sie fest, dass das Drücken der Funktionstaste am Gerät als Auslöser für konfigurierte Aktionen dienen kann. Durch einen Druck von gut einer Sekunde (aber weniger als drei Sekunden) auf die Taste wird der Zustand der Taste auf *Aktiv* gesetzt, durch einen Druck von mehr als drei Sekunden wird er auf *Inaktiv* gesetzt. Aktionen, die vom Zustand der Taste abhängen, werden dann bei der nächsten zyklischen Abfrage gemäß dem **Schedule-Intervall** ausgelöst. Es kann also z. B. eine WLAN-Schnittstelle aktiviert werden, wenn die Funktionstaste eine Sekunde lang gedrückt wird. Bei einem Druck auf die Taste vom mehr als drei Sekunden wird die Schnittstelle wieder deaktiviert.
Überwachte Variable	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie die MIB-Variable aus, deren definierter Wert als Auslöser konfiguriert werden soll. Wählen Sie zunächst das **System** aus, in dem die MIB-Variable gespeichert ist, dann die **MIB-Tabelle** und dann die **MIB-Variable** selber. Es werden nur die MIB-Tabellen und MIB-Variablen

Feld	Beschreibung
	angezeigt, die im jeweiligen Bereich vorhanden sind.
Vergleichsbedingung	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie aus, ob die MIB-Variable *Größer* (Standardwert), *Gleich*, *Kleiner*, *Ungleich* dem in *Vergleichswert* angegebenen Wert sein oder innerhalb von *Bereich* liegen muss, um die Aktion auszulösen.
Vergleichswert	Nur für **Ereignistyp** *MIB/SNMP* Geben Sie den Wert der MIB-Variable ein.
Indexvariablen	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und **Indexwert** ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags. Legen Sie weitere **Indexvariablen** mit **Hinzufügen** an.
Überwachte Schnittstelle	Nur für **Ereignistyp** *Schnittstellenstatus* und *Schnittstellenverkehr* Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.
Schnittstellenstatus	Nur für **Ereignistyp** *Schnittstellenstatus* Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen. Mögliche Werte: • *Aktiv* (Standardwert): Die Schnittstelle ist aktiv. • *Inaktiv*: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen. Mögliche Werte: • *RX* (Standardwert): Der eingehende Datenverkehr wird überwacht. • *TX*: Der ausgehende Datenverkehr wird überwacht.
Bedingung des Schnittstellenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie aus, ob der Wert für Datenverkehr *Größer* (Standardwert) oder *Kleiner* dem in *Übertragener Datenverkehr* angegebenen Wert sein muss, um die Aktion auszulösen.
Übertragener Datenverkehr	Nur für **Ereignistyp** *Schnittstellenverkehr* Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in **kBytes** ein. Der Standardwert ist *0*.
Ziel-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden

Feld	Beschreibung
	soll.
Quell-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll. Mögliche Werte: • *Automatisch* (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • *Spezifisch*: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Status	Nur für **Ereignistyp** *Ping-Test* Wählen Sie aus, ob **Ziel-IP-Adresse** *Erreichbar* (Standardwert) oder *Nicht erreichbar* sein muss, um die Aktion auszulösen.
Intervall	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll. Der Standardwert ist *60* Sekunden.
Versuche	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll. Der Standardwert ist *3*.
Überwachtes Zertifikat	Nur für **Ereignistyp** *Lebensdauer eines Zertifikats* Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.
Verbleibende Gültigkeitsdauer	Nur für **Ereignistyp** *Lebensdauer eines Zertifikats* Geben Sie den gewünschten Wert für die noch verbleibende Gültigkeit des Zertifikats in Prozent ein.
Status der Funktionstaste	Nur für **Ereignistyp** *Funktionstaste* Beim Anlegen des Auslösers können Sie über die Auswahl des **Status der Funktionstaste** festlegen, bei welchem Zustand der Funktionstaste der Auslöser aktiv sein soll. Setzen Sie den Status auf *An*, so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste *Aktiv* ist, und inaktiv, wenn der Zustand der Funktionstaste *Inaktiv* ist. Setzen Sie ihn auf *Aus*, so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste *Inaktiv* ist, und inaktiv, wenn der Zustand der Funktionstaste *Aktiv* ist. Die Zustandsprüfung erfolgt zyklisch im Abstand des konfigurierten Schedule-Intervalls.

Felder im Menü Zeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	Nur für **Ereignistyp** *Zeit* Wählen Sie zunächst die Art der Zeitangabe in **Bedingungstyp** aus. Mögliche Werte: • *Wochentag*: Wählen Sie in **Bedingungseinstellungen** einen Wochen-

Feld	Beschreibung
	tag aus. • *Perioden* (Standardwert): Wählen Sie in **Bedingungseinstellungen** einen bestimmten Turnus aus. • *Tag des Monats*: Wählen Sie in **Bedingungseinstellungen** einen bestimmten Tag im Monat aus. Mögliche Werte für **Bedingungseinstellungen** bei **Bedingungstyp** = *Wochentag*: *Montag* (Standardwert) ... *Sonntag*. Mögliche Werte für **Bedingungseinstellungen** bei **Bedingungstyp** = *Perioden*: • *Täglich*: Der Auslöser wird täglich aktiv (Standardwert). • *Montag-Freitag*: Der Auslöser wird täglich von Montag bis Freitag aktiv. • *Montag-Samstag* : Der Auslöser wird täglich von Montag bis Samstag aktiv. • *Samstag-Sonntag* : Der Auslöser wird Samstag und Sonntag aktiv. Mögliche Werte für **Bedingungseinstellungen** bei **Bedingungstyp** = *Tag des Monats*: *1*... *31*.
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine **Stoppzeit** eingeben oder **Stoppzeit** = **Startzeit** setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

6.2.1.2 Aktionen

Im Menü **Lokale Dienste**->**Scheduling**->**Aktionen** wird eine Liste aller Aktionen angezeigt, die durch die in **Lokale Dienste**->**Scheduling**->**Auslöser** konfigurierten Ereignisse oder Ereignisketten ausgelöst werden sollen.

6.2.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Aktionen zu konfigurieren.

Das Menü **Lokale Dienste**->**Scheduling**->**Aktionen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
Befehlstyp	Wählen Sie die gewünschte Aktion aus. Mögliche Werte: • *Neustart* (Standardwert): Ihr Gerät wird neu gestartet. • *MIB/SNMP*: Für eine MIB-Variable wird der gewünschte Wert eingetragen. • *Schnittstellenstatus*: Der Status einer Schnittstelle wird verän-

Feld	Beschreibung
	dert. • *WLAN-Status*: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID wird verändert. • *Softwareaktualisierung*: Es wird ein Software-Update initiiert. • *Konfigurationsmanagement*: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • *Ping-Test*: Die Erreichbarkeit einer IP-Adresse wird überprüft. • *Zertifikatverwaltung*: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • *5 GHz-WLAN-Bandscan*: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • *WLC: Neuer Neighbor-Scanvorgang*: Nur für Geräte mit WLAN Controller. In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • *WLC: VSS-Status*: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert. • *Betriebsmodus*: Der Betriebsmosdus eines WLAN-Radiomoduls wird verändert.
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in **Lokale Dienste**->**Scheduling**->**Auslöser** angelegt ist.
Bedingung für Ereignisliste	Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird. Mögliche Werte: • *Alle* (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • *Eins*: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • *Keiner*: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • *Eins nicht*: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	Nur bei **Befehlstyp** = *Neustart* Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird. Der Standardwert ist *60* Sekunden.
Hinzuzufügende/zu bearbeitende MIB/ SNMP-Variable	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das **System** aus und dann die **MIB-Tabelle**. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.
Befehlsmodus	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie aus, auf welche Weise der MIB-Eintrag manipuliert werden soll. Zur Verfügung stehen: • *Vorhandenen Eintrag ändern* (Standardwert): Ein bestehender Eintrag soll verändert werden. • *Neuen MIB-Eintrag erstellen*: Ein neuer Eintrag soll angelegt

Feld	Beschreibung
	werden.
Indexvariablen	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und **Indexwert** ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags. Legen Sie weitere **Indexvariablen** mit **Hinzufügen** an.
Status des Auslösers	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie aus, welchen Status das Ereignis haben muss, um die MIB-Variable wie definiert zu verändern. Mögliche Werte: • *Aktiv* (Standardwert): Der Wert der MIB-Variable wird verändert, wenn der Auslöser aktiv ist. • *Inaktiv*: Der Wert der MIB-Variable wird verändert, wenn der Auslöser inaktiv ist. • *Beide*: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.
MIB-Variablen	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll. Ist der Auslöser aktiv (**Status des Auslösers** *Aktiv*), wird die MIB-Variable mit dem in **Aktiver Wert** eingetragenen Wert beschrieben. Ist der Auslöser inaktiv, **Status des Auslösers** *Inaktiv*), wird die MIB-Variable mit dem in **Inaktiver Wert** eingetragenen Wert beschrieben. Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (**Status des Auslösers** *Beide*), wird sie mit einem aktiven Auslöser mit dem in **Aktiver Wert** eingetragenen Wert und mit einem inaktiven Auslöser mit dem in **Inaktiver Wert** eingetragenen Wert beschrieben. Legen Sie weitere Einträge mit **Hinzufügen** an.
Schnittstelle	Nur bei **Befehlstyp** = *Schnittstellenstatus* Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.
Schnittstellenstatus festlegen	Nur bei **Befehlstyp** = *Schnittstellenstatus* Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll. Mögliche Werte: • *Aktiv* (Standardwert) • *Inaktiv* • *Zurücksetzen*
Lokale WLAN-SSID	Nur bei **Befehlstyp** = *WLAN-Status* Wählen Sie das gewünschte Drahtlosnetzwerk aus, dessen Status verändert werden soll.

Feld	Beschreibung
Status festlegen	Nur bei **Befehlstyp** = *WLAN-Status* oder *WLC: VSS-Status* Wählen Sie den Status aus, den das Drahtlosnetzwerk erhalten soll. Mögliche Werte: • *Aktivieren* (Standardwert) • *Deaktivieren*
Quelle	Nur bei **Befehlstyp** = *Softwareaktualisierung* Wählen Sie die gewünschte Quelle für die Software-Aktualisierung aus. Mögliche Werte: • *Aktuelle Software vom Update-Server* (Standardwert): Die aktuelle Software wird vom Update-Server geladen. • *HTTP-Server*: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die *Server-URL* festlegen. • *HTTPS-Server*: Die aktuelle Software wird von einem HTTPS-Server geladen, den Sie über die *Server-URL* festlegen. • *TFTP-Server*: Die aktuelle Software wird von einem TFTP-Server geladen, den Sie über die *Server-URL* festlegen.
Server-URL	Bei **Befehlstyp** = *Softwareaktualisierung* wenn **Quelle** nicht *Aktuelle Software vom Update-Server* Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* mit **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Geben Sie die URL des Servers ein, von dem eine Konfigurationsdatei geholt oder auf den die Konfigurationsdatei gesichert werden soll.
Dateiname	Bei **Befehlstyp** = *Softwareaktualisierung* Geben Sie den Dateinamen der Softwareversion ein. Bei **Befehlstyp** = *Zertifikatverwaltung* mit **Aktion** = *Zertifikat importieren* Geben Sie den Dateinamen der Zertifikatsdatei ein.
Aktion	Bei **Befehlstyp** = *Konfigurationsmanagement* Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll. Mögliche Werte: • *Konfiguration importieren* (Standardwert) • *Konfiguration exportieren* • *Konfiguration umbenennen* • *Konfiguration löschen* • *Konfiguration kopieren* Bei **Befehlstyp** = *Zertifikatverwaltung* Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten.

Feld	Beschreibung
	Mögliche Werte: • *Zertifikat importieren* (Standardwert) • *Zertifikat löschen* • *SCEP*
Protokoll	Nur für **Befehlstyp** = *Zertifikatverwaltung* und *Konfigurationsmanagement* wenn **Aktion** = *Konfiguration importieren* Wählen Sie das Protokoll für die Dateiübertragung aus. Mögliche Werte: • *HTTP* (Standardwert) • *HTTPS* • *TFTP*
CSV-Dateiformat	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob die Datei im CSV-Format übertragen werden soll. Das CSV-Format kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Standardmäßig ist die Funktion aktiv.
Dateiname auf Server	Nur bei **Befehlstyp** = *Konfigurationsmanagement* Für **Aktion** = *Konfiguration importieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server, von dem sie geholt werden soll, gespeichert ist. Für **Aktion** = *Konfiguration exportieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.
Lokaler Dateiname	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren*, *Konfiguration umbenennen* oder *Konfiguration kopieren* Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.
Dateiname in Flash	Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration exportieren* Wählen Sie die Datei aus, die exportiert werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration umbenennen* Wählen Sie die Datei aus, die umbenannt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration löschen* Wählen Sie die Datei aus, die gelöscht werden soll.

Feld	Beschreibung
	Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration kopieren* Wählen Sie die Datei aus, die kopiert werden soll.
Konfiguration enthält Zertifikate/Schlüssel	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen. Standardmäßig ist die Funktion nicht aktiv.
Konfiguration verschlüsseln	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob die Daten der gewählten **Aktion** verschlüsselt werden sollen. Standardmäßig ist die Funktion nicht aktiv.
Nach Ausführung neu starten	Nur bei **Befehlstyp** = *Konfigurationsmanagement* Wählen Sie aus, ob Ihr Gerät nach der gewünschten **Aktion** neu gestartet werden soll. Standardmäßig ist die Funktion nicht aktiv.
Versionsprüfung	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* Wählen Sie aus, ob beim Import einer Konfigurationsdatei überprüft werden soll, ob auf dem Server eine aktuellere Version der schon geladenen Konfiguration vorhanden ist. Wenn nicht, wird der Datei-Import abgebrochen. Standardmäßig ist die Funktion nicht aktiv.
Ziel-IP-Adresse	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.
Quell-IP-Adresse	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll. Mögliche Werte: • *Automatisch* (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • *Spezifisch*: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Intervall	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll.

Feld	Beschreibung
	Der Standardwert ist *1* Sekunde.
Versuche	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll. Der Standardwert ist *3*.
Serveradresse	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.
Lokale Zertifikatsbeschreibung	Bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll. Bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat löschen* Wählen Sie das Zertifikat aus, das gelöscht werden soll.
Kennwort für geschütztes Zertifikat	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie ein geschütztes Zertifikat verwenden möchten, das ein Passwort benötigt, und geben Sie dieses in das Eingabefeld ein. Standardmäßig ist die Funktion nicht aktiv.
Ähnliches Zertifikat überschreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie ein auf Ihrem Gerät schon vorhandenes Zertifikat mit dem neuen überschreiben wollen. Standardmäßig ist die Funktion nicht aktiv.
Zertifikat in Konfiguration schreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungsbeschreibung	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.
SCEP-Server-URL	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie die URL des SCEP-Servers ein, z. B. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Subjektname	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie einen Subjektnamen mit Attributen ein.

Feld	Beschreibung
	Beispiel: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA-Name	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows*. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Passwort	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.
Schlüsselgröße	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind *1024* (Standardwert), *2048* und *4096*.
Autospeichermodus	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert. Standardmäßig ist die Funktion aktiv.
CRL verwenden	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Werte: • *Auto* (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatsperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden. • *Ja*: CRLs werden grundsätzlich überprüft. • *Nein*: Keine Überprüfung von CRLs.
WLAN-Modul auswählen	Nur bei **Befehlstyp** = *5 GHz-WLAN-Bandscan* und *Betriebsmodus* Wählen Sie das WLAN-Modul aus, auf dem ein Scan des Frequenzbands durchgeführt werden soll.
WLC-SSID	Nur bei **Befehlstyp** = *WLC: VSS-Status* Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.
Betriebsmodus (**Aktiv**)	Nur bei **Befehlstyp** = *Betriebsmodus* Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand *Aktiv* befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt

Feld	Beschreibung
	werden. Die Auswahl kann also von Gerät zu Greät abweichen.
Betriebsmodus (**Inaktiv**)	Nur bei **Befehlstyp** = *Betriebsmodus* Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand *Inaktiv* befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Greät abweichen.

6.2.1.3 Optionen

Im Menü **Lokale Dienste**->**Scheduling**->**Optionen** konfigurieren Sie das Schedule-Intervall.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

Feld	Beschreibung
Schedule-Intervall	Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll. Standardmäßig ist das Schedule-Intervall nicht aktiv. Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind. Möglich sind Werte zwischen *0* und *65535*. Empfohlen wird der Wert *300* (5 Minuten Genauigkeit).

6.3 Wartung

Im diesem Menü werden Ihnen zahlreiche Funktionen zur Wartung Ihres Geräts zur Verfügung gestellt. So finden Sie zunächst eine Menü zum Testen der Erreichbarkeit innerhalb des Netzwerks. Sie haben die Möglichkeit Ihre Systemkonfigurationsdateien zu verwalten. Falls aktuellere Systemsoftware zur Verfügung steht, kann die Installation über dieses Menü vorgenommen werden. Falls Sie weitere Sprachen der Konfigurationsoberfläche benötigen, können Sie diese importieren. Auch ein System-Neustart kann in diesem Menü ausgelöst werden.

6.3.1 Benutzer ausloggen

Es kann vorkommen, dass durch eine nicht vollständig abgebaute Konfigurationssitzung Funktionen der Konfigurationsoberfläche beeinträchtigt werden. In diesem Fall können in diesem Menü alle noch bestehenden Verbindungen zum GUI eingesehen und ggf. beendet werden.

6.3.1.1 Benutzer ausloggen

In diesem Menü sehen Sie zunächst eine Auflistung aller aktiven Konfigurationsverbindungen.

Felder im Menü Benutzer ausloggen

Feld	Beschreibung
Klasse	Zeigt die Benutzerklasse an, der der angemeldete Benutzer angehört.
Benutzer	Zeigt den Benutzernamen an.
Entfernte IP-Adresse	Zeigt die IP-Adresse an, von der die Verbindung aufgebaut wurde. Die kann die Adresse eines PCs sein, aber auch die Adresse eines zwischengelagerten Routers.
Läuft ab	Zeigt an, wann die Verbindung automatisch getrennt wird.
Sofort ausloggen	Wenn sie das Kontrollkästchen aktivieren, wird dieser Benutzer mit einm klick auf **Ausloggen** vom System abgemeldet.

6.3.1.1.1 Logout-Optionen

Nachdem Sie die Auswahl der zu beendenden Verbindungen mit Ausloggen bestätigt haben, können Sie wählen ob und welche Konfigurationen, die mit den entsprechenden Sitzungen zusammenhängen, vor dem Abmelden der Benutzer gespeichert werden.

6.3.2 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

6.3.2.1 Ping-Test

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind.

Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: • *IPv4* • *IPv6*
Ping-Befehl testweise an Adresse senden	Geben Sie die zu testende IP-Adresse ein.
Zu verwendende Schnittstelle	Nur für **Test-Ping-Modus** = *IPv6* Wählen Sie für Link-Lokale-Adressen die Schnittstelle, die für den Ping-Test verwendet werden soll. Für globale Adressen kann *Standard* verwendet werden.

Durch Anklicken der **Los**-Schaltfläche wird der Ping-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an.

6.3.2.2 DNS-Test

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domänennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

6.3.2.3 Traceroute-Test

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist.

Felder im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	Wählen Sie die für den Traceroute-Test verwendete IP-Version. Mögliche Werte: • *IPv4* • *IPv6*
Traceroute-Adresse	Geben Sie die zu testende IP-Adresse ein.

Durch Anklicken der **Los**-Schaltfläche wird der Traceroute-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an.

6.3.3 Trace

6.3.3.1 Trace-Schnittstelle

Das Menü **Trace-Schnittstelle** ermöglicht Ihnen eine Aufzeichnung des Datenverkehrs über eine besitmmte Schnittstelle und, nach Ende der Aufzeichnung, das Abspeichern des Mitschnitts als PCAP-Datei.

Felder im Menü Trace-Einstellungen

Feld	Beschreibung
Schnittstellenauswahl	Wählen Sie die Schnittstelle aus, deren Datenverkehr Sie aufzeichnen wollen.
Trace-Modus	Hier können Sie auswählen, auf welchen Ebenen der Datenverkehr der ausgewählten Schnittstelle aufgezeichnet werden soll. Zur Auswahl stehen: • *Layer 2* • *PPP* • *Layer 3* • *IP*

Sobald Sie die Aufzeichnung mit der Schaltfläche **START** beginnen, wird ein Fenster angezeigt, das über die laufende Aufzeichnung informiert. Sie können während der Aufzeichnung das Menü verlassen und das GUI wie gewohnt vewenden. Wenn Sie eine Aufzeichnung mit **STOPP** beenden, werden Informationen zu der erstellten Datei angezeigt, und Sie erhalten die Möglichkeit, diese zu löschen oder im PCAP-Format herunterzuladen.

6.3.3.2 VoIP/SIP-Trace

Das Menü **VoIP/SIP-Trace** gibt Ihnen die Möglichkeit, VoIP/SIP-Meldungen auf verschiedenen Leveln aufzuzeichnen und als Textdatei auf Ihrem Computer zu speichern. Sie können aus den folgenden Trace-Leveln wählen. Eine Beschreibung, welche Informationen aufgezeichnet werden, wird in Abhängigkeit Ihrer Auswahl angezeigt:

- Statusinformation: Das Gerät schreibt den aktuellen Zustand des VoIP/SIP-Subsystems in eine Datei, die Sie dann herunterladen können.
- Ereignisse: Das Gerät schreibt VoIP/SIP-Informationen kontinuierlich in den Trace-Speicher, sobald Sie die Schaltfläche **Start** klicken. Sobald Sie die Schaltfläche **Stop** klicken, bekommen Sie die Möglichkeit, die Datei herunterzuladen.
- SIP: Das Gerät schreibt (nur) alle SIP-Meldungen kontinuierlich in den Trace-Speicher, sobald Sie die Schaltfläche **Start** klicken. Sobald Sie die Schaltfläche **Stop** klicken, bekommen Sie die Möglichkeit, die Datei herunterzuladen.

6.3.4 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

6.3.4.1 Optionen

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Daher müssen Sie gegebenenfalls ein Software-Update durchführen.

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie auf der Hilfeseite der Deut-

schen Telekom *www.telekom.de/digitalisierungsbox-hilfe* .

Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn bintec elmeg GmbH eine explizite Empfehlung dazu ausspricht.

Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen `boot` im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei `boot` verwendet.

Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

Achtung

Sollten Sie eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

Das Menü **Wartung**->**Software & Konfiguration** ->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Aktuell installierte Software

Feld	Beschreibung
BOSS	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
Systemlogik	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
xDSL-Logik	Zeigt die aktuelle Version der xDSL-Logik an, die auf Ihrem Gerät geladen ist.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	Wählen Sie die Aktion aus, die Sie ausführen möchten. Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden. Mögliche Werte: • *Keine Aktion* (Standardwert): • *Konfiguration exportieren*: Die Konfigurationsdatei **Aktueller Dateiname im Flash** wird zu Ihrem lokalen Host transferiert. Wenn Sie auf **Los** klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. • *Konfiguration importieren*: Wählen Sie in **Dateiname** die Konfigurationsdatei aus, die Sie importieren wollen. Hinweis: Durch Klicken auf **Los** wird die Datei zunächst unter dem Namen *boot* in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. • *Konfiguration kopieren*: Die Konfigurationsdatei im Feld **Name der Quelldatei** wird als **Name der Zieldatei** gespeichert. • *Konfiguration löschen*: Die Konfiguration im Feld **Datei auswählen** wird gelöscht. • *Konfiguration umbenennen*: Die Konfigurationsdatei im Feld **Datei auswählen** wird zu **Neuer Dateiname** umbenannt. • *Sicherung wiederherstellen*: Nur, wenn unter **Konfiguration speichern** mit der Einstellung *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern* die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • *Software/Firmware löschen*: Die Datei im Feld **Datei auswählen** wird gelöscht. • *Sprache importieren*: Sie können weitere Sprachversionen des **GUI** auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von *http://telekom.de/hilfe* auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen. • *Systemsoftware aktualisieren*: Sie können eine Aktualisierung der Systemsoftware, der DSL-Logik und des BOOTmonitors initiieren. • *Konfiguration mit Statusinformationen exportieren*: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die **Los**-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. Die folgenden Optionen stehen nur zur Verfügung, wenn Ihr Gerät einen zusätzlichen internen Speicher aufweist. • *Zusätzliche Dateien laden (in den USB-Speicher)*: Sie können zusätzliche Dateien wie Voice-Mail-Ansagen oder Wartemusik als ZIP gepackt in den USB-Speicher laden. Dort wird der Inhalt entpackt und eine entsprechende Verzeichnisstruktur erstellt. Wählen Sie in **Dateiname** die Datei aus, die Sie laden möchten. • *Voice Mail Wave-Dateien importieren*: Wählen Sie in **Dateiname** die Datei *vms_wavfiles.zip* aus, die Sie importieren wollen. • *MMC/SD-Karte formatieren*: Unter Umständen muss der zusätzliche interne Speicher Ihres Geräts neu formatiert werden. Bei der Formatierung wird der gesamte Inhalt des zusätzlichen internen Speichers

Feld	Beschreibung
	gelöscht!
Aktueller Dateiname im Flash	Für **Aktion** = *Konfiguration exportieren* Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.
Zertifikate und Schlüssel einschließen	Für **Aktion** = *Konfiguration exportieren* Wählen Sie aus, ob die gewählte **Aktion** auch für Zertifikate und Schlüssel gelten soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Verschlüsselung der Konfiguration	Nur für **Aktion** = *Konfiguration exportieren*, *Konfiguration importieren*, *Konfiguration mit Statusinformationen exportieren* Wählen Sie aus, ob die Daten der gewählten **Aktion** verschlüsselt werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiviert ist, können Sie in das Textfeld das **Passwort** eingeben.
Dateiname	Nur für **Aktion** = *Konfiguration importieren*, *Sprache importieren*, *Systemsoftware aktualisieren* Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.
Name der Quelldatei	Nur für **Aktion** = *Konfiguration kopieren* Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für **Aktion** = *Konfiguration kopieren* Geben Sie den Namen der Kopie ein.
Datei auswählen	Nur für **Aktion** = *Konfiguration löschen*, *Konfiguration umbenennen* oder *Software/Firmware löschen* Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.
Neuer Dateiname	Nur für **Aktion** = *Konfiguration umbenennen* Geben Sie den neuen Namen der Konfigurationsdatei ein.
Quelle	Nur für **Aktion** = *Systemsoftware aktualisieren* Wählen Sie die Quelle der Aktualisierung aus. Mögliche Werte: • *Lokale Datei* (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert. • *HTTP-Server*: Die Datei ist auf dem entfernten Server gespeichert, der in der **URL** angegeben wird. • *Aktuelle Software vom Update-Server*: Die Datei liegt auf

Feld	Beschreibung
	dem offiziellen Update-Server.
URL	Nur für **Aktion** = *Systemsoftware aktualisieren* und **Quelle** = *HTTP-Server* Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.

Im Menü **Erweiterte Einstellungen** wird die Version der aktuell installierten internen System-Dateien angezeigt.

6.3.5 Neustart

6.3.5.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.

Hinweis

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

6.3.6 Factory Reset

Im Menü **Wartung**->**Factory Reset** können Sie Ihr Gerät über das GUI in den Auslieferungszustand versetzen.

Hinweis

Beachten Sie, dass angeschlossene IP-Geräte nach einem Factory Reset kurz von der Stromversorgung getrennt werden sollten, damit sie vom System wieder erkannt werden.

6.4 Externe Berichterstellung

In diesem Menü legen Sie fest, welche Systemprotokoll-Nachrichten auf welchem Rechner gespeichert werden und ob der Systemadministrator bei bestimmten Ereignissen eine Email erhalten soll. Informationen über den IP-Datenverkehr können - bezogen auf die einzelnen Schnittstellen - ebenfalls gespeichert werden. Darüber hinaus können im Fehlerfall SNMP-Traps an bestimmte Hosts versandt werden.

6.4.1 Systemprotokoll

Ereignisse in den verschiedenen Subsystemen Ihres Geräts (z. B. PPP) werden in Form von Systemprotokoll-Nachrichten (Syslog) protokolliert. Je nach eingestelltem Level (acht Stufen von *Notfall* über *Information* bis *Debug*) werden dabei mehr oder weniger Meldungen sichtbar.

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet

werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.

Warnung

Achten Sie darauf, die Systemprotokoll-Nachrichten nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

6.4.1.1 Syslog-Server

Konfigurieren Sie Ihr Gerät als Syslog-Server, sodass die definierten Systemmeldungen an geeignete Hosts im LAN geschickt werden können.

In diesem Menü definieren Sie, welche Meldungen mit welchen Bedingungen zu welchem Host geschickt werden.

Im Menü **Externe Berichterstellung**->**Systemprotokoll**->**Syslog-Server** wird eine Liste aller konfigurierten Systemprotokoll-Server angezeigt.

6.4.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Das Menü **Externe Berichterstellung**->**Systemprotokoll**->**Syslog-Server**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung* • *Benachrichtigung* • *Information* (Standardwert) • *Debug* (niedrigste Priorität) Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden an den Host gesendet, d. h. dass beim Syslog-Level *Debug* sämtliche erzeugten Meldungen an den Host weitergeleitet werden.
Facility	Geben Sie die Syslog Facility auf dem Host an. Dieses ist nur erforderlich, wenn der **Log Host** ein Unix-Rechner ist. Mögliche Werte: *local0 - 7* (Standardwert) *local0*.

Feld	Beschreibung
Zeitstempel	Wählen Sie das Format des Zeitstempels im Systemprotokoll aus. Mögliche Werte: • *Keiner* (Standardwert): Keine Systemzeitangabe. • *Zeit*: Systemzeit ohne Datum. • *Datum &Uhrzeit*: Systemzeit mit Datum.
Protokoll	Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss. Mögliche Werte: • *UDP* (Standardwert) • *TCP*
Nachrichtentyp	Wählen Sie den Nachrichtentyp aus. Mögliche Werte: • *System &Accounting* (Standardwert) • *System* • *Accounting*

6.4.2 IP-Accounting

In modernen Netzwerken werden häufig aus kommerziellen Gründen Informationen über Art und Menge der Datenpakete gesammelt, die über die Netzwerkverbindungen übertragen und empfangen werden. Für Internet Service Provider, die ihre Kunden nach Datenvolumen abrechnen, ist das von entscheidender Bedeutung.

Aber auch nicht-kommerzielle Zwecke sprechen für ein detailiertes Netzwerk-Accounting. Wenn Sie z. B. einen Server verwalten, der verschiedene Arten von Netzwerkdiensten zur Verfügung stellt, ist es nützlich für Sie zu wissen, wieviel Daten von den einzelnen Diensten erzeugt werden.

Ihr Gerät enthält die Funktion IP-Accounting, die Ihnen die Sammlung vielerlei nützlicher Informationen über den IP-Netzwerkverkehr (jede einzelne IP-Session) ermöglicht.

6.4.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

Im Menü **Externe Berichterstellung**->**IP-Accounting**->**Schnittstellen** wird eine Liste aller auf Ihrem Gerät konfigurierten Schnittstellen angezeigt. Für jeden Eintrag kann durch Setzen eines Hakens die Funktion IP-Accounting aktiviert werden. In der Spalte **IP-Accounting** müssen Sie nicht jeden Eintrag einzeln anklicken. Über die Optionen **Alle auswählen** oder **Alle deaktivieren** können Sie die Funktion IP-Accounting für alle Schnittstellen gleichzeitig aktivieren bzw. deaktivieren.

6.4.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

Im Menü **Externe Berichterstellung**->**IP-Accounting**->**Optionen** können Sie das **Protokollformat** der IP-Accounting-Meldungen festlegen. Die Meldungen können Zeichenketten in beliebiger Reihenfolge, durch umgekehrten Schrägstrich abgetrennte Sequenzen, z. B. `\t` oder `\n` oder definierte Tags enthalten.

Mögliche Format-Tags:

Format-Tags für IP-Accounting Meldungen

Feld	Beschreibung
%d	Datum des Sitzungsbeginns im Format DD.MM.YY
%t	Uhrzeit des Sitzungsbeginns im Format HH:MM:SS
%a	Dauer der Sitzung in Sekunden
%c	Protokoll
%i	Quell-IP-Adresse
%r	Quellport
%f	Quell-Schnittstellen-Index
%I	Ziel-IP-Adresse
%R	Zielport
%F	Ziel-Schnittstellen-Index
%p	Ausgegangene Pakete
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen: *`INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]`*

6.4.3 Benachrichtigungsdienst

Bisher war es möglich Syslog-Meldungen vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Mit dem Benachrichtigungsdienst werden dem Administrator je nach Konfiguration E-Mails gesendet, sobald relevante Syslog-Meldungen auftreten.

6.4.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

6.4.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Benachrichtigungsempfänger anzulegen.

Das Menü **Externe Berichterstellung**->**Benachrichtigungsdienst**->**Benachrichtigungsempfänger**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen. Mögliche Werte: • E-Mail • SMS
Empfänger	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkomprimierung	Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse. Aktivieren oder deaktivieren Sie das Feld. Standardmäßig ist die Funktion aktiv.
Betreff	Sie können einen Betreff eingeben.
Ereignis	Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar. Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll. Mögliche Werte: • *Systemmeldung enthält Zeichenfolge* (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • *Neuer Neighbor-AP gefunden*: Ein neuer benachbarter AP wurde gefunden. • *Neuer Rogue-AP gefunden*: Ein neuer Rough AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • *Neuer Slave-AP (WTP) gefunden*: Eine neuer unkonfigurierter AP hat sich beim WLAN Controller gemeldet. • *Verwalteter AP offline*: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms. Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "*") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
Schweregrad	Wählen Sie den Schweregrad aus, auf dem der im Feld **Enthaltene Zeichenfolge** konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird. Mögliche Werte: *Notfall* (Standardwert), *Alarm*, *Kritisch*, *Fehler*, *Warnung*, *Benachrichtigung*, *Information*, *Debug*

Feld	Beschreibung
Überwachte Subsysteme	Wählen Sie die Subsysteme aus, die überwacht werden sollen. Fügen Sie mit **Hinzufügen** neue Subsysteme hinzu.
Timeout für Nachrichten	Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Benachrichtigungsmails erzwungen wird. Zur Verfügung stehen Werte von `0` bis `86400`. Ein Wert von `0` deaktiviert den Timeout. Der Standardwert ist `60`.
Anzahl Nachrichten	Geben Sie die Anzahl der Syslog-Meldungen ein, die erreicht sein muss, ehe eine Benachrichtigungsmail für diesen Fall gesendet werden kann. Wenn Timeout konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist. Zur Verfügung stehen Werte von `0` bis `99`, der Standardwert ist `1`.

6.4.3.2 Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung**->**Benachrichtigungsdienst**->**Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll. Mit `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Maximale Anzahl von E-Mails pro Minute	Begrenzen Sie die Anzahl der ausgehenden Mails pro Minute. Zur Verfügung stehen Werte von `1` bis `15`, der Standardwert ist `6`.

Felder im Menü E-Mail-Parameter

Feld	Beschreibung
E-Mail-Adresse des Senders	Geben Sie die E-Mail-Adresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll. Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Port	Verschlüsselung von E-Mails (SSL/TLS). Das Feld **SMTP-Port** ist Standardmäßig auf `25` voreingestellt und **SSL** Encryption aktiviert.
SMTP-Authentifizierung	Authentifizierung, die der SMTP-Server erwartet. Mögliche Werte: • `Keiner` (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • `ESMTP`: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • `SMTP after POP`: Der Server verlangt, dass vor dem Versenden einer Mail Mails per POP3 von der sendenden IP aus mit dem richtigen

Feld	Beschreibung
	POP3-Benutzernamen/Passwort abgerufen werden.
Benutzername	Nur wenn **SMTP-Authentifizierung** = *ESMTP* oder *SMTP after POP* Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.
Passwort	Nur wenn **SMTP-Authentifizierung** = *ESMTP* oder *SMTP after POP* Geben Sie das Passwort dieses Benutzers an.
POP3-Server	Nur wenn **SMTP-Authentifizierung** = *SMTP after POP* Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.
POP3-Timeout	Nur wenn **SMTP-Authentifizierung** = *SMTP after POP* Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird. Der Standardwert ist *600* Sekunden.

6.4.4 SIA

6.4.4.1 SIA

Im Menü **Externe Berichterstellung**->**SIA**->**SIA** können Sie eine Datei erstellen lassen, die dem Support umfassende Informationen zum Zustand des Geräts liefert, wie z. B. zur akktuellen Konfiguration, dem verfügbaren Speicherplatz, der Betriebszeit des Geräts u.s.w.

6.5 Internes Protokoll

6.5.1 Systemmeldungen

Im Menü **Monitoring**->**Internes Protokoll**->**Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierten Werte der Felder **Maximale Anzahl der Syslog-Protokolleinträge** und **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** verändert werden.

Werte in der Liste Systemmeldungen

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der System-Meldung an.
Datum	Zeigt das Datum der Aufzeichung an.
Zeit	Zeigt die Uhrzeit der Aufzeichnung an.
Level	Zeigt die hierarchische Einstufung der Meldung an.
Subsystem	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
Nachricht	Zeigt den Meldungstext an.

Kapitel 7 Telefonie (Media Gateway)

7.1 Physikalische Schnittstellen

7.1.1 ISDN-Ports (Media Gateway)

In diesem Menü konfigurieren Sie die ISDN-Schnittstelle Ihres Geräts. Um die ISDN-BRI-Schnittstelle zu konfigurieren, müssen Sie zwei Schritte durchführen:

- Einstellungen Ihres ISDN-Anschlusses eintragen: Hier tragen Sie die wichtigsten Parameter Ihres ISDN-Anschlusses ein.
- MSN-Konfiguration: Hier teilen Sie Ihrem Gerät mit, wie auf eingehende Rufe aus dem WAN reagiert werden soll.

7.1.1.1 ISDN-Konfiguration

Hinweis

Wenn das ISDN-Protokoll nicht erkannt wird, müssen Sie es unter **Port-Verwendung** und **ISDN-Konfigurationstyp** manuell auswählen. Die automatische D-Kanal-Erkennung ist dann ausgeschaltet. Bei falsch eingestelltem ISDN-Protokoll kann kein ISDN-Verbindungsaufbau erfolgen!

Im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN-Konfiguration** wird eine Liste aller ISDN-Ports und deren Konfiguration angezeigt.

7.1.1.1.1 Bearbeiten

Wählen Sie die Schaltfläche , um die Konfiguration des jeweiligen ISDN-Ports zu bearbeiten.

Das Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN-Konfiguration**-> besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Modus	Wählen Sie den Modus aus. Mögliche Werte: • *Extern* • *Intern*
Automatische Konfiguration beim Start	Bei **Modus** = *Extern* Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll. Mit Aktiviert wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Port-Verwendung	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist. Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden

Feld	Beschreibung
	soll. Mögliche Werte: • *Nicht verwendet*: Der ISDN-Anschluss wird nicht genutzt. • *Dialup (Euro-ISDN)* • *Q-SIG*
ISDN-Konfigurationstyp	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist und für **Port-Verwendung** = *Dialup (Euro-ISDN)* gesetzt ist. Wählen Sie die ISDN-Anschlussart aus. Mögliche Werte: • *Punkt-zu-Mehrpunkt* (Standardwert): Mehrgeräteanschluss. • *Punkt-zu-Punkt*: Anlagenanschluss.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
X.31 (X.25 im D-Kanal)	Wählen Sie aus, ob Sie X.31 (X.25 im D-Kanal) z. B. für CAPI-Applikationen nutzen wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
X.31 TEI-Wert	Nur wenn **X.31 (X.25 im D-Kanal)** aktiviert ist Bei ISDN-Autokonfiguration wird der X.31-TEI automatisch erkannt. Hat die Autokonfiguration den TEI nicht erkannt, können Sie hier manuell den Wert eingeben, der von der Vermittlungsstelle zugewiesen wurde. Mögliche Werte sind *0* bis *63*. Standardwert ist *-1* (für automatische Erkennung).
X.31 TEI-Dienst	Nur für **X.31 (X.25 im D-Kanal)** = aktiviert Wählen Sie den Dienst, für den Sie den X.31-TEI nutzen wollen. Mögliche Werte: • *CAPI* • *CAPI-Standard* • *Packet Switch* (Standardwert) *CAPI* und *CAPI-Standard* dienen zur Nutzung des X.31-TEI für CAPI-Applikationen. Bei *CAPI* wird der in der CAPI-Applikation eingestellte TEI-Wert benutzt, bei *CAPI-Standard* wird der Wert der CAPI-Applikation ignoriert und immer der hier eingestellte Standardwert benutzt. *Packet Switch* stellen Sie ein, wenn Sie den X.31-TEI für das X.25-Gerät nutzen möchten.

7.1.1.2 MSN-Konfiguration

In diesem Menü teilen Sie die zur Verfügung stehenden ISDN-Rufnummern den gewünschten Diensten (z. B. PPP-Routing, ISDN-Login) zu.

Falls Sie die ISDN-Schnittstelle für aus- und eingehende Wählverbindungen verwenden, sind in diesem Menü die eigenen Rufnummern für diese Schnittstelle einzutragen (für Festverbindungen sind diese Einstellungen nicht möglich). Entsprechend den Einstellungen in diesem Menü verteilt Ihr Gerät die eingehenden Rufe auf die internen Dienste. Ausgehenden Rufen wird die eigene Rufnummer als Nummer des Anrufers (Calling Party Number) mitgegeben.

Das Gerät unterstützt die Dienste:

- PPP (Routing): Der Dienst PPP (Routing) ist der allgemeine Routing-Dienst Ihres Geräts. Damit werden u. a. ISDN-Gegenstellen Datenverbindungen mit Ihrem LAN ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Hosts in Ihrem LAN zuzugreifen. Genauso ist es möglich, ausgehende Datenverbindungen zu ISDN-Gegenstellen aufzubauen.
- ISDN-Login: Der Dienst ISDN-Login ermöglicht sowohl eingehende Datenverbindungen mit Zugang zur SNMP-Shell Ihres Geräts, als auch ausgehende Datenverbindungen zu anderen **Digitalisierungsbox**-Geräten. So kann Ihr Gerät aus der Ferne konfiguriert und gewartet werden.
- IPSec: Um Hosts, die nicht über feste IP-Adressen verfügen, dennoch eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **Digitalisierungsbox**-Geräte den DynDNS-Dienst. Durch die Funktion IPSec Callback kann mit Hilfe eines direkten ISDN-Rufs bei einem IPSec Peer mit dynamischer IP-Adresse diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.
- X.25 PAD: Mit X.25 PAD wird ein Protokollkonverter zur Verfügung gestellt, der nicht-paketorientierte Protokolle in paketorientierte Kommunikationsprotokolle und umgekehrt konvertiert. Datenendeinrichtungen, die ihre Daten nicht datenpaketorientiert senden bzw. empfangen, können so an Datex-P (öffentliches Datenpaketnetz nach dem Prinzip der Datenpaketvermittlung) angepasst werden.

Wenn ein Ruf eingeht, überprüft Ihr Gerät zunächst anhand der Einträge in diesem Menü die Art des Anrufs (Daten- oder Sprachruf) und die Called Party Number, wobei nur der Teil der Called Party Number das Gerät erreicht, der von der Ortsvermittlung bzw., falls vorhanden, von der TK-Anlage weitergeleitet wird. Anschließend wird der Ruf dem passenden Dienst zugewiesen.

Hinweis

Wenn kein Eintrag vorhanden ist (Auslieferungszustand) wird jeder über ISDN eingehende Ruf vom Dienst ISDN-Login angenommen. Um dies zu vermeiden, machen Sie hier auf jeden Fall die erforderlichen Eintragungen. Sobald ein Eintrag vorhanden ist, werden eingehende Rufe, die keinem Eintrag zugeordnet werden können, an den Dienst CAPI weitergeleitet.

Im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration** wird eine Liste aller MSNs angezeigt.

7.1.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um eine neue MSN einzurichten.

Das Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
ISDN-Port	Wählen Sie den ISDN-Port aus, für den die MSN konfiguriert werden soll.
Dienst	Wählen Sie den Dienst aus, dem ein Ruf auf die untenstehende **MSN** zugewiesen werden soll. Mögliche Werte: • *ISDN-Login* (Standardwert): Ermöglicht Einloggen mit *ISDN-Login*.

Feld	Beschreibung
	• *PPP (Routing)*: Standardeinstellung für PPP-Routing. Enthält die automatische Erkennung der unten genannten PPP-Verbindungen außer *PPP DOVB*. • *IPSec*: Ermöglicht die Festlegung einer Rufnummer für IPSec-Callback. • *Andere (PPP)*: Weitere Dienste können ausgewählt werden: *PPP 64k* (Ermöglicht 64 kBit/s PPP-Datenverbindungen), *PPP 56k* (Ermöglicht 56 kBit/s PPP-Datenverbindungen), *PPP V.110(9600)*, *PPP V.110(14400)*, *PPP V.110(19200)*, *PPP V.110(38400)* (Ermöglicht PPP-Verbindungen mit V.110 und mit Bit-Raten von 9600 Bit/s, 14400 Bit/s, 19200 Bit/s, 38400 Bit/s), *PPP V.120* (Ermöglicht eingehende PPP-Verbindungen mit V.120).
MSN	Geben Sie die Rufnummer ein, die zur Überprüfung der Called Party Number verwendet wird, wobei zur Rufannahme eine Übereinstimmung einzelner Ziffern im Eintrag unter Berücksichtigung der Konfiguration in **MSN-Erkennung** genügt.
MSN-Erkennung	Wählen Sie den Modus aus, mit dem Ihr Gerät den Ziffernvergleich von **MSN** mit der "Called Party Number" des eingehenden Rufes durchführt. Mögliche Werte: • *Rechts nach Links* (Standardwert) • *Links nach Rechts (DDI)*: Immer auswählen, wenn Ihr Gerät mit einem Point-to-Point-Anschluss (Anlagenanschluss) verbunden ist.
Dienstemerkmal	Wählen Sie die Art des eingehenden Rufes (Diensterkennung) aus. Mögliche Werte: • *Daten + Sprache* (Standardwert): Sowohl Daten- als auch Sprachruf. • *Daten*: Datenruf • *Sprache*: Sprachruf (Modem, Sprache, analoges Fax)

7.2 VoIP (Media Gateway)

Voice over IP (VoIP) nutzt das IP-Protokoll für Sprach- und Bildübertragung.

Der wesentliche Unterschied zur herkömmlichen Telefonie besteht darin, dass die Sprachinformationen nicht über eine geschaltete Verbindung in einem Telefonnetz übertragen werden, sondern durch das Internet-Protokoll in Datenpakete aufgeteilt, die auf nicht festgelegten Wegen in einem Netzwerk zum Ziel gelangen. Diese Technologie macht sich so für die Sprachübertragung die Infrastruktur eines bestehenden Netzwerks zu Nutze und teilt sich dieses mit anderen Kommunikationsdiensten.

Das Session Initiation Protocol (SIP) dient dabei zum Aufbau, zum Abbau und zur Steuerung einer Kommunikationssitzung.

7.2.1 Einstellungen

7.2.1.1 Teilnehmer

Hier können Sie die Rufnummern der Endgeräte (=Teilnehmer) konfigurieren, die an das Media Gateway angebunden sind, d.h. die Rufnummern der SIP-Endgeräte sowie der angeschalteten ISDN-Endgeräte abhängig von den verfügbaren Schnittstellen.

Im Menü **VoIP**->**Einstellungen**->**Teilnehmer** wird eine Liste aller vorhandenen Teilnehmer angezeigt.

7.2.1.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Teilnehmer hinzuzufügen.

Das Menü **VoIP**->**Einstellungen**->**Teilnehmer**-> ->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Teilnehmers ein.
Teilnehmer / Benutzername	ISDN-Endgeräte: Geben Sie die Rufnummer des Teilnehmers. SIP-Endgeräte: Geben Sie den Benutzernamen ein. Maximal können 40 Zeichen eingegeben werden.
Schnittstellentyp	Wählen Sie den Schnittstellentyp aus, welcher verwendet werden soll. Die Auswahl ist von den verfügbaren Schnittstellen abhängig. Mögliche Werte: • *SIP*: Ein SIP-Endgerät wird für den Ruf verwendet. • *ISDN*: Ein ISDN-Endgerät wird für den Ruf verwendet. • *Analog*: Ein analoges Endgerät wird für den Ruf verwendet.
Analoge Schnittstelle auswählen	Nur für **Schnittstellentyp** = *Analog* Wählen Sie eine analoge Schnittstelle aus. Mögliche Werte: • fxs4-0 (Standardwert) • fxs4-1
ISDN-Schnittstelle auswählen	Nur für **Schnittstellentyp** = *ISDN* Wählen Sie eine ISDN-Schnittstelle aus. Welche ISDN-Schnittstellen Sie auswählen können, hängt vom verwendeten Gerät ab.
Registrierung	Nur für **Schnittstellentyp** = *SIP* Wählen Sie, ob der Registrierungsmechanismus per SIP REGISTER Meldung benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Abgesehen von diesem Standard-Vorgehen können die relevanten Daten auch an eine bestimmte IP-Adresse geschickt werden, die den Verbindungspartnern bereits bekannt ist. Dann entfallen Registrierung und Authentisierung, in diesem Fall muss die Funktion **Registrierung** deaktiviert sein. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.
Standort	Legen Sie den Standort des VoIP-Teilnehmers fest. Mögliche Werte:

Feld	Beschreibung
	• *Nicht definiert (Registrierung nur in privaten Netzwerken)* (Standardwert): Der VoIP-Teilnehmer wird nur registriert, wenn er sich innerhalb des privaten Netzwerks befindet. • *LAN*: Der VoIP-Teilnehmer wird registriert, wenn er sich im LAN befindet.
Gültigkeit	Nur wenn **Registrierung** aktiviert ist. Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird. Bei Clients wird der externe Port automatisch erkannt und sollte nicht geändert werden. Zur Verfügung stehen Werte von *0* bis *3600*. Der Standardwert ist *60*.
SIP-Endpunkt-IP-Adresse	Nur wenn **Registrierung** deaktiviert ist. Für Konfigurationen, bei denen keine Registrierung vorgesehen ist (z. B. Anbindung an einen Microsoft Exchange Communication Server), kann die Verbindung als statischer Host eingerichtet werden. Hierzu ist es nötig, die statische IP-Adresse des Endgeräts anzugegeben.
Authentifizierungs-ID	Nur für **Schnittstellentyp** = *SIP* Tragen Sie einen Namen ein, der zur Authentifizierung verwendet wird. Maximal können 20 Zeichen eingegeben werden. Den hier vergebenen Namen müssen Sie auch auf dem SIP-Telefon eingeben. Wenn Sie keinen Namen eingeben, wird der Name im Feld **Teilnehmer / Benutzername** verwendet.
Passwort	Nur für **Schnittstellentyp** = *SIP* Geben Sie hier ein Passwort ein. Maximal können 20 Zeichen eingegeben werden. Das hier vergebene Passwort müssen Sie auch auf dem SIP-Telefon eingeben.
Protokoll	Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll. Mögliche Werte: *UDP* (Standardwert), *TCP* oder *TLS*. Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.
Port	Geben Sie die Nummer des UDP, TCP bzw. TLS Ports, der für die Verbindung zum Server bzw. Proxy benutzt werden soll. Mögliche Werte sind *0* bis *65535*. Der Standardwert ist *5060*.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw. Mögliche Werte: • *Standard* (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. • *Qualität*: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • *Niedrigste*: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • *Höchste*: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.

Felder im Menü Sortierreihenfolge

Feld	Beschreibung
Sortierreihenfolge	Wählen Sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld **Codec-Reihenfolge** werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen. Mögliche Werte: • *G.711 uLaw*: ISDN Codec nach US Kennlinie • *G.711 aLaw*: ISDN Codec nach EU Kennlinie • *G.722*: G.722 erfasst den Frequenzbereich von 50 Hz bis 7000 Hz mit einer Abtastrate von 16 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,5. • *G.729*: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • *G.726-40*: Komprimiert von 63 auf 40 KBit/s • *G.726-32*: Komprimiert von 55 auf 32 KBit/s • *G.726-24*: Komprimiert von 47 auf 24 KBit/s • *G.726-16*: Komprimiert von 39 auf 16 KBit/s • *RFC 2833*: Zuerst wird versucht RFC 2833 zu verwenden. Wenn die Gegenstelle diesen Standard nicht "beherrscht", wird SIP-Info verwendet. • *SRTP*: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP). • *Daten (RFC 4040)*: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. • *SIP-Info*: Zur Übertragung von DTMF-Ereignissen wird SIP-Info verwendet. • *T.38 Fax*: Ermöglicht den Versand von Faxmitteilungen über Datennetzwerke. Standardmäßig sind *G.711 uLaw*, *G.711 aLaw* und *G.729* aktiviert. Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs. Von diesen Codecs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	Wählen Sie aus, ob Echounterdrückung verwendet werden soll. Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Comfort Noise Generation (CNG)	Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll. Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Paketgröße	Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält. Zur Verfügung stehen Werte von *5* bis *500*. Der Standardwert ist *20*.

7.2.1.2 SIP-Konten

Wenn Sie Ihr Gerät an andere SIP-Server (z. B. Server von Internet SIP Service Providern) anbinden wollen, können Sie hier die notwendigen Einträge konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Client.

Außerdem können Sie hier die Einträge für SIP-Trunking-Szenarios konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Server für andere SIP-Server. Ein Beispiel hierfür ist die Anbindung einer SIP-PBX (z. B. Asterisk) an das Media Gateway.

Das bedeutet, dass sowohl alle SIP-Provider-Accounts hier konfiguriert werden als auch mit dem Media Gateway verbundene durchwahlfähige Telefonanlagen (Direct Dial-in).

Hinweis

Verwenden Sie dieses Menü auf keinen Fall zur Konfiguration von SIP-Nebenstellen, d.h. für SIP-Clients oder PSTN-Clients wie z. B. SIP-Telefone, Terminal Adapter oder ISDN-Telefone!

SIP-Nebenstellen können Sie im Menü **VoIP**->**Teilnehmer** konfigurieren.

Im Menü **VoIP**->**Einstellungen**->**SIP-Konten** wird eine Liste aller vorhandenen SIP-Konten (SIP Client Modus und SIP Server Modus) angezeigt.

7.2.1.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um neue SIP-Konten hinzuzufügen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. In diesem Menü werden sowohl SIP-Konten im SIP Client Modus als auch im SIP Server Modus konfiguriert.

Das Menü **VoIP**->**Einstellungen**->**SIP-Konten**-> ->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des SIP-Kontos ein.
Administrativer Status	Wählen Sie aus, ob das SIP-Konto aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Trunk-Modus	Wählen Sie aus, ob und in welchem Trunk-Modus das SIP-Konto betrieben werden soll. Durch den Trunk-Modus (DDI, Direct Dial In) wird ermöglicht, dass ein eingehender Ruf genau einem Endgerät zugeordnet werden kann (Durchwahl). Bei einem ausgehenden Ruf kann der Anrufer dem Angerufenen angezeigt werden. Welche Einstellung verwendet werden kann, hängt vom Provider ab. Mögliche Werte: • *Aus* (Standardwert): Der Trunk-Modus wird nicht verwendet. Das SIP-Konto hat nur eine Nummer. • *Client*: Das Media Gateway wird als DDI-Client betrieben. Es erhält eine Durchwahl. • *Server*: Das Media Gateway wird als DDI-Server betrieben, so daß sich DDI-Clients verbinden können. • *Gateway*: Das Media Gateway wird als DDI-Client betrieben, aber als Trunk verwendet. Diese Einstellung dient zum Anschluss einer softwarebasierten IP-Telefonanlage von Swyx.
Registrar	Nur für **Trunk-Modus** = *Aus*, *Client* und *Gateway*. Tragen Sie die IP-Adresse oder den Domänennamen (FQDN) des SIP Registrars ein. Maximale Zeichenzahl ist 40. Einträge mit Leerzeichen sind nicht erlaubt.
SIP-Endpunkt-IP-Adresse	Nur für **Trunk-Modus** = *Server* und **Registrierung** deaktiviert Tragen Sie die IP-Adresse oder den Domänennamen (FQDN) des SIP Proxy Servers ein.
Ausgehender Proxy	Nur für **Trunk-Modus** = *Aus*, *Client* oder *Gateway* Geben Sie den Namen oder die IP-Adresse des SIP Outbound Proxy Servers ein. Maximal können 32 Zeichen eingegeben werden. Hier müssen Sie nur dann einen Eintrag vornehmen, wenn bei allen SIP Sessions die Kommunikation nicht direkt sondern über einen weiteren Proxy erfolgen soll. Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dies explizit vom Provider vorgegeben wird.
Domäne / Realm	Tragen Sie einen weiteren Domänennamen oder eine weitere IP-Adresse des SIP Proxy Servers ein. Wenn Sie keine Angaben machen, wird der Eintrag im Feld **Registrar** verwendet.

Feld	Beschreibung
	Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dieser explizit vom Provider vorgegeben wird.
Protokoll	Wählen Sie das Protokoll aus, welches zum Datentransport verwendet werden soll. Mögliche Werte: • *UDP* (Standardwert) • *TCP* • *TLS* • *Automatisch* - Mit dieser Einstellung unterstützt Ihr Gerät eine automatische Aushandlung des Protokolls mit den Servern Ihres Anbieters. Damit diese Einstellung funktioniert, muss diese Aushandlung vom Anbieter ebenfalls unterstützt werden. Geben Sie den **Port** ein, über den die Daten transportiert werden sollen. Der Standardwert ist *5060*. Im SIP Client Modus: Die Ports können Provider-spezifisch sein. Wenn Sie für diesen Registrar anstelle einer DNS-Abfrage des A-Records eine Abfrage des SRV-Eintrags wünschen, tragen Sie hier den Port *0* ein. Für Anschlüsse der Deutschen Telekom ist dieser Eintrag notwendig, da über den SRV-Eintrag weitere Serveradressen bezogen werden, die ggf. eine bessere Dienstqualität zur Verfügung stellen können. SIP-Provider, die mit dem Schnellstart oder dem Telefonie-Assistenten erstellt werden, werden bereits mit der passenden Portnummer angelegt.
Benutzername	Im SIP Client Modus: Tragen Sie hier den Benutzernamen für die Authentifizierung ein, wenn Ihnen Ihr VoIP-Provider einen solchen zugewiesen hat. Im SIP Server Modus: Sie müssen den Benutzernamen festlegen. Maximal können 40 Zeichen eingegeben werden.
Authentifizierungs-ID	Tragen Sie einen Namen ein, der zur Authentifizierung beim Outbound Proxy verwendet wird. Wenn Sie keinen Namen eingeben, wird der Name im Feld **Benutzername** verwendet. Im SIP Client Modus: Tragen Sie nur dann einen Namen ein, wenn dieser explizit vom Provider vorgegeben wird.
Passwort	Im SIP Client Modus: Der VoIP-Provider weist Ihnen eine PIN bzw. Passwort für die Authentifizierung zu. Diesen Wert müssen Sie hier eingeben. Im SIP Server Modus: Legen Sie eine PIN bzw. ein Passwort fest. Maximal können 40 Zeichen eingegeben werden.
Art der Registrierung	Wählen Sie, wie die Registrierung und Authentifizierung bei einem Provider ausgeführt wird bzw. ob sie entfallen kann. Im letzten Fall werden die relevanten Daten an eine bestimmte IP-Adresse geschickt, die den Verbindungspartnern bereits bekannt ist. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP. Ist eine Registrierung erforderlich kann sie auf zwei Weisen erfolgen: • *Einzeln*: Bei dieser Option meldet wird jeweils eine MSN beim SIP-

Feld	Beschreibung
	Provider registriert. Dieser speichert die aktuelle Adresse des Clients und stellt diese Information für Anrufer zur Verfügung, denen die IP-Adresse des Angerufenen nicht unmittelbar bekannt ist. • *Bulk (BNC)*: Bei dieses Option wird ein SIP DDI (SIP Trunk) beim Provider registriert, d. h. es werden mehrere Rufnummern unter einer Adresse registriert.
Gültigkeit	Nur wenn **Registrierung** aktiviert ist. Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird. Zur Verfügung stehen Werte von *0* bis *38400*. Der Standardwert ist *600*. Ein Server kann in seiner Antwort auf eine REGISTER Anfrage eine andere Gültigkeit festlegen, welche die hier festgelegte überschreibt.
Angerufene Adresse	Legt fest, aus welchem Parameter der angerufenen Adresse die Rufnummer extrahiert wird. Mögliche Werte: • *Standard* (Standardwert): Extrahiert die Rufnummer aus dem ersten Teil der Adresse. Wenn dies fehlschlägt, wird die Rufnummer aus dem zweiten Teil der Adresse extrahiert. • *Anfrage-URI*: In einigen Anwendungsfällen (vor allem bei DDI-Verbindungen) muss die Zieladresse eines SIP-Rufs aus dem Request-URI des SIP Invites gelesen werden muss. Indem Sie diese Option aktivieren, wird die Adresse bevorzugt aus diesem Feld des Sip-Headers gelesen.
Quell-IP-Adresse überprüfen	Ihrem Gerät werden vom SIP-Provider als Antwort auf eine DNS-SRV-Anfrage die Adressen gültiger Registrierungsserver übermittelt. Wenn Sie diese Option aktivieren, wird bei jedem SIP Invite überprüft, ob er von einer der gültigen Adressen stammt. Ist das nicht der Fall, wird die Anfrage ignoriert. Standardmäßig ist die Funktion nicht aktiv.
Überprüfung des TLS-Zertifikats	Nur für DDI- / SIP-Trunk-Verbindungen. Wenn eine Verbindung über TLS (Transport Layer Security) verschlüsselt werden soll, wird das Serverzertifikat der Gegenstelle einer Gültigkeitsprüfung unterzogen, wenn diese Option aktiv ist. Standardmäßig ist die Funktion nicht aktiv.
RTP Dummy senden	Diese Option wird benötigt, wenn die Digitalisierungsbox an ein Gerät mit NAT angeschlossen wird, das den Internetanschluss Richtung SIP-Provider ermöglicht.

Felder im Menü Trunk-Einstellungen

Feld	Beschreibung
SIP-Header-Feld: FROM Display	Nich für **Trunk-Modus** = *Aus* Die Absender-ID wird im SIP Header im Feld "Display" übertragen. Mögliche Werte: • *Keiner* (Standardwert): Die Absender-ID wird nicht übertragen. • *Benutzername*: Der vom Benutzer konfigurierter Benutzername wird angezeigt. • *Anruferadresse*: Die vom Benutzer konfigurierte Rufnummer, die

Feld	Beschreibung
	dem Angerufenen angezeigt werden soll, wird angezeigt. • *Abrechnungsnummer*: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.
SIP-Header-Feld: FROM User	Nich für **Trunk-Modus** = *Aus* Die Absender-ID wird im SIP Header im Feld "User" übertragen. Mögliche Werte: • *Benutzername* (Standardwert): Der vom Benutzer konfigurierter Benutzername wird angezeigt. • *Anruferadresse*: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt. • *Abrechnungsnummer*: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.
SIP-Header-Feld: P-Preferred	Nich für **Trunk-Modus** = *Aus* Der SIP Header wird durch das sogenannte "p-preferred-identity" Feld erweitert, um dort die Absender-ID zu übertragen. Mögliche Werte: • *Keiner* (Standardwert): Die Absender-ID wird nicht übertragen. • *Benutzername*: Der vom Benutzer konfigurierter Benutzername wird angezeigt. • *Anruferadresse*: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt. • *Abrechnungsnummer*: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.
SIP-Header-Feld: P-Asserted	Nich für **Trunk-Modus** = *Aus* Der SIP Header wird durch das sogenannte "p-asserted-identity" Feld erweitert, um dort die Absender-ID zu übertragen. Mögliche Werte: • *Keiner* (Standardwert): Die Absender-ID wird nicht übertragen. • *Benutzername*: Der vom Benutzer konfigurierter Benutzername wird angezeigt. • *Anruferadresse*: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt. • *Abrechnungsnummer*: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.
Rufnummer	Nur für **Trunk-Modus** = *Client* oder *Server* Sie können eine Nummer setzen, die bei ausgehenden Rufen der Absenderrufnummer als Prefix vorangestellt wird und bei eingehenden Rufen von den führenden Stellen der Zielrufnummer abgeschnitten wird. Das entspricht der Rufnummer einer TK-Anlage.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur

Feld	Beschreibung
	Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw. Mögliche Werte: • *Standard* (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. • *Qualität*: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • *Geringe Bandbreite*: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • *Hohe Bandbreite*: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.

Felder im Menü Codecs

Feld	Beschreibung
Codecs	Wählen sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld **Codec-Reihenfolge** werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen. Mögliche Werte: • *G.711 uLaw*: ISDN Codec nach US Kennlinie • *G.711 aLaw*: ISDN Codec nach EU Kennlinie • *G.722*G.722 erfasst den Frequenzbereich von 50 Hz bis 7000 Hz mit einer Abtastrate von 16 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,5. • *G.729*: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • *G.726-40*: Komprimiert von 63 auf 40 KBit/s • *G.726-32*: Komprimiert von 55 auf 32 KBit/s • *G.726-24*: Komprimiert von 47 auf 24 KBit/s • *G.726-16*: Komprimiert von 39 auf 16 KBit/s Standardmäßig sind *G.711 uLaw*, *G.711 aLaw* und *G.729* aktiviert. Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs. Von diesen Codecs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.

Felder im Menü Optionen

Feld	Beschreibung
Optionen	Wählen sie die Option aus, die für die Verbindung verwendet werden sollen. Mögliche Werte: • *RFC 2833*: Zuerst wird versucht RFC 2833 zur Übertragung von DTMF-Ereignissen zu verwenden. Wenn die Gegenstelle diesen Standard nicht "beherrscht", wird SIP-Info verwendet. • *SRTP*: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP).

Feld	Beschreibung
	• *Daten (RFC 4040)*: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. • *SIP-Info*: Zur Übertragung von DTMF-Ereignissen wird SIP Info verwendet. • *T.38 Fax*: Ermöglicht den Versand von Faxmitteilungen über Datennetzwerke. • *SIP 302*: Wählen Sie aus, ob eine Anrufumleitung extern beim SIP-Provider durchgeführt wird. Der Anrufer wird mittels SIP-Status-Code 302 weitergeschaltet. • *MediaSec*: MediaSec handelt die Absicherung der RTP-Daten mit den SIP-Servern aus. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Für eine reibungslose Unterstützung muss eine automatische Aushandlung des Transportprotokolls erfolgen. Bei fest eingestellten Transportprotokollen (UDP und TCP) kann es zu Problemen bei der Registrierung kommen. Darüber hinaus muss die Verwendung von SRTP erlaubt sein. Ihr VoIP-Anbieter muss MediaSec unterstützen.

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	Wählen Sie aus, ob Echounterdrückung verwendet werden soll. Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Comfort Noise Generation (CNG)	Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll. Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Paketgröße	Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält. Zur Verfügung stehen Werte von *5* bis *500*. Der Standardwert ist *20*.

7.2.1.3 Standorte

Im Menü **VoIP**->**Einstellungen**->**Standorte** konfigurieren Sie die Standorte der VoIP-Teilnehmer, die auf Ihrem System konfiguriert sind, und definieren das Bandbreitenmanagement für den VoIP-Traffic.

Zur Verwendung des Bandbreitenmanagements können einzelne Standorte eingerichtet werden. Ein Standort wird anhand seiner festen IP-Adresse bzw. DynDNS-Adresse oder mittels der Schnittstelle, an der das Gerät angeschlossen ist, identifiziert. Für jeden Standort kann die verfügbare VoIP-Bandbreite

(Up- und Downstream) eingestellt werden.

Nur für Kompaktsysteme: Ein vordefinierter Eintrag mit den Parametern **Beschreibung** = *LAN*, **Beinhalteter Standort (Parent)** = *Keiner*, **Typ** = *Schnittstellen*, **Schnittstellen** = *LAN_EN1-0* wird angezeigt.

Felder im Menü Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

Feld	Beschreibung
Standardverhalten	Legen Sie fest, wie das System bei der Registrierung von VoIP-Teilnehmern verfahren soll, für die kein Standort definiert wurde. Mögliche Werte: • *Keine Registrierung*: Der VoIP-Teilnehmer wird nie registriert. • *Registrierung nur in privaten Netzwerken* (Standardwert): Der VoIP-Teilnehmer wird nur registriert, wenn er sich innerhalb des privaten Netzwerks befindet. • *Uneingeschränkte Registrierung*: Der VoIP-Teilnehmer wird immer registriert.

7.2.1.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Einträge hinzuzufügen.

Das Menü **VoIP**->**Einstellungen**->**Standorte**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung des Eintrags ein.
Enthaltener Standort (Parent)	Sie können die SIP-Standorte beliebig kaskadieren. Definieren Sie hier, welcher schon definierte SIP-Standort für den hier zu konfigurierenden SIP-Standort den übergeordneten Knoten bildet.
Typ	Wählen Sie aus, ob der Standort mittels IP-Adressen/DNS-Namen oder Schnittstellen definiert werden soll. Mögliche Werte: • *Adressen* (Standardwert): Der SIP-Standort wird über IP-Adressen bzw. DNS-Namen definiert. • *Schnittstellen*: Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.
Adressen	Nur für **Typ** = *Adressen* Geben Sie die IP-Adressen der Geräte an den SIP-Standorten ein. Klicken Sie auf **Hinzufügen** um neue Adressen zu konfigurieren. Geben Sie unter **IP-Adresse/DNS-Name** die gewünschte IP-Adresse bzw. den DNS-Namen ein. Geben Sie ebenfalls die erforderliche **Netzmaske** ein.
Schnittstellen	Nur für **Typ** = *Schnittstellen* Geben Sie die Schnittstellen an, an denen die Geräte eines SIP-Standorts angeschlossen sind. Klicken Sie auf **Hinzufügen**, um neue Schnittstelle auszuwählen.

Feld	Beschreibung
	Wählen Sie unter **Schnittstelle** die gewünschte Schnittstelle aus.
Bandbreitenbegrenzung Upstream	Legen Sie fest, ob die Upstream-Bandbreite begrenzt werden soll. Mit *Aktiviert* wird die Bandbreite reduziert. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upstream-Bandbreite	Geben Sie die maximale Datenrate in Senderichtung in kBits pro Sekunde ein.
Bandbreitenbegrenzung Downstream	Legen Sie fest, ob die Downstream-Bandbreite begrenzt werden soll. Mit *Aktiviert* wird die Bandbreite reduziert. Standardmäßig ist die Funktion nicht aktiv.
Maximale Downstream-Bandbreite	Geben Sie die maximale Datenrate in Empfangsrichtung in kBits pro Sekunde ein.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü DSCP

Feld	Beschreibung
DSCP-Einstellungen für RTP-Daten	Wählen Sie die Art des Dienstes für RTP-Daten aus (TOS, Type of Service). Mögliche Werte: • *DSCP-Binärwert* (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der vorkonfigurierte Wert ist *101110* • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.

7.2.1.4 ISDN-Trunks

Für die Konfiguration im Menü **ISDN-Trunks** muss Ihr Gerät über mindestens zwei ISDN-Anschlüsse im Punkt-zu-Punkt-Modus (BRI oder PRI) verfügen, die als TE (Sammelanschluss) oder NT konfiguriert sind.

Hinweis

Beachten Sie, dass bei BRI-Anschlüssen der Anschlussmodus (NT Mode oder TE Mode) per Jumper im Gerät umgeschaltet werden muss.

In diesem Menü werden ISDN-Sammelanschlüsse (Bundles) festgelegt.

7.2.1.4.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um einen neuen Sammelanschluss hinzuzufügen.

Das Menü **VoIP**->**Einstellungen**->**ISDN-Trunks** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Sammelanschlusses ein. Maximale Zeichenzahl ist 40.
ISDN-Modus	Wählen Sie den Modus aus, in welchem der Sammelanschluss betrieben wird. Mögliche Werte: • *Extern* (Standardwert): Punkt-zu-Punkt TE-Anschluss (Telekom Sammelanschluss) • *Trunk*: Punkt-zu-Punkt NT-Anschluss (für den Anschluss einer TK-Anlage).
Mitglieder	Wählen Sie die gewünschten ISDN-Schnittstellen aus, die zu diesem Sammelanschluss gehören sollen. Sie können diejenigen ISDN-Schnittstellen auswählen, die im Punkt-zu-Punkt-Modus konfiguriert sind.

7.2.1.5 Optionen

Im Menü **VoIP**->**Einstellungen**->**Optionen** können Sie globale Einstellungen für das Media Gateway vornehmen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Status des Media Gateways	Wählen Sie aus, ob die Funktion Media Gateway aktiviert sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Session Border Controller Modus	Wählen Sie aus, wie sich das Media Gateway in Verbindung mit einem Session Border Controller verhalten soll. Mögliche Werte: • *Auto* (Standardwert): Die Anrufkontrolle wird für alle Nebenstellen, die mit einem existierenden SIP-Konto exakt übereinstimmen, vom Session Border Controller durchgeführt, d.h. alle SIP-Meldungen, die für das entsprechende SIP-Konto konfiguriert sind, werden an den Session Border Controller weitergeleitet. Für alle anderen Nebenstellen wird die Anrufkontrolle vom Media Gateway entsprechend der unter **Anrufkontrolle** konfigurierten Einträge durchgeführt. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup). • *Aus*: Die Anrufkontrolle wird ausschließlich vom Media Gateway ent-

Feld	Beschreibung
	sprechend der unter **Anrufkontrolle** konfigurierten Einträge und der lokalen Nebenstellen durchgeführt. Für Rufe, die über einen bestimmten Provider (SIP-Konto) geroutet werden sollen, müssen Sie einen entsprechenden Anrufkontrolle-Eintrag konfigurieren. Interne Rufe (von interner Nebenstelle zu interner Nebenstelle), die nur lokal geroutet werden müssen, benötigen keinen zusätzlichen Anrufkontrolle-Eintrag. • *<SIP Trunk>*: Wählen Sie ein unter **VoIP**->**Media Gateway**->**SIP-Konten** konfiguriertes SIP Trunk Konto aus. Die Anrufkontolle wird in diesem Fall für alle Nebenstellen vom Session Border Controller ausgeführt, alle SIP-Meldungen werden an den Session Border Controller weitergeleitet. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup). Hinweis: Einträge in **Anrufkontrolle** haben Vorrang vor der Session Border Controller Konfiguration!
Anrufkontrolle für lokale Nummern	Legen Sie fest, ob Routing-Einträge vor Durchwahlnummern favorisiert werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Media Stream Termination	Wählen Sie aus, wie RTP-Sessions vom System kontrolliert werden sollen. Wenn die Funktion aktiv ist, werden die RTP-Sessions auf dem Media Gateway terminiert, d.h. alle RTP Streams werden vom Media Gateway kontrolliert und über das Media Gateway geroutet. Die beteiligten Endgeräte (z. B. SIP-Telefone) sind nicht direkt miteinander verbunden. Beachten Sie, dass das Media Gateway bei VoIP-zu-VoIP-Verbindungen unterschiedliche Codecs der beteiligten VoIP-Endgeräte nicht übersetzt. Daher müssen die Codecs von Media Gateway und VoIP-Endgeräten übereinstimmen. Wenn die Funktion nicht aktiv ist, werden die RTP-Sessions nicht auf dem Media Gateway terminiert, d.h. alle RTP Streams werden ohne Terminierung vom Media Gateway geroutet. Die RTP-Datenpakete können in komplexen Netzen somit auch über andere Gateways gerouted werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Standard-Abwurfnebenstelle	Sie können eine Nebenstelle angeben, zu der eingehende Telefonate geleitet werden, die keiner Extension oder angeschlossenen TK-Anlage zugeordnet werden können.
Wahlpause	Geben Sie die maximale Verzögerungszeit ein bis das System die eingegebene Telefonnummer als vollständig wertet und der SIP-Wählvorgang (Senden der SIP INVITE Message) startet. Diese Zeitspanne wird mit jedem Tastendruck zurückgesetzt. Mögliche Werte sind *0* bis *15*. Der Standardwert ist *5*. Wenn Sie die Rufnummer mit # abschließen, wird sofort gewählt.

Felder im Menü VoIP-Anbieter-Einstellungen

Feld	Beschreibung
DSCP-Einstellungen für SIP-Daten	Wählen Sie die Art des Dienstes für SIP-Daten aus (TOS, Type of Service). Mögliche Werte: • *DSCP-Binärwert* (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der Standardwert ist *110000*. • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
SIP Port	Geben Sie den Port an, über den die SIP-Daten geleitet werden sollen. Standardmäßig ist der Wert *5060* vorgegeben. **Hinweis** Falls Sie den Port im laufenden Betrieb ändern, wird die Änderung erst nach dem nächsten Neustart der Anlage wirksam.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
ISDN Anrufsignalisierung	Hier legen Sie für eine Telefonanlage, die an einer internen ISDN-Schnittstelle angeschlossen ist, fest, wie bei DDI mit der Teilnehmernummer verfahren wird. Für manche Telefonanlagen muss der Rufnummerntyp ermittelt werden und gegebenenfalls die Parameter **Internationaler Präfix / Länderkennzahl** und/oder **Nationaler Präfix / Ortsnetzkennzahl** von der Teilnehmernummer abgeschnitten werden, damit die Teilnehmernummer korrekt erkannt wird. Dies erreichen Sie mit der Einstellung *Spezifisch: International, National oder Teilnehmer*. Mögliche Werte: • *Standard: Immer als unbekannte Nummer*: Der Rufnummerntyp wird nicht ermittelt. • *Spezifisch: International, National oder Teilnehmer*: Der Rufnummerntyp wird ermittelt. Gegebenenfalls wird der Parameter **Internationaler Präfix / Länderkennzahl** und/oder der Parameter **Nationaler Präfix / Ortsnetzkennzahl** von der Teilnehmernummer abgeschnitten.
Kurzwahl	Definieren Sie kurze Ziffernfolgen, die anstatt der kompletten Nummer gewählt werden können.

Feld	Beschreibung
	Klicken Sie auf **Hinzufügen** um neue Kurzwahlen zu konfigurieren. Geben Sie unter **Abkürzung** die gewünschte Kurzwahl für den Benutzer ein, z. B. *123*. Geben Sie unter **Ersetzen durch** die Rufnummer ein, welche anstelle der Kurzwahl gewählt werden soll, z. B. *09119673*. Wenn in obigem Beispiel ein Benutzer **123* eintippt, wählt das Gerät *09119673*. Möchte der Benutzer die Nebenstelle *111* erreichen, so tippt er **123111* ein. Das Gerät wählt *09119673111*. Ein Punkt am Ende der Nummer zeigt eine komplette Nummer an. Diese wird nach dem Einsetzen sofort gewählt. Wenn Sie eine Kurzwahl aus der Liste nutzen wollen, müssen Sie * und dann die Kurzwahl wählen.

Felder im Menü SIP Dual Stack (IPv4/IPv6)

Feld	Beschreibung
SIP Dual Stack (IPv4/IPv6)	Aktivieren Sie die Option wenn IPv6 für VoIP aktiviert werden soll. Sowohl IPv4 als auch IPv6 werden verwendet. Falls ein VoIP-Provider IPv6 unterstützt, wird IPv6 bevorzugt. Unterstützt ein VoIP-Provider kein IPv6, wird IPv4 verwendet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Das bedeutet, das ausschließlich IPv4 verwendet wird.

7.2.2 Media Gateway

Ein Media Gateway dient als Übersetzungsinstanz zwischen verschiedenen Telekommunikationsnetzen wie z. B. zwischen dem herkömmlichen Telefonnetz und den Next Generation Networks (IP-Netzwerken).

Mit der **Digitalisierungsbox** Media Gateway kann ein Unternehmen, das mit einer durchwahlfähigen Telefonanlage an einem leitungsvermittelten Telefonnetz ausgestattet ist, mit einem SIP Trunking Service Provider im Internet verbunden werden und somit IP-Telefonie nutzen.

Die **Digitalisierungsbox** Media Gateway unterstützt die Anbindung mehrerer SIP Provider Accounts. Sie können mit diesem Gateway Nebenstellen einrichten, einen Rufnummernplan anlegen und Telefonanlagen-Funktionen konfigurieren sowie die Sprachdaten-Übertragung bei geringer Bandbreite der Upload-Verbindung optimieren.

7.2.2.1 Anrufkontrolle

Hier können Sie die Bedingungen für das Weiterleiten von Anrufen (Routing) festlegen. Sie legen hier eine Liste mit Regeln oder Regelketten fest, die dazu dienen, die signalisierte Zielrufnummer zu manipulieren.

Im Menü **VoIP**->**Media Gateway**->**Anrufkontrolle** wird eine Liste aller vorhandenen Einträge angezeigt.

7.2.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Einträge hinzuzufügen.

Das Menü **VoIP**->**Media Gateway**->**Anrufkontrolle**-> ->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.
Administrativer Status	Wählen Sie aus, ob derEintrag aktiv sein soll. Mit *Aktivieren* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Typ	Wählen Sie aus, wie der Ruf weitergeleitet werden soll. Mögliche Werte: • *Erlauben*: Für Rufe, die vom Media Gateway an eine Telefonanlage oder einen ISDN-TE-Anschluss oder einen SIP DDI Client weitergeleitet werden sollen. Dazu können verwendet werden: PRI-Schnittstellen im NT-Modus, BRI-Schnittstellen im NT-Modus, SIP-Konten im Trunk-Modus (Server Modus) . • *Verweigern*: Für Rufe, die nicht weitergeleitet (gesperrt) werden sollen.
Anrufende Leitung	Sie können die Anwendung des Eintrags auf die Leitung begrenzen, auf welcher der Ruf ankommt. Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab. Mögliche Werte: • *fxs<Schnittstellen-Index>*: Begrenzt den Eintrag auf die gewählte analoge Schnittstelle. • *bri<Schnittstellen-Index>*: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • *<SIP-Konto>*: Begrenzt den Eintrag auf das gewählte SIP-Konto. • *Beliebig*: Keine Begrenzung des Eintrags.
Anrufende Adresse	Sie können die Anwendung des Eintrags auf einen bestimmten Anrufer begrenzen. Dazu müssen Sie die Rufnummer exakt angeben (keine Wildcards).
Angerufene Adresse	Geben Sie die angerufene Adresse ein, auf die die Regel angewendet werden soll. Dazu geben Sie eine Adresse numerisch (z. B. eine Rufnummer) oder alphanumerisch (z. B. für einen Trunk) ein, die mit der gewählten Adresse verglichen wird. Dabei können Sie folgende Wildcards verwenden: • * bedeutet, dass am Ende einer Zeichenfolge beliebige weitere Zeichen folgen können. • ? dient als Platzhalter für ein beliebiges Zeichen. Wenn die konfigurierte Adresse mit der signalisierten Adresse übereinstimmt, wird der Eintrag angewandt.

Im Bereich **Routing-Regeln** definieren Sie Regeln, die bestimmen, wie die Rufnummer manipuliert wird, bevor sie für den Wahlvorgang verwendet wird.

Legen Sie weitere Einträge mit **Hinzufügen** an.

Felder im Menü Routing-Regeln (Nur für Typ = Erlauben)

Feld	Beschreibung
Priorität	Geben Sie eine ganze Zahl beginnend mit 1 in aufsteigender Reihenfolge ein, um die Reihenfolge der Filterregeln festzulegen. Die Regeln werden in der Liste in der angegebenen Reihenfolge "abgearbeitet". Ist eine Leitung bzw. ein SIP-Konto nicht verfügbar, wird automatisch die nächste Regel verwendet.
Administrativer Status	Wählen Sie aus, ob die Regel aktiv sein soll. Mit *Aktivieren* wird die Regel aktiv. Standardmäßig ist die Regel aktiv.
Leitung	Wählen Sie die Leitung für den ausgehenden Ruf aus.
Transformation der gerufenen Adresse	Geben Sie ein, wie die Rufnummer manipuliert werden soll, bevor sie für den Wahlvorgang verwendet wird. Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen sein. Mehrere Regeln können zu einer Regelkette zusammengefasst werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert. Numerische und alphanumerische Werte sind zulässig. ? dient als Platzhalter für ein beliebiges Zeichen. **Beispiel 7.1. Beispiel für eine Regel** • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

7.2.2.2 CLID-Umwandlung

Hier legen Sie die Bearbeitung der Rufnummer des Anrufers (Calling Party Number) bei eingehenden Anrufen fest. Sie können z. B. zu einer empfangenen Telefonnummer einen Prefix hinzufügen, um entsprechende ausgehende Gespräche über ein bestimmtes SIP-Konto zu routen.

Im Menü **VoIP**->**Media Gateway**->**CLID-Umwandlung** wird eine Liste aller vorhandenen Einträge angezeigt, bei denen die empfangene Rufnummer bearbeitet wird.

7.2.2.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Einträge für CLID-Umwandlung hinzuzufügen.

Das Menü **VoIP**->**Media Gateway**->**CLID-Umwandlung**-> ->  ->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.

Feld	Beschreibung
Rufnummer	Wählen Sie die ISDN-Leitung oder das SIP-Konto, von welcher bzw. von welchem der Anruf kommt. Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab. Mögliche Werte: • *fxs<Schnittstellen-Index>*: Begrenzt den Eintrag auf die gewählte analoge Schnittstelle. • *bri<Schnittstellen-Index>*: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • *<SIP-Konto>*: Begrenzt den Eintrag auf das gewählte SIP-Konto. • *Beliebig*: Keine Begrenzung des Eintrags.
Angerufene Leitung	Sie können optional die Zielleitung des Anrufs angeben. Mögliche Werte: • *fxs<Schnittstellen-Index>*: Begrenzt denEintrag auf die gewählte analoge Schnittstelle. • *bri<Schnittstellen-Index>*: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • *<SIP-Konto>*: Begrenzt den Eintrag auf das gewählte SIP-Konto. • *Beliebig*: Keine Begrenzung des Eintrags. Geben Sie entweder **Angerufene Leitung** oder **Angerufene Adresse** ein. Wird ein Wert gewählt, der nicht *Beliebig* ist, so sollte **Angerufene Adresse** nicht benutzt werden. Ist **Angerufene Leitung** = *Beliebig* gesetzt und wird **Angerufene Adresse** nicht benutzt, so werden alle Anrufe für **Angerufene Leitung** behandelt.
Angerufene Adresse	Sie können optional die Zieladresse des Anrufs angeben. Geben Sie entweder **Angerufene Leitung** oder **Angerufene Adresse** ein. Wird **Angerufene Adresse** benutzt, so sollte **Angerufene Leitung** = *Beliebig* gesetzt sein.
Transformation der rufenden Adresse	Geben Sie die Transformationsregel an, die auf die Rufnummer angewendet werden soll. Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen werden. Mehrere Regeln können zu einer Regelkette zusammengefaßt werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert. ? dient als Platzhalter für eine beliebige Ziffer. **Beispiel 7.2. Beispiel für eine Regel** • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

7.2.2.3 Rufnummerntransformation

Hier können Sie eine Liste zum Umsetzen von Rufnummern erstellen, d.h. in dieser Liste werden externe und interne Nummern einander zugeordnet.

Hinweis

Welche Rufnummer (Called Party Number oder Calling Party Number) umgesetzt wird, hängt von der Richtung (eingehend oder ausgehend) des jeweiligen Rufs ab. Bei eingehenden Rufen wird die Called Party Number, bei ausgehenden Rufen die Calling Party Number umgesetzt.

Sie können z. B. die interne Rufnummer 340 nach außen als 09119673900 darstellen oder einen Ruf von außen, der an die Nummer 09119673200 gehen soll, intern an die Nummer 340 weiterleiten.

Im Menü **VoIP**->**Media Gateway**->**Rufnummerntransformation** wird eine Liste vorhandenen Transformationen angezeigt.

7.2.2.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Einträge für Rufnummerntransformation hinzuzufügen.

Das Menü **VoIP**->**Media Gateway**->**Rufnummerntransformation**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen der Rufnummerntransformation ein.
Richtung	Wählen Sie die Rufrichtung für den Eintrag. Mögliche Werte: • *Beide* (Standardwert): Für eingehende und ausgehende Rufe (bidirektional). • *Eingehend*: Für eingehende Rufe. • *Ausgehend*: Für ausgehende Rufe.
Zugeordnete Leitung	Wählen Sie die ISDN-Leitung oder das SIP-Konto, über die bzw. über das Rufe geleitet werden sollen. Mögliche Werte: • *fxs<Schnittstellen-Index>*: Begrenzt den Ruf auf die gewählte analoge Schnittstelle. • *bri<Schnittstellen-Index>*: Begrenzt den Ruf auf die gewählte BRI-Schnittstelle. • *<SIP-Konto>*: Begrenzt den Ruf auf das gewählte SIP-Konto.
Lokale Adresse	Geben Sie die interne Rufnummer (z. B. Nummer einer Nebenstelle oder TK-Anlage) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld **Externe Adresse**) auf die **Lokale Adresse** umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld **Lokale Adresse**) auf die **Externe Adresse** umgesetzt. Numerische und alphanumerische Zeichen sind zulässig. *?* dient als Platzhalter für eine beliebige Ziffer.

Feld	Beschreibung
	Beachten Sie, dass **Lokale Adresse** und **Externe Adresse** dieselbe Anzahl von Wildcards enthalten müssen.
Externe Adresse	Geben Sie die externe Rufnummer (z. B. ISDN MSN oder die Rufnummer des SIP-Kontos) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld **Externe Adresse**) auf die **Lokale Adresse** umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld **Lokale Adresse**) auf die **Externe Adresse** umgesetzt. Das Feld **Externe Adresse** ist nicht sichtbar, wenn das Feld **Zugeordnete Leitung** = *<SIP-Konto>* gesetzt ist. Als **Externe Adresse** wird in diesem Fall wird der **Benutzername** des gewählten SIP-Kontos verwendet.

7.2.2.4 Sonderrufnummern

Bei ausgehenden Rufen erden die gerufenen Nummern an einem DDI-Anschluss in das internationale E.164-Format umgewandelt. Bei einigen Rufnummern ist diese Umwandlung aber unerwünscht. Diese Nummern können hier konfiguriert werden.

7.2.2.4.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Einträge hinzuzufügen.

Das Menü **VoIP**->**Media Gateway**->**Sonderrufnummern**->->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Sonderrufnummer	Geben Sie die Nummer ein, die von der E.164-Umwandlung ausgenommen werden soll.

Kapitel 8 WLAN

8.1 Wireless LAN

Bei Funk-LAN oder **Wireless LAN** (WLAN = Wireless Local Area Network) handelt es sich um den Aufbau eines Netzwerkes mittels Funktechnik.

Netzwerkfunktionen

Ein WLAN ermöglicht genauso wie ein kabelgebundenes Netzwerk alle wesentlichen Netzwerkfunktionen. Somit steht der Zugriff auf Server, Dateien, Drucker und Mailsystem genauso zuverlässig zur Verfügung wie der firmenweite Internetzugang. Da keine Verkabelung der Geräte nötig ist, hat ein WLAN den großen Vorteil, dass nicht auf bauliche Einschränkungen geachtet werden muss (d. h. der Gerätestandort ist unabhängig von der Position und der Zahl der Anschlüsse).

Derzeit gültiger Standard: IEEE 802.11. Informationen zu den in diesem Standard enthaltenen Modi und den damit erreichbaren Übertragungsgeschwindigkeiten finden Sie z. B. bei *Wikipedia.* Beachten Sie die Informationen zur Sicherheit und Konformität, die Ihrem Produkt beiliegen!

8.1.1 WLAN

Im Menü **Wireless LAN**->**WLAN** können Sie alle WLAN-Module Ihres Geräts konfigurieren.

Je nach Modellvariante sind ein oder zwei WLAN-Module, **WLAN** 1 und ggf. **WLAN** 2 verfügbar.

8.1.1.1 Funkmodul-Einstellungen

Im Menü **Wireless LAN**->**WLAN**->**Funkmodul-Einstellungen** wird eine Übersicht über Konfigurationsoptionen des WLAN-Moduls angezeigt.

8.1.1.1.1 **Funkmodul-Einstellungen**-> ✎

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie das Symbol ✎ um die Konfiguration zu bearbeiten.

Das Menü **Wireless LAN**->**WLAN**->**Funkmodul-Einstellungen**-> ✎ besteht aus folgenden Feldern:

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll. Mögliche Werte: • `Aus` (Standardwert): Das Funkmodul ist nicht aktiv. • `Access-Point`: Ihr Gerät dient als Access Point in Ihrem Netzwerk.
Frequenzband	Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus. Für **Betriebsmodus** = `Access-Point` Mögliche Werte: • `2,4 GHz In/Outdoor` (Standardwert): Ihr Gerät wird mit 2.4 GHz innerhalb oder außerhalb von Gebäuden betrieben. • `5 GHz Indoor`: Ihr Gerät wird mit 5 GHz innerhalb von Gebäuden be-

Feld	Beschreibung
	trieben. • *5 GHz Outdoor*: Ihr Gerät wird mit 5 GHz außerhalb von Gebäuden betrieben. • *5 GHz In/Outdoor*: Ihr Gerät wird mit 5 GHz innerhalb oder außerhalb von Gebäuden betrieben.
Kanal	Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate. **Access-Point-Modus:** Durch das Einstellen des Netzwerknamens (SSID) im Access-Point-Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens 4 Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt. Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden Clients diese Kanäle auch unterstützen. Mögliche Werte: • Für **Frequenzband** = *2,4 GHz In/Outdoor* Mögliche Werte sind *1* bis *13* und *Auto* (Standardwert). • Für **Frequenzband** = *5 GHz Indoor* Mögliche Werte sind *36*, *40*, *44*, *48* und *Auto* (Standardwert) • Für **Frequenzband** = *5 GHz In/Outdoor* und *5 GHz Outdoor* Hier ist nur die Option *Auto* möglich.
Sendeleistung	Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderabhängig. Mögliche Werte: • *Max.* (Standardwert): Die maximale Antennenleistung wird verwendet. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • 17 *dBm*

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	Wählen Sie die Wireless-Technologie aus, die der Access Point anwenden soll. Für **Betriebsmodus** = *Access-Point* und **Frequenzband** = *2,4 GHz In/Outdoo*

Feld	Beschreibung
	Mögliche Werte: • *802.11g*: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • *802.11b*: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • *802.11 mixed (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. • *802.11 mixed long (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind. • *802.11 mixed short (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • *802.11b/g/n*: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • *802.11g/n*: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. Für **Betriebsmodus** = *Access-Point* und **Frequenzband** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* Mögliche Werte: • *802.11a*: Ihr Gerät arbeitet ausschließlich nach 802.11a. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. • *802.11a/n*: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
Bandbreite	Für **Betriebsmodus** = *Access-Point* Nicht für **Frequenzband** = *2,4 GHz In/Outdoor* Wählen Sie aus, wie viele Kanäle verwendet werden sollen. Mögliche Werte: • *20 MHz* (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • *40 MHz*: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontroll-Kanal und der andere als Erweiterungs-Kanal .
Anzahl der Spatial Streams	Nicht für **Drahtloser Modus** = *802.11a* Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen. Mögliche Werte: • *2*: Zwei Datenströme werden verwendet. • *1*: Ein Datenstrom wird verwendet.
Airtime Fairness	Diese Funktion ist nicht für alle Geräte verfügbar. Mit der **Airtime Fairness** -Funktion wird gewährleistet, dass Senderessourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client

Feld	Beschreibung
	(z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen für Betriebsmodus = Access-Point

Feld	Beschreibung
Kanalplan	Nur für **Betriebsmodus** = *Access-Point* und **Kanal** = *Auto* Wählen Sie den gewünschten Kanalplan aus. Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d. h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen. Mögliche Werte: • *Alle*: Alle Kanäle können bei der Kanalwahl gewählt werden. • *Auto*: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • *Benutzerdefiniert*: Wählen Sie die gewünschten Kanäle selbst aus.
Ausgewählte Kanäle	Nur für **Kanalplan** = *Benutzerdefiniert* Hier werden die aktuell gewählten Kanäle angezeigt. Mit **Hinzufügen** können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen. Mithilfe von -Symbol können Sie Einträge löschen.
RTS Threshold	Hier wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll. Wählen Sie *Benutzerdefiniert* aus, können Sie in das Eingabefeld den Schwellwert in Bytes (1 - 2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet werden, indem die Werte *Immer aktiv* bzw. *Immer inaktiv* (Standardwert) ausgewählt werden.
Short Guard Interval	Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Fragmentation Threshold	Geben Sie die maximale Größe an, ab der Datenpakete fragmentiert (d. h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen emp-

Feld	Beschreibung
	fehlenswert. Möglich Werte sind *256* bis *2346*. Der Standardwert ist *2346* Bytes.

8.1.1.2 Drahtlosnetzwerke (VSS)

Wenn Sie Ihr Gerät im Access-Point-Modus betreiben (**Wireless LAN**->**WLAN**->**Einstellungen Funkmodul**-> ->**Betriebsmodus** = *Access-Point*), können Sie im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**->**Neu** die gewünschten Drahtlosnetzwerke Bearbeiten oder neue einrichten.

Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

- **Sicherheitsmodus** = *WPA-PSK*
- **WPA-Modus** = *WPA und WPA 2*
- **WPA Cipher** sowie **WPA2 Cipher** = *AES und TKIP*
- Der **Preshared Key** ist mit einem systeminternen Wert belegt, den Sie bei der Konfiguration abändern müssen.

Einstellen von Netzwerknamen

Im Gegensatz zu einem über Ethernet eingerichteten LAN verfügt ein Wireless LAN nicht über Kabelstränge, mit denen eine feste Verbindung zwischen Server und Clients hergestellt wird. Daher kann es bei unmittelbar benachbarten Funknetzen zu Störungen oder zu Zugriffsverletzungen kommen. Um dies zu verhindern, gibt es in jedem Funknetz einen Parameter, der das Netz eindeutig kennzeichnet und vergleichbar mit einem Domainnamen ist. Nur Clients, deren Netzwerk-Konfiguration mit der ihres Geräts übereinstimmt, können in diesem WLAN kommunizieren. Der entsprechende Parameter heißt Netzwerkname. Er wird im Netzwerkumfeld manchmal auch als SSID bezeichnet.

Absicherung von Funknetzwerken

Da im WLAN Daten über das Übertragungsmedium Luft gesendet werden, können diese theoretisch von jedem Angreifer, der über die entsprechenden Mittel verfügt, abgefangen und gelesen werden. Daher muss der Absicherung der Funkverbindung besondere Beachtung geschenkt werden.

Es gibt drei Sicherheitsstufen, WEP, WPA-PSK und WPA Enterprise. WPA Enterprise bietet die höchste Sicherheit, diese Sicherheitsstufe ist allerdings eher für Unternehmen interessant, da ein zentraler Authentisierungsserver benötigt wird. Privatanwender sollten WEP oder besser WPA-PSK mit erhöhter Sicherheit als Sicherheitsstufe auswählen.

WEP

802.11 definiert den Sicherheitsstandard **WEP** (Wired Equivalent Privacy = Verschlüsselung der Daten mit 40 Bit (**Sicherheitsmodus** = *WEP 40*) bzw. 104 Bit (**Sicherheitsmodus** = *WEP 104*). Das verbreitet genutzte **WEP** hat sich jedoch als anfällig herausgestellt. Ein höheres Maß an Sicherheit erreicht man jedoch nur durch zusätzlich zu konfigurierende, auf Hardware basierende Verschlüsselung (wie z. B. 3DES oder AES). Hierdurch können auch sensible Daten ohne Angst vor Datendiebstahl über die Funkstrecke übertragen werden.

IEEE 802.11i

Der Standard IEEE 802.11i für Wireless-Systeme beinhaltet grundsätzliche Sicherheitsspezifikationen für Funknetze, besonders im Hinblick auf Verschlüsselung. Er ersetzt das unsichere Verschlüsselungsverfahren **WEP** (Wired Equivalent Privacy) durch **WPA** (Wi-Fi Protected Zugriff). Zudem sieht er die Ver-

wendung des Advanced Encryption Standard (AES) zur Verschlüsselung von Daten vor.

WPA

WPA (Wi-Fi Protected Access) bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) über 802.1x (z. B. RADIUS) an.

Die Authentifizierung über EAP wird meist in großen Wireless-LAN-Installationen genutzt, da hierfür eine Authentifizierungsinstanz in Form eines Servers (z. B. eines RADIUS-Servers) benötigt wird. In kleineren Netzwerken, wie sie im SoHo (Small Office, Home Office) häufig vorkommen, werden meist PSKs (Pre-Shared-Keys) genutzt. Der entsprechende PSK muss somit allen Teilnehmern des Wireless LAN bekannt sein, da mit seiner Hilfe der Sitzungsschlüssel generiert wird.

WPA 2

Die Erweiterung von **WPA** ist **WPA 2**. In **WPA 2** wurde nicht nur der 802.11i-Standard erstmals vollständig umgesetzt, sondern es nutzt auch einen anderen Verschlüsselungsalgorithmus (AES, Advanced Encryption Standard).

Zugangskontrolle

Sie können kontrollieren, welche Clients über Ihr Gerät auf Ihr Wireless LAN zugreifen dürfen, indem Sie eine Access Control List anlegen (**Zugriffskontrolle** oder **MAC-Filter**). In der Access Control List tragen Sie die MAC-Adressen der Clients ein, die Zugriff auf Ihr Wireless LAN haben dürfen. Alle anderen Clients haben keinen Zugriff.

Sicherheitsmaßnahmen

Zur Absicherung der über das WLAN übertragenen Daten sollten Sie im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**->**Neu** gegebenenfalls folgende Konfigurationsschritte vornehmen:

- Ändern Sie die Zugangspasswörter Ihres Geräts.
- Ändern Sie die Standard-SSID, **Netzwerkname (SSID)** = *default*, Ihres Access Points. Setzen Sie **Sichtbar** = *Aktiviert*. Damit werden alle WLAN-Clients ausgeschlossen, die mit dem allgemeinen Wert für **Netzwerkname (SSID)** *Beliebig* einen Verbindungsaufbau versuchen und welche die eingestellten SSIDs nicht kennen.
- Nutzen Sie die zur Verfügung stehenden Verschlüsselungsmethoden. Wählen Sie dazu **Sicherheitsmodus** = *WEP 40*, *WEP 104*, *WPA-PSK* oder *WPA-Enterprise* und tragen Sie den entsprechenden Schlüssel im Access Point unter **WEP-Schlüssel 1 - 4** bzw. **Preshared Key** sowie in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmäßig geändert werden. Wechseln Sie dazu den **Übertragungsschlüssel**. Wählen Sie den längeren 104-Bit-WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevanten Informationen sollte der **Sicherheitsmodus** = *WPA-Enterprise* mit **WPA-Modus** = *WPA 2* konfiguriert werden. Diese Methode beinhaltet eine hardwarebasierte Verschlüsselung und RADIUS-Authentifizierung des Clients. In Sonderfällen ist auch eine Kombination mit IPSec möglich.
- Beschränken Sie den Zugriff im WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkkarten dieser Clients in die **Erlaubte Adressen**-Liste im Menü **MAC-Filter** ein (siehe *Felder im Menü MAC-Filter* auf Seite 95).

Im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)** wird eine Liste aller WLAN-Netzwerke angezeigt.

8.1.1.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Drahtlosnetzwerke zu konfigurieren.

Das Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**-> ->**Neu** besteht aus folgenden Feldern:

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	Geben Sie den Namen des Wireless Netzwerks (SSID) ein. Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein. Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** übertragen werden soll. Mit Auswahl von *Sichtbar* wird der Netzwerkname sichtbar übertragen. Standardmäßig ist er sichtbar.
Intra-cell Repeating	Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum Internet haben aber keinen Zugriff auf das Intranet der Firma. Um das zu verhindern, muss die Option deaktiviert sein.
U-APSD	Wählen Sie aus, ob der Stromsparmodus Unscheduled Automatic Power Save Delivery (U-APSD) aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den **Sicherheitsmodus** (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: • *Inaktiv* (Standardwert): Weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11i/TKIP
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 40* oder *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1-4	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für *WEP 40* benötigen Sie eine Zeichenfolge mit 5 Zeichen, für *WEP 104* mit 13 Zeichen.
WPA-Modus	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise*

Feld	Beschreibung
	Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: • *WPA und WPA 2* (Standardwert): **WPA und WPA 2** können angewendet werden. • *WPA*: Nur **WPA** wird angewendet. • *WPA 2*: Nur **WPA 2** wird angewendet.
WPA Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie **WPA** anwenden wollen. Mögliche Werte: • *AES* : AES wird angewendet. • *TKIP*: TKIP wird angewendet • *AES und TKIP* (Standardwert): AES oder TKIP werden angewendet.
WPA2 Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA 2* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie **WPA 2** anwenden wollen. Mögliche Werte: • *AES* : AES wird angewendet. • *AES und TKIP* (Standardwert): AES oder TKIP werden angewendet.
Preshared Key	Nur für **Sicherheitsmodus** = *WPA-PSK* Geben Sie das WPA-Passwort ein. Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein. **Hinweis** Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!
EAP-Vorabauthentifizierung	Nur für **Sicherheitsmodus** = *WPA-Enterprise* Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen. Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis. Mögliche Werte sind ganze Zahlen von *1* bis *254*. Der Standardwert ist *32*.
Max. Anzahl Clients - Soft Limit	Diese Funktion wird nicht von allen Geräten unterstützt. Um eine vollständie Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehent. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des **Max. Anzahl Clients - Hard Limit** werden Anfragen strikt abgelehnt. Der Wert der **Max. Anzahl Clients - Soft Limit** muss gleich oder kleiner sein als der **Max. Anzahl Clients - Hard Limit**. Der Standardwert ist *28*. Sie können diese Funktion deaktivieren, indem Sie **Max. Anzahl Clients - Soft Limit** und **Max. Anzahl Clients - Hard Limit** auf den gleichen Wert einstellen.
Auswahl des Client-Bands	Diese Funktion wird nicht von allen Geräten unterstützt. Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist. Die Option **Auswahl des Client-Bands** ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht. Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming*(Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • *2,4-GHz-Band bevorzugt*: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • *5-GHz-Band bevorzugt*: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	Wählen Sie aus, ob für dieses Wireless Netzwerk nur bestimmte Clients zugelassen werden sollen.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Erlaubte Adressen	Nur bei **Zugriffskontrolle** = *Aktiviert* Legen Sie Einträge mit **Hinzufügen** an und geben Sie die MAC-Adressen der Clients (**MAC-Adresse**) ein, die zugelassen werden sollen.

Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung. Mögliche Werte sind • *Keine Begrenzung* (Standardwert) • *0,25 Mbit/s*, *0,5 Mbit/s*, *1 Mbit/s* bis *10 Mbit/s* in Einerschritten, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* und *50 Mbit/s*.
Tx Shaping	Wählen Sie die Begrenzung der Bandbreite in Senderichtung. Mögliche Werte sind • *Keine Begrenzung* (Standardwert) • *0,25 Mbit/s*, *0,5 Mbit/s*, *1 Mbit/s* bis *10 Mbit/s* in Einerschritten, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* und *50 Mbit/s*.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DTIM Period	Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an. Das DTIM-Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *2*.
IGMP Snooping	IGMP Snooping reduziert den Datenverkehr und damit die Netzlast, weil Multicast Pakete aus dem LAN nicht weitergeleitet werden. Es werden ausschließlich Multicast-Pakete weitergeleitet, die von den entsprechenden Clients angefordert werden. Wenn Sie IGMP Snooping aktivieren, gibt IGMP Snooping daher den Rahmen vor, in dem Multicast angewendet wird. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

8.1.2 Verwaltung

Das Menü **Wireless LAN**->**Verwaltung** enthält grundlegende Einstellungen, um Ihr Gateway als Access Point (AP) zu betreiben.

8.1.2.1 Einstellungen

Das Menü **Wireless LAN**->**Verwaltung**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü WLAN Administration

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Access Point betrieben werden soll. Mögliche Werte sind alle auf dem Wireless-Modul des Geräts vorkonfigurierten Länder. Der Bereich der auswählbaren Kanäle (**Kanal** im Menü **Wireless LAN**->**WLAN**->**Einstellungen Funkmodul**) variiert je nach Ländereinstellung. Der Standardwert ist `Germany`.

8.2 Wireless LAN Controller

Mit dem Wireless LAN Controller können Sie eine WLAN-Infrastruktur mit mehreren Access Points (APs) aufbauen und verwalten. Der WLAN Controller verfügt über einen Wizard, der Sie bei der Konfiguration Ihrer Access Points unterstützt. Das System nutzt das CAPWAP-Protokoll (Control and Provisioning of Wireless Access Points Protocol) für die Kommunikation zwischen Master und Slaves.

Sobald der Controller alle APs in seinem System "gefunden" hat, bekommen diese nacheinander jeweils ein neues Passwort und eine neue Konfiguration, d.h. sie werden über den WLAN Controller verwaltet und sind nicht mehr von "außen" manipulierbar.

Mit dem **WLAN Controller** können Sie im einzelnen

- Access Points (APs) automatisch erkennen und zu einem WLAN vernetzen
- Eine Systemsoftware in die APs laden
- Eine Konfiguration in die APs laden
- APs überwachen und verwalten.

Die Anzahl der APs, die Sie mit dem Wireless LAN Controller Ihres Gateways verwalten können, sowie die Information über die notwendigen Lizenzen entnehmen Sie bitte dem Datenblatt Ihres Gateways.

8.2.1 Wizard

Das Menü **Wizard** bietet eine Schritt-für-Schritt-Anleitung für das Einrichten einer WLAN-Infrastruktur. Der Wizard führt Sie durch die Konfiguration.

Hinweis

Wir empfehlen Ihnen, den Wizard auf jeden Fall bei der Erstkonfiguration Ihrer WLAN-Infrastruktur zu verwenden.

8.2.1.1 Wireless LAN Controller Wizard

Sie können hier alle Einstellungen konfigurieren, die Sie für den eigentlichen Wireless LAN Controller benötigen.

8.2.1.1.1 Einstellungen

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

Wählen Sie das Land, in welchem der Wireless Controller betrieben werden soll.

Hinweis: Der Bereich der verwendbaren Kanäle variiert je nach Ländereinstellung.

Schnittstelle

Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.

DHCP-Server

Wählen Sie aus, ob ein externer DHCP-Server die IP-Adressen an die APs vergeben soll bzw. ob Sie selbst feste IP-Adressen vergeben wollen. Alternativ können Sie Ihr Gerät als DHCP-Server verwenden. Bei diesem internen DHCP-Server ist die CAPWAP Option 138 aktiv, um die Kommunikation zwischen Master und Slaves zu ermöglichen.

Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** im Feld **Manuelle IP-Adresse des WLAN-Controller** eintragen.

Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist.

Wenn Sie z. B. ein **Digitalisierungsbox** Gateway als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**->**Erweiterte Einstellungen** im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen**. Wählen Sie als **Option** *CAPWAP Controller* und tragen Sie im Feld **Wert** die IP-Adresse des WLAN Controllers ein.

IP-Adressbereich

Wenn die IP-Adressen intern vergeben werden sollen, müssen Sie die Anfangs-und End-IP-Adresse des gewünschten Bereiches eingeben.

Hinweis: Wenn Sie auf **Weiter** klicken, erscheint eine Warnung, dass beim Fortfahren die Wireless-LAN-Controller-Konfiguration überschrieben wird. Mit Klicken auf **OK** sind Sie einverstanden und fahren mit der Konfiguration fort.

8.2.1.1.2 Funkmodulprofil

Wählen Sie aus, welches Frequenzband Ihr WLAN Controller verwenden soll.

Mit der Einstellung *2.4 GHz Radio Profile* wird das 2.4-GHz-Frequenzband verwendet.

Mit der Einstellung *5 GHz Radio Profile* wird das 5-GHz-Frequenzband verwendet.

Wenn das entsprechende Gerät zwei Funkmodule enthält, können Sie **Zwei unabhängige Funkmodulprofile verwenden**. Modul 1 wird dadurch das *2.4 GHz Radio Profile* zugeordnet, Modul 2 das *5 GHz Radio Profile* .

Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Standardmäßig ist die Funktion nicht aktiv.

8.2.1.1.3 Drahtlosnetzwerk

In der Liste werden alle konfigurierten Drahtlosnetzwerke (VSS) angezeigt. Es ist mindestens ein Drahtlosnetzwerk (VSS) angelegt. Dieser Eintrag kann nicht gelöscht werden.

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

Mithilfe von -Symbol können Sie Einträge löschen.

Mit **Hinzufügen** können Sie neue Einträge anlegen. Für ein Funkmodul können Sie bis zu acht Drahtlosnetzwerke (VSS) anlegen.

Hinweis

Wenn Sie das standardmäßig angelegte Drahtlosnetzwerk verwenden wollen, müssen Sie mindestens den Parameter **Preshared Key** ändern. Andernfalls erscheint eine Aufforderung.

8.2.1.1.3.1 Drahtlosnetzwerke ändern oder hinzufügen

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

Mit **Hinzufügen** können Sie neue Einträge anlegen.

Folgende Parameter stehen zur Verfügung

Netzwerkname (SSID)

Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.

Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.

Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** *Sichtbar* übertragen werden soll.

IGMP Snooping

IGMP Snooping reduziert den Datenverkehr und damit die Netzlast, weil Multicast Pakete aus dem LAN nicht weitergeleitet werden. Es werden ausschließlich Multicast-Pakete weitergeleitet, die von den entsprechenden Clients angefordert werden. Wenn Sie IGMP Snooping aktivieren, gibt IGMP Snooping daher den Rahmen vor, in dem Multicast angewendet wird.

Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Standardmäßig ist die Funktion aktiv.

Sicherheitsmodus

Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.

Hinweis: *WPA-Enterprise* bedeutet 802.11x.

WPA-Modus

Wählen Sie für **Sicherheitsmodus** = *WPA-PSK* oder *WPA-Enterprise* aus, ob Sie WPA oder WPA 2 oder beides anwenden wollen.

Preshared Key

Geben Sie für **Sicherheitsmodus** = *WPA-PSK* das WPA-Passwort ein.

Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.

Wichtig

Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!

RADIUS-Server

Sie können den Zugang zu einem Drahtlosnetzwerk über einen RADIUS-Server regeln.

Mit **Hinzufügen** können Sie neue Einträge anlegen.

Geben Sie die IP-Adresse und das Passwort des gewünschten RADIUS-Servers ein.

EAP-Vorabauthentifizierung

Wählen Sie für **Sicherheitsmodus** = *WPA-Enterprise* aus, ob EAP-Vorabauthentifizierung *Aktiviert* werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden.

VLAN

Wählen Sie aus, ob für dieses Drahtlosnetzwerk VLAN-Segmentierung verwendet werden soll.

Wenn Sie VLAN-Segmentierung verwenden wollen, geben Sie in das Eingabefeld einen Zahlenwert zwischen *2* und *4094* ein, um das VLAN zu identifizieren (VLAN ID *1* ist nicht möglich!).

Hinweis

Bevor Sie fortfahren, stellen Sie sicher, dass alle Access Points, die der WLAN Controller verwalten soll, korrekt verkabelt und eingeschaltet sind.

8.2.1.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

Wenn Sie die Einstellungen eines gefundenen APs ändern wollen, klicken Sie im entsprechenden Eintrag auf .

Sie sehen die Einstellungen des gewählten Access Points. Sie können diese Einstellungen ändern.

Folgende Parameter stehen im Menü **Access-Point-Einstellungen** zur Verfügung:

Standort

Zeigt den angegebenen Standort des APs. Sie können einen anderen Standort eingeben.

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

(Wenn der AP über zwei Funkmodule verfügt, werden die Abschnitte Funkmodul 1 und Funkmodul 2 angezeigt.)

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

- *Ein* (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk.
- *Aus*: Das Funkmodul ist nicht aktiv.

Aktives Funkmodulprofil

Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.

Kanal

Zeigt den zugewiesenen Kanal. Sie können einen alternativen Kanal wählen.

Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.

Hinweis

Durch das Einstellen des Netzwerknamens (SSID) im Access-Point-Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens vier Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.

Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden APs diese Kanäle unterstützen.

Sendeleistung

Zeigt die Sendeleistung in dBm. Sie können eine andere Sendeleistung wählen.

Mit **OK** übernehmen Sie die Einstellungen.

Wählen Sie die Access Points, welche der WLAN Controller verwalten soll. Klicken Sie dazu in der Spalte **Manage** auf die gewünschten Einträge oder klicken Sie auf **Alle auswählen**, um alle Einträge auszuwählen. Klicken Sie auf die Schaltfläche **Alle deaktivieren**, um alle Einträge zu deaktivieren und danach bei Bedarf einzelne Einträge auszuwählen (z. B. bei großen Listen).

Klicken Sie auf **Start**, um das WLAN zu installieren und die Frequenzen automatisch zuordnen zu lassen.

Hinweis

Falls nicht genügend Lizenzen zur Verfügung stehen, erscheint die Meldung "Die maximale Anzahl der verwaltbaren Slave Access Points wird überschritten. Bitte überprüfen Sie Ihre Lizenzen!" Wenn diese Meldung angezeigt wird, sollten Sie gegebenenfalls zusätzliche Lizenzen erwerben.

Während der Installation des WLANs und der Zuordnung der Frequenzen sehen Sie an den angezeigten Meldungen, wie weit die Installation fortgeschritten ist. Die Anzeige wird laufend aktualisiert.

Sobald für alle Access Points überlappungsfreie Funkkanäle gefunden sind, wird die Konfiguration, die im Wizard festgelegt ist, an die Access Points übertragen.

Wenn die Installation abgeschlossen ist, sehen Sie eine Liste der **Managed** Access Points.

Klicken Sie unter **Benachrichtigungsdienst für WLAN-Überwachung konfigurieren** auf **Start**, um Ihre Managed APs überwachen zu lassen. Zur Konfiguration werden Sie in das Menü **Externe Berichterstellung**->**Benachrichtigungsdienst**->**Benachrichtigungsempfänger** mit der Voreinstellung **Ereignis** = *Verwalteter AP offline* geleitet. Sie können festlegen, dass Sie mittels E-Mail informiert werden, wenn das Ereignis *Verwalteter AP offline* eintritt.

Klicken Sie unter **Benachbarte APs neu scannen** auf **Start**, um benachbarte APs erneut zu scannen. Sie erhalten eine Warnung, dass dazu die Funkmodule der Access Points für eine bestimmte Zeitspanne deaktiviert werden müssen. Wenn Sie den Vorgang mit **OK** starten, wird ein Fortschrittsbalken angezeigt. Die Anzeige der gefundenen APs wird alle zehn Sekunden aktualisiert.

8.2.1.2 Wireless LAN Controller VLAN-Konfiguration

Um WLANs (VSS) voneinander zu trennen, können Sie bei der Konfiguration eines VSS die Funktion VLAN aktivieren und eine VLAN-ID vergeben. Damit die Trennung von anderen Schnittstellen wirksam ist, müssen Sie für dieses VLAN eine virtuelle Schnittstelle mit einer eigenen IP-Konfiguration anlegen und ggf. einen DHCP Pool erstellen, aus dem Clients innerhalb dieses VLANs mit IP-Adressen versorgt werden. Sie können diese Einstellungen wie bisher in den Menüs **LAN**->**IP-Konfiguration** bzw. **Lokale Dienste**->**DHCP Server** vornehmen oder das hier angebotene Menü nutzen. Einstellungen, die Sie hier vornehmen, werden automatisch in die anderen Menüs übernommen.

Sie sehen eine Übersicht der bisher angelegten VLANs mit ihren IDs und der jeweils zugeordneten IP- bzw. DHCP-Konfiguration. Um einen Eintrag zu bearbeiten, wählen Sie das Symbol in der entsprechenden Zeile, um einen neuen Eintrag hinzuzufügen, klicken Sie auf **Neu**. Einen neuen Eintrag können Sie nur für ein VSS mit einer VLAN-ID erstellen, das noch keine VLAN-Konfiguration hat.

8.2.1.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere VLANs zu konfigurieren.

Das Menü **Wireless LAN Controller**->**Wizard**->**Wireless LAN Controller VLAN-Konfiguration**->**Neu** besteht aus folgenden Feldern:

Felder im Menü VSS VLAN Netzwerkonfiguration

Feld	Beschreibung
VLAN-ID	Wählen Sie eine der existierenden VLAN-IDs aus dem Auswahlmenü. Es werden nur IDs angezeigt, für die noch keine Konfiguration vorliegt.
IP-Adresse/Netzmaske	Geben Sie hier die IP-Konfiguration der neuen Schnittstelle ein. Achten Sie darauf, dass diese noch nicht verwendet worden ist.
DHCP-Server	Um Clients, die sich mit diesem VLAN verbinden, eine IP-Konfiguration zuzuweisen, können Sie einen externen oder den internen DHCP-Server Ihres Geräts verwenden. Mögliche Werte: • *Extern oder statisch*: Verwenden Sie diese Option, wenn Sie in Ihrem Netzwerk bereits einen DHCP-Server betreiben oder die Clients, die sich mit den VLAN verbinden, eine statische IP-Konfiguration haben. Achten Sie darauf, dass ein externer DHCP-Server aus dem Netzwerk des VLAN erreichbar ist. • *Intern*: Verwenden Sie diese Option, wenn Sie Ihr Gerät als DHCP-Server für das VLAN einsetzen wollen.
IP-Adressbereich	Nur bei **DHCP-Server** = *Intern* Geben Sie hier die erste und die letzte IP-Adresse ein, die Ihr Gerät innerhalb des VLAN vergeben soll. Achten Sie darauf, dass der Adressraum zur IP-Adresse der Schnittstelle dieses VLAN passt und sich nicht mit anderen IP-Adress-Pools überschneidet. Für die DHCP-Konfiguration wird automatisch Ihr Gerät als Gateway eingetragen, die Lease Time beträgt 120 Minuten. Wenn Sie diese Einstellungen anpassen wollen, gehen Sie in das Menü **Lokale Dienste**->**DHCP Server**->**DHCP-Konfiguration**.

8.2.2 Controller-Konfiguration

In diesem Menü nehmen Sie die Grundeinstellungen für den Wireless LAN Controller vor.

8.2.2.1 Allgemein

Das Menü **Wireless LAN Controller**->**Controller-Konfiguration**->**Allgemein** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Status	Aktivieren Sie die Funktion, um die Grundeinstellungen für den Wireless LAN Controller vorzunehmen.

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Wireless LAN Controller betrieben werden soll. Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder. Der Bereich der verwendbaren Kanäle variiert je nach Ländereinstellung. Der Standardwert ist *Germany*.
Schnittstelle	Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.
DHCP-Server	Wählen Sie aus, ob ein externer DHCP-Server die IP-Adressen an die APs vergeben soll bzw. ob Sie selbst feste IP-Adressen vergeben wollen. Alternativ können Sie Ihr Gerät als DHCP-Server verwenden. Bei diesem internen DHCP-Server ist die CAPWAP Option 138 aktiv, um die Kommunikation zwischen Master und Slaves zu ermöglichen. Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist. Wenn Sie z. B. eine **Digitalisierungsbox** als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**->**Erweiterte Einstellungen** im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen**. Wählen Sie als **Option** *CAPWAP Controller* und tragen Sie im Feld **Wert** die IP-Adresse des WLAN Controllers ein. Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** im Feld **Manuelle IP-Adresse des WLAN-Controller** eintragen. Mögliche Werte: • *Extern oder statisch* (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs. • *Intern*: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	Nur für **DHCP-Server** = *Intern* Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.
Slave-AP-Standort	Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden. Mögliche Werte: • *Lokal (LAN)* (Standardwert) • *Entfernt (WAN)* Die Einstellung *Entfernt (WAN)* ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die APs über VPN angebunden sind, kann es vorkommen, dass eine Verbindung unterbrochen wird. In diesem Fall behält der entsprechende AP mit der Einstellung *Entfernt (WAN)* seine Konfiguration bis die Verbindung wieder hergestellt ist. Da-

Feld	Beschreibung
	nach bootet er und anschließend synchronisieren sich Controller und AP erneut.
Slave-AP-LED-Modus	Wählen Sie das Leuchtverhalten der Slave-AP-LEDs. Mögliche Werte: • *Status* (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • *Blinkend*: Die LEDs zeigen ihr Standardverhalten. • *Aus*: Alle LEDs sind deaktiviert.

8.2.2.2 Slave-AP-Autoprofil

Der Wireless LAN Controller bietet die Möglichkeit, Access Points, die in das ihm zugängliche Netz integriert werden, automatisch in die Verwaltung zu übernehmen und zu konfigurieren. Um einem neuen Access Point automatisch eine Konfiguration zuweisen zu können, erstellen Sie in diesem Menü ein Profil, das für alle neu zu verwaltenden Access Points Gültigkeit hat, auf die bestimmte Kriterien zutreffen.

8.2.2.2.1 Bearbeiten oder Neu

Das Menü **Wireless LAN Controller**->**Controller-Konfiguration**->**Slave-AP-Autoprofil**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Access-Point-Filter

Feld	Beschreibung
MAC-Adresse	Geben Sie die MAC-Adresse eines Access Points ein, der bei seiner Integration in das Netzwerk automatisch konfiguriert werden soll. Standardmäßig ist **Alle** aktiviert, so dass der Eintrag auf jeden neu hinzukommenden Access Point zutrifft.
IP-Adresse/Netzmaske	Geben Sie eine IP-Adresse und eine Netzmaske ein. Sie können hier Host- ebenso wie auch Netzwerkadressen angeben und so einzelne Access Points ebenso herausfiltern wie auch Gruppen von Access Points in einem Subnetz.

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Standort	Geben Sie den Standort des APs an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für den AP ein.

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	Wählen Sie aus, ob der Betriebsmodus vom verwendeten Funkmodulprofil bestimmt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Aktives Funkmodulprofil	Nur für **Betriebsmodus** = *Aktiviert* Wählen Sie ein Funkmodulprofil aus. Mögliche Werte: • *2.4 GHz Radio Profile* • *5 GHz Radio Profile*

Feld	Beschreibung
Zugewiesene Drahtlos-netzwerke (VSS)	Nur für **Betriebsmodus** = *Aktiviert* Fügen Sie mit **Hinzufügen** ein Drahtlosnetzwerk hinzu.

8.2.3 Slave-AP-Konfiguration

In diesem Menü finden Sie alle Einstellungen, die Sie zur Verwaltung der Slave Access Points benötigen.

8.2.3.1 Slave Access Points

Im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Slave Access Points** wird eine Liste aller mit Hilfe des Wizards gefundenen APs angezeigt.

Für jeden Access Point sehen Sie einen Eintrag mit einem Parametersatz (**Standort**, **Name**, **IP-Adresse**, **LAN-MAC-Adresse**, **Kanal**, **Kanalsuche**, **Status**, **Aktion**). Durch Klicken auf die ⌃-Schaltfläche oder der ⌄-Schaltfläche in der Spalte **Aktion** wählen Sie aus, ob der gewählte Access Point vom WLAN Controller verwaltet werden soll.

Sie können den Access Point vom WLAN Controller trennen und ihn somit aus Ihrer WLAN-Infrastruktur entfernen, indem Sie auf die ⌄-Schaltfläche klicken. Der Access Point bekommt dann den Status *Gefunden*, aber nicht mehr *Managed*.

Klicken Sie unter **Neue Kanalfestlegung** auf die Schaltfläche **START**, um die zugewiesenen Kanäle erneut zuzuweisen, z. B. wenn ein neuer Access Point hinzugekommen ist.

Mögliche Werte für Status

Status	Bedeutung
Gefunden	Der AP hat sich beim Wireless LAN Controller gemeldet. Der Controller hat die Systemparameter vom AP abgefragt.
Initialisiere	Der WLAN Controller und die APs "verständigen sich" über CAPWAP. Die Konfiguration wird an die APs übertragen und aktiviert.
Managed	Der AP ist auf den Status Managed gesetzt. Der Controller hat eine Konfiguration zum AP geschickt und diese aktiviert. Der AP wird vom Controller zentral verwaltet und kann nicht über das **GUI** konfiguriert werden.
Keine Lizenz vorhanden	Der WLAN Controller verfügt über keine freie Lizenz für diesen AP.
Aus	Der AP ist entweder administrativ deaktiviert oder ausgeschaltet bzw. ohne Stromversorgung o.ä.

8.2.3.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Mithilfe von -Symbol können Sie Einträge löschen. Wenn Sie APs gelöscht haben, werden diese erneut gefunden, jedoch ohne Konfiguration.

Im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Slave Access Points**-> werden die Daten für Funkmodul 1 und Funkmodul 2 angezeigt, wenn der entsprechende Access Point über zwei Funkmodule verfügt. Bei Geräten, die mit einem einzigen Funkmodul bestückt sind, werden die Daten für Funkmodul 1 angezeigt.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.

Feld	Beschreibung
Standort	Zeigt den Standort des APs. Wenn kein Standort angegeben ist, werden die Standorte nummeriert. Sie können einen anderen Standort eingeben.
Name	Zeigt den Namen des APs. Sie können den Namen ändern.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den AP ein.
CAPWAP-Verschlüsselung	Wählen Sie aus, ob die Kommunikation zwischen Master und Slaves verschlüsselt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Sie können die Verschlüsselung aufheben, um die Kommunikation zu Debug-Zwecken einzusehen.

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	Zeigt, in welchem Modus das Funkmodul betrieben werden soll. Sie können den Modus ändern. Mögliche Werte: • *Ein* (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk. • *Aus*: Das Funkmodul ist nicht aktiv.
Aktives Funkmodulprofil	Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.
Kanal	Zeigt den zugewiesenen Kanal. Sie können einen anderen Kanal wählen. Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate. Access Point Modus Durch das Einstellen des Netzwerknamens (SSID) im Access Point Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens vier Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt. Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden APs diese Kanäle auch unterstützen. Mögliche Werte (entsprechend dem gewählten Funkmodulprofil): • Für **Aktives Funkmodulprofil** = *2,4 GHz Radio Profile* Mögliche Werte sind *1* bis *13* und *Auto* (Standardwert). • Für **Aktives Funkmodulprofil** = *5 GHz Radio Profile* Mögliche Werte sind *36*, *40*, *44*, *48* und *Auto* (Standardwert)
Verwendeter Kanal	Nur für Managed APs.

Feld	Beschreibung
	Zeigt den aktuell benutzten Kanal.
Sendeleistung	Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen. Mögliche Werte: • *Max.* (Standardwert): Die maximale Antennenleistung wird verwendet. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*
Zugewiesene Drahtlos-netzwerke (VSS)	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

8.2.3.2 Funkmodulprofile

Im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Funkmodulprofile** wird eine Übersicht aller angelegten Funkmodulprofile angezeigt. Ein Profil mit 2.4 GHz und ein Profil mit 5 GHz sind standardmäßig angelegt, das 2.4-GHz-Profil kann nicht gelöscht werden.

Für jedes Funkmodulprofil sehen Sie einen Eintrag mit einem Parametersatz (**Funkmodulprofile**, **Konfigurierte Funkmodule**, **Frequenzband**, **Drahtloser Modus**).

8.2.3.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Funkmodulprofile anzulegen.

Das Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Funkmodulprofile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Funkmodulprofil-Konfiguration

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung des Funkmodulprofils ein.
Betriebsmodus	Legen Sie fest, in welchem Modus das Funkmodulpofil betrieben werden soll. Mögliche Werte: • *Aus* (Standardwert): Das Funkmodulprofil ist nicht aktiv. • *Access-Point*: Ihr Gerät dient als Access Point in Ihrem Netzwerk.
Frequenzband	Wählen Sie das Frequenzband des Funkmodulprofils aus. Mögliche Werte: • *2,4 GHz In/Outdoor* (Standardwert): Ihr Gerät wird mit 2,4 GHz (Mode 802.11b, Mode 802.11g und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • *5 GHz Indoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb von Gebäuden betrieben. • *5 GHz Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) außerhalb von Gebäuden betrieben.

Feld	Beschreibung
	• *5 GHz In/Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • *5,8 GHz Outdoor*: Nur für so genannte Broadband Fixed Wireless Access (BFWA) Anwendungen. Die Frequenzen im Frequenzbereich von 5 755 MHz bis 5 875 MHz dürfen nur in Verbindung mit gewerblichen Angeboten für öffentliche Netzzugänge genutzt werden und bedürfen einer Anmeldung bei der Bundesnetzagentur.

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll. Für **Frequenzband** = *2,4 GHz In/Outdoor* Mögliche Werte: • *802.11g*: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • *802.11b*: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • *802.11 mixed (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. • *802.11 mixed long (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind. • *802.11 mixed short (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • *802.11b/g/n*: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • *802.11g/n*: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. Für **Frequenzband** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* oder *5,8 GHz Outdoor* Mögliche Werte: • *802.11a*: Ihr Gerät arbeitet ausschließlich nach 802.11a. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. • *802.11a/n*: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n. • *802.11ac/a/n*: (sofern von Ihrem Gerät unterstützt) Ihr Gerät arbeitet nach 802.11 ac, 802.11a oder nach 802.11n. • *802.11ac/n*: (sofern von Ihrem Gerät unterstützt) Ihr Gerät arbeitet entweder nach 802.11ac oder 802.11n.
Bandbreite	Nicht für **Frequenzband** = *2,4 GHz In/Outdoor* Wählen Sie aus, wieviele Kanäle verwendet werden sollen. Mögliche Werte: • *20 MHz* (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet.

Feld	Beschreibung
	• *40 MHz*: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal. • *80 MHz*: Im Modus 802.11ac steht zusätzlich eine Bandbreite von 80 MHz zur Verfügung.
Anzahl der Spatial Streams	Nicht für **Frequenzband** = *2,4 GHz In/Outdoor* und **Drahtloser Modus** = *802.11g*, *802.11b*, *802.11 mixed (b/g)*, *802.11 mixed long (b/g)*, *802.11 mixed short (b/g)* und für **Frequenzband** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* oder *5,8 GHz Outdoor* und **Drahtloser Modus**= *802.11a* Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen. Mögliche Werte: • *3*: Drei Datenströme werden verwendet. • *2*: Zwei Datenströme werden verwendet. • *1*: Ein Datenstrom wird verwendet.
Airtime Fairness	Diese Funktion ist nicht für alle Geräte verfügbar. Mit der **Airtime Fairness** -Funktion wird gewährleistet, dass Senderessourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.
Wiederkehrender Hintergrund-Scan	Diese Funktion wird nicht von allen Geräten unterstützt. Um in regelmäßigen Abständen automatisch nach benachbarten oder Rogue Access Points im Netzwerk zu suchen, können Sie die Funktion **Wiederkehrender Hintergrund-Scan** aktivieren. Diese Suche erfolgt ohne eine Beeinträchtigung der Funktion als Access Point. Aktivieren oder deaktivieren Sie die Funktion **Wiederkehrender Hintergrund-Scan**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion deaktiviert.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Kanalplan	Wählen Sie den gewünschten Kanalplan aus. Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d.h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen.

Feld	Beschreibung
	Mögliche Werte: • *Alle*: Alle Kanäle können bei der Kanalwahl gewählt werden. • *Auto*: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • *Benutzerdefiniert*: Sie können die gewünschten Kanäle selbst auswählen.
Benutzerdefinierter Kanalplan	Nur für **Kanalplan** = *Benutzerdefiniert* Hier werden die aktuell gewählten Kanäle angezeigt. Mit **Hinzufügen** können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen. Mithilfe von -Symbol können Sie Einträge löschen.
Beacon Period	Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an. Dieser Wert wird in Beacon und Probe Response Frames übermittelt. Mögliche Werte sind *1* bis *65535*. Der Standardwert ist *100*.
DTIM Period	Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an. Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *2*.
RTS Threshold	Sie können hier den Schwellwert in Bytes (1..2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden.
Short Guard Interval	Aktivieren Sie diese Funktion, um den Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Max. Übertragungsrate	Wählen Sie die Übertragungsgeschwindigkeit aus. Mögliche Werte: • *Auto* (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • *<Wert>*: Je nach Einstellung für **Frequenzband**, **Bandbreite**, **Anzahl der Spatial Streams** und **Drahtloser Modus** stehen verschiedene feste Werte in MBit/s zur Auswahl.
Short Retry Limit	Geben Sie die maximale Anzahl von Sendeversuchen eines Frames ein, dessen Länge kürzer oder gleich dem in **RTS Threshold** definierten Wert ist. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.

Feld	Beschreibung
	Mögliche Werte sind `1` bis `255`. Der Standardwert ist `7`.
Long Retry Limit	Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, dessen Länge größer ist als der in **RTS Threshold** definierte Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen. Mögliche Werte sind `1` bis `255`. Der Standardwert ist `4`.
Fragmentation Threshold	Geben Sie die maximale Größe in Byte an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind `256` bis `2346`. Der Standardwert ist `2346`.

8.2.3.3 Drahtlosnetzwerke (VSS)

Im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke (VSS)** wird eine Übersicht aller angelegten Drahtlosnetzwerke angezeigt. Ein Drahtlosnetzwerk ist standardmäßig angelegt.

Für jedes Drahtlosnetzwerk (VSS) sehen Sie einen Eintrag mit einem Parametersatz (**VSS-Beschreibung**, **Netzwerkname (SSID)**, **Anzahl der zugeordneten Funkmodule**, **Sicherheit**, **Status**, **Aktion**).

Klicken Sie unter **Nicht zugewiesenes VSS allen Funkmodulen zuweisen** auf die Schaltfläche **Start**, um ein neu angelegtes VSS allen Funkmodulen zuzuweisen.

8.2.3.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfäche **Neu**, um weitere Drahtlosnetzwerke zu konfigurieren.

Das Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke (VSS)**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein. Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein. Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** übertragen werden soll. Mit Auswahl von `Sichtbar` wird der Netzwerkname sichtbar übertragen. Standardmäßig ist er sichtbar.
Intra-cell Repeating	Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum

Feld	Beschreibung
	Internet haben aber keinen Zugriff auf das Intranet der Firma. Um das zu verhindern, muss die Option deaktiviert sein.
U-APSD	Wählen Sie aus, ob der Stromsparmodus Unscheduled Automatic Power Save Delivery (U-APSD) aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
IGMP Snooping	IGMP Snooping reduziert den Datenverkehr und damit die Netzlast, weil Multicast Pakete aus dem LAN nicht weitergeleitet werden. Es werden ausschließlich Multicast-Pakete weitergeleitet, die von den entsprechenden Clients angefordert werden. Wenn Sie IGMP Snooping aktivieren, gibt IGMP Snooping daher den Rahmen vor, in dem Multicast angewendet wird. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: • *Inaktiv* (Standardwert): Weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11x
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 40* oder *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1-4	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für *WEP 40* benötigen Sie eine Zeichenfolge mit 5 Zeichen, für *WEP 104* mit 13 Zeichen.
WPA-Modus	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: • *WPA und WPA 2* (Standardwert): WPA und WPA 2 können angewendet werden. • *WPA*: Nur WPA wird angewendet.

Feld	Beschreibung
	• *WPA 2*: Nur WPA2 wird angewendet.
WPA Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen. Mögliche Werte: • *TKIP* (Standardwert): TKIP wird angewendet. • *AES*: AES wird angewendet. • *AES und TKIP*: AES oder TKIP wird angewendet.
WPA2 Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA 2* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie WPA2 anwenden wollen. Mögliche Werte: • *AES* (Standardwert): AES wird angewendet. • *TKIP*: TKIP wird angewendet. • *AES und TKIP*: AES oder TKIP wird angewendet.
Preshared Key	Nur für **Sicherheitsmodus** = *WPA-PSK* Geben Sie das WPA-Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein. Beachten Sie: Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!
RADIUS-Server	Sie können den Zugang zu einem Drahtlosnetzwerk über einen RADIUS-Server regeln. Mit **Hinzufügen** können Sie neue Einträge anlegen. Geben Sie die IP-Adresse und das Passwort des RADIUS-Servers ein.
EAP-Vorabauthentifizierung	Nur für **Sicherheitsmodus** = *WPA-Enterprise* Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen. Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden

Feld	Beschreibung
	können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis. Mögliche Werte sind ganze Zahlen von *1* bis *254*. Der Standardwert ist *32*.
Max. Anzahl Clients - Soft Limit	Diese Funktion wird nicht von allen Geräten unterstützt. Um eine vollständie Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehent. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des **Max. Anzahl Clients - Hard Limit** werden Anfragen strikt abgelehnt. Der Wert der **Max. Anzahl Clients - Soft Limit** muss gleich oder kleiner sein als der **Max. Anzahl Clients - Hard Limit**. Der Standardwert ist *28*. Sie können diese Funktion deaktivieren, indem Sie **Max. Anzahl Clients - Soft Limit** und **Max. Anzahl Clients - Hard Limit** auf den gleichen Wert einstellen.
Auswahl des Client-Bands	Diese Funktion wird nicht von allen Geräten unterstützt. Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist. Die Option **Auswahl des Client-Bands** ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht. Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming* (Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • *2,4-GHz-Band bevorzugt*: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • *5-GHz-Band bevorzugt*: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
Erlaubte Adressen	Legen Sie Einträge mit **Hinzufügen** an und geben Sie die MAC-Adressen der Clients (**MAC-Adresse**) ein, die zugelassen werden sollen.
Dynamische Black List	Mithilfe der Funktion **Dynamische Black List** ist es möglich, Clients, die sich möglicherweise unbefugt Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden. Ein gesperrten Client wird auf allen vom Wireless LAN Controller verwalteten APs für das betroffene VSS gesperrt, kann sich also auch nicht in einer anderen Funkzelle an diesem VSS anmelden. Soll ein Client permanent gesperrt bleiben, so kann dies im Menü **Wireless LAN Controller**->**Monitoring**->**Rogue Clients** erfolgen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiviert.
Fehlversuche per Zeitraum	Geben Sie hier die Anzahl der Fehlversuche ein, die innerhalb einer bestimmten Zeit von einer MAC-Adresse ausgehen müssen, damit ein Eintrag in der dynamischen Black List angelegt wird. Standardwerte sind *10* Fehlversuche in *60* Sekunden.
Sperrzeit für Black List	Geben Sie die Zeit ein, für die ein Eintrag in der dynamischen Black List gelten soll. Der Standardwert ist *500* Sekunden.

Felder im Menü VLAN

Feld	Beschreibung
VLAN	Wählen Sie aus, ob für dieses Drahtlosnetzwerk VLAN-Segmentierung verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
VLAN-ID	Geben Sie den Zahlenwert ein, der das VLAN identifiziert. Mögliche Werte sind *2* bis *4094*. VLAN ID 1 ist nicht möglich, da sie bereits verwendet wird.

Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung. Mögliche Werte sind • *Keine Begrenzung* (Standardwert) • *1 Mbit/s*, *1 Mbit/s*, *1 Mbit/s* bis *10 Mbit/s* in Einerschritten, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* und *50 Mbit/s*.
Tx Shaping	Wählen Sie die Begrenzung der Bandbreite in Senderichtung. Mögliche Werte sind • *Keine Begrenzung* (Standardwert) • *1 Mbit/s*, *1 Mbit/s*, *1 Mbit/s* bis *10 Mbit/s* in Einerschritten,

Feld	Beschreibung
	15 Mbit/s, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* und *50 Mbit/s*.

8.2.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

Hinweis

Um ein korrektes Timing zwischen dem WLAN Controller und den Slave APs sicher zu stellen, sollte auf dem WLAN Controller der interne Zeitserver aktiviert werden.

8.2.4.1 WLAN Controller

Im Menü **Wireless LAN Controller**->**Monitoring**->**WLAN Controller** wird eine Übersicht der wichtigsten Parameter des Wireless LAN Controllers angezeigt. Die Anzeige wird alle 30 Sekunden aktualisiert.

Werte in der Liste Übersicht

Status	Bedeutung
AP gefunden	Zeigt die Anzahl der gefundenen Access Points an.
AP offline	Zeigt die Anzahl der Access Points an, die nicht mit dem Wireless LAN Controller verbunden sind.
AP verwaltet	Zeigt die Anzahl der verwalteten Access Points an.
WLAN Controller: VSS-Durchsatz	Zeigt den empfangenen und den gesendeten Datenverkehr in Bytes pro Sekunde zeitabhängig an.
CPU-Last [%]	Zeigt die CPU-Auslastung in Prozent zeitabhängig an.
Speicherverbrauch [%]	Zeigt den Speicherverbrauch in Prozent zeitabhängig an.
Verbundene Clients/VSS	Zeigt die Anzahl der verbundenen Clients pro Drahtlosnetzwerk (VSS) zeitabhängig an.

8.2.4.2 Slave Access Points

Im Menü **Wireless LAN Controller**->**Monitoring**->**Slave Access Points** wird eine Übersicht aller erkannten Access Points angezeigt. Für jeden Access Point sehen Sie einen Eintrag mit folgendem Parametersatz: **Standort**, **Name**, **IP-Adresse**, **LAN-MAC-Adresse**, **Kanal**, **Tx-Bytes** und **Rx-Bytes**. Außerdem sehen Sie, ob die Access Points *Managed* oder *Gefunden* sind.

Über das -Symbol öffnen Sie eine Übersicht mit weiteren Details zu den **Slave Access Points**.

8.2.4.2.1 Übersicht

Im Menü **Übersicht** werden zusätzliche Informationen zum gewählten Access Point angezeigt. Die Anzeige wird alle 30 Sekunden aktualisiert.

Werte in der Liste Übersicht

Status	Bedeutung
Durchsatz	Zeigt den empfangenen und den gesendeten Datenverkehr pro Funkmodul zeitabhängig an.
Verbundene Clients	Zeigt die Anzahl der angeschlossenen Clients pro Funkmodul zeitabhängig an.

8.2.4.2.2 Funkmodul 1

Im Menü **Funkmodul** wird der empfangene und der gesendete Datenverkehr pro Client zeitabhängig angezeigt. Jeder Graph in der Darstellung ist über eine Farbe und eine MAC-Adresse eindeutig einem Client zugeordnet.

Werte in der Liste Funkmodul

Status	Bedeutung
Durchsatz/Client	Zeigt den empfangenen und den gesendeten Datenverkehr pro Client zeitabhängig an.

8.2.4.3 Aktive Clients

Im Menü **Wireless LAN Controller**->**Monitoring**->**Aktive Clients** werden die aktuellen Werte aller aktiven Clients angezeigt.

Für jeden Client sehen Sie einen Eintrag mit folgendem Parametersatz: **Standort**, **Name des Slave-APs**, **VSS**, **Client MAC**, **Client-IP-Adresse**, **Signal : Noise (dBm)** , **Tx-Bytes**, **Rx-Bytes**, **Tx Discards**, **Rx Discards**, **Status** und **Uptime**.

Mögliche Werte für Status

Status	Bedeutung
Keiner	Der Client befindet sich in keinem gültigen Zustand.
Angemeldet	Der Client meldet sich gerade beim WLAN an.
Zugeordnet	Der Client ist beim WLAN angemeldet.
Authentifizieren	Der Client wird gerade authentifiziert.
Authentifiziert	Der Client ist authentifiziert.

Über das -Symbol öffnen Sie eine Übersicht mit weiteren Details zu den **Aktive Clients**. Die Anzeige wird alle 30 Sekunden aktualisiert.

Werte in der Liste WLAN Client

Status	Bedeutung
Durchsatz	Zeigt den Datenverkehr getrennt nach empfangenen und gesendeten Daten für den gewählten WLAN Client zeitabhängig an.
Signal	Zeigt die Signalstärke für den gewählten WLAN Client zeitabhängig an.

8.2.4.4 Drahtlosnetzwerke (VSS)

Im Menü **Wireless LAN Controller**->**Monitoring**->**Drahtlosnetzwerke (VSS)** wird eine Übersicht über die aktuell verwendeten AP angezeigt. Sie sehen, welches Funkmodul welchem Drahtlosnetzwerk zugeordnet ist. Für jedes Funkmodul wird ein Parametersatz angezeigt (**Standort**, **Name des Slave-APs**, **VSS**, **MAC-Adresse (VSS)**, **Kanal**, **Status**).

8.2.4.5 Client-Verwaltung

Im Menü **Wireless LAN Controller**->**Monitoring**->**Client-Verwaltung** zeigt die Verwaltung der Clients durch die Access Points. Sie sehen u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Mithilfe des -Symbols können Sie die Werte für den gewünschten Eintrag löschen.

8.2.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Acces Points und Clients.

8.2.5.1 Benachbarte APs

Im Menü **Wireless LAN Controller**->**Umgebungs-Monitoring**->**Benachbarte APs** werden die benachbarten APs angezeigt, die während des Scannens gefunden wurden. **Rogue APs**, d.h. APs, die eine vom WLAN-Controller verwaltete SSID verwenden, aber nicht vom WLAN-Controller administriert werden, sind rot hinterlegt.

Hinweis

Überprüfen Sie die angezeigten APs sorgfältig, denn ein Angreifer könnte versuchen, über einen Rogue AP Daten in Ihrem Netz auszuspähen.

Jeder AP wird zwar mehrmals gefunden, aber nur einmal mit der größten Signalstärke angezeigt. Für jeden AP sehen Sie folgende Parameter **SSID**, **MAC-Adresse**, **Signal dBm**, **Kanal**, **Sicherheit**, **Zuletzt gesehen**, **Stärkstes Signal empfangen von**, **Gesamtdetektionen**.

Die Einträge werden alphabetisch nach **SSID** sortiert angezeigt. **Sicherheit** zeigt die Sicherheitseinstellungen des AP. Unter **Stärkstes Signal empfangen von** sehen Sie die Parameter **Standort** und **Name** desjenigen AP, über den der angezeigte AP gefunden wurde. **Summe der Erkennungen** zeigt an, wie oft der entsprechende AP während des Scannens gefunden wurde.

Klicken Sie unter **Benachbarte APs neu scannen** auf **Start**, um benachbarte APs erneut zu scannen. Sie erhalten eine Warnung, dass dazu die Funkmodule der Access Points für eine bestimmte Zeitspanne deaktiviert werden müssen. Wenn Sie den Vorgang mit **OK** starten, wird ein Fortschrittsbalken angezeigt. Die Anzeige der gefundenen APs wird alle zehn Sekunden aktualisiert.

8.2.5.2 Rogue APs

Im Menü **Wireless LAN Controller**->**Umgebungs-Monitoring**->**Rogue APs** werden die APs angezeigt, die eine SSID des eigenen Netzes verwenden, aber nicht vom **Wireless LAN Controller** verwaltet werden. **Rogue APs**, die neu gefunden wurden, sind rot hinterlegt.

Für jeden Rogue AP sehen Sie einen Eintrag mit folgendem Parametersatz: **SSID**, **MAC-Adresse**, **Signal dBm**, **Kanal**, **Zuletzt gesehen**, **Gefunden durch AP**, **Angenommen**.

Hinweis

Überprüfen Sie die angezeigten Rogue APs sorgfältig, denn ein Angreifer könnte versuchen, über einen Rogue AP Daten in Ihrem Netz auszuspähen.

Sie können einen Rogue AP als vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte **Angenommen** aktivieren. Ein eventuell konfigurierter Alarm wird dadurch gelöscht und ab sofort nicht mehr gesendet. Der rote Hintergrund verschwindet.

Klicken Sie unter **Benachbarte APs neu scannen** auf **Start**, um benachbarte APs erneut zu scannen. Sie erhalten eine Warnung, dass dazu die Funkmodule der Access Points für eine bestimmte Zeitspanne deaktiviert werden müssen. Wenn Sie den Vorgang mit **OK** starten, wird ein Fortschrittsbalken angezeigt. Die Anzeige der gefundenen APs wird alle zehn Sekunden aktualisiert.

8.2.5.3 Rogue Clients

Im Menü **Wireless LAN Controller**->**Umgebungs-Monitoring**->**Rogue Clients** werden die Clients angezeigt, die versucht haben, unbefugten Zugang zum Netzwerk herzustellen und sich daher auf der Blacklist befinden. Die Konfiguration der Blacklist erfolgt für jedes VSS im Menü **Wireless LAN Controller**->**Slave-AP-Konfiguration**->**Drahtlosnetzwerke (VSS)**. Sie können ebenfalls Einträge zur statischen Blacklist hinzufügen.

Mögliche Werte für Rogue Clients

Status	Bedeutung
MAC-Adresse des Rogue Clients	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
Netzwerkname (SSID)	Zeigt die beteiligten SSID an.
Angegriffener Access Point	Zeigt den betroffenen AP an.
Signal dBm	Zeigt die Signalstärke des Clients während des Zugriffsversuchs an.
Art des Angriffs	Hier wird die Art des möglichen Angriffs angezeigt, z. B. eine fehlerhafte

Status	Bedeutung
	Authentifizierung.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Zugriffsversuchs an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Zugriffsversuchs an.
Statische Black List	Sie können einen Rogue Client als nicht vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte **Statische Black List** aktivieren. Die Sperrung des Clients endet dann nicht automatisch, sondern muss von Ihnen manuell wieder aufgehoben werden.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

8.2.5.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Einträge anzulegen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Neuer Eintrag in die Blacklist

Feld	Beschreibung
MAC-Adresse des Rogue Clients	Geben SIe die MAC-Adresse des Clients ein, der der statischen Blacklist hinzugefügt werden soll.
Netzwerkname (SSID)	Wählen Sie das Drahtlosnetzwerk aus, von dem der Rogue Client ausgeschlossen werden soll.

8.2.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

8.2.6.1 Firmware-Wartung

Im Menü **Wireless LAN Controller**->**Wartung**->**Firmware-Wartung** wird eine Liste aller **Managed Access Points** angezeigt.

Für jeden managed AP sehen Sie einen Eintrag mit folgendem Parametersatz: **Firmware aktualisieren**, **Standort**, **Gerät**, **IP-Adresse**, **LAN-MAC-Adresse**, **Firmware-Version**, **Status**.

Klicken Sie auf die Schaltfläche **Alle auswählen**, um alle Einträge für eine Aktualisierung der Firmware auswählen. Klicken Sie auf die Schaltfläche **Alle deaktivieren**, um alle Einträge zu deaktivieren und danach bei Bedarf einzelne Einträge auszuwählen (z. B. wenn bei vielen Einträgen nur die Software einzelner APs aktualisiert werden soll).

Mögliche Werte für Status

Status	Bedeutung
Image bereits vorhanden.	Das Software Image ist bereits vorhanden, es ist kein Update nötig.
Fehler	Es ist ein Fehler aufgetreten.
Wird ausgeführt	Das Update wird gerade ausgeführt.
Fertig	Das Update ist beendet.

Das Menü **Wireless LAN Controller**->**Wartung**->**Firmware-Wartung** besteht aus folgenden Feldern:

Felder im Menü Firmware-Wartung

Feld	Beschreibung
Aktion	Wählen Sie die Aktion aus, die Sie ausführen wollen. Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.

Feld	Beschreibung
	Mögliche Werte: • *Systemsoftware aktualisieren*: Sie können eine Aktualisierung der Systemsoftware initiieren. • *Konfiguration mit Statusinformationen sichern*: Sie können eine Konfiguration sichern, welche Statusinformationen der APs enthält.
Quelle	Wählen Sie die Quelle für die Aktion aus. Mögliche Werte: • *HTTP-Server* (Standardwert): Die Datei ist bzw. wird auf dem entfernten Server gespeichert, der in der **URL** angegeben wird. • *Aktuelle Software vom Update-Server*: Die Datei liegt auf dem offiziellen Update-Server. (Nur für **Aktion** = *Systemsoftware aktualisieren*) • *TFTP-Server*: Die Datei ist bzw. wird auf dem TFTP-Server gespeichert, der in der **URL** angegeben wird.
URL	Nur für **Quelle** = *HTTP-Server* oder *TFTP-Server* Geben Sie die URL des Servers ein, von dem die Systemsoftware-Datei geladen werden soll bzw. auf dem die Konfigurationsdatei gespeichert werden soll.

8.3 Monitoring

Dieses Menü enthält Informationen, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle Ihres Geräts, ermöglichen.

8.3.1 WLAN

8.3.1.1 WLANx

Im Menü **Monitoring**->**WLAN**->**WLAN** werden die aktuellen Werte und Aktivitäten der WLAN-Schnittstelle angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

Werte in der Liste WLANx Statistik

Feld	Beschreibung
Mbit/s	Zeigt die möglichen Datenraten auf diesem Funkmodul an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete für die in **Mbit/s** angezeigte Datenrate an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete für die in **Mbit/s** angezeigte Datenrate an.

Über die Schaltfläche **Erweitert** gelangen Sie in eine Übersicht über weitere Details.

Werte in der Liste Erweitert

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des angezeigten Werts an.
Wert	Zeigt den entsprechenden statistischen Wert an.

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Unicast MSDUs erfolgreich übertragen	Zeigt die Anzahl der erfolgreich an Unicast-Adressen versandten MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wurde ein Acknowled-

Beschreibung	Bedeutung
	gement empfangen.
Erfolgreich übertragene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich an Multicast-Adressen (inklusive der Broadcast MAC-Adresse) versandten MSDUs an.
Übertragene MPDUs	Zeigt die Anzahl der erfolgreich empfangenen MPDUs an.
Erfolgreich empfangene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Multicast-Adresse versandt wurden.
Unicast MPDUs erfolgreich erhalten	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Unicast-Adresse versandt wurden.
MSDUs, die nicht übertragen werden konnten	Zeigt die Anzahl der MSDUs an, die nicht gesendet werden konnten.
Doppelte empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDUs erhalten	Zeigt die Anzahl der empfangenen MPDUs an, die nicht entschlüsselt werden konnten. Ein Grund dafür könnte sein, dass kein passender Schlüssel eingetragen wurde.
RTS Frames ohne CTS	Zeigt die Anzahl der RTS-Frames an, für die kein CTS empfangen wurde.
Fehlerhafte Erhaltene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

8.3.1.2 VSS

Im Menü **Monitoring**->**WLAN**->**VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

Werte in der Liste Client-Node-Tabelle

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s. Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rx Discards	Zeigt die Anzahl der empfangenen Datenpakete, die verworfen wurden, wenn im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**-> im Feld **Rx Shaping** die Bandbreite für eingehenden Datenverkehr begrenzt wurde.
Tx Discards	Zeigt die Anzahl der gesendeten Datenpakete, die verworfen wurden, wenn im Menü **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**-> im Feld **Rx Shaping** die Bandbreite für ausgehenden Datenverkehr be-

Feld	Beschreibung
	grenzt wurde.

VSS - Details für Verbundene Clients

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen Indikator für die Qualität der Verbindung im Funk dar. Werte: • > 25 dB exzellent • 15 – 25 dB gut • 2 – 15 dB grenzwertig • 0 – 2 dB schlecht.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Rx Discards	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.
Tx Discards	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.

8.3.1.3 Client-Verwaltung

Im Menü **Monitoring**->**WLAN**+**Client-Verwaltung** wird eine Übersicht des **Client-Verwaltung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Werte in der Liste Client-Verwaltung

Feld	Beschreibung
VSS-Beschreibung	Zeigt die eindeutige Beschreibung des Drahtlosnetzwerks (VSS) an.
Netzwerkname (SSID)	Zeigt den Namen des Wireless Netzwerks (SSID) an.
MAC-Adresse	Zeigt die MAC Adresse, die für dieses VSS verwendet wird, an.
Aktive Clients	Zeigt die Anzahl der aktiven Clients.
2,4/5-GHz-Übergang	Zeigt die Anzahl der Clients, die über die Funktion **2,4/5-GHz-Übergang** in ein anderes Frequenzband verschoben worden sind.
Abgewiesene Clients soft/ hard	Zeigt die Anzahl der abgewiesenen Clients, nachdem die absolute Anzahl an zulässigen Clients erreicht wurde.

Kapitel 9 Internet & Netzwerk

9.1 Physikalische Schnittstellen

9.1.1 Ethernet-Ports

Eine Ethernet-Schnittstelle ist eine physikalische Schnittstelle zur Anbindung an das lokale Netzwerk oder zu externen Netzwerken.

Die Ethernet-Ports **LAN1** bis **LAN4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.2.1* und **Netzmaske** *255.255.255.0* vorkonfiguriert.

Hinweis

Um die Erreichbarkeit Ihres Systems zu gewährleisten, achten Sie beim Aufteilen der Ports darauf, dass die Ethernet-Schnittstelle *en1-0* mit der vorkonfigurierten IP-Adresse und Netzmaske einem Port zugewiesen wird, der per Ethernet erreichbar ist.

ETH1 - ETH4

Die Schnittstellen können separat genutzt werden. Sie werden voneinander logisch getrennt, indem jedem Port im Menü **Portkonfiguration** im Feld **Ethernet-Schnittstellenauswahl** die gewünschte logische Ethernet-Schnittstelle zugewiesen wird. Für jede zugewiesene Ethernet-Schnittstelle wird im Menü **LAN**->**IP-Konfiguration** eine weitere Schnittstelle in der Liste angezeigt und eine jeweils vollständig eigenständige Konfiguration der Schnittstelle ermöglicht.

VLANs für Routing-Schnittstellen

Konfigurieren Sie VLANs, um z. B. einzelne Netzwerksegmente voneinander zu trennen (z. B. einzelne Abteilungen einer Firma) oder um bei der Verwendung von Managed Switches mit QoS-Funktion eine Bandbreitenreservierung für einzelne VLANs vorzunehmen.

9.1.1.1 Portkonfiguration

Portseparation

Ihr Gerät bietet die Möglichkeit, die Switch Ports als eine Schnittstelle zu betreiben oder diese logisch voneinander zu trennen und als eigenständige Ethernet-Schnittstellen zu konfigurieren.

Bei der Konfiguration sollten Sie Folgendes beachten: Die Aufteilung der Switch Ports auf mehrere Ethernet-Schnittstellen trennt diese nur logisch voneinander. Die verfügbare Gesamtbandbreite von max. 1000 Mbit/s Full Duplex für alle entstandenen Schnittstellen bleibt unverändert. Wenn Sie also z. B. alle Switch Ports voneinander trennen, verfügt jede der entstehenden Schnittstellen nur über einen Teil der vollen Bandbreite. Wenn Sie mehrere Switch Ports zu einer Schnittstelle zusammenfassen, so stehen für alle Ports gemeinsam die volle Bandbreite von max. 1000 Mbit/s Full Duplex zur Verfügung.

Das Menü **Physikalische Schnittstellen**->**Ethernet-Ports**->**Portkonfiguration** besteht aus folgenden Feldern:

Felder im Menü Portkonfiguration, Switch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Ethernet-	Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-

Feld	Beschreibung
Schnittstellenauswahl	Schnittstelle zu. Zur Auswahl stehen vier Schnittstellen, *en1-0* bis *en1-3*. In der Grundeinstellung ist Switch Port **1**-**4** die Schnittstelle *en1-0* zugeordnet.
Konfigurierte Geschwindigkeit / Konfigurierter Modus	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vollständige automatische Aushandlung* (Standardwert) • *Auto 1000 Mbit/s only* • *Auto 100 Mbit/s only* • *Auto 10 Mbit/s only* • *Auto 100 Mbit/s / Full Duplex* • *Auto 100 Mbit/s / Half Duplex* • *Auto 10 Mbit/s / Full Duplex* • *Auto 10 Mbit/s / Half Duplex* • *Fest 1000 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Half Duplex* • *Fest 10 Mbit/s / Full Duplex* • *Fest 10 Mbit/s / Half Duplex* • *Keiner*: Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an. Mögliche Werte: • *1000 Mbit/s / Full Duplex* • *100 Mbit/s / Full Duplex* • *100 Mbit/s / Half Duplex* • *10 Mbit/s / Full Duplex* • *10 Mbit/s / Half Duplex* • *Inaktiv*
Flusskontrolle	Wählen Sie aus, ob auf der entsprechenden Schnittstelle eine Flusskontrolle vorgenommen werden soll. Mögliche Werte: • *Deaktiviert* (Standardwert): Es wird keine Flusskontrolle vorgenommen. • *Aktiviert*: Es wird eine Flusskontrolle durchgeführt. • *Auto*: Es wird eine automatische Flusskontrolle durchgeführt.

9.1.2 DSL-Modem

Das DSL-Modem eignet sich für den High-Speed Internetzugang und den Remote-Access-Einsatz in kleinen bis mittleren Unternehmen oder Remote-Offices.

9.1.2.1 DSL-Konfiguration

In diesem Menü nehmen Sie grundlegende Einstellungen Ihrer ADSL-Verbindung vor.

Das Menü **Physikalische Schnittstellen**->**DSL-Modem**->**DSL-Konfiguration** besteht aus folgenden Feldern:

Felder im Menü DSL-Portstatus

Feld	Beschreibung
Physikalische Verbindung	Zeigt den aktuellen DSL-Betriebsmodus an. Der Wert kann nicht verändert werden. Mögliche Werte: • *Unbekannt*: Der Link ist nicht aktiv. • *ADSL1*: ADSL classic, G.DMT, ITU-T G.992.1 • *ADSL2*: G.DMT.Bis, ITU-T G.992.3 • *ADSL2 Plus*: ADSL2 Plus, ITU-T G.992.5 • *ADSL2+ Annex J*: ITU-T G.992.5 • *VDSL2*: ITU-T G.993.2
Downstream	Zeigt die Datenrate in Empfangsrichtung (Richtung von CO/DSLAM zu CPE/Router) in Bits pro Sekunde an. Der Wert kann nicht verändert werden.
Upstream	Zeigt die Datenrate in Senderichtung (Richtung CPE/Router zu CO/DSLAM) in Bits pro Sekunde an. Der Wert kann nicht verändert werden.
DSL-Chipsatz	Zeigt die Kennung des eingebauten Chipsatzes an.

Felder im Menü DSL-Parameter

Feld	Beschreibung
DSL-Modus	Zeigt den gewählten DSL-Betriebsmodus an. Mögliche Werte: • *Inaktiv*: Der Link ist nicht aktiv. • *ETSI T1.413*: ETSI T1.413 • *ADSL1*: ADSL classic, G.DMT, ITU-T G.992.1 • *Automatischer Modus (ADSL)* (Standardwert, wenn das Gerät als Telefonanlage betrieben wird): Automatische Erkennung des ADSL-Modus *ADSL1*, *ADSL2* oder *ADSL2 Plus* • *ADSL2*: G.DMT.Bis, ITU-T G.992.3 • *ADSL2 Plus*: ADSL2 Plus, ITU-T G.992.5 • *VDSL*: VDSL2 (ITU-T G.993.2) • *VDSL/ADSL Multimodus* (Standardwert, wenn das Gerät als Media Gateway betrieben wird): Automatische Erkennung des DSL-Modus *ADSL1*, *ADSL2* , *ADSL2 Plus* oder *VDSL*
Transmit Shaping	Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig. Mögliche Werte: • *Standard (Leitungsgeschwindigkeit)* (Standardwert): Die Datenrate in Senderichtung wird nicht reduziert. • *128.000 Bit/s* bis *2.048.000 Bit/s*: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 bit/s bis 2.048.000 bit/s in festgesetzten Schritten.

Feld	Beschreibung
	• *Benutzerdefiniert*: Die Datenrate wird reduziert auf den in **Maximale Upstream-Bandbreite** eingegebenen Wert.
Maximale Upstream-Bandbreite	Nur für **Transmit Shaping** = *Benutzerdefiniert* Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.
Rauschabstand	Der Signal-Rausch-Abstand (SNR) kann über den Schieberegler von 0 bis 5 dB geregelt werden. Ändern Sie den Wert nur bei DSL-Leitungsproblemen.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Profile

Feld	Beschreibung
DSL-Leitungsprofil	Wählen Sie den gewünschten Internet-Service-Provider und damit implizit den von diesem Provider verwendeten Modem-Parametersatz aus. *Deutsche Telekom* ist als Standardwert voreingestellt. Wenn Sie Ihren Provider in der Liste nicht finden, verwenden Sie die Einstellung *Standard*.

9.2 LAN

In diesem Menü konfigurieren Sie die Adressen in Ihrem LAN und haben die Möglichkeit ihr lokales Netzwerk durch VLANs zu strukturieren.

9.2.1 IP-Konfiguration

In diesem Menü kann die IP-Konfiguration der LAN und Ethernet-Schnittstellen Ihres Geräts bearbeitet werden.

9.2.1.1 Schnittstellen

In Menü **LAN**->**IP-Konfiguration**->**Schnittstellen** werden die vorhandenen IP-Schnittstellen aufgelistet. Sie haben die Möglichkeit, die IP-Konfiguration der Schnittstellen zu bearbeiten oder virtuelle Schnittstellen für Spezialanwendungen anzulegen. Hier werden alle im Menü **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen** konfigurierten Schnittstellen (logische Ethernet-Schnittstellen und solche in den Subsystemen erstellten) aufgelistet.

Über das Symbol bearbeiten Sie die Einstellungen einer vorhandenen Schnittstelle (Bridge-Gruppen, Ethernet-Schnittstellen im Routing-Modus).

Über die Schaltfläche **Neu** haben Sie die Möglichkeit, virtuelle Schnittstellen anzulegen. Dieses ist jedoch nur in Spezialanwendungen (BRRP u. a.) nötig.

Abhängig von der gewählten Option, stehen verschiedene Felder und Optionen zur Verfügung. Im Folgenden finden Sie eine Auflistung aller Konfigurationsmöglichkeiten.

Durch Klicken auf die -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert.

Über die -Schaltfläche können Sie die Details einer vorhandenen Schnittstelle anzeigen lassen.

Hinweis

Beachten Sie bei IPv4:

Hat Ihr Gerät bei der Erstkonfiguration dynamisch von einem in Ihrem Netzwerk betriebenen DHCP-Server eine IP-Adresse erhalten, so wird die Standard-IP-Adresse automatisch gelöscht und Ihr Gerät ist darüber nicht mehr erreichbar.

Sollten Sie dagegen bei der Erstkonfiguration eine Verbindung zum Gerät über die Standard-IP-Adresse aufgebaut oder eine IP-Adresse mit dem **Dime Manager** vergeben haben, ist es nur noch über diese IP-Adresse erreichbar. Es kann nicht mehr dynamisch über DHCP eine IP-Konfguration erhalten.

Beispiel Teilnetze

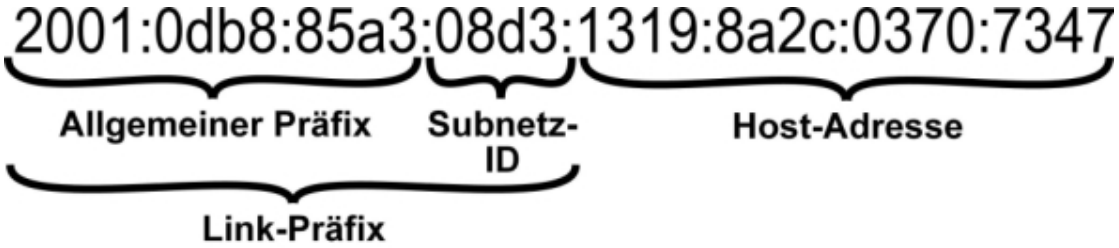
Falls Ihr Gerät an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie für das zweite Teilnetz eine zweite **IP-Adresse / Netzmaske** eintragen.

Im ersten Teilnetz gibt es z. B. zwei Hosts mit den IP-Adressen 192.168.42.1 und 192.168.42.2, im zweiten Teilnetz zwei Hosts mit den IP-Adressen 192.168.46.1 und 192.168.46.2. Um mit dem ersten Teilnetz Datenpakete austauschen zu können, benutzt Ihr Gerät z. B. die IP-Adresse 192.168.42.3, für das zweite Teilnetz 192.168.46.3. Die Netzmasken für beide Teilnetze müssen ebenfalls angegeben werden.

IPv6-Adressen konfigurieren

Zusätzlich zu IPv4-Adressen können Sie IPv6-Adressen verwenden.

Im Folgenden sehen Sie ein Beispiel für eine IPv6-Adresse:



Ihr Gerät kann auf einer Schnittstelle entweder als Router oder als Host agieren. In der Regel agiert es auf den LAN-Schnittstellen als Router und auf den WAN- sowie den PPP-Verbindungen als Host.

Wenn Ihr Gerät als Router agiert, so können seine eigenen IPv6-Adressen folgendermaßen gebildet werden: ein Link-Präfix kann von einem Allgemeinen Präfix abgeleitet werden oder Sie können einen statischen Wert eingeben. Eine Host-Adresse kann über *Auto eui-64* erzeugt werden, für weitere Host-Adressen können Sie statische Werte eingeben.

Wenn Ihr Gerät als Router agiert, so verteilt es den konfigurierten Link-Präfix in der Regel per Router Advertisements an die Hosts. Über einen DHCP-Server werden Zusatzinformationen, wie z. B. die Adresse eines Zeitservers, an die Hosts übermittelt. Der Client kann sich seine Host-Adresse entweder über Stateless Address Autoconfiguration (SLAAC) erzeugen oder diese Adresse von einem DHCP-Server zugeteilt bekommen.

Verwenden Sie für den oben beschriebenen Router-Modus im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** die Einstellungen **IPv6-Modus** = *Router*, **Router Advertisement übertragen** *Aktiviert* **DHCP-Server** *Aktiviert* und **IPv6-Adressen Hinzufügen**.

Wenn Ihr Gerät als Host agiert, wird ihm ein Link-Präfix von einem anderen Router per Router Advertisement zugeteilt. Die Host- Adresse wird dann per SLAAC automatisch erzeugt. Zusatzinformationen, wie z. B. der Allgemeine Präfix vom Provider oder die Adresse eines Zeitservers können per DHCP bezogen werden. Verwenden Sie dazu im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** die Einstellungen **IPv6-Modus** = *Client*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** = *Aktiviert*.

9.2.1.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um virtuelle Schnittstellen zu erstellen.

Das Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird. Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
Schnittstellenmodus	Nur bei physikalischen Schnittstellen im Routing-Modus und bei virtuelle Schnittstellen. Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: • *Untagged* (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • *Tagged (VLAN)*: Diese Option gilt nur für Routing-Schnittstellen. Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu. Dies geschieht über die VLAN-ID, die in diesem Modus angezeigt wird und konfiguriert werden kann. Die Definition einer MAC-Adresse in **MAC-Adresse** ist in diesem Modus optional.
VLAN-ID	Nur für **Schnittstellenmodus** = *Tagged (VLAN)* Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben. Mögliche Werte sind *1* (Standardwert) bis *4094*.
MAC-Adresse	Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde, wenn Sie **Voreingestellte verwenden** aktivieren. Die VLAN IDs müssen sich jedoch unterscheiden. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden). Wenn **Voreingestellte verwenden** aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet. Standardmäßig ist **Voreingestellte verwenden** aktiv.

Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig*: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.

Feld	Beschreibung
	• *Nicht Vertrauenswürdig*: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
Adressmodus	Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird. Mögliche Werte: • *Statisch* (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in **IP-Adresse / Netzmaske** zugewiesen. • *DHCP*: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
DHCP Metrik	Es ist möglich, einer Schnittstelle, die per DHCP konfiguriert wird eine Metrik für die erhaltenen Routen zuzuweisen. Dies kann bei der Konfiguration von Backup-Verbindungen notwendig sein, um ein sauberes Umschalten zum Backup und wieder zurück zu gewährleisten. Der Standardwert ist *1*. Für eine Backup-Lösung sollte der Wert erhöht werden, damit die Backup-Route nicht eine zu hohe Priorität bekommt.
IP-Adresse / Netzmaske	Nur für **Adressmodus** = *Statisch* Fügen Sie mit **Hinzufügen** einen neuen Adresseintrag hinzu und geben Sie die **IP-Adresse** und die entsprechende **Netzmaske** der virtuellen Schnittstelle ein.

Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
IPv6	Wählen Sie aus, ob die gewählte Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Hier nur für **IPv6** = *Aktiviert* Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig* (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. • *Nicht Vertrauenswürdig*: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert*

Feld	Beschreibung
	Wählen Sie, ob die Schnittstelle im Host- oder im Router-Modus betrieben werden soll. Abhängig von der getroffenen Auswahl werden unterschiedliche Parameter angezeigt, die Sie konfigurieren müssen. Mögliche Werte: • *Router (Router-Advertisement übermitteln)* (Standardwert): Die Schnittstelle wird im Router-Modus betrieben. • *Host*: Die Schnittstelle wird im Host-Modus betrieben.
DHCP-Server	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Router* Legen Sie fest, ob Ihr Gerät als DHCP-Server agieren soll, d.h ob es DHCP-Options versenden soll, um z. B. Informationen zu den DNS-Servern an die Clients weiterzuleiten. Aktivieren Sie diese Option, wenn Hosts IPv6-Adressen per SLAAC erzeugen sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird z. B. die Präfix-Liste erstellt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll, d.h. ob es DHCP-Options empfangen soll, um z. B. Informationen zu den DNS-Servern zu erhalten. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
IPv6-Adressen	Nur für **IPv6** = *Aktiviert* Sie können der gewählten Schnittstelle **IPv6-Adressen** zuordnen. Mit **Hinzufügen** können Sie einen oder mehrere Adresseinträge anlegen. Ein zusätzliches Fenster öffnet sich, in dem Sie eine IPv6-Adresse bestehend aus einem Link-Präfix und einem Host-Anteil festlegen können. Wenn Ihr Gerät im Host-Modus arbeitet (**IPv6-Modus** = *Host*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** *Aktiviert*), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen. Wenn Ihr Gerät im Router-Modus arbeitet (**IPv6-Modus** = *Router*, **Router Advertisement übertragen** *Aktiviert* und **DHCP-Server** *Aktiviert*), so müssen Sie hier seine IPv6-Adressen konfigurieren.

Legen Sie weitere Einträge mit **Hinzufügen** an.

Felder im Menü Basisparameter

Feld	Beschreibung
Ankündigen	Nur für **IPv6-Modus** = *Router* Hier können Sie - bezogen auf den Link-Präfix, der im aktuellen Fenster definiert wird - festlegen, ob dieser Präfix per Router Advertisement über die gewählte Schnittstelle versendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Link-Präfix

Feld	Beschreibung
Art der Einrichtung	Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll. Mögliche Werte: • *Von Allgemeinem Präfix* (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet. • *Statisch*: Sie können den Link-Präfix eingeben.
Allgemeiner Präfix	Nur für **Art der Einrichtung** = *Von Allgemeinem Präfix* Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes**->**Neu** angelegt sind.
Automatische Subnetzerstellung	Nur wenn **Art der Einrichtung** = *Von Allgemeinem Präfix* und wenn ein **Allgemeiner Präfix** gewählt ist. Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID *0* verwendet, für das zweite Subnetz die Subnetz-ID *1*, usw. Mögliche Werte für die **Subnetz-ID** sind *0* bis *255*. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Bei der Subnetzerstellung wird der dezimale ID-Wert in einen hexadezimalen Wert umgerechnet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die Funktion nicht aktiv ist, so können Sie durch Eingabe der Subnetz-ID ein Subnetz definieren.
Subnetz-ID	Nur wenn **Automatische Subnetzerstellung** nicht aktiv ist. Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Mögliche Werte sind *0* bis *255*. Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.
Link-Präfix	Nur für **Art der Einrichtung** = *Statisch* Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit *::* enden. Seine Länge ist mit *64* vorgegeben.

Felder im Menü Host-Adresse

Feld	Beschreibung
Erzeugungsmethode	Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. EUI-64 setzt folgenden Prozess in Gang: • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird *FFFE* eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf *1* gesetzt.
Statische Adressen	Sie können, unabhängig von der automatischen Erzeugung, die unter **Erzeugungsmethode** festgelegt ist, mit **Hinzufügen** den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit *64* vorgegeben. Beginnen Sie die Eingabe mit *::* .

Die Felder im Menü **Erweitert** sind Bestandteil der Präfix-Informationen, die im Router Advertisement gesendet werden, wenn **Ankündigen** aktiv ist. Das Menü **Erweitert** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
On Link Flag	Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll. Dadurch fügt der Host das Präfix der Präfixliste hinzu. Mit Auswahl von *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Autonomous Flag	Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll. Dadurch nutzt ein Host das Präfix und eine Schnittstellen-ID, um daraus seine Adresse abzuleiten. Mit Auswahl von *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Bevorzugte Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden ein. Während dieser Zeit werden die Adressen, die mit Hilfe des Präfix per SLAAC erzeugt wurden, bevorzugt verwendet. Der Standardwert ist *604800* Sekunden.
Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist. Der Standardwert ist *2592000* Sekunden. **Hinweis** Der Wert für die Gültigkeitsdauer sollte niedriger sein als derjenige, der unter **Erweiterte IPv6-Einstellungen** für die Option **Router-Gültigkeitsdauer** konfiguriert ist.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
DHCP-MAC-Adresse	Nur für **Adressmodus** = *DHCP* Ist **Voreingestellte verwenden** aktiviert (Standardeinstellung) wird die Hardware-MAC-Adresse der Ethernet-Schnittstelle verwendet. Bei physikalischen Schnittstellen ist die aktuelle MAC-Adresse standardmäßig eingetragen. Wenn Sie **Voreingestellte verwenden** deaktivieren, geben Sie eine MAC-Adresse für die virtuelle Schnittstelle ein, z. B. *00:e1:f9:06:bf:03*. Manche Provider verwenden hardware-unabhängige MAC-Adressen, um ihren Clients IP-Adressen dynamisch zuzuweisen. Sollte Ihnen Ihr Provider eine MAC-Adresse zugewiesen haben, so tragen Sie diese hier ein.
DHCP-Hostname	Nur für **Adressmodus** = *DHCP* Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.
DHCP Broadcast Flag	Nur für **Adressmodus** = *DHCP* Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Standardroute erstellen	Nur für **Adressmodus** = *DHCP* Wählen Sie aus, ob für diese Schnittstelle eine Standardroute festgelegt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Proxy ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-MSS-Clamping	Wählen Sie aus, ob Ihr Gerät das Verfahren MSS Clamping anwenden soll. Um die Fragmentierung von IP-Paketen zu verhindern, wird hierbei vom Gerät automatisch die MSS (Maximum Segment Size) auf den hier einstellbaren Wert verringert. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert *1350* eingetragen.

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
Router-Gültigkeitsdauer	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *Router* und **Router Advertisement übertragen** = *Aktiviert* Geben Sie eine Zeitspanne in Sekunden an. Für dieses Intervall verbleibt der Router in der Default Router List. Der Standardwert ist *600* Sekunden. Der Maximalwert ist *65520* Sekunden. Ein Wert von *0* besagt, dass der Router kein Standardrouter ist und nicht in die Default Router List eingetragen werden soll. **Hinweis** Der Wert für die **Router-Gültigkeitsdauer** sollte höher sein als die kürzeste Link-Präfix-Gültigkeitsdauer, die im unter **Grundlegende IPv6-Parameter** für die Schnittstelle konfiguriert ist.
Router-Präferenz	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *Router* und **Router Advertisement übertragen** = *Aktiviert* Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien. Mögliche Werte: • *Hoch* • *Mittel* (Standardwert) • *Niedrig*
DHCP-Modus	Nur für **IPv6** = *Aktiviert*, **IPv6-Modus** = *Router* und **Router Advertisement übertragen** = *Aktiviert* Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus. **Hinweis** Der Router muss nicht als DHCP-Server eingerichtet sein. Mit Auswahl von *Andere - DNS-Server, SIP-Server* (Standardwert) werden nicht-adressbezogene Informationen, wie z. B. DNS, VoIP, usw. durchgeleitet. Aktivieren Sie diese Option, wenn die Hosts im Netzwerk ihre IP-Adresse über SLAAC automatisch bilden sollen. Der Router sendet in diesem Fall ausschließlich nicht-adressbezogene Daten über DHCP. Mit Auswahl von *Verwaltet - IPv6-Adressverwaltung* werden sowohl die IPv6-Adressen als auch alle nicht adressbezogenen Daten vom Host per DHCP bezogen.
DNS-Propagation	Nur für **IPv6-Modus** = *Router* und **Router Advertisement übertragen** *Aktiviert* Wählen Sie aus, ob DNS-Server-Adressen über Router Advertisements propagiert werden sollen und wenn ja, auf welche Weise. Es werden maximal zwei DNS-Server-Adressen propagiert. Mögliche Werte:

Feld	Beschreibung

	• *Aus*: Es wird keine DNS-Server-Adresse propagiert.
	• *Selbst*: Die eigene IP-Adresse wird als DNS-Server-Adresse propagiert. Bei mehreren Adressen, werden die Adressen in folgender Reihenfolge propagiert:
	  • Globale Adressen
	  • ULA (Unique Local Addresses)
	  • Link-Lokale-Adressen
	• *Sonstige*: Die statisch konfigurierten und die dynamisch gelernten DNS-Server-Einträge werden gemäß ihrer Priorität propagiert. Sind keine Einträge vorhanden, werden keine Adressen propagiert.

9.2.2 VLAN

Durch die Implementierung der VLAN-Segmentierung nach 802.1Q ist die Konfiguration von VLANs auf Ihrem Gerät möglich. Insbesondere sind Funk-Ports eines Access Points in der Lage, das VLAN-Tag eines Frames, das zu den Clients gesendet wird, zu entfernen und empfangene Frames mit einer vorab festgelegten VLAN-ID zu taggen. Durch diese Funktionalität ist ein Access Point nichts anderes als eine VLAN-fähiger Switch mit der Erweiterung, Clients in VLAN-Gruppen zusammenzufassen. Generell ist die VLAN-Segmentierung mit allen Schnittstellen konfigurierbar.

VLAN für Bridging und VLAN für Routing

Im Menü **LAN**->**VLAN** werden VLANs (virtuelle LANs) mit Schnittstellen, die im Bridging-Modus arbeiten, konfiguriert. Über das Menü **VLAN** können Sie alle dafür notwendigen Einstellungen vornehmen und deren Status abfragen.

Achtung

Für Schnittstellen, die im Routing-Modus arbeiten, wird der jeweiligen Schnittstelle lediglich eine VLAN-ID zugewiesen. Dies definieren Sie über die Parameter **Schnittstellenmodus** = *Tagged (VLAN)* und das Feld **VLAN-ID** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**.

9.2.2.1 VLANs

In diesem Menü können Sie sich alle bereits konfigurierten VLANs anzeigen lassen, Ihre Einstellungen bearbeiten und neue VLANs erstellen. Standardmäßig ist das VLAN *Management* mit **VLAN Identifier** = *1* vorhanden, dem alle Schnittstellen zugeordnet sind.

9.2.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere VLANs zu konfigurieren.

Das Menü **LAN**->**VLAN**->**VLANs**->**Neu** besteht aus folgenden Feldern:

Felder im Menü VLAN konfigurieren

Feld	Beschreibung
VLAN Identifier	Geben Sie die Ziffer ein, die das VLAN identifiziert. Im -Menü kann dieser Wert nicht mehr verändert werden. Mögliche Werte sind *1* (Standardwert) bis *4094*
VLAN-Name	Geben Sie einen eindeutigen Namen für das VLAN ein. Möglich ist eine Zeichenkette mit bis zu 32 Zeichen.

Feld	Beschreibung
	Der voreingestellt VLAN-Name ist *Management*.
VLAN-Mitglieder	Wählen Sie die Ports aus, die zu diesem VLAN gehören sollen. Über die Schaltfläche **Hinzufügen** können Sie weitere Mitglieder hinzufügen. Wählen Sie weiterhin zu jedem Eintrag aus, ob die Frames, die von diesem Port übertragen werden, *Tagged* (also mit VLAN-Information) oder *Untagged* (also ohne VLAN-Information) übertragen werden sollen.

9.2.2.2 Portkonfiguration

In diesem Menü können Sie Regeln für den Empfang von Frames an den Ports des VLANs festlegen und einsehen.

Das Menü **LAN->VLANs->Portkonfiguration** besteht aus folgenden Feldern:

Felder im Menü Portkonfiguration

Feld	Beschreibung
Schnittstelle	Zeigt den Port an, für den Sie die PVID definieren und Verarbeitungsregeln definieren.
PVID	Weisen Sie dem ausgewählten Port die gewünschte PVID (Port VLAN Identifier) zu. Wenn ein Paket ohne VLAN-Tag diesen Port erreicht, wird es mit dieser PVID versehen.
Frames ohne Tag verwerfen	Wenn die Option aktiviert ist, werden ungetaggte Frames verworfen. Ist die Option deaktiviert, werden ungetaggte Frames mit der in diesem Menü definierten PVID getaggt.
Nicht-Mitglieder verwerfen	Wenn die Option aktiviert ist, werden alle getaggten Frames verworfen, die mit einer VLAN-ID getaggt sind, in der der ausgewählte Port nicht Mitglied ist.

9.2.2.3 Verwaltung

In diesem Menü nehmen Sie allgemeine Einstellungen für ein VLAN vor. Die Optionen sind für jede Bridge-Gruppe separat zu konfigurieren.

Das Menü **LAN->VLANs->Verwaltung** besteht aus folgenden Feldern:

Felder im Menü Bridge-Gruppe br<ID> VLAN-Optionen

Feld	Beschreibung
VLAN aktivieren	Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe für VLAN. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion deaktiviert.

9.3 Netzwerk

9.3.1 Routen

Standard-Route (Default Route)

Bei einer Standard-Route werden automatisch alle Daten auf eine Verbindung geleitet, wenn keine andere passende Route verfügbar ist. Wenn Sie einen Zugang zum Internet einrichten, dann tragen Sie die Route zu Ihrem Internet-Service-Provider (ISP) als Standard-Route ein. Wenn Sie z. B. eine Firmennetzanbindung durchführen, dann tragen Sie die Route zur Zentrale bzw. zur Filiale nur dann als Standard-Route ein, wenn Sie keinen Internetzugang über Ihr Gerät einrichten. Wenn Sie z. B. sowohl einen Zugang zum Internet, als auch eine Firmennetzanbindung einrichten, dann tragen Sie zum ISP eine Standard-Route und zur Firmenzentrale eine Netzwerk-Route ein. Sie können auf Ihrem Gerät mehrere Standard-Routen eintragen, nur eine einzige aber kann jeweils wirksam sein. Achten Sie daher auf unterschiedliche Werte für die **Metrik**, wenn Sie mehrere Standard-Routen eintragen.

9.3.1.1 Konfiguration von IPv4-Routen

Im Menü **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen** wird eine Liste aller konfigurierten Routen angezeigt.

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = *192.168.2.0*, **Netzmaske** = *255.255.255.0*,**Gateway** = *192.168.2.1*, **Schnittstelle** = *LAN_EN1-0*, **Routentyp** = *Netzwerkroute via Schnittstelle* angezeigt,

9.3.1.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Routen anzulegen.

Wird die Option *Erweitert* für die **Routenklasse** ausgewählt, öffnet sich ein weiterer Konfigurationsabschnitt.

Das Menü **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: • *Standardroute über Schnittstelle*: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Standardroute über Gateway*: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Host-Route über Schnittstelle*: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • *Host-Route via Gateway*: Route zu einem einzelnen Host über ein spezifisches Gateway. • *Netzwerkroute via Schnittstelle* (Standardwert): Route zu einem Netzwerk über eine spezifische Schnittstelle. • *Netzwerkroute via Gateway*: Route zu einem Netzwerk über ein spzifisches Gateway. Nur für Schnittstellen, die im DHCP-Client-Modus betrieben werden: Auch wenn eine Schnittstelle für den DHCP-Client-Betrieb konfiguriert ist, ist es möglich, Routen für den Datenverkehr über diese Schnittstelle zu konfigurieren. Die vom DHCP-Server erhaltenen Einstellungen werden dann mit den hier konfigurierten gemeinsam in die aktive Routing-Tabelle übernommen. Dadurch ist es z. B. möglich, bei dynamisch wechselnden Gateway-Adressen bestimmte Routen aufrecht zu erhalten oder Routen mit unterschiedlicher Metrik (d. h. unteschiedlicher Priorität) festzulegen. Wenn der DHCP-Server allerdings statische Routen (sog. Classless Static Routes) übermittelt, werden die hier konfigurierten Einstellungen nicht

Feld	Beschreibung
	ins Routing übernommen. • *Vorlage für Standardroute per DHCP*: Die Information, welches Gateway verwendet werden soll, wird per DHCP empfangen und in die Route übernommen. • *Vorlage für Host-Route per DHCP*: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt. • *Vorlage für Netzwerkroute per DHCP*: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Netzwerk ergänzt. **Hinweis** Durch dem Ablauf des DHCP Leases oder durch einen Neustart des Geräts werden die Routen, die aus der Kombination von DHCP- und hier vorgenommenen Einstellungen entstehen, zunächst wieder aus dem aktiven Routing gelöscht. Mit einer erneuten DHCP-Konfiguration werden sie dann neu generiert und wieder aktiviert.
Schnittstelle	Wählen Sie die Schnittstelle aus, welche für diese Route verwendet werden soll.
Routenklasse	Wählen Sie die Art der **Routenklasse** aus. Mögliche Werte: • *Standard* (Standardwert): Definiert eine Route mit den Standardparametern. • *Erweitert*: Wählen Sie aus, ob die Route mit erweiterten Parametern definiert werden soll. Ist die Funktion aktiv, wird eine Route mit erweiterten Routing-Parametern wie Quell-Schnittstelle und Quell-IP-Adresse sowie Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und der Status der Geräte-Schnittstelle angelegt.

Felder im Menü Routenparameter

Feld	Beschreibung
Lokale IP-Adresse	Nur für **Routentyp** = *Standardroute über Schnittstelle*, *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die eigene IP-Adresse des Routers auf der ausgewählten Schnittstelle ein.
Ziel-IP-Adresse/Netzmaske	Nur für **Routentyp** *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein. Bei **Routentyp** = *Netzwerkroute via Schnittstelle* Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.
Gateway-IP-Adresse	Nur für **Routentyp** = *Standardroute über Gateway*, *Host-Route via Gateway* oder *Netzwerkroute via Gateway*

Feld	Beschreibung
	Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *15*, der Standardwert ist *1*.

Felder im Menü Erweiterte Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IP-Route ein.
Quellschnittstelle	Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen. Der Standardwert ist *Keine*.
Quell-IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
Layer 4-Protokoll	Wählen Sie ein Protokoll aus. Mögliche Werte: *AH*, *Beliebig* , *ESP*, *GRE*, *ICMP*, *IGMP*, *L2TP*, *OSPF*, *PIM*, *TCP*, *UDP*. Der Standardwert ist *Beliebig*.
Quell-Port	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Quellport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port- Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
Zielport	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Zielport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte:

Feld	Beschreibung
	• *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port- Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
DSCP-/TOS-Wert	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F. Geben Sie für *DSCP-Binärwert*, *DSCP-Dezimalwert*, *DSCP-Hexadezimalwert*, *TOS-Binärwert*, *TOS-Dezimalwert* und *TOS-Hexadezimalwert* den entsprechenden Wert ein.
Modus	Wählen Sie aus, wann die in **Routenparameter**->**Schnittstelle** definierte Schnittstelle benutzt werden soll. Mögliche Werte: • *Wählen und warten* (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • *Verbindlich*: Die Route ist immer benutzbar. • *Wählen und fortfahren*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • *Nie einwählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • *Immer wählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv"

Feld	Beschreibung
	ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

9.3.1.2 Konfiguration von IPv6-Routen

Im Menü **Netzwerk**->**Routen**->**Konfiguration von IPv6-Routen** wird eine Liste aller konfigurierten IPv6-Routen angezeigt.

9.3.1.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Routen anzulegen.

Routen, die über kein -Symbol verfügen, wurden vom Router automatisch erstellt und können nicht bearbeitet werden.

Das Menü **Netzwerk**->**Routen**->**Konfiguration von IPv6-Routen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.
Route aktiv	Wählen Sie, ob die Route aktiv oder inaktiv sein soll. Mit *Aktiviert* wird die Route auf den Status aktiv gesetzt. Standardmäßig ist die Funktion aktiv.
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: • *Standardroute über Schnittstelle* : Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Standardroute über Gateway* : Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist. • *Host-Route über Schnittstelle*: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • *Host-Route via Gateway*: Route zu einem einzelnen Host über ein spezifisches Gateway. • *Netzwerkroute via Schnittstelle*: Route zu einem Netzwerk über eine spezifische Schnittstelle. • *Netzwerkroute via Gateway* (Standardwert): Route zu einem Netzwerk über ein spzifisches Gateway.
Zielschnittstelle	Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll. Sie können unter den Schnittstellen wählen, die unter **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** angelegt sind und für welche die Nutzung von IPv6 aktiviert ist.
Quelladresse/Länge	Geben Sie die IPv6-Quelladresse mit der entsprechenden Präfixlänge ein. Die Eingabe *::* beschreibt eine unspezifische Adresse.

Feld	Beschreibung
	Standardmäßig ist eine Präfixlänge von `64` vorgegeben.
Zieladresse/Länge	Geben Sie die IPv6-Zieladresse mit der entsprechenden Präfixlänge ein. Die Eingabe `::` beschreibt eine unspezifische Adresse. Standardmäßig ist eine Präfixlänge von `64` vorgegeben.
Gateway-Adresse	Geben Sie die IPv6-Adresse für den nächsten Hop ein.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von `0` bis `255`, der Standardwert ist `1`.

9.3.1.3 IPv4-Routing-Tabelle

Im Menü **Netzwerk**->**Routen**->**IPv4-Routing-Tabelle** wird eine Liste aller im System aktiven IPv4-Routen angezeigt.

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = `192.168.2.0`, **Netzmaske** = `255.255.255.0`,**Gateway** = `192.168.2.1`, **Schnittstelle** = `LAN_EN1-0`, **Routentyp** = `Netzwerkroute via Schnittstelle`, **Protokoll** = `Lokal` angezeigt,

Felder im Menü IPv4-Routing-Tabelle

Feld	Beschreibung
Ziel-IP-Adresse	Zeigt die IP-Adresse des Ziel-Hosts bzw. Zielnetzes an.
Netzmaske	Zeigt die Netzmaske des Ziel-Hosts bzw. Zielnetzes an.
Gateway	Zeigt die Gateway IP-Adresse an. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Routentyp	Zeigt den Routentyp an.
Erweiterte Route	Zeigt an, ob eine Route mit erweiterten Parametern konfiguriert worden ist.
Protokoll	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell (`Lokal`) oder über eins der verfügbaren Protokolle.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

9.3.1.4 IPv6-Routing-Tabelle

Im Menü **Netzwerk**->**Routen**->**IPv6-Routing-Tabelle** wird eine Liste aller im System aktiven IPv6-Routen angezeigt.

Felder im Menü IPv6-Routing-Tabelle

Feld	Beschreibung
Route	Zeigt die Quell- und die Zieladresse, die für diese Route verwendet wird an, sowie die Gateway IP-Adresse. Im Falle von per DHCP erhaltenen

Feld	Beschreibung
	Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Protokoll	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell (*Lokal*) oder über eins der verfügbaren Protokolle.

9.3.1.5 Optionen

Überprüfung der Rückroute

Hinter dem Begriff "Überprüfung der Rückroute" (engl. "Back Route Verify") versteckt sich eine einfache, aber sehr leistungsfähige Funktion. Wenn die Überprüfung bei einer Schnittstelle aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden. Dadurch können Sie - auch ohne Filter - die Akzeptanz von Paketen mit gefälschten IP-Adressen verhindern.

Im Auslieferungszustand werden mit der Standardeinstellung *Für bestimmte Schnittstellen aktivieren* die beiden Einträge *en1-0* und *ethoa35-5* angezeigt.

Das Menü **Netzwerk**->**Routen**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Überprüfung der Rückroute

Feld	Beschreibung
Modus	Wählen Sie hier aus, wie die Schnittstellen spezifiziert werden sollen, für die eine Überprüfung der Rückroute aktiviert wird. Mögliche Werte: • *Für alle Schnittstellen aktivieren*: Überprüfung der Rückroute wird für alle Schnittstellen aktiviert. • *Für bestimmte Schnittstellen aktivieren* (Standardwert): Eine Liste aller Schnittstellen wird angezeigt, in der Überprüfung der Rückroute nur für spezifische Schnittstellen aktiviert wird. • *Für alle Schnittstellen deaktivieren*: Überprüfung der Rückroute wird für alle Schnittstellen deaktiviert.
Nr.	Nur für **Modus** = *Für bestimmte Schnittstellen aktivieren* Zeigt die laufende Nummer des Listeneintrags an.
Schnittstelle	Nur für **Modus** = *Für bestimmte Schnittstellen aktivieren* Zeigt den Namen der Schnittstelle an.
Überprüfung der Rückroute	Nur für **Modus** = *Für bestimmte Schnittstellen aktivieren* Wählen Sie aus, ob *Überprüfung der Rückroute* für diese Schnittstelle aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion für alle Schnittstellen deaktiviert.

9.3.2 Allgemeine IPv6-Präfixe

Allgemeine IPv6-Präfixe werden in der Regel von IPv6-Providern vergeben. Sie können statisch zugewiesen oder über DHCP bezogen werden. Meist handelt es sich um /48- oder /56-Netze. Aus diesen Allgemeinen Präfixen können Sie /64-Subnetze erzeugen und in Ihrem Netz weiterverteilen lassen.

Das Konzept der Allgemeinen Präfixe hat zwei entscheidende Vorteile:

- Zwischen Provider und Kunde genügt eine einzige Route.
- Wenn der Provider einen neuen Allgemeinen Präfix per DHCP zuteilt oder einen statisch zugeteilten Allgemeinen Präfix ändern muss, haben Sie als Kunde keinen oder wenig Konfigurationsaufwand: Über DHCP erhalten Sie den neuen Allgemeinen Präfix automatisch. Im Falle des statisch zugeteilten Allgemeinen Präfixes müssen Sie diesen einmal in Ihr System eingeben. Alle aus diesem Allgemeinen Präfix abgeleiteten Subnetze und IPv6-Adressen ändern sich bei einem Update des Allgemeinen Präfixes automatisch.

Um IPv6 zu verwenden, müssen Sie konfigurieren, wie Sie Subnetze und IPv6-Adressen festlegen und verteilen lassen wollen (siehe "IPv6-Adressen konfigurieren unter *Schnittstellen* auf Seite 126 sowie die für IPv6 relevanten Parameter im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**.

9.3.2.1 Konfiguration eines Allgemeinen Präfixes

Im Menü **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes** wird eine Liste aller konfigurierten IPv6-Präfixe angezeigt.

9.3.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Präfixe zu konfigurieren.

Optionen im Menü Basisparameter

Feld	Beschreibung
Aktiver Allgemeiner Präfix	Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll. Mit `Aktiviert` wird das Präfix auf den Status aktiv gesetzt. Standardmäßig ist das Präfix aktiv.
Name	Geben Sie einen Namen für das Allgemeine Präfix ein. Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.
Typ	Wählen Sie, wie der Adressraum zugewiesen werden soll. Mögliche Werte: • `Dynamisch` (Standardwert): Der Allgemeine Präfix wird dynamisch mittels einer DHCP-Übertragung festgesetzt, z. B. von einem Provider. • `Statisch`: Das Präfix wird fest vorgegeben, z. B. durch einen Provider.
Von Schnittstelle	Nur bei **Typ** = `Dynamisch` Wählen Sie die IPv6-Schnittstelle aus, von welcher ein **Allgemeiner Präfix** bezogen werden soll. Sie können unter den Schnittstellen wählen, die unter **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** angelegt sind und die folgende Bedingungen erfüllen: • **IPv6** ist `Aktiviert`.

Feld	Beschreibung
	• **IPv6-Modus** = *Host* • **DHCP-Client** ist *Aktiviert*.
Benutzter Präfix/Länge	Nur bei **Typ** = *Statisch* Geben Sie das Präfix ein, das verwendet werden soll. Geben Sie die zugehörige Länge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Länge von *48* vorgegeben.

9.3.3 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in *NAT-Konfiguration* auf Seite 146).

9.3.3.1 NAT-Schnittstellen

Im Menü **Netzwerk**->**NAT**->**NAT-Schnittstellen** wird eine Liste aller NAT-Schnittstellen angezeigt.

Für jede NAT-Schnittstelle sind die Optionen *NAT aktiv*, *Loopback aktiv*, *Verwerfen ohne Rückmeldung* und *PPTP-Passthrough* auswählbar.

Außerdem wird in *Portweiterleitungen* angezeigt, wie viele Portweiterleitungsregeln für diese Schnittstelle konfiguriert wurden.

Optionen im Menü NAT-Schnittstellen

Feld	Beschreibung
NAT aktiv	Wählen Sie aus, ob NAT für die Schnittstelle aktiviert werden soll. Standardmäßig ist die Funktion nicht aktiv.
Loopback aktiv	Mithilfe der NAT-Loopback-Funktion ist Network Address Translation auch bei Anschlüssen möglich, auf denen NAT nicht aktiv ist. Dies wird verwendet, um Anfragen aus dem LAN so zu interpretieren, als ob sie aus dem WAN kämen. Sie können damit Server Services testen. Standardmäßig ist die Funktion nicht aktiv.
Verwerfen ohne Rückmeldung	Wählen Sie aus, ob IP-Pakete stillschweigend durch NAT abgelehnt werden sollen. Ist diese Funktion deaktiviert, wird der Absender der abgelehnten IP-Pakete mit einer entsprechenden ICMP- oder TCP-RST-Nachricht informiert. Standardmäßig ist die Funktion nicht aktiv.
PPTP-Passthrough	Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll. Standardmäßig ist die Funktion nicht aktiv. Wenn **PPTP-Passthrough** aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.
Portweiterleitungen	Zeigt die Anzahl der in **Netzwerk**->**NAT**->**NAT-Konfiguration** konfigurierten Portweiterleitungsregeln an.

9.3.3.2 NAT-Konfiguration

Im Menü **Netzwerk**->**NAT**->**NAT-Konfiguration** können Sie neben dem Umsetzen von Adressen und Ports einfach und komfortabel Daten von NAT ausnehmen. Für ausgehenden Datenverkehr können Sie verschiedene NAT-Methoden konfigurieren, d. h. Sie können festlegen, wie ein externer Host eine Verbindung zu einem internen Host herstellen darf.

9.3.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um NAT einzurichten.

Das Menü **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu** besteht aus folgenden Feldern:

Feld im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll. Mögliche Werte: • *Beliebig* (Standardwert): NAT wird für alle Schnittstellen konfiguriert. • *<Schnittstellenname>*: Wählen Sie eine der Schnittstellen aus der Liste aus.
Art des Datenverkehrs	Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll. Mögliche Werte: • *eingehend (Ziel-NAT)* (Standardwert): Der Datenverkehr, der von außen kommt. • *ausgehend (Quell-NAT)*: Der Datenverkehr, der nach außen geht. • *exklusiv (ohne NAT)*: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden. Mögliche Werte: • *full-cone* (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiierende Quelladresse und den initialen Quellport senden. • *restricted-cone* (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. • *port-restricted-cone* (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • *symmetrisch* (Standardwert) Für beliebige Protokolle: In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

Im Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** können Sie konfigurieren, für welchen Datenverkehr NAT verwendet werden soll.

Felder im Menü Ursprünglichen Datenverkehr angeben

Feld	Beschreibung
Dienst	Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. Wählen Sie einen der vorkonfigurierten Dienste aus. Mögliche Werte: • *Benutzerdefiniert* (Standardwert) • *<Dienstname>*
Aktion	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)* Wählen Sie, welche Datenpakete von NAT ausgenommen werden. Mögliche Werte: • *Ausschließen* (Standardwert): Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) übereinstimmen, werden von NAT ausgenommen. • *Nicht ausschließen*: Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) nicht übereinstimmen, werden von NAT ausgenommen.
Protokoll	Nur für bestimmte Dienste. Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. In diesem Fall wird UDP automatich festgelegt. Wählen Sie ein Protokoll aus. Je nach ausgewähltem **Dienst** stehen verschiedene Protokolle zur Verfügung. Mögliche Werte: • *Beliebig* (Standardwert) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP*

Feld	Beschreibung
	• *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* oder *exklusiv (ohne NAT)* Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-Port/Bereich	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Originale Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Quell-Port/Bereich	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist. Wenn Sie *Port angeben* wählen, können Sie einen einzelnen Port angeben, mit der Auswahl von *Portbereich angeben* können Sie einen zusammenhängenden Bereich von Ports definieren, der als Filter für den ausgehenden Datenverkehr verwendet wird.
Quell-Port/Bereich	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Quell-Port bzw. den Quell-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)* bzw. *aus-*

Feld	Beschreibung
IP-Adresse/Netzmaske	*gehend (Quell-NAT)* und **NAT-Methode** = *symmetrisch* Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Ziel-Port/Bereich	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* oder **Art des Datenverkehrs** = *exklusiv (ohne NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.

Im Menü **NAT-Konfiguration** ->**Substitutionswerte** können Sie, abhängig davon, ob es sich um eingehenden oder ausgehenden Datenverkehr handelt, neue Adressen und Ports definieren, auf welche bestimmte Adressen und Ports aus dem Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** umgesetzt werden.

Felder im Menü Substitutionswerte

Feld	Beschreibung
Neue Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* Geben Sie diejenige Ziel-IP-Adresse und die zugehörige Netzmaske ein, auf welche die ursprüngliche Ziel-IP-Adresse umgesetzt werden soll.
Neuer Ziel-Port	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll. Mit Auswahl von *Original* belassen Sie den ursprünglichen Ziel-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Ziel-Port eingeben. Standardmäßig ist *Original* aktiv.
Neue Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *symmetrisch* Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.
Neuer Quell-Port	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch*, **Dienst** = *Benutzerdefiniert*, **Protokoll** = *TCP*, *UDP*, *TCP/UDP* und **Original Quell-Port/Bereich**= *-Alle-* oder *Port angeben* Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll. Mit Auswahl von *Original* belassen Sie den ursprünglichen Quell-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist *Original* aktiv. Haben Sie für **Original Quell-Port/Bereich** *Portbereich angeben* gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung:

Feld	Beschreibung
	• *Original Quell-Port/Bereich verwenden*: Der in **Original Quell-Port/Bereich** angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten. • *Original Port/Bereich beginnt mit*: Es erscheint ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

9.3.4 Lastverteilung

Zunehmender Datenverkehr über das Internet erfordert die Möglichkeit, Daten über unterschiedliche Schnittstellen senden zu können, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. IP-Lastverteilung ermöglicht die geregelte Verteilung von Datenverkehr innerhalb einer bestimmten Gruppe von Schnittstellen.

9.3.4.1 Lastverteilungsgruppen

Wenn Schnittstellen zu Gruppen zusammengefasst sind, wird der Datenverkehr innerhalb einer Gruppe nach folgenden Prinzipien aufgeteilt:

- Im Unterschied zu Multilink-PPP-basierten Lösungen funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.
- Session-based Load Balancing wird realisiert.
- Zusammenhängende (abhängige) Sessions werden immer über dieselbe Schnittstelle geroutet.
- Eine Distributionsentscheidung fällt nur bei ausgehenden Sessions.

Im Menü **Netzwerk**->**Lastverteilung**->**Lastverteilungsgruppen** wird eine Liste aller konfigurierten Lastverteilungsgruppen angezeigt. Mit einem Klick auf das -Symbol neben einem Listeneintrag gelangen Sie zu einer Übersicht diese Gruppe betreffende Grundparameter.

Hinweis

Beachten Sie, dass die Schnittstellen, die zu einer Lastverteilungsgruppe zusammengefasst werden, Routen mit gleicher Metrik besitzen müssen. Gehen Sie ggf. in das Menü **Netzwerk**->**Routen** und überprüfen Sie dort die Einträge.

9.3.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Gruppen einzurichten.

Das Menü **Netzwerk**->**Lastverteilung**->**Lastverteilungsgruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
Verteilungsrichtlinie	Wählen Sie aus, auf welche Art der Datenverkehr auf die für die Gruppe konfigurierten Schnittstellen verteilt werden soll. Mögliche Werte: • *Sitzungs-Round-Robin* (Standardwert): Eine neu hinzukommende Session wird je nach prozentualer Belegung der Schnittstellen mit Sessions einer der Gruppen-Schnittstellen zugewiesen. Die Anzahl der Sessions ist maßgeblich. • *Lastabhängige Bandbreite*: Eine neu hinzukommende Session wird je nach Anteil der Schnittstellen an der Gesamtdatenrate einer der Gruppen-Schnittstellen zugewiesen. Maßgeblich ist die aktuelle Daten-

Feld	Beschreibung
	rate, wobei der Datenverkehr sowohl in Sende- als auch in Empfangsrichtung berücksichtigt wird.
Berücksichtigen	Nur für **Verteilungsrichtlinie** = *Lastabhängige Bandbreite* Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll. Optionen: • *Download*: Nur die Datenrate in Empfangsrichtung wird berücksichtigt. • *Upload*: Nur die Datenrate in Senderichtung wird berücksichtigt. Standardmäßig sind die Optionen *Download* und *Upload* deaktiviert.
Verteilungsmodus	Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden. Mögliche Werte: • *Immer* (Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen. • *Nur aktive Schnittstellen verwenden*: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.

Im Bereich **Schnittstelle** fügen Sie Schnittstellen hinzu, die dem aktuellen Gruppenkontext entsprechen und konfigurieren diese. Sie können auch Schnittstellen löschen.

Legen Sie weitere Einträge mit **Hinzufügen** an.

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Zeigt die Beschreibung der Schnittstellen-Gruppe an.
Verteilungsrichtlinie	Zeigt die gewählte Art des Datenverkehrs an.

Felder im Menü Schnittstellenauswahl für Verteilung

Feld	Beschreibung
Schnittstelle	Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, die der Gruppe angehören sollen.
Verteilungsverhältnis	Geben Sie an, welchen Prozentsatz des Datenverkehrs eine Schnittstelle übernehmen soll. Die Bedeutung unterscheidet sich je nach verwendetem **Verteilungsverhältnis**: • Für *Sitzungs-Round-Robin* wird die Anzahl verteilter Sessions zugrunde gelegt. • Für *Lastabhängige Bandbreite* ist die Datenrate maßgeblich.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Routenselektor	Der Parameter **Routenselektor** ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwen-

Feld	Beschreibung
	dungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing -Gruppe bilanzieren zu können. Für die Anwendung des Parameters gelten folgende Regeln: • Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig. • Ist eine Schnittstelle mehreren Lastverteilungsgruppenn zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich. • Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein. Wählen Sie die **Ziel-IP-Adresse** der gewünschten Route aus. Sie können unter allen Routen und allen erweiterten Routen wählen.
IP-Adresse zur Nachverfolgung	Mit dem Parameter **IP-Adresse zur Nachverfolgung** können Sie eine bestimmte Route überwachen lassen. Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden kann dies im Menü **Lokale Dienste**->**Überwachung**->**Hosts**. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion **Überwachen** berücksichtigt werden. Über die Konfiguration der **IP-Adresse zur Nachverfolgung** im Menü **Lastverteilung**->**Lastverteilungsgruppen**->**Erweiterte Einstellungen** erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit vom Status des zugewiesenen Host-Überwachungseintrages. Wählen Sie die IP-Adresse der Route, die überwacht werden soll. Sie können unter den IP-Adressen wählen, die Sie im Menü **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu** unter **Überwachte IP-Adresse** eingegeben haben und die mit Hilfe des Feldes **Auszuführende Aktion** überwacht werden (**Aktion** = *Überwachen*) .

9.3.4.2 Special Session Handling

Special Session Handling ermöglicht Ihnen einen Teil des Datenverkehrs auf Ihrem Gerät über eine bestimmte Schnittstelle zu leiten. Dieser Datenverkehr wird von der Funktion **Lastverteilung** ausgenommen.

Die Funktion **Special Session Handling** können Sie zum Beispiel beim Online Banking verwenden, um sicherzustellen, dass der HTTPS-Datenverkehr auf einen bestimmten Link übertragen wird. Da beim Online Banking geprüft wird, ob der gesamte Datenverkehr aus derselben Quelle stammt , würde ohne **Special Session Handling** die Datenübertragung bei Verwendung von **Lastverteilung** unter Umständen abgebrochen.

Im Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling** wird eine Liste mit Einträgen angezeigt. Wenn Sie noch keine Einträge konfiguriert haben, ist die Liste leer.

Jeder Eintrag enthält u. a. Parameter, welche die Eigenschaften eines Datenpakets mehr oder weniger detailliert beschreiben. Das erste Datenpaket, auf das die hier konfigurierten Eigenschaften zutreffen, legt die Route für bestimmte nachfolgende Datenpakete fest.

Welche Datenpakete danach über diese Route geleitet werden, wird im Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling**->**Neu**->**Erweiterte Einstellungen** konfiguriert.

Wenn Sie zum Beispiel im Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling**->**Neu** den Parameter **Dienst** = *http (SSL)* wählen (und bei allen anderen Parametern die Standardwerte belassen), so legt das erste HTTPS-Paket die **Zieladresse** und den **Zielport** (d.h. Port 443 bei HTTPS) für später gesendete Datenpakete fest.

Wenn Sie unter **Unveränderliche Parameter** für die beide Parameter **Zieladresse** und **Zielport** die Standardeinstellung *aktiviert* belassen, so werden die HTTPS-Pakete mit derselben Quell-IP-Adresse wie das erste HTTPS-Paket über Port 443 zur selben **Zieladresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

9.3.4.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Einträge anzulegen.

Das Menü **Netzwerk**->**Lastverteilung**->**Special Session Handling**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob Special Session Handling aktiv sein soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *Benutzerdefiniert*.
Protokoll	Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Ziel-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* (Standardwert) • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Geben Sie, falls gewünscht, eine Ziel-Port-Nummer bzw. einen Bereich

Feld	Beschreibung
	von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Ziel-Port-Bereich ein.
Quellschnittstelle	Wählen Sie, falls gewünscht, die Quellschnittstelle Ihres Geräts aus.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* (Standardwert) • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Geben Sie, falls gewünscht, eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Quell-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Quell-Port ein. • *Portbereich angeben*: Geben Sie einen Quell-Port-Bereich ein.
Special Handling Timer	Geben Sie ein, während welcher Zeitspanne die spezifizierten Datenpakete über den festgelegten Weg geroutet werden sollen. Der Standardwert ist *900* Sekunden.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Unveränderliche Parameter	Legen Sie fest, ob die beiden Parameter **Zieladresse** und **Zielport** bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d. h. ob die nachfolgenden Datenpakete über denselben **Zielport** zur selben **Zieladresse** geroutet werden müssen. Standardmäßig sind die beiden Parameter **Zieladresse** und **Zielport** aktiv. Belassen Sie die Voreinstellung *Aktiviert* bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parameters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket. Sie können, falls gewünscht, einen oder beide Parameter deaktivieren. Der Parameter **Quell-IP-Adresse** muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.

9.3.5 QoS

QoS (Quality of Service) ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt und Bandbreite für diese reserviert werden. Vor allem für zeitkritische Anwendungen wie z. B. Voice over IP ist das von Vorteil.

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren

9.3.5.1 IPv4/IPv6-Filter

Im Menü **Netzwerk**->**QoS**->**IPv4/IPv6-Filter** werden IP-Filter konfiguriert.

Die Liste zeigt ebenfalls alle ggf. konfigurierten Einträge aus **Netzwerk**->**Zugriffsregeln**->**Regelketten**.

9.3.5.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Filter zu definieren.

Das Menü **Netzwerk**->**QoS**->**IPv4/IPv6-Filter**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *any*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Typ	Nur für **Protokoll** = *ICMP* Wählen Sie einen Typ aus. Mögliche Werte: *Beliebig*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Siehe RFC 792. Der Standardwert ist *Beliebig*.
Verbindungsstatus	Bei **Protokoll** = *TCP* können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt.

Feld	Beschreibung
	Mögliche Werte: • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete.
IPv4-Zieladresse/-netzmaske	Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP*, *UDP* oder *TCP/UDP* Geben Sie eine Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Zielport ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
IPv4-Quelladresse/-netzmaske	Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP*, *UDP* oder *TCP/UDP*

Feld	Beschreibung
	Geben Sie eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Quellport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Quellport ein. • *Portbereich angeben*: Geben Sie einen Quellport-Bereich ein.
DSCP / Traffic Class Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Wertebereich *0* bis *7*. Der Standardwert ist *Nicht beachten*.

9.3.5.2 QoS-Klassifizierung

Im Menü **Netzwerk**->**QoS**->**QoS-Klassifizierung** wird der Datenverkehr klassifiziert, d. h. der Datenverkehr wird mittels Klassen-ID verschiedenen Klassen zugeordnet. Sie erstellen dazu Klassenpläne zur Klassifizierung von IP-Paketen anhand zuvor definierter IP-Filter. Jeder Klassenplan wird über seinen ersten Filter mindestens einer Schnittstelle zugeordnet.

9.3.5.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Datenklassen einzurichten.

Das Menü **Netzwerk**->**QoS**->**QoS-Klassifizierung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an.

Feld	Beschreibung
	• *<Name des Klassenplans>*: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	Nur für **Klassenplan** = *Neu* Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll. Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü **Netzwerk**->**QoS**->**IPv4/IPv6-Filter** konfiguriert sein.
Richtung	Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen. Mögliche Werte: • *Eingehend*: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet. • *Ausgehend* (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet. • *Beide*: Eingehende und ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet.
High-Priority-Klasse	Aktivieren oder deaktivieren Sie die High-Priority-Klasse. Wenn die High-Priority-Klasse aktiv ist, werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet, die Priorität 0 wird automatisch gesetzt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Klassen-ID	Nur für **High-Priority-Klasse** nicht aktiv. Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist. **Hinweis** Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.) Mögliche Werte sind ganze Zahlen zwischen *1* und *254*.
DSCP/Traffic-Class-Filter setzen (Layer 3)	Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (**Klassen-ID**) setzen bzw. ändern. Mögliche Werte: • *Erhalten* (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC

Feld	Beschreibung
	3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
Setzen Sie den COS Wert (802.1p/Layer 2)	Im Header der Ethernet-Pakete, die vom ausgewählten Filter erfasst werden, können Sie hier die Serviceklasse (Layer-2-Priorität) setzen/ändern. Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Der Standardwert ist *Erhalten*.
Schnittstellen	Nur für **Klassenplan** = *Neu* Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.

9.3.5.3 QoS-Schnittstellen/Richtlinien

Im Menü **Netzwerk**->**QoS**->**QoS-Schnittstellen/Richtlinien** legen Sie die Priorisierung der Daten fest.

Hinweis

Daten können nur ausgehend priorisiert werden.

Pakete der High-Priority-Klasse haben immer Vorrang vor Daten mit Klassen-ID 1 - 254.

Es ist möglich, jeder Queue und somit jeder Datenklasse einen bestimmten Anteil an der Gesamtbandbreite der Schnittstelle zuzuweisen bzw. zu garantieren. Darüber hinaus können Sie die Übertragung von Sprachdaten (Real-Time-Daten) optimieren.

Abhängig von der jeweiligen Schnittstelle wird für jede Klasse automatisch eine Queue (Warteschlange) angelegt, jedoch nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr. Den automatisch angelegten Queues wird hierbei eine Priorität zugeordnet. Der Wert der Priorität ist dabei gleich dem Wert der Klassen-ID. Sie können diese standardmäßig gesetzte Priorität einer Queue ändern. Wenn Sie neue Queues hinzufügen, können Sie über die Klassen-ID auch Klassen anderer Klassenpläne verwenden.

9.3.5.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Priorisierungen einzurichten.

Das Menü **Netzwerk**->**QoS**->**QoS-Schnittstellen/Richtlinien**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.
Priorisierungsalgorithmus	Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausge-

Feld	Beschreibung
	wählten Schnittstelle. Mögliche Werte: • *Priority Queueing*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. • *Weighted Round Robin*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (weight) der Queues verteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig behandelt. • *Weighted Fair Queueing*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. • *Deaktiviert* (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für **Traffic Shaping** = aktiviert. Geben Sie für die ausgewählte Schnittstelle eine maximale Datenrate in kBit pro Sekunde in Senderichtung ein. Mögliche Werte sind *0* bis *1000000*. Der Standardwert ist *0*, d. h. es erfolgt keine Begrenzung, die ausgewählte Schnittstelle kann ihre maximale Bandbreite belegen.
Größe des Protokoll-Headers unterhalb Layer 3	Nur für **Traffic Shaping** = aktiviert. Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen. Mögliche Werte: • *Benutzerdefiniert* Wert in Byte. Mögliche Werte sind *0* bis *100*. • *Undefiniert (Protocol Header Offset=0)* (Standardwert) Nur für Ethernet-Schnittstellen auswählbar • *Ethernet* • *Ethernet und VLAN* • *PPP over Ethernet* • *PPPoE und VLAN* Nur für IPSec-Schnittstellen auswählbar: • *IPSec über Ethernet* • *IPSec über Ethernet und VLAN*

Feld	Beschreibung
	• *IPSec via PPP over Ethernet* • *IPSec via PPPoE und VLAN*
Verschlüsselungsmethode	Nur wenn als **Schnittstelle** ein IPSec Peer gewählt ist, **Traffic Shaping** *Aktiviert* ist und die **Größe des Protokoll-Headers unterhalb Layer 3** nicht *Undefiniert (Protocol Header Offset=0)* ist. Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird. Mögliche Werte: • *DES, 3DES, Blowfish, Cast - (Cipher-Blockgröße = 64 Bit)* • *AES128, AES192, AES256, Twofish - (Cipher-Blockgröße = 128 Bit)*
Real Time Jitter Control	Nur für **Traffic Shaping** = aktiviert Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite. Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s). Aktivieren oder deaktivieren Sie Real Time Jitter Control. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Kontrollmodus	Nur für **Real Time Jitter Control** = aktiviert. Wählen Sie den Modus für die Optimierung der Sprachübertragung. Mögliche Werte: • *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. • *Inaktiv*: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • *Nur kontrollierte RTP-Streams*: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW. • *Immer*: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.

Felder im Menü Queues/Richtlinie

Feld	Beschreibung
Queues/Richtlinien	Konfigurieren Sie die gewünschten QoS-Queues. Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und

Feld	Beschreibung
	hier angezeigt (nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr). Fügen Sie mit **Hinzufügen** neue Einträge hinzu. Das Menü **Queue/ Richtlinie bearbeiten** öffnet sich. Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag DEFAULT mit der niedrigsten Priorität 255 erstellt.

Das Menü **Queue/Richtlinie bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Queue/Richtlinie bearbeiten

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungsqueue	Wählen Sie den Typ für die Priorisierung der Queue aus. Mögliche Werte: • *Klassenbasiert* (Standardwert): Queue für "normal"-klassifizierte Daten. • *Hohe Priorität*: Queue für "high-priority"- klassifizierte Daten. • *Standard*: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	Nur für **Priorisierungsqueue** = *Klassenbasiert* Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll. Dazu muss vorher im Menü **Netzwerk**->**QoS**->**QoS-Klassifizierung** mindestens eine Klassen-ID vergeben worden sein.
Priorität	Nur für **Priorisierungsqueue** = *Klassenbasiert* Wählen Sie die Priorität der Queue. Mögliche Werte sind *1 (hohe Priorität)* bis *254 (niedrige Priorität)*. Der Standardwert ist *1*.
Gewichtung	Nur für **Priorisierungsalgorithmus** = *Weighted Round Robin* oder *Weighted Fair Queueing* Wählen Sie die Gewichtung der Queue. Mögliche Werte sind *1* bis *254*. Der Standardwert ist *1*.
RTT-Modus (Realtime-Traffic-Modus)	Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen. Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.

Feld	Beschreibung
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung. Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.) Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für **Traffic Shaping** = aktiviert. Geben Sie eine maximale Datenrate in kBit pro Sekunde für die ausgewählte Schnittstelle ein. Mögliche Werte sind *0* bis *1000000*. Der Standardwert ist *0*, d. h. es erfolgt keine Begrenzung, die ausgewählte Schnittstelle kann ihre maximale Bandbreite belegen.
Überbuchen zugelassen	Nur für **Traffic Shaping** = aktiviert. Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten. Bei aktiviertem **Überbuchen zugelassen** kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist. Bei deaktiviertem **Überbuchen zugelassen** kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Burst-Größe	Nur für **Traffic Shaping** = aktiviert. Geben Sie die maximale Anzahl an Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist. Mögliche Werte sind *0* bis *64000*. Der Standardwert ist *0*.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Dropping-Algorithmus	Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird. Mögliche Werte: • *Tail Drop* (Standardwert): Das neu hinzugekommene Paket wird verworfen. • *Head Drop*: Das älteste Paket in der Queue wird verworfen. • *Random Drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von Daten-	Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpake-

Feld	Beschreibung
stau (RED)	ten. Pakete, deren Datengröße zwischen **Min. Queue-Größe** und **Max. Queue-Größe** liegt, werden vorbeugend verworfen, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden können. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Min. Queue-Größe	Geben Sie den unteren Schwellwert für das Verfahren **Vermeidung von Datenstau (RED)** in Byte ein. Mögliche Werte sind *0* bis *262143*. Der Standardwert ist *0*.
Max. Queue-Größe	Geben Sie den oberen Schwellwert für das Verfahren **Vermeidung von Datenstau (RED)** in Byte ein. Mögliche Werte sind *0* bis *262143*. Der Standardwert ist *16384*.

9.3.6 Zugriffsregeln

Mit Access-Listen werden Zugriffe auf Daten und Funktionen eingegrenzt (welcher Benutzer welche Dienste und Dateien nutzen darf).

Sie definieren Filter für IP-Pakete, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, dass über das Gateway unzulässige Verbindungen aufgebaut werden. Access-Listen definieren die Art des IP-Traffics, den das Gateway annehmen oder ablehnen soll. Die Zugangsentscheidung basiert auf Informationen, die in den IP-Paketen enthalten sind, z. B.:

- Quell- und/oder Ziel IP-Adresse
- Protokoll des Pakets
- Quell- und/oder Ziel-Port (Portbereiche werden unterstützt)

Möchten z. B. Standorte, deren LANs über eine **Digitalisierungsbox** miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

Access-Filter auf dem Gateway basieren auf der Kombination von Filtern und Aktionen zu Filterregeln (= rules) und der Verknüpfung dieser Regeln zu sogenannten Regelketten. Sie wirken auf die eingehenden Datenpakete und können so bestimmten Daten den Zutritt zum Gateway erlauben oder verbieten.

Ein Filter beschreibt einen bestimmten Teil des IP-Datenverkehrs, basierend auf Quell- und/oder Ziel-IP-Adresse, Netzmaske, Protokoll, Quell- und/ oder Ziel-Port.

Mit den Regeln, die Sie in Access Lists organisieren, teilen Sie dem Gateway mit, wie es mit gefilterten Datenpaketen umgehen soll – ob es sie annehmen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Für die Definition von Regeln bzw. Regelketten gibt es verschiedene Ansätze:

Nehme alle Pakete an, die nicht explizit verboten sind, d. h.:

- Weise alle Pakete ab, auf die Filter 1 zutrifft.

- Weise alle Pakete ab, auf die Filter 2 zutrifft.
- ...
- Lass den Rest durch.

oder

Nehme nur Pakete an, die explizit erlaubt sind, d. h.:

- Nehme alle Pakete an, auf die Filter 1 zutrifft.
- Nehme alle Pakete an, auf die Filter 2 zutrifft.
- ...
- Weise den Rest ab.

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

Es können mehrere getrennte Regelketten angelegt werden. Eine gemeinsame Nutzung von Filtern in verschiedenen Regelketten ist dabei möglich.

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.

Achtung

Achten Sie darauf, dass Sie sich beim Konfigurieren der Filter nicht selbst aussperren.

Greifen Sie zur Filter-Konfiguration möglichst mit ISDN-Login auf Ihr Gateway zu.

9.3.6.1 Zugriffsfilter

In diesem Menü werden die Access-Filter konfiguriert. Jedes Filter beschreibt einen bestimmten Teil des IP-Traffic und definiert z. B. die IP-Adressen, das Protokoll, den Quell- oder Ziel-Port.

Im Menü **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter** wird eine Liste aller Access Filter angezeigt.

9.3.6.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Access Filter zu konfigurieren.

Das Menü **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *any*.

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Typ	Nur bei **Protokoll** = *ICMP* Mögliche Werte: • *Beliebig* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* Der Standardwert ist *Beliebig*. Siehe RFC 792.
Verbindungsstatus	Nur bei **Protokoll** = *TCP* Sie können ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt. Mögliche Werte: • *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete. • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden.
IPv4-Zieladresse/-netzmaske	Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
Ziel-Port/Bereich	Nur bei **Protokoll** = *TCP*, *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein, auf den das Filter passt. Mögliche Werte:

Feld	Beschreibung
	• *-Alle-* (Standardwert): Das Filter gilt für alle Port-Nummern • *Port angeben*: Ermöglicht Eingabe einer Port-Nummer. • *Portbereich angeben*: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
IPv4-Quelladresse/-netzmaske	Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	Nur bei **Protokoll** = *TCP*, *UDP* Geben Sie die Quell-Port-Nummer bzw. den Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Das Filter gilt für alle Port-Nummern • *Port angeben*: Ermöglicht Eingabe einer Port-Nummer. • *Portbereich angeben*: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
DSCP / Traffic Class Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.

Feld	Beschreibung
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Der Standardwert ist *Nicht beachten*.

9.3.6.2 Regelketten

Im Menü **Regelketten** werden Regeln für IP-Filter konfiguriert. Diese können separat angelegt oder in Regelketten eingebunden werden.

Im Menü **Netzwerk**->**Zugriffsregeln**->**Regelketten** werden alle angelegten Filterregeln aufgelistet.

9.3.6.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Access Lists zu konfigurieren.

Das Menü **Netzwerk**->**Zugriffsregeln**->**Regelketten**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Regelkette	Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. • *<Name der Regelkette>*: Wählen Sie eine bereits angelegte Regelkette aus und fügen ihr somit eine weitere Regel hinzu.
Beschreibung	Geben Sie die Bezeichnung der Regelkette ein.
Zugriffsfilter	Wählen Sie ein IP-Filter aus. Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll. Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *Zulassen, wenn Filter passt* (Standardwert): Paket annehmen, wenn das Filter passt. • *Zulassen, wenn Filter nicht passt*: Paket annehmen, wenn das Filter nicht passt. • *Verweigern, wenn Filter passt*: Paket abweisen, wenn das Filter passt. • *Verweigern, wenn Filter nicht passt*: Paket abweisen, wenn das Filter nicht passt. • *Nicht beachten*: Nächste Regel anwenden.

Um die Regeln einer Regelkette in eine andere Reihenfolge zu bringen, wählen Sie im Listenmenü bei dem Eintrag, der verschoben werden soll, die Schaltfläche . Daraufhin öffnet sich ein Dialog, bei dem Sie unter **Verschieben** entscheiden können, ob der Eintrag *unter* (Standardwert) oder *über* eine andere Regel dieser Regelkette verschoben wird.

9.3.6.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten den einzelnen Schnittstellen zugeordnet und das Verhalten des Gateways beim Abweisen von IP-Paketen festgelegt.

Im Menü **Netzwerk**->**Zugriffsregeln**->**Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

9.3.6.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Zuordnungen zu konfigurieren.

Das Menü **Netzwerk**->**Zugriffsregeln**->**Schnittstellenzuweisung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.
Verwerfen ohne Rückmeldung	Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll. • *Aktiviert* (Standardwert) : Der Absender wird nicht informiert. • *Deaktiviert*: Der Absender erhält eine ICMP-Nachricht.
Berichtsmethode	Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll. Mögliche Werte: • *Kein Bericht*: Keine Syslog-Meldung. • *Info* (Standardwert): Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IPAdresse und Quell-Port-Nummer wird generiert. • *Dump*: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

9.4 Multicast

Was ist Multicasting?

Viele jüngere Kommunikations-Technologien basieren auf der Kommunikation von einem Sender zu mehreren Empfängern. Daher liegt auf der Reduzierung des Datenverkehrs ein Hauptaugenmerk von modernen Telekommunikationssystemen wie Voice-over-IP oder Video- und Audio-Streaming (z. B. IPTV oder Webradio), z. B. im Rahmen von TriplePlay (Voice, Video, Daten). Multicast bietet eine kostengünstige Lösung zur effektiven Bandbreitennutzung, dadurch dass der Sender das Datenpaket, welches mehrere Empfänger empfangen können, nur einmal senden muss. Dabei wird an eine virtuelle Adresse gesendet, die als Multicast-Gruppe bezeichnet wird. Interessierte Empfänger melden sich bei diesen Gruppen an.

Weitere Anwendungsbereiche

Ein klassischer Einsatzbereich von Multicast sind Konferenzen (Audio/Video) mit mehreren Empfängern. Allen voran dürften die bekanntesten MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) und das Whiteboard (WB) sein. Mit Hilfe von VAT können Audiokonferenzen durchgeführt werden.

Hierzu werden alle Gesprächspartner in einem Fenster sichtbar gemacht und der/die Sprecher mit einem schwarzen Kasten gekennzeichnet. Andere Anwendungsgebiete sind vor allem für Firmen interessant. Hier bietet Multicasting die Möglichkeit, die Datenbanken mehrerer Server gleichzeitig zu synchronisieren, was für multinationale oder auch für Firmen mit nur wenigen Standorten lohnenswert ist.

Adressbereich für Multicast

Für IPv4 sind im Klasse-D-Netzwerk die IP-Adressen 224.0.0.0 bis 239.255.255.255 (224.0.0.0/4) für Multicast reserviert. Eine IP-Adresse aus diesem Bereich repräsentiert eine Multicast-Gruppe, für die sich mehrere Empfänger anmelden können. Der Multicast-Router leitet dann gewünschte Pakete in alle Subnetze mit angemeldeten Empfängern weiter.

Multicast Grundlagen

Multicast ist verbindungslos, d. h. eine etwaige Fehlerkorrektur oder Flusskontrolle muss auf Applikationsebene gewährleistet werden.

Auf der Transportebene kommt fast ausschließlich UDP zum Einsatz, da es im Gegensatz zu TCP nicht an eine Punkt-zu-Punkt-Verbindung angelehnt ist.

Der wesentliche Unterschied besteht somit auf IP-Ebene darin, dass die Zieladresse keinen dedizierten Host adressiert, sondern an eine Gruppe gerichtet ist, d. h. beim Routing von Multicast-Paketen ist allein entscheidend, ob sich in einem angeschlossenen Subnetz ein Empfänger befindet.

Im lokalen Netzwerk sind alle Hosts angehalten, alle Multicast-Pakete zu akzeptieren. Das basiert bei Ethernet oder FDD auf einem sogenannten MAC-Mapping, bei dem die jeweilige Gruppen-Adresse in die Ziel-MAC-Adresse kodiert wird. Für das Routing zwischen mehreren Netzen müssen sich bei den jeweiligen Routern vorerst alle potentiellen Empfänger im Subnetz bekannt machen. Dies geschieht durch sog. Membership-Management-Protokolle wie IGMP bei IPv4 und MLP bei IPv6.

Membership-Management-Protokoll

IGMP (Internet Group Management Protocol) ist in IPv4 ein Protokoll, mit dem Hosts dem Router Multicast-Mitgliedsinformationen mitteilen können. Hierbei werden für die Adressierung IP-Adressen des Klasse-D-Adressraums verwendet. Eine IP-Adresse dieser Klasse repräsentiert eine Gruppe. Ein Sender (z. B. Internetradio) sendet an diese Gruppe. Die Adressen (IP) der verschiedenen Sender innerhalb einer Gruppe werden als Quell(-Adressen) bezeichnet. Es können somit mehrere Sender (mit unterschiedlichen IP-Adressen) an dieselbe Multicast-Gruppe senden. So kommt eine 1-zu-n-Beziehung zwischen Gruppen- und Quelladressen zustande. Diese Informationen werden an den Router über Reports weitergegeben. Ein Router kann bei eingehenden Multicast-Datenverkehr anhand dieser Informationen entscheiden, ob ein Host in seinem Subnetz diesen empfangen will oder nicht. Ihr Gerät unterstützt die aktuelle Version IGMP V3, welche abwärtskompatibel ist, d. h. es können sowohl V3- als auch V1- und V2-Hosts verwaltet werden.

Ihr Gerät unterstützt folgende Multicast-Mechanismen:

- Forwarding (Weiterleiten): Dabei handelt es sich um statisches Forwarding, d.h. eingehender Datenverkehr für eine Gruppe wird auf jeden Fall weitergeleitet. Dies bietet sich an, wenn Multicast-Datenverkehr permanent weitergeleitet werden soll.
- IGMP: Mittels IGMP werden Informationen über die potentiellen Empfänger in einem Subnetz gesammelt. Bei einem Hop kann dadurch eingehender Multicast-Datenverkehr ausgesondert werden.

Tipp

Bei Multicast liegt das Hauptaugenmerk auf dem Ausschluss von Datenverkehr ungewünschter Multicast-Gruppen. Beachten Sie daher, dass bei einer etwaigen Kombination von Forwarding mit IGMP die Pakete an die im Forwarding angegebenen Gruppen auf jeden Fall weitergeleitet werden können.

9.4.1 Allgemein

9.4.1.1 Allgemein

Im Menü **Multicast**->**Allgemein**->**Allgemein** können Sie die Multicast-Funktionalität aus- bzw. einschalten.

Das Menü besteht aus den folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Multicast Routing	Wählen Sie aus, ob **Multicast Routing** verwendet werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

9.4.2 IGMP

Mit IGMP (Internet Group Management Protocol, siehe RFC 3376) werden die Informationen über die Gruppen (zugehörigkeit) in einem Subnetz signalisiert. Somit gelangen nur diejenigen Pakete in das Subnetz, die explizit von einem Host gewünscht sind.

Spezielle Mechanismen sorgen für die Vereinigung der Wünsche der einzelnen Clients. Derzeit gibt es drei Versionen von IGMP (V1 - V3), wobei aktuelle Systeme meist V3, seltener V2, benutzen.

Bei IGMP spielen zwei Paketarten die zentrale Rolle: Queries und Reports.

Queries werden ausschließlich von einem Router versendet. Sollten mehrere IGMP-Router in einem Netzwerk existieren, so wird der Router mit der niedrigeren IP-Adresse der sogenannte Querier. Hierbei unterscheidet man das General Query (versendet an 224.0.0.1), die Group-Specific Query (versendet an jeweilige Gruppenadresse) und die Group-and-Source-Specific Query (versendet an jeweilige Gruppenadresse). Reports werden ausschließlich von Hosts versendet, um Queries zu beantworten.

9.4.2.1 IGMP

In diesem Menü konfigurieren Sie die Schnittstellen, auf denen IGMP aktiv sein soll.

9.4.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um IGMP auf weiteren Schnittstellen zu konfigurieren.

Das Menü **Multicast**->**IGMP**->**IGMP**->**Neu** besteht aus den folgenden Feldern:

Felder im Menü IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage-Intervall	Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen. Möglich Werte sind *0* bis *600*. Der Standardwert ist *125*.
Maximale Antwortzeit	Geben Sie für das Senden von Queries an, in welchem Zeitintervall in Sekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Intervall zufällig eine Verzögerung, bis die Antwort gesendet wird.

Feld	Beschreibung
	Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung erreichen. Möglich Werte sind *0,0* bis *25,0*. Der Standardwert ist *10,0*.
Robustheit	Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency). Möglich Werte sind *2* bis *8*. Der Standardwert ist *2*.
Antwortintervall (Letztes Mitglied)	Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet. Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen. Möglich Werte sind *0,0* bis *25,0*. Der Standardwert ist *1,0*.
Maximale Anzahl der IGMP-Statusmeldungen	Limitieren Sie die Anzahl der Reports/Queries pro Sekunde für die gewählte Schnittstelle.
Modus	Wählen Sie aus, ob die hier definierte Schnittstelle nur im Host-Modus oder auch im Routing Modus arbeitet. Mögliche Werte: • *Routing* (Standardwert): Die Schnittstelle wird im Routing-Modus betrieben. • *Host*: Die Schnittstelle wird nur im Host-Modus betrieben.

IGMP Proxy

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IGMP Proxy	Wählen Sie aus, ob Ihr Gerät die IGMP-Meldungen der Hosts im Subnetz über seine definierte **Proxy-Schnittstelle** weiterleiten soll.
Proxy-Schnittstelle	Nur für **IGMP Proxy** = aktiviert Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.
Fallback-Proxy-Schnittstelle 1	Nur für **IGMP Proxy** = aktiviert Wählen Sie die Fallback-Schnittstelle 1 Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen. Diese wird verwendet, wenn die IGMP-Proxy-Funktion über die **Proxy-Schnittstelle** nicht ausgeführt werden kann.

Feld	Beschreibung
Fallback-Proxy-Schnittstelle 2	Nur für **IGMP Proxy** = aktiviert Wählen Sie die Fallback-Schnittstelle 2 Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen. Diese wird verwendet, wenn die IGMP-Proxy-Funktion über die **Fallback-Proxy-Schnittstelle 1** nicht ausgeführt werden kann.

9.4.2.2 Optionen

In diesem Menü haben Sie die Möglichkeit, IGMP auf Ihrem System zu aktivieren bzw. zu deaktivieren. Außerdem können Sie bestimmen, ob IGMP im Kompatibilitätsmodus verwendet werden soll oder nur IGMP V3-Hosts akzeptiert werden sollen.

Das Menü **Multicast**->**IGMP**->**Optionen** besteht aus den folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
IGMP-Status	Wählen Sie den IGMP-Status aus. Mögliche Werte: • *Auto* (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden. • *Aktiv*: Multicast ist immer aktiv. • *Inaktiv*: Multicast ist immer inaktiv.
Modus	Nur für **IGMP-Status** = *Aktiv* oder *Auto* Wählen Sie den Multicast-Modus aus. Mögliche Werte: • *Kompatibilitätsmodus* (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen konnte. • *Nur Version 3*: Nur IGMP Version 3 wird verwendet.
Maximale Gruppen	Geben Sie ein, wie viele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen. Der Standardwert ist *64*.
Maximale Quellen	Geben Sie die maximale Anzahl der Quellen ein, die in den Reports der Version 3 spezifiziert sind, als auch die maximale Anzahl der intern verwalteten Quellen pro Gruppe. Der Standardwert ist *64*.
Maximale Anzahl der IGMP-Statusmeldungen	Geben Sie die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Meldungen pro Sekunde ein. Der Standardwert ist *0*, d. h. die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.

Der Abschnitt **Erweiterte Einstellungen** ermöglicht es, die Funktion des IGMP Snooping an- und auszuschalten. IGMP Snooping stellt sicher, dass Multicast-Datenverkehr nur an diejenigen Clients gesendet wird, die einen bestimmten Multicast Stream auch angefordert haben.

Die Funktion ist standardmäßig aktiv.

9.4.3 Weiterleiten

9.4.3.1 Weiterleiten

In diesem Menü legen Sie fest, welche Multicast-Gruppen zwischen den Schnittstellen Ihres Geräts immer weitergeleitet werden.

9.4.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um Weiterleitungsregeln für neue Multicast-Gruppen zu erstellen.

Das Menü **Multicast**->**Weiterleiten**->**Weiterleiten**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Alle Multicast-Gruppen	Wählen Sie aus, ob alle Multicast-Gruppen, d. h. der komplette Multicast-Adressraum 224.0.0.0/4, von der definierten **Quellschnittstelle** an die definierte **Zielschnittstelle** weitergeleitet werden soll. Setzen Sie dazu den Haken für *Aktiviert*. Möchten Sie nur eine definierte Multicast-Gruppe an eine bestimmte Schnittstelle weiterleiten, deaktivieren Sie die Option. Standardmäßig ist die Option nicht aktiv.
Multicast-Gruppen-Adresse	Nur für **Alle Multicast-Gruppen** = nicht aktiv Geben Sie hier die Adresse der Multicast-Gruppe ein, die Sie von einer definierten **Quellschnittstelle** an eine definierte **Zielschnittstelle** weiterleiten möchten.
Quellschnittstelle	Wählen Sie die Schnittstelle Ihres Geräts aus, an dem die gewünschte Multicast-Gruppe eingeht.
Zielschnittstelle	Wählen Sie die Schnittstelle Ihres Geräts aus, zu der die gewünschte Multicast-Gruppe weitergeleitet werden soll.

9.5 WAN

Dieses Menü stellt Ihnen verschiedene Möglichkeiten zur Verfügung, Zugänge bzw. Verbindungen aus Ihrem LAN zum WAN zu konfigurieren. Außerdem können Sie hier die Sprachübertragung bei Telefongesprächen über das Internet optimieren.

9.5.1 Internet + Einwählen

In diesem Menü können Sie Internetzugänge oder Einwahl-Verbindungen einrichten.

Darüber hinaus können Sie Adress-Pools für die dynamische Vergabe von IP-Adressen anlegen.

Um mit Ihrem Gerät Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner auf Ihrem Gerät einrichten. Dies gilt sowohl für ausgehende Verbindungen (z. B. Ihr Gerät wählt sich bei einem entfernten Partner ein), als auch für eingehende Verbindungen (z. B. ein entfernter Partner wählt sich bei Ihrem Gerät ein).

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät die Protokolle PPP-over-Ethernet (PPPoE), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist ebenfalls konfigurierbar.

Hinweis

Beachten Sie die Vorgaben Ihres Providers!

Einwahl-Verbindungen über ISDN dienen dazu, zu Netzwerken oder Hosts außerhalb Ihres LANs eine Verbindung herzustellen.

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **Benutzername**n, die **Authentifizierung** und den aktuellen **Status** enthält.

Das Feld **Status** kann folgende Werte annehmen:

Mögliche Werte für Status

Feld	Beschreibung
	verbunden
	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich
	nicht verbunden (z. B. ist aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich)
	administrativ auf inaktiv gesetzt (deaktiviert); Verbindungsaufbau nicht möglich

Standard-Route (Default Route)

Bei einer Standard-Route werden automatisch alle Daten auf eine Verbindung geleitet, wenn keine andere passende Route verfügbar ist. Ein Zugang zum Internet sollte immer als Standard-Route zum Internet-Service-Provider (ISP) eingerichtet sein. Weitergehende Informationen zum möglichen Routentyp finden Sie unter **Netzwerk**->**Routen**.

NAT aktivieren

Mit Network Address Translation (NAT) verbergen Sie Ihr gesamtes Netzwerk nach außen hinter nur einer IP-Adresse. Für die Verbindung zum Internet Service Provider (ISP) sollten Sie dies auf jeden Fall tun.

Bei aktiviertem NAT sind zunächst nur ausgehende Sessions zugelassen. Um bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen diese explizit definiert und zugelassen werden.

Timeout bei Inaktivität festlegen

Der Timeout bei Inaktivität wird festgelegt, um die Verbindung bei Nichtbenutzen, d.h. wenn keine Nutzdaten mehr gesendet werden, automatisch zu trennen und somit ggf. Gebühren zu sparen.

Blockieren nach Verbindungsfehler

Mit dieser Funktion richten Sie eine Wartezeit für ausgehende Verbindungsversuche ein, nachdem ein Verbindungsversuch durch Ihr Gerät fehlgeschlagen ist.

Authentifizierung

Wenn bei ISDN-Verbindungen ein Ruf eingeht, wird über den ISDN-D-Kanal die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann Ihr Gerät den Anrufer identifizieren (CLID), wenn dieser auf Ihrem Gerät eingetragen ist. Nach der Identifizierung mit CLID kann Ihr Gerät zusätzlich eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird.

Für alle PPP-Verbindungen benötigt Ihr Gerät Vergleichsdaten, die Sie eintragen müssen. Legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll und tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider

oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Callback

Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann der Callback-Mechanismus für jede Verbindung über eine ISDN- oder über eine AUX-Schnittstelle verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufer eindeutig identifiziert wurde. Ihr Gerät kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch von einem Verbindungspartner einen Rückruf anfordern. Die Identifizierung kann aufgrund der Calling Party Number oder aufgrund der PAP/CHAP/MS-CHAP-Authentifizierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party Number über den ISDN-D- Kanal übermittelt wird, im zweiten Fall mit Rufannahme.

Kanalbündelung

Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Kanalbündelung kann nur bei ISDN-Verbindungen für Bandbreitenerhöhung bzw. als Backup angewendet werden. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch

Dynamisch

Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle für Verbindungen zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen.

Falls auf der Gegenstelle Geräte anderer Fabrikate verwendet werden, stellen Sie sicher, dass diese dynamische Kanalbündelung für Bandbreitenerhöhung bzw. als Backup unterstützen.

Statisch

Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät für Verbindungen nutzen soll, unabhängig von der übertragenen Datenrate.

9.5.1.1 PPPoE

Im Menü **WAN**->**Internet + Einwählen**->**PPPoE** wird eine Liste aller PPPoE-Schnittstellen angezeigt.

PPP over Ethernet (PPPoE) ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird heute bei ADSL-Anschlüssen in Deutschland verwendet. In Österreich wurde ursprünglich für ADSL-Zugänge das Point To Point Tunneling Protocol (PPTP) verwendet. Mittlerweile wird allerdings PPPoE auch dort von einigen Providern angeboten.

9.5.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere PPPoE Schnittstellen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**PPPoE**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (*Standard*) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (*Mehrfachverbindung*). Wählen Sie *Mehrfachverbindung*, so können Sie mehrere DSL-Verbindungen eines Providers über PPP als statische Bündel koppeln, um mehr Bandbreite

Feld	Beschreibung
	zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung. Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Port-Modus zu betreiben und für jede PPPoE-Verbindung eine eigene Ethernet-Schnittstelle zu benutzen, z. B. *en1-1*, *en1-2*. Wenn Sie für PPPoE Multilink zusätzlich ein externes Modem benutzen wollen, müssen Sie den Ethernet-Switch Ihres Geräts im Split-Port-Modus betreiben.
PPPoE-Ethernet-Schnittstelle	Nur für **PPPoE-Modus** = *Standard* Wählen Sie die Ethernet-Schnittstelle aus, die für eine Standard-PPPoE-Verbindung vorgegeben wird. Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist. Bei Verwendung des internen DSL-Modems, wählen Sie hier die in **WAN**->**ATM**->**Profile**->**Neu** für diese Verbindung konfigurierte EthoA-Schnittstelle aus. Wählen Sie den Wert *Automatisch* um den automatischen VDSL-/ADSL-Modus zu unterstützen. In diesem Modus wird die Schnittstelle für der Internetzugang automatisch gewählt. Achten Sie darauf, dass für einen ADSL-Zugang im Menü **ATM** eine Schnittstelle angelegt sein muss, für einen VDSL-Zugang ist dies nicht notwendig.
PPPoE-Schnittstelle für Mehrfachlink	Nur für **PPPoE-Modus**= *Mehrfachverbindung* Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die **Hinzufügen**-Schaltfläche, um weitere Einträge anzulegen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
VLAN	Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter **VLAN-ID** einen Wert eingeben zu können.
VLAN-ID	Nur wenn **VLAN** aktiviert ist. Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold.

Feld	Beschreibung
	Der Standardwert ist *300*. Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig* : Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *IP-Adresse abrufen* (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • *Statisch*: Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur bei **IP-Adressmodus** = *Statisch* Geben Sie die statische IP-Adresse des Verbindungspartners ein.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig*: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* Die gewählte PPPoE-Schnittstelle wird im Host-Modus betrieben.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über die Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie die Präfix-Liste erstellt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
IPv6-Adressen	Nur für **IPv6** = *Aktiviert* Sie können der gewählten Schnittstelle **IPv6-Adressen** zuordnen. Mit **Hinzufügen** können Sie einen oder mehrere Adresseinträge anlegen. Ein zusätzliches Fenster öffnet sich, in dem Sie eine IPv6-Adresse bestehend aus einem Link-Präfix und einem Host-Anteil festlegen können. Wenn Ihr Gerät im Host-Modus arbeitet (**IPv6-Modus** = *Host*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** *Aktiviert*), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen.

Feld	Beschreibung
	Wenn Ihr Gerät im Router-Modus arbeitet (**IPv6-Modus** = *Router (Router-Advertisement übermitteln)*, **Router Advertisement übertragen** *Aktiviert* und **DHCP-Server** *Aktiviert*), so müssen Sie hier seine IPv6-Adressen konfigurieren.

Legen Sie weitere Einträge mit **Hinzufügen** an.

Felder im Menü Link-Präfix

Feld	Beschreibung
Art der Einrichtung	Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll. Mögliche Werte: • *Von Allgemeinem Präfix* (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet. • *Statisch*: Sie können den Link-Präfix eingeben.
Allgemeiner Präfix	Nur für **Art der Einrichtung** = *Von Allgemeinem Präfix* Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes**->**Neu** angelegt sind.
Automatische Subnetzerstellung	Nur wenn **Art der Einrichtung** = *Von Allgemeinem Präfix* und wenn ein **Allgemeiner Präfix** gewählt ist. Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID *0* verwendet, für das zweite Subnetz die Subnetz-ID *1*, usw. Mögliche Werte für die **Subnetz-ID** sind *0* bis *65535*. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Bei der Subnetzerstellung wird der dezimale ID-Wert in einen hexadezimalen Wert umgerechnet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die Funktion nicht aktiv ist, so können Sie durch Eingabe der Subnetz-ID ein Subnetz definieren.
Subnetz-ID	Nur wenn **Automatische Subnetzerstellung** nicht aktiv ist. Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Mögliche Werte sind *0* bis *65535*. Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.
Link-Präfix	Nur für **Art der Einrichtung** = *Statisch* Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit *::* enden. Seine Länge ist mit *64* vorgegeben.

Felder im Menü Host-Adresse

Feld	Beschreibung
Erzeugungsmethode	Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. EUI-64 setzt folgenden Prozess in Gang: • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird *FFFE* eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf *1* gesetzt.
Statische Adressen	Sie können, unabhängig von der automatischen Erzeugung, die unter **Erzeugungsmethode** festgelegt ist, mit **Hinzufügen** den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit *64* vorgegeben. Beginnen Sie die Eingabe mit *::* .

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *60*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*. Der Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
MTU	Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung verwendet werden darf. Mit dem Standardwert *Automatisch* wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben. Wenn Sie *Automatisch* deaktivieren, können Sie einen Wert eingeben. Mögliche Werte sind *1* bis *8192*. Der Standardwert ist *0*.

9.5.1.2 PPPoA

Im Menü **WAN**->**Internet + Einwählen**->**PPPoA** wird eine Liste aller PPPoA-Schnittstellen angezeigt.

In diesem Menü konfigurieren Sie eine xDSL-Verbindung, die zum Verbindungsaufbau PPPoA verwendet. Bei PPPoA wird die Verbindung so konfiguriert, dass ein PPP-Datenstrom direkt über ein ATM-Netzwerk transportiert wird (RFC 2364). Dieses ist bei manchen Providern erforderlich. Achten Sie bitte auf die Spezifikationen Ihres Providers!

Bei Verwendung des internen DSL-Modems, muss in **WAN**->**ATM**->**Profile**->**Neu** für diese Verbindung eine PPPoA-Schnittstelle mit **Client-Typ** = *Auf Anforderung* konfiguriert werden.

9.5.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere PPPoA-Schnittstellen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**PPPoA**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü **ATM**->**Profile** angelegtes ATM-Profil, darge-

Feld	Beschreibung
	stellt durch die vom Provider vorgegebenen globalen ID VPI und VCI.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort für die PPPoA-Verbindung ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen soll. Mögliche Werte sind *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold. Der Standardwert ist *300*. Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig* : Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IP-Adressmodus	Wählen Sie aus, ob Ihr Gerät eine statische IP-Adresse hat oder diese dynamisch erhält. Mögliche Werte: • *IP-Adresse abrufen* (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • *Statisch*: Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden

Feld	Beschreibung
	soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur für **IP-Adressmodus** = *Statisch* Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	Wählen Sie aus, ob das gewählte ATM-Profil das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung das gewählte ATM-Profil betrieben werden soll. Mögliche Werte: • *Nicht Vertrauenswürdig* (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig*: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* Das gewählte ATM-Profil wird im Host-Modus betrieben.
Router Advertisement annehmen	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Wählen Sie, ob Router Advertisements über das ATM-Profil empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie die Präfix-Liste erstellt.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Host* Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
IPv6-Adressen	Nur für **IPv6** = *Aktiviert* Sie können der gewählten Schnittstelle **IPv6-Adressen** zuordnen. Mit **Hinzufügen** können Sie einen oder mehrere Adresseinträge anlegen. Ein zusätzliches Fenster öffnet sich, in dem Sie eine IPv6-Adresse bestehend aus einem Link-Präfix und einem Host-Anteil festlegen können. Wenn Ihr Gerät im Host-Modus arbeitet (**IPv6-Modus** = *Host*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** *Aktiviert*), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen. Wenn Ihr Gerät im Router-Modus arbeitet (**IPv6-Modus** = *Router (Router-Advertisement übermitteln)*, **Router Advertisement übertragen** *Aktiviert* und **DHCP-Server** *Aktiviert*), so müssen Sie hier seine IPv6-Adressen konfigurieren.

Legen Sie weitere Einträge mit **Hinzufügen** an.

Felder im Menü Link-Präfix

Feld	Beschreibung
Art der Einrichtung	Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll. Mögliche Werte: • *Von Allgemeinem Präfix* (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet. • *Statisch*: Sie können den Link-Präfix eingeben.
Allgemeiner Präfix	Nur für **Art der Einrichtung** = *Von Allgemeinem Präfix* Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes**->**Neu** angelegt sind.
Automatische Subnetzerstellung	Nur wenn **Art der Einrichtung** = *Von Allgemeinem Präfix* und wenn ein **Allgemeiner Präfix** gewählt ist. Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID *0* verwendet, für das zweite Subnetz die Subnetz-ID *1*, usw. Mögliche Werte für die **Subnetz-ID** sind *0* bis *65535*. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Bei der Subnetzerstellung wird der dezimale ID-Wert in einen hexadezimalen Wert umgerechnet.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die Funktion nicht aktiv ist, so können Sie durch Eingabe der Subnetz-ID ein Subnetz definieren.
Subnetz-ID	Nur wenn **Automatische Subnetzerstellung** nicht aktiv ist. Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Mögliche Werte sind *0* bis *65535*. Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.
Link-Präfix	Nur für **Art der Einrichtung** = *Statisch* Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit *::* enden. Seine Länge ist mit *64* vorgegeben.

Felder im Menü Host-Adresse

Feld	Beschreibung
Erzeugungsmethode	Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. EUI-64 setzt folgenden Prozess in Gang: • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird *FFFE* eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf *1* gesetzt.
Statische Adressen	Sie können, unabhängig von der automatischen Erzeugung, die unter **Erzeugungsmethode** festgelegt ist, mit **Hinzufügen** den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit *64* vorgegeben. Beginnen Sie die Eingabe mit *::* .

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *60*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*. Der Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung

Feld	Beschreibung
	aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

9.5.1.3 ISDN

Im Menü **WAN**->**Internet + Einwählen**->**ISDN** wird eine Liste aller ISDN-Schnittstellen angezeigt.

In diesem Menü konfigurieren Sie folgende ISDN-Verbindungen:

- Internetzugang über ISDN
- LAN-zu-LAN-Kopplung über ISDN
- Remote (Mobile) Dial-in
- Nutzung der Funktion ISDN Callback

9.5.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere ISDN-Schnittstellen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**ISDN**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
Verbindungstyp	Wählen Sie aus, welches Layer-1-Protokoll Ihr Gerät nutzen soll. Diese Einstellung gilt für ausgehende Verbindungen zum Verbindungspartner und nur für eingehende Verbindungen vom Verbindungspartner, wenn sie anhand der Calling Party Number identifiziert werden konnten. Mögliche Werte: • *ISDN 64 kbit/s*: Für ISDN-Datenverbindungen mit 64 kbit/s • *ISDN 56 kbit/s*: Für ISDN-Datenverbindungen mit 56 kbit/s
Benutzername	Geben Sie die Kennung Ihres Geräts (lokaler PPP-Benutzername) ein.
Entfernter Benutzer (nur Einwahl)	Geben Sie die Kennung der Gegenstelle (entfernter PPP-Benutzername) ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Der Standardwert ist *20*.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *Statisch* (Standardwert): Sie geben eine statische IP-Adresse ein. • *IP-Adresse bereitstellen*: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	Nur bei **IP-Adressmodus** = *Statisch* und *IP-Adresse abrufen* Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
NAT-Eintrag erstellen	Nur bei **IP-Adressmodus** = *Statisch* und *IP-Adresse abrufen* Wenn eine ISDN-Internetverbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur bei **IP-Adressmodus** = *Statisch* Weisen Sie der ISDN-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.
IP-Zuordnungspool	Nur bei **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *300*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*. Der Standardwert ist *5*.
Nutzungsart	Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle. Mögliche Werte: • *Standard* (Standardwert): Kein spezieller Typ ist ausgewählt. • *Nur Einwahl*: Die Schnittstelle wird für eingehende Wählverbindungen und für von außen initiierten Callback verwendet. • *Mehrfacheinwahl (Nur Einwahl)*: Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich

Feld	Beschreibung
	mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	Nur für **Authentifizierung** = *MS-CHAPv2* Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiv ist. Wenn **Verschlüsselung** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner* (Standardwert): Es wird keine MPP-Verschlüsselung angewendet. • *Aktiviert*: Die MPP-Verschlüsselung V2 mit 128 bit wird nach RFC 3078 angewendet. • *Windows-kompatibel*: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.

Callback-Modus	Wählen Sie die Funktion Callback-Modus.
	
	Mögliche Werte:
	
	• *Keiner* (Standardwert): Ihr Gerät führt keinen Rückruf aus.
	• *Aktiv*: Wählen Sie eine der folgenden Optionen:
	  • *Keine PPP-Aushandlung*: Ihr Gerät ruft den Verbindungspartner an, um einen Rückruf anzufordern.
	  • *Windows-Clientmodus*: Ihr Gerät ruft den Verbindungspartner an, um über CBCP (Callback Control Protocol) einen Rückruf anzufordern. Wird für Windows Clients benötigt.
	• *Passiv*: Wählen Sie eine der folgenden Optionen:
	  • *PPP-Aushandlung oder CLID*: Ihr Gerät ruft sofort zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert wird.
	  • *Windows-Servermodus*: Ihr Gerät ruft nach einer vom Microsoft Client vorgeschlagenen Zeit (NT: 10 Sekunden, neuere Systeme: 12 Sekunden) zurück. Es verwendet die Rufnummer (**Einträge**->**Rufnummer**) mit dem **Modus** *Ausgehend* oder *Beide*, die für den Verbindungspartner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP-Aushandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheits-

Feld	Beschreibung
	gründen möglichst nicht zu verwenden. Bei der Anbindung von mobilen Microsoft-Clients über ein DFÜ-Netzwerk ist dies derzeit nicht vermeidbar. • *Verzögert, nur CLID*: Ihr Gerät ruft nach ca. vier Sekunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID. • *Windows-Servermodus, Rückruf optional*: Wie *Windows-Servermodus* mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit **Abbrechen** geschlossen wird.

Felder im Menü Optionen für Bandbreite auf Anforderung

Feld	Beschreibung
Kanalbündelung	Wählen Sie aus, ob Kanalbündelung bzw. welche Art von Kanalbündelung für ISDN-Verbindungen mit dem Verbindungspartner genutzt werden soll. Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet. Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen. Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät nutzen soll, unabhängig von der übertragenen Datenrate. Mögliche Werte: • *Keiner* (Standardwert): Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. • *Statisch*: Statische Kanalbündelung. • *Dynamisch*: Dynamische Kanalbündelung.

Feld im Menü Wahlnummern

Feld	Beschreibung
Einträge	Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

Felder im Menü Konfiguration der Wahlnummern (erscheint nur für Einträge = Hinzufügen)

Feld	Beschreibung
Modus	Nur wenn **Einträge** = *Hinzufügen* Die Calling Party Number des Rufes wird mit der unter **Rufnummer** eingetragenen Nummer verglichen. Wählen Sie aus, ob **Rufnummer** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte: • *Beide* (Standardwert): Für eingehende und ausgehende Rufe. • *Eingehend*: Für eingehende Rufe, wenn der Verbindungspartner sich bei Ihrem Gerät einwählen soll. • *Ausgehend*: Für ausgehende Rufe, wenn Sie sich beim Verbindungspartner einwählen wollen.

Feld	Beschreibung
	Die Nummer des Anrufers eines eingehenden Rufs (Calling Party Number) wird mit der unter **Rufnummer** eingetragenen Nummer verglichen.
Rufnummer	Geben Sie die Rufnummern des Verbindungspartners ein.
Port-Verwendung	Wählen Sie aus, welcher Port zu verwenden ist.

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellen Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • *Aktiv*: OSPF ist für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantwortet werden. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *Aktiv* oder *Ruhend* ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *aktiv* ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** und **WINS-Server Primär** und **Sekundär** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

9.5.1.4 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools angezeigt.

Ihr Gerät kann als dynamischer IP-Adress-Server für PPP-Verbindungen agieren. Dafür stellen Sie einen oder mehrere Pools von IP-Adressen zur Verfügung. Diese IP-Adressen können für die Dauer der Verbindung an einwählende Verbindungspartner vergeben werden.

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden zu-

nächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

9.5.1.4.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

9.5.2 ATM

ATM (Asynchronous Transfer Mode) ist ein Datenübertragungsverfahren, das ursprünglich für Breitband-ISDN konzipiert wurde.

Aktuell wird ATM u.a. in Hochgeschwindigkeitsnetzen verwendet. Sie benötigen ATM z. B., wenn Sie über das integrierte ADSL- bzw. SHDSL-Modem einen Hochgeschwindigkeitszugang ins Internet realisieren wollen.

In einem ATM-Netz können unterschiedliche Anwendungen wie z. B. Sprache, Video und Daten nebeneinander im asynchronen Zeitmultiplexverfahren übertragen werden. Jedem Sender werden dabei Zeitabschnitte zum Übertragen seiner Daten zur Verfügung gestellt. Beim asynchronen Verfahren werden ungenutzte Zeitabschnitte eines Senders von einem anderen Sender verwendet.

Bei ATM handelt es sich um ein verbindungsorientiertes Paketvermittlungsverfahren. Für die Datenübertragung wird eine virtuelle Verbindung genutzt, die zwischen Sender und Empfänger ausgehandelt oder auf beiden Seiten konfiguriert wird. Es wird z. B. der Weg festgelegt, den die Daten nehmen sollen. Über eine einzige physikalische Schnittstelle können mehrere virtuelle Verbindungen eingerichtet werden.

Die Daten werden in sogenannten Zellen oder Slots konstanter Größe übermittelt. Jede Zelle besteht aus 48 Byte Nutzdaten und 5 Byte Steuerinformation. Die Steuerinformation enthält u.a. die ATM-Adresse vergleichbar der Internetadresse. Die ATM-Adresse setzt sich aus den Bestandteilen Virtual Path Identifier (VPI) und Virtual Connection Identifier (VCI) zusammen; sie identifiziert die virtuelle Verbindung.

Über ATM werden verschiedene Arten von Datenströmen transportiert. Um den unterschiedlichen Ansprüchen dieser Datenströme an das Netz, z. B. bezüglich Zellverlust und Verzögerungszeit, gerecht zu werden, können mit Hilfe der Dienstkategorien dafür geeignete Werte festgelegt werden. Für unkomprimierte Videodaten werden z. B. andere Parameter benötigt als für zeitunkritische Daten.

In ATM-Netzen steht Quality of Service (QoS) zur Verfügung, d. h. die Größe verschiedener Netzparameter wie z. B. Bitrate, Delay und Jitter kann garantiert werden.

OAM (Operation, Administration and Maintenance) dient der Überwachung der Datenübertragung bei ATM. OAM umfasst Konfigurationsmanagement, Fehlermanagement und Leistungsmessung.

9.5.2.1 Profile

Im Menü **WAN**->**ATM**->**Profile** wird eine Liste aller ATM-Profile angezeigt.

Wenn die Verbindung für Ihren Internetzugang über das interne Modem aufgebaut wird, müssen dafür die ATM-Verbindungsparameter eingestellt werden. Ein ATM-Profil fasst einen Satz Parameter für einen bestimmten Provider zusammen.

Hinweis

Die ATM-Enkapsulierungen sind in den RFCs 1483 und 2684 beschrieben. Sie finden die RFCs auf den entsprechenden Seiten der IETF (*www.ietf.org/rfc.html*).

9.5.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere ATM-Profile einzurichten.

Das Menü **WAN**->**ATM**->**Profile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü ATM-Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profile für Ihren Provider aus der Liste aus oder definieren Sie mit `-- Benutzerdefiniert --` ein Profil.
Beschreibung	Nur für **Provider** = `-- Benutzerdefiniert --` Geben Sie eine beliebige Beschreibung für die Verbindung ein.
ATM-Schnittstelle	Nur, wenn mehrere ATM-Schnittstellen verfügbar sind, z. B. wenn bei Geräten mit SHDSL mehrere Schnittstellen separat konfiguriert sind. Wählen Sie die ATM-Schnittstelle, die Sie für die Verbindung verwenden wollen.
Typ	Nur für **Provider** = `-- Benutzerdefiniert --` Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: • `Ethernet über ATM` (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet. • `Geroutete Protokolle über ATM`: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) werden geroutete Protokolle über ATM (RPoA) verwendet. • `PPP über ATM`: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtual Path Identifier (VPI)	Nur für **Provider** = `-- Benutzerdefiniert --` Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind `0` bis `255`. Der Standardwert ist `8`.
Virtual Channel Identifier (VCI)	Nur für **Provider** = `-- Benutzerdefiniert --` Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers.

Feld	Beschreibung
	Mögliche Werte sind *32* bis *65535*. Der Standardwert ist 32.
Enkapsulierung	Nur für **Provider** = *-- Benutzerdefiniert --* Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte (nach RFC 2684): • *LLC Bridged no FCS* (Standardwert für Ethernet über ATM): Wird nur für **Typ** = *Ethernet über ATM* angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen). • *LLC Bridged FCS*: Wird nur für **Typ** = *Ethernet über ATM* angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen). • *Nicht ISO* (Standardwert für Geroutete Protokolle über ATM): Wird nur für **Typ** = *Geroutete Protokolle über ATM* angezeigt. Enkapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing. • *LLC*: Wird nur für **Typ** = *PPP über ATM* angezeigt. Enkapsulierung mit LLC-Header. • *VC-Multiplexing* (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).

Felder im Menü Einstellungen für Ethernet über ATM (erscheint nur für Typ = Ethernet über ATM)

Feld	Beschreibung
Standard-Ethernet für PPPoE-Schnittstellen	Nur für **Typ** = *Ethernet über ATM* Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PPPoE-Verbindungen verwendet werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Adressmodus	Nur für **Typ** = *Ethernet über ATM* Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen werden soll. Mögliche Werte: • *Statisch* (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in **IP-Adresse / Netzmaske** zugewiesen. • *DHCP*: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse/Netzmaske	Nur für **Adressmodus** = *Statisch* Geben Sie die IP-Adressen (**IP-Adresse**) und die entsprechenden Netzmasken (**Netzmaske**) der ATM-Schnittstellen ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

Feld	Beschreibung
MAC-Adresse	Geben Sie der routerinternen Schnittstelle der ATM-Verbindung eine MAC-Adresse, z. B. `00:a0:f9:06:bf:03`. Ein Eintrag wird nur in speziellen Fällen benötigt. Für Internetverbindungen ist es ausreichend, die Option **Voreingestellte verwenden** (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des `en1-0` abgeleitet ist.
DHCP-MAC-Adresse	Nur für **Adressmodus** = `DHCP` Geben Sie die MAC-Adresse der routerinternen Schnittstelle der ATM-Verbindung ein, z. B. `00:e1:f9:06:bf:03`. Sollte Ihnen Ihr Provider eine MAC-Adresse für DHCP zugewiesen haben, so tragen Sie diese hier ein. Sie haben auch die Möglichkeit, die Option **Voreingestellte verwenden** (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des `en1-0` abgeleitet ist.
DHCP-Hostname	Nur für **Adressmodus** = `DHCP` Geben Sie ggf. den beim Provider registrierten Host-Namen an, der von Ihrem Gerät für DHCP-Anfragen verwendet werden soll. Die maximale Länge des Eintrags beträgt 45 Zeichen.

Felder im Menü Einstellungen für geroutete Protokolle über ATM (erscheint nur für Typ = Geroutete Protokolle über ATM)

Feld	Beschreibung
IP-Adresse/Netzmaske	Geben Sie die IP-Adressen (**IP-Adresse**) und die entsprechenden Netzmasken (**Netzmaske**) der ATM-Schnittstelle ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld im Menü Einstellungen für PPP über ATM (erscheint nur für Typ = PPP über ATM)

Feld	Beschreibung
Client-Typ	Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll. Mögliche Werte: • `Auf Anforderung` (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang. Zusätzliche Informationen zu PPP über ATM finden Sie unter *PPPoA* auf Seite 182.

9.5.2.2 Dienstkategorien

Im Menü **WAN**->**ATM**->**Dienstkategorien** wird eine Liste aller bereits konfigurierten ATM-Verbindungen (PVC, Permanent Virtual Circuit) angezeigt, denen spezifische Datenverkehrsparameter zugewiesen wurden.

Ihr Gerät unterstützt QoS (Quality of Service) für ATM-Schnittstellen.

Achtung

ATM QoS ist nur anzuwenden, wenn Ihr Provider eine Liste an Datenverkehrsparametern (Traffic Contract) vorgibt.

Die Konfiguration von ATM QoS erfordert umfangreiches Wissen über die ATM-Technologie und die Funktionsweise der **Digitalisierungsbox**. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

9.5.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Kategorien einzurichten.

Das Menü **WAN**->**ATM**->**Dienstkategorien**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Virtual Channel Connection (VCC)	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Dienstkategorie festgelegt werden soll.
ATM-Dienstkategorie	Wählen Sie aus, auf welche Art der Datenverkehr der ATM-Verbindung geregelt werden soll. Durch die Auswahl der ATM-Dienstkategorie wird implizit eine Priorität zugeordnet: von CBR (höchste Priorität) über VBR.1 /VBR.3 bis VBR (niedrigste Priorität). Zur Verfügung stehen: • *Unspecified Bit Rate (UBR)* (Standardwert): Der Verbindung wird keine bestimmte Datenrate garantiert. Die **Peak Cell Rate (PCR)** legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen. • *Constant Bit Rate (CBR)*: Der Verbindung wird eine garantierte Datenrate zugewiesen, die von der **Peak Cell Rate (PCR)** bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen. • *Variable Bit Rate V.1 (VBR.1)*: Der Verbindung wird eine garantierte Datenrate zugewiesen - **Sustained Cell Rate (SCR)**. Diese darf insgesamt um das in **Maximale Burst-Größe (MBS)** konfigurierte Volumen überschritten werden. Jeglicher weiterer ATM-Traffic wird verworfen. Die **Peak Cell Rate (PCR)** bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen. • *Variable Bit Rate V.3 (VBR.3)*: Der Verbindung wird eine garantierte Datenrate zugewiesen - **Sustained Cell Rate (SCR)**. Diese darf insgesamt um das in **Maximale Burst-Größe (MBS)** konfigurierte Volumen überschritten werden. Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die **Peak Cell Rate (PCR)** bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.
Peak Cell Rate (PCR)	Geben Sie einen Wert für die maximale Datenrate in Bits pro Sekunde ein.

Feld	Beschreibung
	Mögliche Werte: *0* bis *10000000*. Der Standardwert ist *0*.
Sustained Cell Rate (SCR)	Nur für **ATM-Dienstkategorie** = *Variable Bit Rate V.1 (VBR.1)* oder *Variable Bit Rate V.3 (VBR.3)* Geben Sie einen Wert für die mindestens zur Verfügung stehende, garantierte Datenrate in Bits pro Sekunde ein. Mögliche Werte: *0* bis *10000000*. Der Standardwert ist *0*.
Maximale Burst-Größe (MBS)	Nur für **ATM-Dienstkategorie** = *Variable Bit Rate V.1 (VBR.1)* oder *Variable Bit Rate V.3 (VBR.3)* Geben Sie hier einen Wert für die maximale Anzahl in Bits pro Sekunde ein, um welche die PCR kurzzeitig überschritten werden darf. Mögliche Werte: *0* bis *100000*. Der Standardwert ist *0*.

9.5.2.3 OAM-Regelung

OAM ist ein Dienst zur Überwachung von ATM-Verbindungen. In OAM sind insgesamt fünf Hierarchien (Flow Level F1 bis F5) für den Informationsfluss definiert. Für eine ATM-Verbindung sind die wichtigsten Informationsflüsse F4 und F5. Der F4-Informationsfluss betrifft den virtuellen Pfad (VP), der F5-Informationsfluss den virtuellen Kanal (VC). Der VP wird durch den VPI-Wert definiert, der VC durch VPI und VCI.

Hinweis

Im Allgemeinen geht die Überwachung nicht vom Endgerät aus, sondern wird seitens des ISP initiiert. Ihr Gerät muss dann lediglich korrekt auf die empfangenen Signale reagieren. Dies ist auch ohne eine spezifische OAM-Konfiguration sowohl auf den Flow Level 4 als auch dem Flow Level 5 gewährleistet.

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: Loopback-Tests und OAM Continuity Check (OAM CC). Sie können unabhängig voneinander konfiguriert werden.

Achtung

Die Konfiguration von OAM erfordert umfangreiches Wissen über die ATM-Technologie und die Funktionsweise der **Digitalisierungsbox**. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

Im Menü **WAN**->**ATM**->**OAM-Regelung** wird eine Liste aller überwachten OAM-Fluss-Levels angezeigt.

9.5.2.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Fluss-Levels einzurichten.

Das Menü **WAN**->**ATM**->**OAM-Regelung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü OAM-Flusskonfiguration

Feld	Beschreibung
OAM-Fluss-Level	Wählen Sie den zu überwachenden OAM-Fluss-Level. Mögliche Werte: • *F5*: (Virtual Channel Level) Die OAM-Einstellungen werden auf den virtuellen Kanal angewendet (Standardwert). • *F4*: (Virtual Path Level) Die OAM-Einstellungen werden auf den virtuellen Pfad angewendet.
Virtual Channel Connection (VCC)	Nur für **OAM-Fluss-Level** = *F5* Wählen Sie die zu überwachende bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus.
Virtual Path Connection (VPC)	Nur für **OAM-Fluss-Level** = *F4* Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.

Felder im Menü Loopback

Feld	Beschreibung
Loopback Ende-zu-Ende	Wählen Sie aus, ob Sie den Loopback-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Ende-zu-Ende-Sendeintervall	Nur wenn **Loopback Ende-zu-Ende** aktiviert ist. Geben Sie das Zeitintervall in Sekunden an, nach dem jeweils eine Loopback-Zelle gesendet werden soll. Mögliche Werte sind *0* bis *999*. Der Standardwert ist *5*.
Ausstehende Ende-zu-Ende-Anforderungen	Nur wenn **Loopback Ende-zu-Ende** aktiviert ist. Geben Sie ein, wie viele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird. Mögliche Werte sind *1* bis *99*. Der Standardwert ist *5*.
Loopback-Segment	Wählen Sie aus, ob Sie den Loopback-Test für die Segment-Verbindung (Segment = Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Segment-Sendeintervall	Nur wenn **Loopback-Segment** aktiviert ist. Geben Sie das Zeitintervall in Sekunden an, nach dem jeweils eine Loopback-Zelle gesendet wird. Mögliche Werte sind *0* bis *999*. Der Standardwert ist *5*.

Feld	Beschreibung
Ausstehende Segment-Anforderungen	Nur wenn **Loopback-Segment** aktiviert ist. Geben Sie ein, wie viele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird. Mögliche Werte sind *1* bis *99*. Der Standardwert ist *5*.

Felder im Menü CC-Aktivierung

Feld	Beschreibung
Continuity Check (CC) Ende-zu-Ende	Wählen Sie aus, ob Sie den OAM-CC-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen. Mögliche Werte: • *Passiv* (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • *Aktiv*: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • *Beide*: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • *Keine Aushandlung*: Je nach Einstellung im Feld **Richtung** werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt. • *Passiv*: Die Funktion ist nicht aktiv. Wählen Sie außerdem aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen. Mögliche Werte: • *Beide* (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • *Senke*: CC-Daten werden empfangen. • *Quelle*: CC-Daten werden generiert.
Continuity Check (CC) Segment	Wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-Verbindung (Segment=Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen. Mögliche Werte: • *Passiv* (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • *Aktiv*: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • *Beide*: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • *Keine Aushandlung*: Je nach Einstellung im Feld **Richtung** werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt. • *Keiner*: Die Funktion ist nicht aktiv. Wählen Sie weiterhin aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen. Zur Verfügung stehen:

Feld	Beschreibung
	• *Beide* (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • *Senke*: CC-Daten werden empfangen. • *Quelle*: CC-Daten werden generiert.

9.5.3 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Spachdaten-Pakete normalerweise höchste Priorität. Trotzdem können bei geringer Bandbreite der Upload Verbindung während eines Telefongesprächs merkbare Verzögerungen bei der Sprachübertragung auftreten, wenn gleichzeitig andere Datenpakete geroutet werden.

Die Funktion Real Time Jitter Control löst dieses Problem. Um die "Leitung" für die Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

9.5.3.1 Regulierte Schnittstellen

Im Menü **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen** wird eine Liste der Schnittstellen angezeigt, für welche die Funktion Real Time Jitter Control konfiguriert ist.

9.5.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um für weitere Schnittstellen die Sprachübertragung zu optimieren.

Das Menü **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
Kontrollmodus	Wählen Sie den Modus für die Optimierung aus. Mögliche Werte: • *Nur kontrollierte RTP-Streams* (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung. • *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. • *Inaktiv*: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • *Immer*: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.
Maximale Upload-Geschwindigkeit	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

9.6 VPN

Als VPN (Virtual Private Network) wird eine Verbindung bezeichnet, die das Internet als "Transportmedium" nutzt, aber nicht öffentlich zugänglich ist. Nur berechtigte Benutzer haben Zugang zu einem solchen VPN, das anschaulich auch als VPN-Tunnel bezeichnet wird. Üblicherweise werden die über ein VPN transportierten Daten verschlüsselt.

Über ein VPN kann z. B. ein Außendienstmitarbeiter oder ein Mitarbeiter im Home Office auf die Daten

im Firmennetz zugreifen. Filialen können ebenfalls über VPN an die Zentrale angebunden werden.

Die Authentifizierung der Verbindungspartner erfolgt über ein Passwort, mithilfe von Preshared Keys oder über Zertifikate. Zur Verschlüsselung der Daten werden z. B. AES oder 3DES verwendet.

9.6.1 IPSec

IPSec ermöglicht den Aufbau von gesicherten Verbindungen zwischen zwei Standorten (VPN). Hierdurch lassen sich sensible Unternehmensdaten auch über ein unsicheres Medium wie z. B. das Internet übertragen. Die eingesetzten Geräte agieren hierbei als Endpunkte des VPN Tunnels. Bei IPSec handelt es sich um eine Reihe von Internet-Engineering-Task-Force-(IETF)-Standards, die Mechanismen zum Schutz und zur Authentifizierung von IP-Paketen spezifizieren. IPSec bietet Mechanismen, um die in den IP-Paketen übermittelten Daten zu verschlüsseln und zu entschlüsseln. Darüber hinaus kann die IPSec Implementierung nahtlos in eine Public-Key-Umgebung (PKI, siehe *Zertifikate* auf Seite 30) integriert werden. Die IPSec-Implementierung erreicht dieses Ziel zum einen durch die Benutzung des Authentication-Header-(AH)-Protokolls und des Encapsulated-Security-Payload-(ESP)-Protokolls. Zum anderen werden kryptografische Schlüsselverwaltungsmechanismen wie das Internet-Key-Exchange-(IKE)-Protokoll verwendet.

Zusätzlicher Filter des IPv4-Datenverkehrs

Digitalisierungsbox unterstützt zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IPSec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des IPv4-Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des IPv4-Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des IPv4-Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.

Hinweis

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.

Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

9.6.1.1 IPSec-Peers

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Im Menü **VPN**->**IPSec**->**IPSec-Peers** wird eine Liste aller konfigurierter IPSec-Peers nach Priorität sortiert angezeigt.

Peer Überwachung

Das Überwachungsmenü eines Peers wird durch Auswahl der -Schaltfläche beim entsprechenden Peer in der Peerliste aufgerufen. Siehe *Werte in der Liste IPSec-Tunnel* auf Seite 266.

9.6.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPSec-Peers einzurichten.

Das Menü **VPN**->**IPSec**->**IPSec-Peers**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	Wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Peer-Konfiguration versetzen wollen. Mögliche Werte: • `Aktiv` (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. • `Inaktiv`: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Peer-Adresse	Wählen Sie die **IP-Version** aus. Sie können wählen, ob IPv4 oder IPv6 bevorzugt verwendet werden soll oder ob nur eine der beiden IP-Versionen erlaubt sein soll. **Hinweis** Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird. Mögliche Werte: • `IPv4 bevorzugt` • `IPv6 bevorzugt` • `Nur IPv4` • `Nur IPv6` Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein. Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.
Peer-ID	Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein. Die Eingabe kann in bestimmten Konfigurationen entfallen.

Feld	Beschreibung
	Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen. Mögliche ID-Typen: • *Fully Qualified Domain Name (FQDN)*: Beliebige Zeichenkette • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)* • *Schlüssel-ID*: Beliebige Zeichenkette Auf dem Peer-Gerät entspricht diese ID dem Parameter **Lokaler ID-Wert**.
IKE (Internet Key Exchange)	Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll. Mögliche Werte: • *IKEv1* (Standardwert): Internet Key Exchange Protocol Version 1 • *IKEv2*: Internet Key Exchange Protocol Version 2
Authentifizierungsmethode	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Wählen Sie die Authentifizierungsmethode aus. Mögliche Werte: • *Preshared Keys* (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Preshared Keys wählen. Diese werden bei der Peerkonfiguration im Menü **IPSec-Peers** konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • *RSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.
Lokaler ID-Typ	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Wählen Sie den Typ der lokalen ID aus. Mögliche ID-Typen: • *Fully Qualified Domain Name (FQDN)* • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)* • *Schlüssel-ID*: Beliebige Zeichenkette
Lokale ID	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Geben Sie die ID Ihres Geräts ein. Für **Authentifizierungsmethode** = *DSA-Signatur* oder *RSA-Signatur* wird die Option **Subjektname aus Zertifikat verwenden** angezeigt. Wenn Sie die Option **Subjektname aus Zertifikat verwenden** aktivieren, wird der im Zertifikat angegebene Subjektname verwendet.
Preshared Key	Geben Sie das mit dem Peer vereinbarte Passwort ein. Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer *0x* am Anfang des Eintrags.

Feld	Beschreibung
IP-Version des Tunnel-netzwerks	Wählen Sie aus, ob IPv4 oder IPv6 oder beide Versionen für den VPN-Tunnel verwendbar sein sollen. Mögliche Werte: • *IPv4* • *IPv6* • *IPv4 und IPv6*

Felder im Menü IPv4-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vertrauenswürdig* (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • *Nicht Vertrauenswürdig*: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
IPv4-Adressvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: • *Statisch* (Standardwert): Geben Sie eine statische IP-Adresse ein. • *Client im IKE-Konfigurationsmodus*: Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server eine IP-Adresse erhalten soll. • *Server im IKE-Konfigurationsmodus*: Wählen Sie diese Option, wenn Ihr Gateway als Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten **IP-Zuordnungspool** entnommen.
Konfigurationsmodus	Nur bei **IPv4-Adressvergabe** = *Server im IKE-Konfigurationsmodus* oder *Client im IKE-Konfigurationsmodus* Mögliche Werte: • *Pull* (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • *Push*: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen. Dieser Wert muss für beide Seiten des Tunnels identisch sein.
IP-Zuordnungspool	Nur bei **IPv4-Adressvergabe** = *Server im IKE-Konfigurationsmodus* Wählen Sie einen im Menü **VPN**->**IPSec**->**IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.
Standardroute	Nur für **IPv4-Adressvergabe** = *Statisch* oder *Client im IKE-*

Feld	Beschreibung
	Konfigurationsmodus Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur für **IPv4-Adressvergabe** = *Statisch* oder *Server im IKE-Konfigurationsmodus* Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.
Metrik	Nur für **IPv4-Adressvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* und **Standardroute** = *Aktiviert* Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *15*. der Standardwert ist *1*.
Routeneinträge	Nur für **IPv4-Adressvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* Definieren Sie Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -LANs. • *Netzmaske*: Netzmaske zu *Entfernte IP-Adresse*. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0 - 15*). der Standardwert ist *1*.

Felder im Menü Zusätzlicher Filter des IPv4-Datenverkehrs

Feld	Beschreibung
Zusätzlicher Filter des IPv4-Datenverkehrs	Nur für **IKE (Internet Key Exchange)** = *IKEv1* Legen Sie mithilfe von **Hinzufügen** einen neuen Filter an.

Felder im Menü IPv6-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: • *Nicht Vertrauenswürdig* : Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenwürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • *Vertrauenswürdig* (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.

Feld	Beschreibung
	Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 228 konfigurieren.
Lokales IPv6-Netzwerk	Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu** angelegt sind. Geben Sie die Lokale IPv6-Adresse mit der entsprechenden Präfixlänge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.
Entferntes IPv6-Netzwerk	Fügen Sie mit **Hinzufügen** einen neuen **Präfix** hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine **Länge** von *64* und eine **Priorität** von *1* vorgegeben. Je niederiger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.

Zusätzlicher Filter des Datenverkehrs

Digitalisierungsbox unterstützt zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IPSec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des IPv4-Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des IPv4-Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des IPv4-Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.

Hinweis

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.

Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

Fügen Sie weitere Filter mit **Hinzufügen** hinzu.

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk* (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie den Quell-Port der Datenpakete ein. Die Standardeinstellung *-Alle-* (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
Ziel-Port	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung *-Alle-* (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPSec-Optionen

Feld	Beschreibung
Phase-1-Profile	Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: • *Keines (Standardprofil verwenden)*: Verwendet das Profil, das in **VPN**->**IPSec**->**Phase-1-Profile** als Standard markiert ist • *Multi-Proposal*: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü . • *<Profilname>*: Verwendet ein Profil, das im Menü **VPN**->**IPSec**->**Phase-1-Profile** für Phase 1 konfiguriert wurde.
Phase-2-Profil	Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: • *Keines (Standardprofil verwenden)*: Verwendet das Profil, das in **VPN**->**IPSec**->**Phase-2-Profile** als Standard markiert ist • **Multi-Proposal*: Verwendet ein spezielles Profil, das für Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü **VPN**->**IPSec**->**Phase-2-Profile**. • *<Profilname>*: Verwendet ein Profil, das im Menü **VPN**->**IPSec**->**Phase-2-Profile** für Phase 2 konfiguriert wurde.

Feld	Beschreibung
XAUTH-Profil	Wählen Sie ein in **VPN**->**IPSec**->**XAUTH-Profile** angelegtes Profil aus, wenn Sie zur Authentifizierung dieses IPSec-Peers XAuth verwenden möchten. Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.
Anzahl erlaubter Verbindungen	Wählen Sie aus, wieviele Benutzer sich mit diesem Peer-Profil verbinden dürfen. Mögliche Werte: • *Ein Benutzer* (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden. • *Mehrere Benutzer*: Es können sich mehrere Peers mit den in diesem Profil definierten Daten verbinden. Bei jeder Verbindungsanfrage mit den in diesem Profil definierten Daten, wird der Peer-Eintrag dupliziert. Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten. Die Clients, die sich mit dem Gateway verbinden, müssen jedoch über eine **Lokale ID** verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen. Informationen, wie dieser Parameter für Ihren IPSec-Client einzustellen ist, entnehmen Sie der entsprechenden Dokumentation. Der resultierende Peer auf dem Gateway würde nun auf alle eingehenden Tunnel-Requests zutreffen. Daher ist es notwendig, ihn an das Ende der IPSec-Peer-Liste zu stellen. Andernfalls wären alle in der Listen folgenden Peers inaktiv.
Startmodus	Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll. Mögliche Werte: • *Auf Anforderung* (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt. • *Immer aktiv*: Der Peer ist immer aktiv.
Backup Peer	Nur für IKEv2-Peers. Wenn der Peer im **Startmodus** *Immer aktiv* ist, können Sie hier einen weiteren bereits konfigurierten Peer als Rückfalloption auswählen. Wenn der aktuelle Peer z. B. aufgrund einer Störung des zentralen VPN-Einwahlknotens inaktiv wird, kann der Backup Peer eine Verbindung zu einem Backup-VPN-Einwahlknoten aufbauen. Im Fall der Wiedererreichbarkeit des primären zentralen Einwahlknotens wird die Verbindung nahtlos wieder dorthin aufgebaut. Bei dieser Lösung ist zu beachten, dass für beide Peers das Routing so konfiguriert ist, dass eine Verbindung zur Gegenstelle auch tatsächlich über beide Peers erfolgen kann. Darüber hinaus sollte die Metrik der Routen für den Backup Peer schlechter sein als die für den primären Peer. Nur so ist gewährleistet, dass der Tunnel wieder über den primären Peer aufgebaut wird, sobald dessen Verbindung wieder verfügbar ist.
Verzögerung bis zur Rückkehr zum primären Peer	Wenn im Fall eines Fallbacks der primäre Peer wieder erreichbar ist, kann es wünschenswert sein, die Nutzung des primären Peers und damit den Reset des sekundären Peers zu verzögern. Diese Option definiert

Feld	Beschreibung
	die gewünschte Verzögerungszeit.

Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Öffentliche Schnittstelle	Legen Sie diejenige öffentliche (oder WAN-) Schnittstelle fest, über die dieser Peer sich mit seinem VPN-Partner verbinden soll. Wenn Sie *Vom Routing ausgewählt* auswählen, wird die Entscheidung, über welche Schnittstelle der Datenverkehr geleitet wird, gemäß der aktuellen Routingtabelle getroffen. Wenn Sie eine Schnittstelle auswählen, wird unter Beachtung der Einstellung unter **Öffentlicher Schnittstellenmodus** diese Schnittstelle verwendet.
Öffentlicher Schnittstellenmodus	Legen Sie fest, wie strikt die Einstellung unter **Öffentliche Schnittstelle** gehandhabt wird. Mögliche Werte: • *Erzwingen*: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet. • *Bevorzugt*: Die Prioritäten der aktuellen Routingtabelle werden verwendet. Nur wenn mehrere gleichwertige Routen zur Verfügung stehen, wird die Route über die gewählte Schnittstelle verwendet.
Öffentliche IPv4-Quelladresse	Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die **Öffentliche IPv4-Quelladresse** aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll. Standardmäßig ist die Funktion nicht aktiv.
Öffentliche IPv6-Quelladresse	Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die **Öffentliche IPv6-Quelladresse** aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll. Standardmäßig ist die Funktion nicht aktiv.
Überprüfung der IPv4-Rückroute	Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
MobIKE	Nur für Peers mit IKEv2. **MobIKE** ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen. Standardmäßig ist die Funktion aktiv. Beachten Sie, dass MobIKE einen aktuellen IPSec Client voraussetzt, z. B. den aktuellen Windows-7- oder Windows-8-Client oder die neuste Version des bintec elmeg IPSec Clients.

Feld	Beschreibung
IPv4 Proxy ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer *aktiv* (aktiv) oder *Ruhend* (ruhend) ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer *aktiv* (aktiv) ist, wenn also bereits eine Verbindung zum IPSec Peer besteht.
CA-Zertifikate	Wenn Sie die Option **Folgenden CA-Zertifikaten vertrauen** aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen. Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **Digitalisierungsbox**-Geräte den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit IPSec-Callback geschaffen: Mithilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf von Ihrem Gerät nicht angenommen werden muss. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muss zunächst auf der passiven Seite im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Dienst** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf dieser Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Bei aktivem Callback wird, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlasst, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer (**MSN** im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu** für **Dienst** *IPSec*) eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.

Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst die Schnittstelle aktiviert, über die der Tunnel realisiert werden soll. Sofern auf dem lokalen Gerät IPSec mit DynDNS konfiguriert ist, wird die eigene IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gerät abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gerät das lokale auch tatsächlich erreichen kann, wenn es den Tunnelaufbau initiiert.

Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Geräts über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, können so umgangen werden.

Hinweis

Um die Funktion IP-Adressübermittlung über ISDN nutzen zu können, benötigen Sie eine kostenfreie Zusatzlizenz.

Diese Lizenz erhalten Sie bei Bedarf über Ihren Vertriebspartner oder über unseren Support.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Auslösers auf indirektem Wege (z. B. über DynDNS) ermittelt werden konnte. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus (Haupt Modus) für den Tunnelaufbau zu verwenden.

Funktionsweise: Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü IPv4 IPSec Callback* auf Seite 213 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der automatischen Auswahl durch das Gerät sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.

Hinweis

Damit Ihr Gerät die Informationen des gerufenen Peers über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Geräten analog vorgenommen werden.

Folgende Rollenverteilungen sind möglich:

- Eine Seite übernimmt die aktive, die andere die passive Rolle.
- Beide Seiten können beide Rollen (Beide) übernehmen.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

(1) Peer A (der Auslöser des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.

(2) Ihr Gerät erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.

(3) Ihr Gerät setzt den initialen ISDN-Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.

(4) Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party Number (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.

(5) Der IPSec-Daemon auf Ihrem Gerät von Peer B kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil des Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.

(6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.

Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPv4 IPSec Callback

Feld	Beschreibung
Modus	Wählen Sie den Callback-Modus aus. Mögliche Werte: • *Inaktiv* (Standardwert): IPSec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • *Passiv*: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • *Aktiv*: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • *Beide*: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	Nur für **Modus** = *Passiv* oder *Beide* Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.
Ausgehende Rufnummer	Nur für **Modus** = *Aktiv* oder *Beide* Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.
Eigene IP-Adresse per ISDN/GSM übertragen	Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Übertragungsmodus	Nur für **Eigene IP-Adresse per ISDN/GSM übertragen** = aktiviert Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen. Mögliche Werte:

Feld	Beschreibung
	• *Automatische Erkennung des besten Modus*: Ihr Gerät bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird. (Die Verwendung des B-Kanals verursacht Kosten.) • *Nur D-Kanalmodi automatisch erkennen*: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • *Spezifischen D-Kanalmodus verwenden*: Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. • *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen*: Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übetragen. (Dies verursacht Kosten.) • *Nur B-Kanalmodus verwenden*: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	Nur für **Übertragungsmodus** = *Spezifischen D-Kanalmodus verwenden* oder *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen* Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen. Mögliche Werte: • *LLC* (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • *SUBADDR*: Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • *LLC und SUBADDR*: Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.

9.6.1.2 Phase-1-Profile

Im Menü **VPN**->**IPSec**->**Phase-1-Profile** wird eine Liste aller konfigurierter IPSec-Phase-1-Profile angezeigt.

In der Spalte **Standard** können Sie das Profil markieren, das als Standard-Profil verwendet werden soll.

9.6.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu** (bei **Neues IKEv1-Profil erstellen** bzw. **Neues IKEv2-Profil erstellen**), um weitere Profile einzurichten.

Das Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Phase-1-Parameter (IKE) / Phase-1-Parameter (IKEv2)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
Proposals	In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Nachrichten-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Nachrichten-Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Mindestens ein Proposal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden. Verschlüsselungsalgorithmen (**Verschlüsselung**):

Feld	Beschreibung
	• *3DES* : 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • *Twofish*: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • *Blowfish*: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • *CAST*: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • *DES*: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • *AES* (Standardwert): Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter *AES* gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • *AES-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. Hash-Algorithmen (**Authentifizierung**): • *MD5*: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • *SHA1* (Standardwert): SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. • *RipeMD 160*: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • *Tiger192*: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. • *SHA2-256*: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • *SHA2-384*: SHA-2 mit 384 Bit Hash-Länge. • *SHA2-512*: SHA-2 mit 512 Bit Hash-Länge. Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung. Beachten Sie, dass die Qualität der Algorithmen relativen Gesichtpunkten unterliegt und sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern kann.

Feld	Beschreibung
DH-Gruppe	Nur für **Phase-1-Parameter (IKE)** Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von **Digitalisierungsbox** unterstützt wird, steht für "modular exponentiation". Mögliche Werte: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie die Lebensdauer für Phase-1-Schlüssel fest. Folgende Optionen stehen für die Definition der **Lebensdauer** zur Verfügung: • Eingabe in **Sekunden**: Geben Sie die Lebensdauer für Phase-1-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist *14400*, das bedeutet, dass die Schlüssel erneuert werden, wenn vier Stunden abgelaufen sind. • Eingabe in **kBytes**: Geben Sie die Lebensdauer für Phase-1- Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist *0*; das bedeutet, dass die Anzahl der gesendeten kBytes keine Rolle spielt.
Authentifizierungsmethode	Nur für **Phase-1-Parameter (IKE)** Wählen Sie die Authentifizierungsmethode aus. Mögliche Werte: • *Preshared Keys* (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Pre Shared Keys wählen. Diese werden bei der Peerkonfiguration im Menü **VPN**->**IPSec**->**IPSec-Peers** konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • *DSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • *RSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert. • *RSA-Verschlüsselung*: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	Nur für **Phase-1-Parameter (IKE)** Nur für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.

Feld	Beschreibung
Modus	Nur für **Phase-1-Parameter (IKE)** Wählen Sie den Phase-1-Modus aus. Mögliche Werte: • *Aggressiv* (Standardwert): Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden. Er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals. • *Main Modus (ID Protect)*: Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec-SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (**Strikt**) oder der Peer auch einen anderen Modus vorschlagen kann.
Lokaler ID-Typ	Nur für **Phase-1-Parameter (IKE)** Wählen Sie den Typ der lokalen ID aus. Mögliche Werte: • *Fully Qualified Domain Name (FQDN)* • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)*
Lokaler ID-Wert	Nur für **Phase-1-Parameter (IKE)** Geben Sie die ID Ihres Geräts ein. Für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* wird die Option **Subjektname aus Zertifikat verwenden** angezeigt. Wenn Sie die Option **Subjektname aus Zertifikat verwenden** aktivieren, wird der im Zertifikat angegebene Subjektname verwendet.

Erreichbarkeitsprüfung

In der Kommunikation zweier IPSec-Peers kann es dazu kommen, dass einer der beiden z. B. aufgrund von Routing-Problemen oder aufgrund eines Neustarts nicht erreichbar ist. Dies ist aber erst dann feststellbar, wenn das Ende der Lebensdauer der Sicherheitsverbindung erreicht ist. Bis zu diesem Zeitpunkt gehen die Datenpakete verloren. Um dies zu verhindern, gibt es verschiedene Mechanismen einer Erreichbarkeitsprüfung. Im Feld **Erreichbarkeitsprüfung** wählen Sie aus, ob ein Mechanismus angewendet werden soll, um die Erreichbarkeit eines Peers zu überprüfen.

Hierbei stehen zwei Mechanismen zur Verfügung: Heartbeats und Dead Peer Detection.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Erreichbarkeitsprüfung	Nur für **Phase-1-Parameter (IKE)** Wählen Sie die Methode aus, mit der die Funktionalität der IPSec-

Feld	Beschreibung
	Verbindung überprüft werden soll. Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird Mögliche Werte: • *Automatische Erkennung* (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • *Inaktiv*: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • *Heartbeats (Nur erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • *Heartbeats (Nur senden)*: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • *Heartbeats (Senden &Erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • *Dead Peer Detection*: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen. • *Dead Peer Detection (Idle)*: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen. **Hinweis** Da die beiden Verfahren zur Erreichbarkeitsprüfung unterschiedliche Methoden verwenden, empfiehlt es sich nicht, sie in Phase 1 und Phase 2 kombiniert zu verwenden. In Phase 2 werden lediglich Heartbeats unterstützt, so dass diese deaktiviert werden sollten, wenn in Phase 1 Dead Peer Detection vorgeschrieben ist. Nur für **Phase-1-Parameter (IKEv2)** Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung. Standardmäßig ist die Funktion aktiv.
Blockzeit	Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche. Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* bedeutet die Übernahme des Wertes im Standardprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird. Der Standardwert ist *30*. Wenn ein Peer im Modus "Immer aktiv" konfiguriert ist, besteht eine implizite Minimalblockzeit von 15 Sekunden, die unabhängig vom eingegebenen Wert angewendet wird.

Feld	Beschreibung
NAT-Traversal	NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist. Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gerät zu einem anderen Host bzw. Gerät. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Geräten, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet. Nur für *IKEv1-Profile* Mögliche Werte: • *Aktiviert* (Standardwert): NAT-Traversal ist aktiv. • *Deaktiviert*: NAT-Traversal ist deaktiviert. • *Erzwingen*: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. Nur für *IKEv2-Profile* Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
CA-Zertifikate	Nur für **Phase-1-Parameter (IKE)** Nur für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* Wenn Sie die Option **Folgenden CA-Zertifikaten vertrauen** aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen. Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.

9.6.1.3 Phase-2-Profile

Ebenso wie für Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Im Menü **VPN**->**IPSec**->**Phase-2-Profile** wird eine Liste aller konfigurierten IPSec-Phase-2-Profile angezeigt.

In der Spalte **Standard** können Sie das Profil markieren, das als Standardprofil verwendet werden soll.

9.6.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Profile einzurichten.

Das Menü **VPN**->**IPSec**->**Phase-2-Profile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und

Feld	Beschreibung
	zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld. Verschlüsselungsalgorithmen (**Verschlüsselung**): • *3DES*: 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • *-- ALLE --*: Alle Optionen können verwendet werden. • *AES* (Standardwert): Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter *AES* gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • *AES-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. • *Twofish*: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • *Blowfish*: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • *CAST*: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • *DES*: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. Hash-Algorithmen (**Authentifizierung**): • *MD5*: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • *-- ALLE --*: Alle Optionen können verwendet werden. • *SHA1* (Standardwert): SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. • *SHA2-256*: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • *SHA2-384*: SHA-2 mit 384 Bit Hash-Länge. • *SHA2-512*: SHA-2 mit 512 Bit Hash-Länge. Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.

Feld	Beschreibung
	Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.
PFS-Gruppe verwenden	Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (*Aktiviert*), sind die Optionen die gleichen, wie bei der Konfiguration von **DH-Gruppe** im Menü **VPN**->**IPSec**->**Phase-1-Profile**. PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind. Das Feld hat folgende Optionen: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)* (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen. Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind. Folgende Optionen stehen für die Definition der **Lebensdauer** zur Verfügung: • Eingabe in **Sekunden**: Geben Sie die Lebensdauer für Phase-2-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Der Standardwert ist *7200*. • Eingabe in **kBytes**: Geben Sie die Lebensdauer für Phase-2- Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Der Standardwert ist *0*. **Schlüssel erneut erstellen nach**: Legen Sie fest, bei welchem Prozentsatz des Ablaufes der Lebensdauer die Schlüssel der Phase 2 neu erstellt werden. Die eingegebene Prozentzahl wird sowohl auf die Lebensdauer in Sekunden als auch auf die Lebensdauer in kBytes angewendet. Der Standardwert ist *80* %.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IP-Komprimierung	Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder nicht komprimierbaren Daten wird von

Feld	Beschreibung
	der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Erreichbarkeitsprüfung	Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen. Mögliche Werte: • *Automatische Erkennung* (Standardwert): Automatische Erkennung, ob die Gegenstelle eine **Digitalisierungsbox** ist. Wenn ja, wird *Heartbeats (Senden &Erwarten)* (bei Gegenstelle mit **Digitalisierungsbox**) oder *Inaktiv* (bei Gegenstelle ohne **Digitalisierungsbox**) gesetzt. • *Inaktiv*: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • *Heartbeats (Nur erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • *Heartbeats (Nur senden)*: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • *Heartbeats (Senden &Erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. **Hinweis** In Phase 1 und Phase 2 unterstützt Ihr Gerät unterschiedliche Verfahren zur Erreichbarkeitsprüfung: In Phase 1 die sog. Dead Peer Detection sowie Heartbeats, in Phase 2 lediglich Heartbeats. Da die beiden Verfahren zur Erreichbarkeitsprüfung unterschiedliche Methoden verwenden, empfiehlt es sich nicht, sie in Phase 1 und Phase 2 kombiniert zu verwenden. In Phase 2 sollten Heartbeats daher deaktiviert werden, wenn in Phase 1 Dead Peer Detection vorgeschrieben ist.
PMTU propagieren	Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

9.6.1.4 XAUTH-Profile

Im Menü **XAUTH-Profile** wird eine Liste aller XAuth-Profile angezeigt.

Extended Authentication für IPSec (XAuth) ist eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Mehrere Benutzer können sich entweder nacheinander einzeln oder über einen Multi Peer gleichzeitig einwählen. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpassworts (One Time Password, OTP) kann die Passwortüberprüfung von einem Token-Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS-Server installiert ist.

Wenn eine Firmenzentrale über IPSec mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden, zum Beispiel ein Peer für je eine Filiale. Für jeden dieser Peers, also für jede Filiale, wird ein Passwort vergeben. Neben dieser Möglichkeit der Authentifizierung pro Filiale bietet XAuth eine zusätzliche Möglichkeit, mit der sich ein Benutzer individuell und unabhängig vom Standort über sein persönliches Passwort anmelden kann. Damit kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet und er jeweils vor Ort individuellen Zugriff auf den Tunnel benötigt.

Bei einem sogenannten Multi Peer verwenden alle Benutzer dasselbe Passwort, also ein Gruppenpasswort. Auch hier eröffnet XAuth einem Benutzer eine individuelle Authentifizierungsmöglichkeit. Wenn zum Beispiel in einer Filiale mehrere Benutzer über einen Multi Peer Zugriff auf den Tunnel haben, kann es bei unterschiedlichen Aufgaben der Benutzer von Vorteil sein, wenn sich jeder Benutzer mit seinem individuellen Passwort einwählt.

Nachdem IPSec IKE (Phase 1) erfolgreich beendet ist und bevor IKE (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.

9.6.1.4.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Profile einzurichten.

Das Menü **VPN**->**IPSec**->**XAUTH-Profile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für dieses XAuth-Profil ein. Mit den Einstellungen **Rolle** = *Server* und **Modus** = *Lokal* oder **Rolle** = *Client* (siehe unten) können Sie bis zu 10 XAuth-Profile anlegen. Die Zahl der Benutzer
Rolle	Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus. Mögliche Werte: • *Server* (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an. • *Client*: Das Gateway weist seine Berechtigung nach.
Modus	Nur für **Rolle** = *Server* Wählen Sie aus, wie die Authentifizierung durchgeführt wird. Mögliche Werte: • *RADIUS* (Standardwert): Die Authentifizierung wird über einen RADIUS-Server durchgeführt. Dieser wird im Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS** konfiguriert und im Feld **RADIUS-Server Gruppen-ID** ausgewählt.

Feld	Beschreibung
	• *Lokal*: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	Nur für **Rolle** = *Client* Geben Sie den Authentifizierungsnamen des Clients ein.
Passwort	Nur für **Rolle** = *Client* Geben Sie das Authentifizierungspasswort ein.
RADIUS-Server Gruppen-ID	Nur für **Rolle** = *Server* Wählen Sie die gewünschte in **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS** konfigurierte RADIUS-Gruppe aus.
Benutzer	Nur für **Rolle** = *Server* und **Modus** = *Lokal* Ist Ihr Gateway als XAuth-Server konfiguriert, können die Clients über eine lokal konfigurierte Benutzerliste authentifiziert werden. Definieren Sie hier die Mitglieder der Benutzergruppe dieses XAUTH-Profils, indem Sie den Authentifizierungsnamen des Clients (**Name**) und das Authentifizierungspasswort (**Passwort**) eingeben. Fügen Sie weitere Mitglieder mit **Hinzufügen** hinzu. Die Zahl der Benutzer pro XAuth-Profil ist unbeschränkt.

9.6.1.5 IP Pools

Hinweis

Beachten Sie, dass das Menü **IP Pools** nur dann verfügbar ist wenn ein Port im Menü **Physikalische Schnittstellen**->**ISDN-Ports**-> **ISDN-Konfiguration** in den externen Betrieb (TE-Modus) geschaltet ist. Dafür muss ein Adapter angeschlossen sein (als Zubehör erhältlich).

Im Menü **IP Pools** wird eine Liste aller IP Pools für Ihre konfigurierten IPSec-Verbindungen angezeigt.

Wenn Sie bei einem IPSec-Peer für **IPv4-Adressvergabe** *Server im IKE-Konfigurationsmodus* eingestellt haben, müssen Sie hier die IP-Pools, aus denen die IP-Adressen vergeben werden, definieren.

9.6.1.5.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers

Feld	Beschreibung
	ein.

9.6.1.6 Optionen

Das Menü **VPN**->**IPSec**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	Wählen Sie, ob Sie IPSec aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.
Vollständige IPSec-Konfiguration löschen	Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts. Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen. Das Löschen der Konfiguration ist nur möglich mit **IPSec aktivieren** = nicht aktiviert.
IPSec-Debug-Level	Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung* • *Benachrichtigung* • *Information* • *Debug* (Standardwert, niedrigste Priorität) Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level "Debug" sämtliche erzeugten Meldungen aufgezeichnet werden.

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen **Digitalisierungsbox**-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	Wählen Sie aus, ob IPSec über TCP verwendet werden soll. IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese

Feld	Beschreibung
	Technologie sorgt dafür, dass der Datenverkehr (IKE, ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Initial Contact Message senden	Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
SAs mit dem Status der ISP-Schnittstelle synchronisieren	Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von *Aktiv* zu *Inaktiv*, *Ruhend* oder *Blockiert* geändert hat. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zero Cookies verwenden	Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen. Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall *Aktiviert*.
Größe der Zero Cookies	Nur für **Zero Cookies verwenden** = aktiviert. Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein. Der Standardwert ist *32*.
Dynamische RADIUS-Authentifizierung	Wählen Sie aus, ob die RADIUS-Authentifizierung über IPSec aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	Wählen Sie aus, ob Zertifikatanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungs-Payloads senden	Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Zertifikatsketten senden	Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.

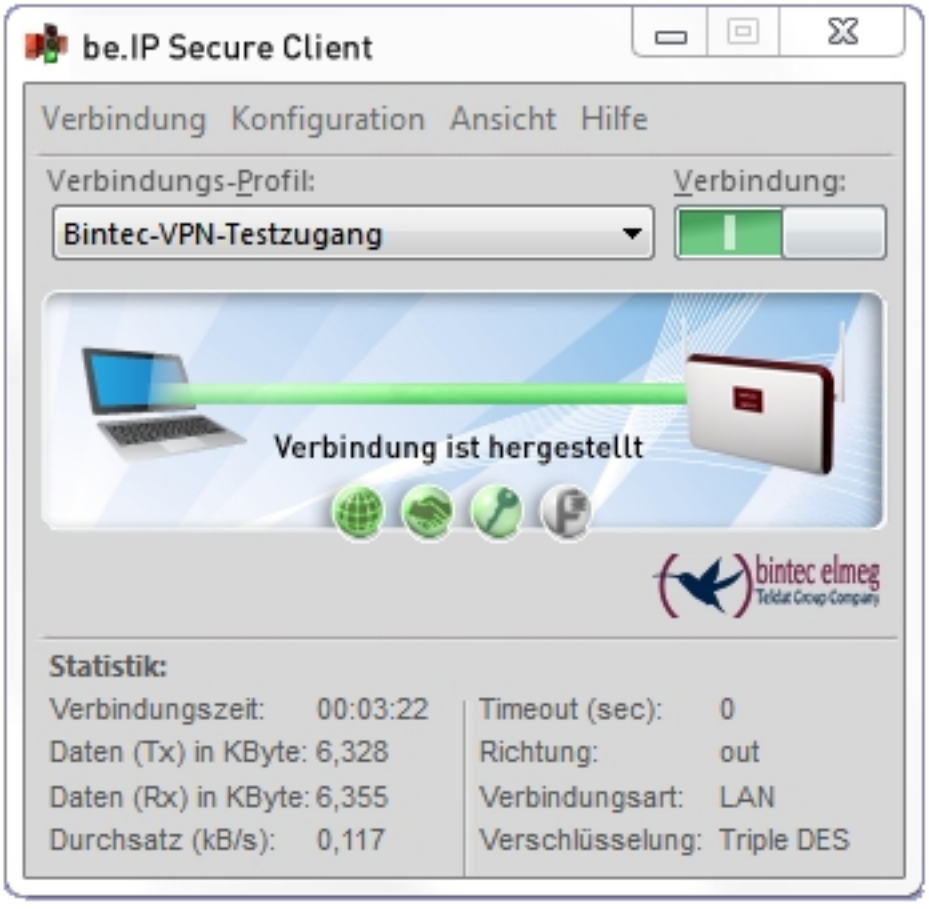
Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.
CRLs senden	Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Key Hash Payloads senden	Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen. Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit *Aktiviert*, um dieses Verhalten zu unterdrücken.

9.6.2 Digitalisierungsbox Secure Client

Hier können Sie die aktuelle Secure IPSec Client Software herunterladen. Weitere Informationen finden Sie auf auf www.bintec-elmeg.com.

Wichtig

Beachten Sie, dass der Client ausschließlich für Windows zu Verfügung steht.



9.7 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügt die **Digitalisierungsbox** über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder Ports, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Die Aushandlung einer FTP-Verbindung findet zum Beispiel über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

Die Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der **Digitalisierungsbox** ein. Systemen wie Network Address Translation (NAT) und IP-Zugriffs-Listen (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf eine Schnittstelle beschränkt sind.

Grundsätzlich werden aber dieselben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der einzelnen Sicherheitsinstanzen und ihrer Funktionsweise.

NAT

Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ISP zugewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, welches Ihr Gerät nicht einer bereits bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem WAN auf das LAN ab.

IP Access Listen

Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird nicht berücksichtigt (außer bei **Dienste** = *TCP*).

SIF

Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl ein "Verweigern", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch ein "Ablehnen", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die eingehenden Pakete werden folgendermaßen bearbeitet:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne dass eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ICMPHost-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.
- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen (= Standardverhalten).

9.7.1 Richtlinien

9.7.1.1 IPv4-Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Verwerfen-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Dem Sicherheitskonzept liegt die Vorstellung zugrunde, dass die Infrastruktur aus vertrauenswürdigen und nicht vertrauenswürdigen Zonen besteht. Die beiden Sicherheitsrichtlinien *Vertrauenswürdig* bzw. *Nicht Vertrauenswürdig* beschreiben diese Vorstellung. Sie definieren die beiden Filterregeln **Vertrauenswürdige Schnittstellen** und **Nicht vertrauenswürdige Schnittstellen**, die standardmäßig angelegt sind und nicht gelöscht werden können.

Falls Sie die **Sicherheitsrichtlinie** *Vertrauenswürdig* verwenden, werden alle Datenpakete akzeptiert. Sie können nun zusätzliche Filterregeln definieren, die bestimmte Pakete verwerfen. Auf die gleiche Weise können Sie für die Einstellung *Nicht Vertrauenswürdig* ausgewählte Datenpakete freigeben.

Im Menü **Firewall**->**Richtlinien**->**IPv4-Filterregeln** wird eine Liste aller konfigurierten IPv4-Filterregeln angezeigt.

Mit der Schaltfläche in der Zeile **Vertrauenswürdige Schnittstellen** können Sie festlegen, welche Schnittstellen **Vertrauenswürdig** sind. Es öffnet sich ein neues Fenster mit einer Schnittstellenliste. Sie können die einzelnen Schnittstellen als vertrauenswürdig markieren.

Mit der Schaltfläche können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

Mit der Schaltfläche können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

9.7.1.1.1 Neu

Hinweis

Informationen zur Auswahl der Vertrauenswürdige Schnittstellen finden Sie hier: *IPv4-Filterregeln* auf Seite 229.

Wählen Sie die Schaltfläche **Neu**, um weitere Parameter einzurichten.

Das Menü **Firewall**->**Richtlinien**->**IPv4-Filterregeln**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus. In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl. Der Wert *Beliebig* bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.
Ziel	Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus. In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl. Der Wert *Beliebig* bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* Weitere Dienste werden in **Firewall**->**Dienste**->**Diensteliste** angelegt. Außerdem stehen die in **Firewall**->**Dienste**->**Gruppen** konfigurierten Dienstegruppen zur Auswahl.
Aktion	Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll. Möglichen Werte: • *Zugriff* (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • *Verweigern*: Die Pakete werden abgewiesen. • *Zurückweisen*: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

9.7.1.2 IPv6-Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Verwerfen-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Dem Sicherheitskonzept liegt die Vorstellung zugrunde, dass die Infrastruktur aus vertrauenswürdigen und nicht vertrauenswürdigen Zonen besteht. Die beiden Sicherheitsrichtlinien *Vertrauenswürdig* bzw. *Nicht Vertrauenswürdig* beschreiben diese Vorstellung. Sie definieren die beiden Filterregeln **Vertrauenswürdige Schnittstellen** und **Nicht vertrauenswürdige Schnittstellen**, die standardmäßig angelegt sind und nicht gelöscht werden können.

Falls Sie die **Sicherheitsrichtlinie** *Vertrauenswürdig* verwenden, werden alle Datenpakete akzeptiert. Sie können nun zusätzliche Filterregeln definieren, die bestimmte Pakete verwerfen. Auf die gleiche Weise können Sie für die Einstellung *Nicht Vertrauenswürdig* ausgewählte Datenpakete freigeben.

Datenpakete, die das Neighbour Discovery Protocol verwenden, sind grundsätzlich erlaubt, auch für die Filterregel *Nicht Vertrauenswürdig*.

Im Menü **Firewall**->**Richtlinien**->**IPv6-Filterregeln** wird eine Liste aller konfigurierter IPv6-Filterregeln angezeigt.

Mit der Schaltfläche in der Zeile **Vertrauenswürdige Schnittstellen** können Sie festlegen, welche Schnittstellen **Vertrauenswürdig** sind. Es öffnet sich ein neues Fenster mit einer Schnittstellenliste. Sie können die einzelnen Schnittstellen als vertrauenswürdig markieren.

Hinweis

Beachten Sie, dass die Schnittstellenliste für IPv6 leer ist, solange IPv6 für keine Schnittstelle aktiviert ist.

Mit der Schaltfläche können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

Mit der Schaltfläche können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

9.7.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Parameter einzurichten.

Das Menü **Firewall**->**Richtlinien**->**IPv6-Filterregeln**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus. In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**IPv6-Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl, für die IPv6 aktiviert ist.

Feld	Beschreibung
Ziel	Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus. In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**IPv6-Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl, für die IPv6 aktiviert ist.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* Weitere Dienste werden in **Firewall**->**Dienste**->**Diensteliste** angelegt. Außerdem stehen die in **Firewall**->**Dienste**->**Gruppen** konfigurierten Dienstegruppen zur Auswahl.
Aktion	Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll. Mögliche Werte: • *Zugriff* (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • *Verweigern* : Die Pakete werden abgewiesen. • *Zurückweisen* : Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

9.7.1.3 Optionen

In diesem Menü können Sie die IPv4-Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wie vielen Sekunden Inaktivität eine Sitzung beendet werden soll.

Hinweis

Beachten Sie, dass die IPv6-Firewall immer eingeschaltet ist und nicht ausgeschaltet werden kann.

Das Menü **Firewall**->**Richtlinien**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Status der IPv4-Firewall	Aktivieren oder deaktivieren Sie die IPv4-Firewall-Funktion. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion aktiv.

Feld	Beschreibung
Protokollierte Aktionen	Wählen Sie den Firewall-Syslog-Level aus. Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme. Mögliche Werte: • *Alle* (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • *Verweigern*: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion". • *Annehmen*: Nur Accept-Ereignisse werden angezeigt. • *Keiner*: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige IPv4-Filterung	Bei TCP-Sessions überwacht die SIF im ersten Schritt, ob eine Session korrekt und vollständig aufgebaut wird. Unvollständige Sessions werden blockiert. Im zweiten Schritt erfolgt die eigentliche Filterung. Für diesen "Normalfall" ist die Standardeinstellung **Vollständige IPv4-Filterung** *Aktivieren* vorgesehen. Wenn bei zweiseitiger Kommunikation eine Richtung des Datenverkehrs über den Router läuft, die Datenpakete der entgegengesetzten Richtung aber einen anderen Weg nehmen, so ist die TCP-Session aus Sicht der SIF unvollständig und der Router würde diesen Datenverkehr nicht zulassen. Um Datenverkehr solcher unvollständiger TCP-Sessions beim Spezialfall identischer Eingangs- und Ausgangsschnittstelle zu erlauben, müssen Sie **Vollständige IPv4-Filterung** deaktivieren. Etwaige existierende SIF-Filterregeln dazu werden ignoriert.
STUN Handler	Wenn Sie Geräten (vor allem SIP Clients) in Ihrem Netzwerk erlauben wollen, über STUN den Modus der Network Address Translation sowie die öffentliche IP-Adresse zu ermittlen, so aktivieren Sie diese Option. Die Firewall erstellt dann temporäre Regeln, die den RTP-Datenverkehr für SIP-Gespräche ermöglichen.
Port-STUN-Server	Nur für **STUN Handler** = Aktiviert Geben Sie Nummer des Ports ein, der für die Verbindung zum STUN-Server benutzt werden soll. Standardmäßig ist der Wert *3478* vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.

Felder im Menü Sitzungstimer

Feld	Beschreibung
UDP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine UDP -Session als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *180*.
TCP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP -Session als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *3600*.
PPTP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine PPTP-Session als

Feld	Beschreibung
	abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *86400*.
Andere Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *30*.

Felder im Menü Firewall auf Werkseinstellungen zurücksetzen

Feld	Beschreibung
Firewall auf Werkseinstellungen zurücksetzen	Klicken Sie auf **Zurücksetzen** um die Firewall auf Werkseinstellungen zurückzusetzen.

9.7.2 Schnittstellen

9.7.2.1 IPv4-Gruppen

Im Menü **Firewall**->**Schnittstellen**->**IPv4-Gruppen** wird eine Liste aller konfigurierter Schnittstellen-Gruppen angezeigt.

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

9.7.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Schnittstellen-Gruppen einzurichten.

Das Menü **Firewall**->**Schnittstellen**->**IPv4-Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

9.7.2.2 IPv6-Gruppen

Im Menü **Firewall**->**Schnittstellen**->**IPv6-Gruppen** wird eine Liste aller konfigurierter IPv6-Schnittstellen-Gruppen angezeigt.

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dies vereinfacht die Konfiguration von Firewall-Regeln.

9.7.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Schnittstellen-Gruppen einzurichten.

Das Menü **Firewall**->**Schnittstellen**->**IPv6-Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.

Feld	Beschreibung
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

9.7.3 Adressen

9.7.3.1 Adressliste

Im Menü **Firewall**->**Adressen**->**Adressliste** wird eine Liste aller konfigurierter Adressen angezeigt.

9.7.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Adressen einzurichten.

Das Menü **Firewall**->**Adressen**->**Adressliste**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adresse ein.
IPv4	Erlaubt die Konfiguration von IPv4-Adresslisten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Adresstyp	Nur für **IPv4** = *Aktiviert* Wählen Sie aus, welche Art von Adresse Sie angeben wollen. Mögliche Werte: • *Adresse/Subnetz* (Standardwert): Sie geben eine IP-Adresse mit Subnetzmaske ein. • *Adressbereich*: Sie geben einen IP-Adressbereich mit Anfangs- und Endadresse ein.
Adresse/Subnetz	Nur für **IPv4** = *Aktiviert* und **Adresstyp** = *Adresse/Subnetz* Geben Sie die IP-Adresse des Hosts oder eine Netzwerk-Adresse und die zugehörige Netzmaske ein. Standardwert ist jeweils *0.0.0.0*.
Adressbereich	Nur für **IPv4** = *Aktiviert* und **Adresstyp** = *Adressbereich* Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein.
IPv6	Erlaubt die Konfiguration von IPv6-Adresslisten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Adresse/Präfix	Nur für **IPv6** = *Aktiviert* Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.

9.7.3.2 Gruppen

Im Menü **Firewall**->**Adressen**->**Gruppen** wird eine Liste aller konfigurierter Adressgruppen angezeigt.

Sie können Adressen zu Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

9.7.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Adressgruppen einzurichten.

Das Menü **Firewall**->**Adressen**->**Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adressgruppe ein.
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte: • *IPv4* • *IPv6* Standardmäßig ist *IPv4* ausgewählt.
Auswahl	Wählen Sie aus den zur Verfügung stehenden **Adressen** die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

9.7.4 Dienste

9.7.4.1 Diensteliste

Im Menü **Firewall**->**Dienste**->**Diensteliste** wird eine Liste aller zur Verfügung stehender Dienste angezeigt.

9.7.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Dienste einzurichten.

Das Menü **Firewall**->**Dienste**->**Diensteliste**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	Nur für **Protokoll** = *TCP*, *UDP/TCP* oder *UDP* Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll. Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind *1* bis *65535*.
Quellportbereich	Nur für **Protokoll** = *TCP*, *UDP/TCP* oder *UDP* Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port an.

Feld	Beschreibung
	Soll ein Portnummernbereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Portbereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind *1* bis *65535*.
Typ	Nur für **Protokoll** = *ICMP* Das Feld **Typ** gibt die Klasse der ICMP-Nachrichten an, das Feld **Code** spezifiziert die Art der Nachricht genauer. Mögliche Werte: • *Beliebig* (Standardwert) • *Echo Reply* • *Destination Unreachable* • *Source Quench* • *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Nur für **Typ** = *Destination Unreachable* stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung. Mögliche Werte: • *Beliebig* (Standardwert) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

9.7.4.2 Gruppen

Im Menü **Firewall**->**Dienste**->**Gruppen** wird eine Liste aller konfigurierter Service-Gruppen angezeigt.

Sie können Dienste in Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

9.7.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Service-Gruppen einzurichten.

Das Menü **Firewall**->**Dienste**->**Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Service-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Service-Aliasen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

9.8 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)

9.8.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste**->**DNS**->**DNS-Server**->**Neu** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der schnittstellengebundenen Name-Server kann Ihr Gerät auch dynamisch via PPP oder DHCP erhalten bzw. diese ggf. übermitteln.

Strategie zur Namensauflösung auf Ihrem Gerät

Eine DNS-Anfrage wird von Ihrem Gerät folgendermaßen behandelt:

(1) Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt mit IP-Adresse

oder negativer Antwort beantwortet.

(2) Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(3) Ansonsten werden, falls Name-Server eingetragen sind, unter Berücksichtigung der konfigurierten Priorität und wenn der entsprechende Schnittstellenstatus "up" ist, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(4) Ansonsten werden, falls eine Internet- oder Einwählverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(5) Ansonsten wird, falls im Menü **WAN**->**Internet + Einwählen** ein Eintrag angelegt wurde und das Überschreiben der Adressen der globalen Name-Server zulässig ist (**Schnittstellenmodus** = *Dynamisch*), eine Verbindung zur ersten Internet- bzw. Einwählverbindung ggf. kostenpflichtig aufgebaut, die so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert werden können (**DNS-Aushandlung** = *Aktiviert*) - soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung stehen diese Name-Server somit für weitere Anfragen zur Verfügung.

(6) Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit `non-existent domain` antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

9.8.1.1 Globale Einstellungen

Das Menü **Lokale Dienste**->**DNS**->**Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server **Primär** **Sekundär**	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Negativer Cache	Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
Cache-Größe	Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein. Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird **Cache-Größe** vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. **Cache-Größe** kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden. Mögliche Werte: *0*.. *1000*. Der Standardwert ist *100*.
Maximale TTL für positive Cacheeinträge	Geben Sie den Wert ein, auf den die TTL für einen positiven dynamischen DNS-Eintrag im Cache gesetzt werden soll, wenn dessen TTL *0* ist oder dessen TTL den Wert für **Maximale TTL für positive Cacheeinträge** überschreitet. Der Standardwert ist *86400*.
Maximale TTL für negative Cacheeinträge	Geben Sie den Wert ein, auf den die TTL bei einem negativen dynamischen Eintrag im Cache gesetzt werden soll. Der Standardwert ist *86400*.
Alternative Schnittstelle, um DNS-Server zu erhalten	Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren. Der Standardwert ist *Automatisch*, d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.

Felder im Menü Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse

Feld	Beschreibung
Als DHCP-Server	Wählen Sie aus, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn Ihr Gerät als DHCP-Server genutzt wird. Mögliche Werte: • *Keiner*: Es wird keine Name-Server-Adresse übermittelt. • *Eigene IP-Adresse* (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • *DNS-Einstellung*: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermittelt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird. Mögliche Werte: • *Keiner*: Es wird keine Name-Server-Adresse übermittelt. • *Eigene IP-Adresse*: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • *DNS-Einstellung* (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

9.8.1.2 DNS-Server

Im Menü **Lokale Dienste**->**DNS**->**DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

9.8.1.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere DNS-Server einzurichten.

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.

Das Menü **Lokale Dienste**->**DNS**->**DNS-Server**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob der DNS-Server aktiv sein soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	Weisen Sie dem DNS-Server eine Priorität zu. Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) oder mehreren Schnittstellen mehrere Paare von DNS-Servern (**Primärer DNS-Server** und **Sekundärer DNS-Server**) zuweisen. Verwendet wird das Paar mit der höchsten Priorität, wenn die Schnittstelle im Zustand "up" ist. Mögliche Werte von *0* (höchste Priorität) bis *9* (niedrigste Priorität). Der Standardwert ist *5*.
Schnittstellenmodus	Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen. Mögliche Werte: • *Statisch* • *Dynamisch* (Standardwert)
Schnittstelle	Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll. Die gewählte Schnittstelle ist für ausgehende DNS-Anfragen relevant. Diese Schnittstelle wird für DNS-Client-Anfragen verwendet, die an den Router gerichtet sind oder vom Router selbst erzeugt wurden. Bei **Schnittstellenmodus** = *Dynamisch* Mit der Einstellung *Keine* wird ein globaler DNS-Server angelegt. Bei **Schnittstellenmodus** = *Statisch*

Feld	Beschreibung
	Mit der Einstellung *Beliebig* wird ein DNS-Server für alle Schnittstellen konfiguriert.
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte: • *IPv4* • *IPv6* Standardmäßig ist *IPv4* ausgewählt.
Primärer IPv4-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie die IPv4-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.
Sekundärer IPv4-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie optional die IPv4-Adresse eines alternativen Name-Servers ein.
Primärer IPv6-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie die IPv6-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.
Sekundärer IPv6-DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie optional die IPv6-Adresse eines alternativen Name-Servers ein.

9.8.1.3 Statische Hosts

Im Menü **Lokale Dienste**->**DNS**->**Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

9.8.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Das Menü **Lokale Dienste**->**DNS**->**Statische Hosts**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Standarddomäne	Hier wird die Domäne angezeigt, die Sie im Menü **DNS**->**Globale Einstellungen** als Domänennamen eingetragen haben.
DNS-Hostname	Geben Sie den Host-Namen ein, dem die in diesem Menü definierte **IP-Adresse** zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt. Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.bintec-elmeg.com. Wenn Sie einen einfachen Namen angeben (z. B. *router*), wird dieser durch die Standarddomäne zu einem vollständigen DNS-Namen (Fully Qualified Domain Name, FQDN) ergänzt. Wenn Sie einen Namen in der Struktur eines FQDN eingeben (also durch "." getrennte Zeichenfolgen), so wird der Eintrag als FQDN interpretiert und nicht erweitert. Der für einen vollständigen FQDN erforderliche, schließende "." wird ggf. auto-

Feld	Beschreibung
	matisch ergänzt. Einträge mit Leerzeichen sind nicht erlaubt.
Antwort	Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus. Mögliche Werte: • *Negativ*: Eine DNS-Anfrage nach **DNS-Hostname** wird negativ beantwortet. • *Positiv* (Standardwert): Eine DNS-Anfrage nach **DNS-Hostname** wird mit der dazugehörigen **IP-Adresse** beantwortet. • *Keine*: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IPv4-Adresse	Nur bei **Antwort** = *Positiv* Geben Sie die IPv4-Adresse ein, die nach **DNS-Hostname** zugeordnet wird.
IPv6-Adresse	Nur bei **Antwort** = *Positiv* Geben Sie die IPv6-Adresse ein, die nach **DNS-Hostname** zugeordnet wird.

9.8.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

9.8.1.4.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Weiterleitungen einzurichten.

Das Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob Anfragen bezüglich eines Hosts oder einer Domäne weitergeleitet werden soll. Mögliche Werte: • *Host* (Standardwert) • *Domäne*
Host	Nur für **Weiterleiten** = *Host* und **Weiterleiten an** = *DNS-Server* Geben Sie den Namen des Hosts ein, für den Anfragen weitergeleitet werden sollen. Bei Eingabe eines Namens ohne "." wird nach Bestätigung mit **OK** der Eintrag mit dem im Menü **Lokale Dienste**->**DNS**->**Globale Einstellungen** unter **Domänenname** eingetragenen Namen ergänzt.
Domäne	Nur für **Weiterleiten** = *Domäne* und **Weiterleiten an** = *DNS-Server*

Feld	Beschreibung
	Geben Sie den Namen der Domäne ein, für die Anfragen weitergeleitet werden sollen. Der Eintrag kann mit der Wildcard "*" beginnen, z. B. "*.mustermann.lan". Bei Eingabe eines Namens ohne führende Wildcard "*" wird nach Bestätigung mit **OK** automatisch eine führende Wildcard "*" eingefügt.
Weiterleiten an	Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer **Schnittstelle** oder an einen manuell konfigurierten **DNS-Server** weitergeleitet werden sollen. Mögliche Werte: • *Schnittstelle* (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konfigurierten Schnittstelle weitergeleitet. • *DNS-Server*: Anfragen werden an den definierten **DNS-Server** weitergeleitet.
Zielschnittstelle	Nur für **Weiterleiten an** = *Schnittstelle* Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfragen weitergeleitet werden sollen.
Quellschnittstelle	Hier können Sie eine Quellschnittstelle der DNS-Anfragen für die Domainweiterleitung festlegen. Diese Option steht sowohl für Weiterleitungen an eine Schnittstelle als auch für Weiterleitungen an bestimme DNS-Server zu Verfügung. Dies ermöglicht es, DNS-Anfragen aus verschiedenen Netzsegmenten auch an verschiedene DNS-Server zu senden. So können Sie z. B. die Anfragen aus einem Gästenetz an einen Webfilter-DNS leiten und unerwünschte Inhalte ausfiltern.
Primärer DNS-Server (IPv4/IPv6)	Nur für **Weiterleiten an** = *DNS-Server* Geben Sie IPv4/IPv6-Adresse des primären DNS-Servers ein.
Sekundärer DNS-Server (IPv4/IPv6)	Nur für **Weiterleiten an** = *DNS-Server* Geben Sie IPv4/IPv6-Adresse des sekundären DNS-Servers ein.

9.8.1.5 Dynamische Hosts

Im Menü **Lokale Dienste**->**DNS**->**Dynamische Hosts** sehen Sie die relevanten Angaben zu den dynamischen DNS-Einträgen.

9.8.1.6 Cache

Im Menü **Lokale Dienste**->**DNS**->**Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

9.8.1.7 Statistik

Im Menü **Lokale Dienste**->**DNS**->**Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der **Cache-Treffer** pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

9.8.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und authentifizierte Verbindung mittels SSL aufzubauen.

9.8.2.1 HTTPS-Server

Im Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Das Menü besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll. Möglich sind Werte von *0* bis *65535*. Der Standardwert ist *443*.
Lokales Zertifikat	Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll. Mögliche Werte: • *Intern* (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möchten. • *<Zertifikatsname>*: Wählen Sie ein unter **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** eingetragenes Zertifikat aus.

9.8.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie die Aufgabe, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Geräts zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Geräts informiert ist, kontaktiert Ihr Gerät beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

9.8.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

9.8.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

Das Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Aktualisierung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Weitere DynDNS-Provider können im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider** konfiguriert werden. Der Standardwert ist *DynDNS* .
Aktualisierung aktivieren	Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert wer-

Feld	Beschreibung
	den soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Mail-Exchanger (MX)	Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.
Wildcard	Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von **Hostname** zur aktuellen IP-Adresse von **Schnittstelle** aktiviert werden soll (Erweiterte Namensauflösung). Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

9.8.3.2 DynDNS-Provider

Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

9.8.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

Das Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. Der Standardwert ist *80*.
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: • *DynDNS* (Standardwert)

Feld	Beschreibung
	• *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Aktualisierungsintervall	Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf. Der Standardwert ist *300* Sekunden.

9.8.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine DHCP-Anfrage (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server." Daraufhin erhält der Client (im Zuge einer kurzen Kommunikation) vom bintec elmeg seine IP-Adresse.

Sie müssen so den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem Ihr Gerät jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain-Name-Servers (DNS), des NetBIOS Name Servers (WINS) und des Standard-Gateways.

9.8.4.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch in anderen Menüs konfigurierte Pools an.

9.8.4.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers

Feld	Beschreibung
	ein.

9.8.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** wird eine Liste aller konfigurierter DHCP-Pools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.

Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.2.100 bis 192.168.2.199 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

9.8.4.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DHCP-Pools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Das Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, über welche die in **IP-Adressbereich** definierten Adressen an anfragende DHCP-Clients vergeben werden. Wenn eine DHCP-Anfrage über diese **Schnittstelle** eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP-Poolname	Wählen Sie einen im Menü **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration** konfigurierten IP-Poolnamen aus.
Pool-Verwendung	Wählen Sie aus, ob der DHCP-Pool für Anfragen von DHCP-Clients in einem direkt an Schnittstelle angeschlossenen Ethernet verwendet werden soll oder für DHCP-Anfragen, die aus einem abgesetzt liegenden Ethernet stammen und über eine DHCP-Relaisstation an Ihr Gerät weitergeleitet wurden. In letzterem Fall ist es möglich, einen IP-Adresspool für ein entfernt liegendes Netz zu verwenden. Mögliche Werte: • *Lokal* (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen aus einem direkt an Schnittstelle angeschlossenen Ethernet verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus einem abgesetzt liegenden Ethernet verwendet. • *Lokal/Relais*: Der DHCP-Pool kann für lokale und für weitergeleitete DHCP-Anfragen aus direkt angeschlossenen bzw. abgesetzt liegenden Ethernets verwendet werden.
Beschreibung	Geben Sie eine beliebige Beschreibung ein, um den DHCP-Pool eindeutig zu benennen.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Gateway	Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll. Mögliche Werte: • *Router als Gateway verwenden* (Standardwert): Hier wird die für die **Schnittstelle** definierte IP-Adresse übertragen. • *Kein Gateway*: Hier wird keine IP-Adresse übermittelt. • *Angeben*: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll. Nachdem **Lease Time** abgelaufen ist, kann die Adresse durch den Server neu vergeben werden. Der Standardwert ist *120*.
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen. Mögliche Werte für **Option**: • *Zeitserver* (Standardwert): Geben Sie die IP-Adresse des Zeitservers ein, die dem Client übermittelt werden soll. • *DNS-Server*: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • *DNS-Domänenname*: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • *WINS/NBNS-Server*: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • *WINS/NBT Node Type*: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • *TFTP-Server*: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • *CAPWAP Controller*: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • *URL (Provisionierungsserver)*: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. Verwenden Sie diese Option, um anfragenden **IP1x0**-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form *http://<IP-Adresse des Provisionierungsservers>/eg_prov* haben. Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche **Hinzufügen** ein.

Herstellerspezifische Informationen (DHCP-Option 43)

Mit den Optionen für einen **Hersteller-String** bzw. eine herstellerspezifische Gruppe von DHCP-Optionen (**Herstellergruppe**) können Sie einen DHCP Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen oder Konfigurationseinstellungen übermitteln oder auch ganze Gruppen von DHCP-Optionen festlegen, die dem Client übermittelt werden.

Hinweis

Für einige Produkte sind in diesem Bereich Einstellungen hinterlegt, die für eine reibungslose Einbindung von Telefonen oder LTE-Zugangsroutern notwendig sind. Diese Einstellungen sollten weder geändert noch entfernt werden.

Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten oder eine der Schaltflächen zum Hinzufügen entsprechender Einträge. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

Felder im Menü Basisparameter für Hersteller-Strings

Feld	Beschreibung
Hersteller auswählen	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: • *Sonstige* (Standardwert) • *-bintec-*
APN	Nur für **Hersteller auswählen** = *-bintec-* Geben Sie den Access Point Namen (APN) der SIM-Karte ein.
PIN	Nur für **Hersteller auswählen** = *-bintec-* Geben Sie die PIN der SIM-Karte ein.
Herstellerbeschreibung	Nur für **Hersteller auswählen** = *Sonstige* Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Hersteller-ID	Nur für **Hersteller auswählen** = *Sonstige* Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
Herstellerspezifische Informationen	Nur für **Hersteller auswählen** = *Sonstige* Geben Sie die Hersteller spezifischen Konfigurationsparameter ein.

Felder im Menü Basisparameter für Herstellergruppen

Feld	Beschreibung
Hersteller auswählen	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: • *Siemens* (Standardwert) • *Sonstige*
Provisioning-Server (code 3)	Nur für **Hersteller auswählen** = *Siemens* Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll. Für die Einstellung **Hersteller auswählen** = *Siemens* wird der Standardwert *sdlp* angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.
Herstellerbeschreibung	Nur für **Hersteller auswählen** = *Sonstige*

Feld	Beschreibung
	Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Hersteller-ID	Nur für **Hersteller auswählen** = *Sonstige* Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
Benutzerdefinierte DHCP-Optionen	Nur für **Hersteller auswählen** = *Sonstige* Fügen Sie mit **Hinzufügen** weitere Einträge hinzu. Sie können DHCP-Optionen hinzufügen.

9.8.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.

Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration** IP-Adressbereiche konfiguriert wurden, und im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** dem DHCP-Server ein gültiger IP-Pool zugewiesen ist.

9.8.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

Das Menü **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen **MAC-Adresse** die **IP-Adresse** gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in **MAC-Adresse** angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in **IP-Adresse** angegebene IP-Adresse zugewiesen werden soll.

9.8.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Das Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen. Der Standardwert ist `0.0.0.0`.
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein. Der Standardwert ist `0.0.0.0`.

9.8.5 DHCPv6-Server

Sie können Ihr Gerät als DHCPv6-Server verwenden. Dieser DHCPv6-Server kann IP- Adressen und DHCP-Optionen an Clients verteilen oder auch nur DHCP-Optionen ohne Adressen. Diese Parameter werden in einem sogenannten "Option Set" zusammengefasst. Ein Option Set kann an eine Schnittstelle gebunden werden (siehe unter **Lokale Dienste**->**DHCPv6-Server**->**DHCPv6-Server**->**Neu**) oder es kann global konfiguriert werden (siehe unter **Lokale Dienste**->**DHCPv6-Server**->**Globale DHCPv6-Optionen**->**Neu**). DHCP-Optionen können zum Beispiel Informationen über DNS-Server oder Zeitserver enthalten.

Hinweis

Ein IPv6-Adress-Pool ensteht durch die Zuweisung eines IPv6-Link-Präfixes (Subnetz mit der Länge /64) zu einem DHCPv6 Option Set. Die Definition eines eigenen Abschnitts von IPv6-Aderssen, wie z. B. fc00:1:2:3::1..fc00:1:2:3::100 ist anders als im DHCPv4 nicht vorgesehen.

Für die Konfiguration eines IPv6-Adress-Pools müssen folgende Voraussetzungen erfüllt sein:

(a) IPv6 muss auf der betreffenden Schnittstelle aktiviert sein.

(b) Ein IPv6-Link-Präfix (Subnetz) mit der Länge /64 muss auf der gewünschten Schnittstelle konfiguriert sein. Ein IPv6-Link-Präfix kann auf zwei Arten definiert sein:

- Der IPv6-Link-Präfix ist von einem Allgemeinen IPv6-Präfix (Präfix mit einer Länge von zum Beispiel /56 oder /48) abgeleitet. In diesem Fall muss der Allgemeine IPv6-Präfix im Menü **Netzwerk**->**Allgemeine IPv6-Präfixe**->**Konfiguration eines Allgemeinen Präfixes** konfiguriert sein.
- Der IPv6-Link-Präfix mit Länge /64 wird manuell auf der entsprechenden Schnittstelle konfiguriert und nicht von einem Allgemeinen IPv6-Präfix abgeleitet.

(c) Die Option **DHCP-Server** muss für die Schnittstelle aktiviert sein.

Darüber hinaus sind folgende Einstellungen empfehlenswert:

- Die Werte für die Optionen **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer** sollten auf Werte gesetzt werden, die größer sind als der Wert für **Router-Gültigkeitsdauer**.

  Bei einer **Router-Gültigkeitsdauer** von 600 Sekunden, empfehlen sich z. B. eine **Bevorzugte Gültigkeitsdauer** von 900 Sekunden und eine **Gültigkeitsdauer** von 1800 Sekunden.
- Die Option **DHCP-Modus** sollte aktiviert sein.

Zur Einstellung der o.g. Optionen wählen Sie das Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**. Mit dem Symbol wählen Sie die gewünschte Schnittstelle. Aktivieren Sie IPv6 und setzen den **IPv6-Modus** auf `Router (Router-Advertisement übermitteln)`. Klicken Sie im Feld **IPv6-Adressen** auf **Hinzufügen** und konfigurieren Sie den Link-Präfix. Bestätigen Sie Ihre Konfiguration mit **Übernehmen**. Die Konfiguration der empfohlenen Einstellungen erfolgt dann in folgenden Menüs:

- **Router-Gültigkeitsdauer**: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**->**Erweiterte Einstellungen**->**Erweiterte IPv6-Einstellungen**
- **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer**: **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**->**Grundlegende IPv6-Parameter**->**Hinzufügen**->**Er-**

weitert

9.8.5.1 DHCPv6-Server

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.

9.8.5.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um ein Option Set anzulegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Name	Geben Sie einen Namen für das Option Set ein.
Schnittstelle	Wählen Sie die IPv6-Schnittstelle, an die das Option Set gebunden sein soll. Zur Auswahl stehen Schnittstellen mit folgender Konifguration: • IPv6 ist aktiviert. • Die Option **DHCP-Server** ist aktiviert. Im Auslieferungszustand ist IPv6 für alle Schnittstellen deaktiviert. Erscheint die gewünschte Schnittstelle nicht in der Auswahl, konfigurieren Sie sie im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen** gemäß den in der Einleitung genannten Vorgaben.
Adresszuweisung	Die Definition eines IPv6-Adresspools erfolgt durch Zuweisung eines IPv6-Link-Präfixes (Subnetz mit Länge /64) zu einem DHCPv6 Option Set. Der IPv6-Adress-Pool umfasst immer den kompletten 64-Bit-Adressraum des gewählten IPv6-Link-Präfixes. Die Adressvergabe erfolgt zufällig. Mit **Hinzufügen** können Sie dem IPv6 Option Set einen oder mehrere IPv6-Link-Präfixe zuordnen. **Hinweis** Bitte beachten Sie, dass hier ausschließlich die IPv6-Link-Präfixe zur Auswahl stehen, die der gewählten Schnittstelle zugewiesen sind.

Felder im Menü Server-Optionen

Feld	Beschreibung
DNS-Domänen-Suchliste	Mit **Hinzufügen** können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
DNS-Server	Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server"). In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld **DNS-Propagation** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->  ->**Erweiterte Einstellungen** mit **IPv6** = *Aktiviert* konfiguriert.) Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option **RA oder globalen Fallback-DNS-Server verwenden** und erstellen Sie mit **Hinzufügen** die gewünschten DNS-Server-Einträge.
SNTP-Server	Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit **Hinzufügen** können Sie die gewünschten Zeitserver-Einträge anlegen.

9.8.5.2 Globale DHCPv6-Optionen

In diesem Menü können Sie die für den DHCPv6-Server global gültigen DHCPv6-Optionen konfigurieren. Eine hier konfigurierte Option wird immer dann propagiert, wenn für diese Option keine exaktere Definition (z.B. keine schnittstellenspezifische oder Vendor-ID-spezifische Definition) existiert.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter, Server-Fallback-Optionen

Feld	Beschreibung
DNS-Domänen-Suchliste	Mit **Hinzufügen** können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt. Der Domain-Name (z. B. dev.bintec.de.) muss mit Punkt (.) enden.

Das Menü **Erweiterte Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Erweiterte Einstellung

Feld	Beschreibung
Server-Priorität	In den vom DHCPv6 Server an die Clients gesendeten DHCPv6 Advertisements kann die DHCPv6-Option 7 Preference enthalten sein. Mögliche Werte sind *0...255*. In einem Netzwerk mit mehreren DHCPv6 Servern wird über diese Option gesteuert, welcher DHCPv6-Server im Netzwerk die höchste Priorität besitzt. Empfängt ein Client DHCPv6 Advertisements mit unterschiedlicher Priorität von verschiedenen Servern, so wird der Client in der Regel die Werte des Servers mit der höchsten Priorität übernehmen. Der Client kann jedoch auch DHCPv6 Advertisements mit niedrigerer Priorität akzeptieren, wenn der im DHCPv6 Advertisement enthaltene Parametersatz mehr den vom Client angeforderten Optionen entspricht. Der Wert *0* bedeutet "nicht spezifiziert" (niedrigste Priorität), *255* bedeutet höchste Priorität.

Felder im Menü Erweiterte Server-Fallback-Optionen

Feld	Beschreibung
DNS-Server	Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propa-

Feld	Beschreibung
	giert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server"). In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld **DNS-Propagation** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->  ->**Erweiterte Einstellungen** mit **IPv6** = *Aktiviert* konfiguriert.) Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option **RA oder globalen Fallback-DNS-Server verwenden** und erstellen Sie mit **Hinzufügen** die gewünschten DNS-Server-Einträge.
SNTP-Server	Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit **Hinzufügen** können Sie die gewünschten Zeitserver-Einträge anlegen.

9.8.5.3 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

9.8.5.4 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

9.8.5.4.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um Einträge für Stateful Clients anzulegen. Normalerweise müssen Sie keine Einträge anlegen. Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten. Sie sollten jeden automatisch angelegten Eintrag einmal aufrufen, um den Inhalt zu prüfen und gegebenenfalls anzupassen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DUID	Ein Client verwendet das Feld **DUID** (DHCP Unique Identifier), um sich zu identifizieren und eine IP-Adresse vom DHCPv6-Server zu beziehen. Wenn Sie mit der Schaltfläche **Neu** einen Eintrag anlegen, können Sie die **DUID** als 16- bis 20-stellige HEX-Zahl eingeben. Sie können sie mit den Trennzeichen Minus eingeben wie unter Windows oder als Block ohne Trennzeichen wie unter Linux.
Client FQDN akzeptieren	Wenn **Client FQDN akzeptieren** aktiviert ist, wird der Client mit dem Parameter FQDN (Fully Qualified Domain Name) im Cache des Domain Name Servers eingetragen.
Administrative FQDNs	Mit **Hinzufügen** können Sie - auch bei automatisch angelegten Einträgen - den Parameter FQDN (Fully Qualified Domain Name) eingeben.
Kennung der statischen Schnittstelle	Das Feld **Kennung der statischen Schnittstelle** ist der Host-Anteil der IPv6-Adresse, d.h. die letzten 64 Bit der IPv6-Adresse. Dieser Präfix muss mit :: anfangen.

9.8.6 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

9.8.6.1 Hosts

Im Menü **Lokale Dienste**->**Überwachung**->**Hosts** wird eine Liste aller überwachten Hosts angezeigt.

9.8.6.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Überwachungsaufgaben einzurichten.

Das Menü **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	Wenn die Erreichbarkeit einer Gruppe von Hosts bzw. des Standard-Gateways von Ihrem Gerät überwacht werden soll, wählen Sie eine ID für die Gruppe bzw. für das Standard-Gateway. Die Gruppen-IDs werden automatisch von `0` bis `255` angelegt. Ist noch kein Eintrag angelegt, wird durch die Option `Neue ID` eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen. Jeder zu überwachende Host muss einer Gruppe zugeordnet werden. Der für die ausgewählte **Schnittstelle** konfigurierte Vorgang wird nur dann ausgeführt, wenn kein Gruppenmitglied erreicht werden kann. Darüber hinaus müssen die Gruppenmitglieder die gleiche Kombination von Aktion und Schnittstelle haben.

Felder im Menü Trigger

Feld	Beschreibung
Überwachte IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll. Mögliche Werte: • `Standard-Gateway` (Standardwert): Das Standard-Gateway wird überwacht. • `Spezifisch`: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.
Quell-IP-Adresse	Wählen Sie aus, wie die IP-Adresse ermittelt werden soll, die Ihr Gerät als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird. Mögliche Werte: • `Automatisch` (Standardwert): Die IP-Adresse wird automatisch ermittelt. • `Spezifisch`: Geben Sie in das nebenstehende Eingabefeld die IP-

Feld	Beschreibung
	Adresse ein.
Intervall	Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll. Mögliche Werte sind *1* bis *65536*. Der Standardwert ist *10*. Innerhalb einer Gruppe wird das kleinste **Intervall** der Gruppenmitglieder verwendet.
Erfolgreiche Versuche	Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird. Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird. Mögliche Werte sind *1* bis *65536*. Der Standardwert ist *3*.
Fehlgeschlagene Versuche	Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird. Mögliche Werte sind *1* bis *65536*. Der Standardwert ist *3*.
Auszuführende Aktion	Nicht für **Aktion** = *Überwachen*. Wählen Sie aus, welche **Aktion** ausgeführt werden soll, wenn der Host als unerreichbar angesehen wird. Für die meisten Aktionen wählen Sie eine **Schnittstelle**, auf die sich die **Aktion** bezieht. Auswählbar sind alle IP-Schnittstellen. Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (*Aktivieren*), deaktiviert (*Deaktivieren*, Standardwert) oder zurückgesetzt (*Zurücksetzen*) werden soll oder ob die Verbindung erneut aufgebaut (*Erneut wählen*) werden soll. Die **Aktionen** *Aktivieren* und *Deaktivieren* werden ebenfalls abgebrochen, wenn die Hosts wieder als erreichbar angesehen werden. Mit **Aktion** = *Überwachen* können Sie die IP-Adresse überwachen, die unter **Überwachte IP-Adresse** angegeben ist. Diese Information kann für andere Funktionen genutzt werden, z. B. für die **IP-Adresse zur Nachverfolgung**, die bei der IP-Lastverteilung verwendet wird.

9.8.6.2 Schnittstellen

Im Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

9.8.6.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Das Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von **Überwachte Schnittstelle** aus, der eine bestimmte **Schnittstellenaktion** auslösen soll. Mögliche Werte: • *Schnittstelle wird aktiviert.* (Standardwert) • *Schnittstelle wird deaktiviert.*
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in **Trigger** definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in **Schnittstelle** ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: • *Aktivieren* (Standardwert): Aktivierung der Schnittstelle(n) • *Deaktivieren*: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter **Schnittstelle** festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen *Alle PPP-Schnittstellen* und *Alle IPSec-Schnittstellen*.

9.8.6.3 Ping-Generator

Im Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

9.8.6.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Pings einzurichten.

Das Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. Mögliche Werte: • *Automatisch*: Die IP-Adresse wird automatisch ermittelt.

Feld	Beschreibung
	• *Spezifisch* (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in **Entfernte IP-Adresse** angegebene Adresse abgesetzt werden soll. Mögliche Werte sind *1* bis *65536*. Der Standardwert ist *10*.
Versuche	Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen. Der Standardwert ist *3*.

9.8.7 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist *5678*. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch zugewesenen Ports liegen im Bereich von *5004* bis *65535*. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf *www.upnp.org* .

9.8.7.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

Das Menü **Lokale Dienste**->**UPnP**->**Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der Schnittstelle an, für welche die UPnP-Einstellungen

Feld	Beschreibung
	vorgenommen werden. Der Eintrag kann nicht verändert werden.
Auf Client-Anfrage antworten	Legen Sie fest, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle (aus dem lokalen Netzwerk) beantwortet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

9.8.7.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

Das Menü **Lokale Dienste**->**UPnP**->**Allgemein** besteht aus folgenden Feldern:

Felder im Menü Allgemein

Feld	Beschreibung
UPnP-Status	Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt. Mit *Aktiviert* wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Clients beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients. Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.
UPnP TCP Port	Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht. Mögliche Werte sind *1* bis *65535*, der Standardwert ist *5678*.

9.8.8 Wake-On-LAN

Mit der Funktion **Wake-On-LAN** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

9.8.8.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

9.8.8.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Filter einzutragen.

Das Menü **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter**->**Neu** besteht aus folgenden Fel-

dern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *any*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Typ	Nur für **Protokoll** = *ICMP* Wählen Sie einen Typ aus. Mögliche Werte: *Beliebig*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Siehe RFC 792. Der Standardwert ist *Beliebig*.
Verbindungsstatus	Bei **Protokoll** = *TCP* können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt. Mögliche Werte: • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete.
IPv4-Zieladresse/-netzmaske	Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.

Feld	Beschreibung
	• *Host*: Geben Sie die Ziel-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP*, *UDP* oder *TCP/UDP* Geben Sie eine Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Zielport ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
IPv4-Quelladresse/-netzmaske	Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein. Mögliche Werte: • *Beliebig* (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP*, *UDP* oder *TCP/UDP* Geben Sie eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Quellport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Quellport ein. • *Portbereich angeben*: Geben Sie einen Quellport-Bereich ein.
DSCP / Traffic Class Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach

Feld	Beschreibung
	RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Wertebereich *0* bis *7*. Der Standardwert ist *Nicht beachten*.

9.8.8.2 WOL-Regeln

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** wird eine Liste aller konfigurierten WOL-Regeln angezeigt.

9.8.8.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Regeln einzutragen.

Das Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Wake-On-LAN-Regelkette	Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. • *<Name der Regelkette>*: Zeigt eine bereits angelegte Regelkette, die Sie auswählen und bearbeiten können.
Beschreibung	Nur für **Wake-On-LAN-Regelkette** = *Neu* Geben Sie die Bezeichnung der Regelkette ein.
Wake-on-LAN-Filter	Wählen Sie ein WOL-Filter aus. Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll. Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** konfiguriert sein.
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *WOL aufrufen, wenn Filter zutrifft*: WOL ausführen, wenn der Filter zutrifft.

Feld	Beschreibung
	• *Aufrufen, wenn Filter nicht zutrifft*: WOL ausführen, wenn der Filter nicht zutrifft. • *WOL verweigern, wenn Filter zutrifft*: WOL nicht ausführen, wenn der Filter zutrifft. • *WOL verweigern, wenn Filter nicht zutrifft*: WOL nicht ausführen, wenn der Filter nicht zutrifft. • *Regel ignorieren und zu nächster Regel springen*: Diese Regel wird ignoriert und die in der Kette folgende wird überprüft.
Typ	Wählen Sie aus, ob das Wake on LAN Magic Packet als UDP-Paket oder als Ethernet Frame über die Schnittstelle gesendet werden soll, die in **Sende WOL-Paket über Schnittstelle** festgelegt wird.
Sende WOL-Paket über Schnittstelle	Wählen Sie die Schnittstelle aus, über die das Wake on LAN Magic Packet gesendet werden soll.
Ziel-MAC-Adresse	Nur für **Aktion** = *WOL aufrufen, wenn Filter zutrifft* und *Aufrufen, wenn Filter nicht zutrifft* Geben Sie die MAC-Adresse desjenigen Netzwerkgerätes ein, das mittels WOL aktiviert werden soll.
Passwort	Nur für **Aktion** = *WOL aufrufen, wenn Filter zutrifft* und *Aufrufen, wenn Filter nicht zutrifft* Wenn das Netzwerkgerät, das aktiveirt werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.

9.8.8.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

9.8.8.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Einträge zu erstellen.

Das Menü **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.

9.9 Monitoring

Dieses Menü enthält Informationen, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle Ihres Geräts, ermöglichen.

9.9.1 IPSec

9.9.1.1 IPSec-Tunnel

Im Menü **Monitoring**->**IPSec**->**IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

Durch Klicken auf die ^-Schaltfläche oder der v-Schaltfläche in der Spalte **Aktion** wird der Status der IPSec-Verbindung geändert.

Durch Klicken auf die Q-Schaltfläche wird eine ausführliche Statistik zu der jeweiligen IPSec-Verbindung angezeigt.

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.
IKE (Phase-1) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

9.9.1.2 IPSec-Statistiken

Im Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

Das Menü besteht aus folgenden Feldern:

Feld im Menü Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (**In Verwendung**) und die Anzahl der maximal verwendbaren Lizenzen (**Maximal**) an.

Feld im Menü Peers

Feld	Beschreibung
Status	Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an. • **Aktiv**: Aktuell aktive IPSec-Verbindungen. • **Aktivieren**: IPSec-Verbindungen, die sich aktuell in der Tunnelaufbau-Phase befinden. • **Blockiert**: IPSec-Verbindungen, die geblockt sind. • **Ruhend**: Aktuell inaktive IPSec-Verbindungen. • **Konfiguriert**: Konfigurierte IPSec-Verbindungen.

Felder im Menü SAs

Feld	Beschreibung
IKE (Phase-1)	Zeigt die Anzahl der aktiven Phase-1-SAs (**Hergestellt**) zur Gesamtzahl der Phase-1-SAs (**Gesamt**) an.
IPSec (Phase-2)	Zeigt die Anzahl der aktiven Phase-2-SAs (**Hergestellt**) zur Gesamtzahl der Phase-2-SAs (**Gesamt**) an.

Felder im Menü Paketstatistiken

Feld	Beschreibung
Gesamt	Zeigt die Anzahl aller verarbeiteten eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Weitergeleitet	Zeigt die Anzahl der eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an, die im Klartext weitergeleitet wurden.
Verworfen	Zeigt die Anzahl der verworfenen eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Verschlüsselt	Zeigt die Anzahl der durch IPSec geschützten eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Fehler	Zeigt die Anzahl der eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an, bei deren Behandlung es zu Fehlern gekommen ist.

9.9.2 ISDN/Modem (Media Gateway)

9.9.2.1 Aktuelle Anrufe

Im Menü **Monitoring**->**ISDN/Modem**->**Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

Werte in der Liste Aktuelle Anrufe

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden ist: *PPP*, *IPSec*, *X.25*, *POTS*.

Feld	Beschreibung
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: *Eingehend*, *Ausgehend*.
Kosten	Zeigt die Kosten der laufenden Verbindung an.
Dauer	Zeigt die Dauer der laufenden Verbindung an.
Stack	Zeigt den zugehörigen ISDN-Port (STACK) an.
Kanal	Zeigt die Nummer des ISDN-B-Kanals an.
Status	Zeigt den Status der Verbindung an: *null*, *c-initiated*, *ovl-send*, *oc-procd*, *c-deliverd*, *c-present*, *c-recvd*, *ic-procd*, *aktiv*, *discon-req*, *discon-ind*, *suspd-req*, *resum-req*, *ovl-recv*.

9.9.2.2 Anrufliste

Im Menü **Monitoring**->**ISDN/Modem**->**Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

Werte in der Liste Anrufliste

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden war: *PPP*, *IP-Sec*, *X.25*, *POTS*.
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: *Eingehend*, *Ausgehend*.
Kosten	Zeigt die Kosten der Verbindung an.
Startzeit	Zeigt die Uhrzeit an, zu welcher der Ruf aus- bzw. einging.
Dauer	Zeigt die Dauer der Verbindung an.

9.9.3 Schnittstellen

9.9.3.1 Statistik

Im Menü **Monitoring**->**Schnittstellen**->**Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

Durch Klicken auf die ⌃-Schaltfläche oder der ⌄-Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert.

Werte in der Liste Statistik

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld	Beschreibung
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt die MAC-Adresse an.
IP-Adresse/Netzmaske	Zeigt die IP-Adresse und die Netzmaske an.
NAT	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld im Menü TCP-Verbindungen

Feld	Beschreibung
Status	Zeigt den Status einer aktiven TCP-Verbindung an.
Lokale Adresse	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
Lokaler Port	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

9.9.3.2 Netzwerk-Status

Im Menü **Monitoring**->**Schnittstellen**->**Netzwerk-Status** finden Sie eine Übersicht über alle IP-Schnittstellen, die auf dem Gerät konfiguriert sind. Sie können den Status der Schnittstelle sowie wesentliche Parameter wie die IPv4- bzw. IPv6-IP-Adresse, die MAC-Adresse der Schnittstelle sowie die aktuell gültige MTU ablesen.

9.9.4 Bridges

9.9.4.1 br<x>

Im Menü **Monitoring**->**Bridges**-> **br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

Werte in der Liste br<x>

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

9.9.5 QoS

Im Menü **Monitoring**->**QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

9.9.5.1 QoS

Im Menü **Monitoring**->**QoS**->**QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Index