Benutzerhandbuch
bintec RXL-Serie und bintec PSU XL

Referenz

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.

Inhaltsverzeichnis

1 Inbetriebnahme

Achtung

Vor Installation und Inbetriebnahme Ihres Geräts lesen Sie bitte aufmerksam die Sicherheitshinweise. Diese sind im Lieferumfang enthalten.

1.1 Aufstellen und Anschließen

Hinweis

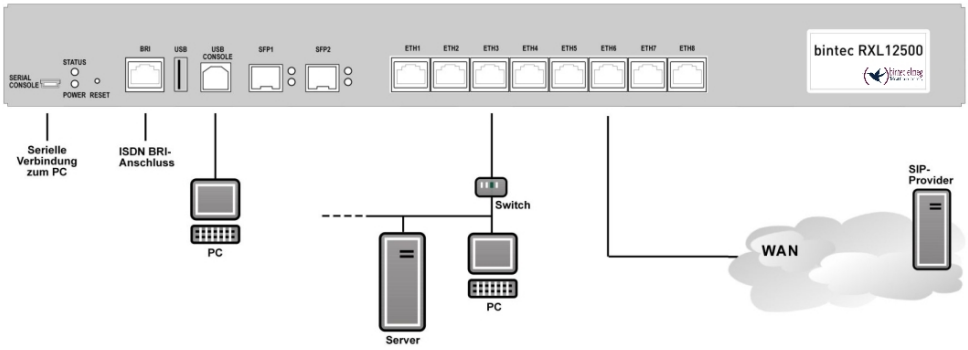
Für die Durchführung benötigen Sie keine weiteren Hilfsmittel als die mitgelieferten Kabel.

Achtung

Bei falscher Verkabelung der ISDN- und ETH-Schnittstellen kann es zum Defekt Ihres Geräts kommen! Verbinden Sie immer nur die ETH-Schnittstelle des Geräts mit der LAN-Schnittstelle des Rechners/Switches oder eine ggf. vorhandenen ISDN-Schnittstelle des Geräts nur mit dem ISDN-Anschluss.

Hinweis

Wenn Sie ein unkonfiguriertes Gerät parallel zu einer Telefonanlage an einen ISDN-Anschluss anschließen, kann die Telefonanlage solange keine Rufe annehmen, bis auf dem Gerät eine ISDN-Nummer konfiguriert ist. Wenn kein Eintrag vorhanden ist, wird jeder über ISDN eingehende Ruf vom Dienst ISDN-Login angenommen.



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

(1) Befestigen Sie die mitgelieferten Gummifüßchen an den markierten Flächen an der Unterseite des Geräts.

(2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage oder installieren Sie Ihr Gerät mit Hilfe der mitgelieferten Winkel in einem 19-Zoll-Schrank.

(3) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet verbinden Sie den ersten Switch-Port (**ETH1**) Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

(4) Netzanschluss

Schließen Sie das Gerät an eine Steckdose an. Der Netzanschluss befindet sich auf der Geräterückseite.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- ISDN-BRI

  Schließen Sie die ISDN-BRI-Schnittstelle (**BRI1**) des Geräts mit dem mitgelieferten ISDN-BRI-Kabel an Ihre ISDN-Dose an.

- Weitere LANs und WAN

  Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports **ETH2** bis **ETH4** und Ihre WAN-Verbindung(en) an die Ports **ETH5** bis **ETH8** Ihres Geräts mittels weiterer Ethernet-Kabel an.

- Serielle Verbindung

  Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit einer der seriellen Schnittstellen des Geräts (**USB Console** oder **Serial Console**). Beide Konsolenanschlüsse sind im Auslieferungszustand auf eine Geschwindigkeit von 115200 Baud eingestellt. Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

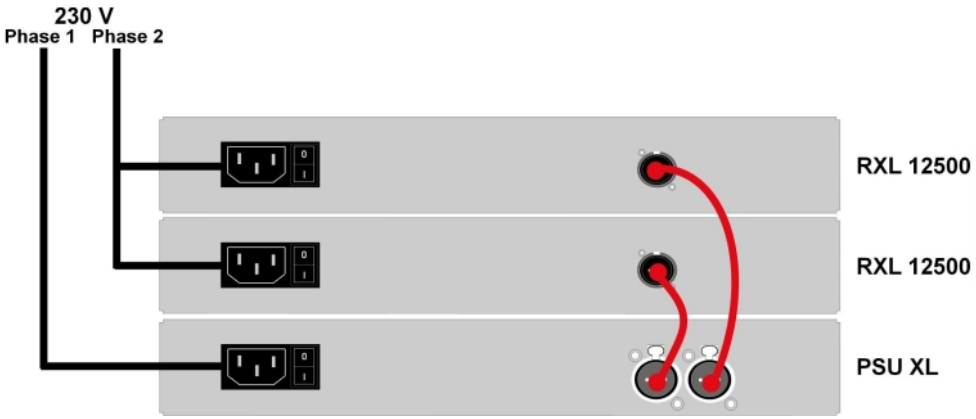
Das Gerät ist nun für die Konfiguration mit dem **GUI** vorbereitet. Im Kapitel *Grundkonfiguration* auf Seite 15 finden Sie ausführliche Schritt-für-Schritt-Anleitungen zu den grundlegenden Funktionen Ihres Geräts.

1.1.1 bintec PSU XL

Warnung

Um einen zuverlässigen Betrieb zu gewährleisten, verwenden Sie nur die mitgelieferten Kabel.

Am **bintec PSU XL** stehen Ihnen zwei XLR-Einbaubuchsen für elektrische Steckverbindungen zur Verfügung.



Siehe auch die Belegung der XLR-Einbaubuchsen *XLR-Einbaubuchse am bintec RXL12x00* auf Seite 13 und*XLR-Einbaubuchsen am bintec PSU XL* auf Seite 14.

1.2 Anschlüsse

Der Netzanschluss, der Ein/Aus-Schalter und die XLR-Buchsen befinden sich auf der Geräterückseite.

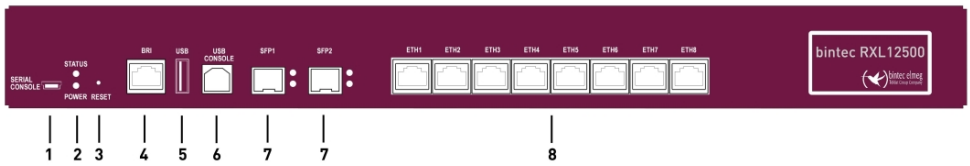
Netzanschluss und die XLR-Buchse (**bintec RXL12x00**)

Netzanschluss und die XLR-Buchsen (**bintec PSU XL**)

Alle anderen Anschlüsse befinden sich auf der Vorderseite des Geräts.

bintec RXL12x00 verfügt über einen 8-Port Ethernet Switch, eine serielle R232-Schnittstelle, einen USB-Konsolenanschluss, eine ISDN-BRI-Schnittstelle sowie zwei SFP LAN-Anschlüsse und einen USB-Anschluss.

Die Anschlüsse sind folgendermaßen angeordnet:



bintec RXL12x00 Vorderseite

1	SERIAL CONSOLE	Serielle Schnittstelle, Mini USB, keine USB-Signale
2	POWER / STATUS	Leuchtanzeige für Power und Statusanzeige
3	RESET	Reset-Taste
4	BRI	ISDN-BRI-Schnittstelle
5	USB	USB-Anschluss Typ A
6	USB CONSOLE	USB-Anschluss Typ B
7	SFP	SFP Slot für 10/100/1000 Mbit/s Ethernet SFP Module
8	ETH1 - ETH8	10/100/1000 Base-T Ethernet-Schnittstelle

1.3 LEDs

Die LEDs geben Aufschluss über Aktivitäten und Zustände des Geräts.

Der **bintec PSU XL** hat auf der Vorderseite zwei Status LEDs, Power 1 und Power 2.

Die LEDs Ihres **bintec RXL12x00** sind folgendermaßen angeordnet:

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
POWER	grün	an	Stromversorgung ist angeschlossen.
		aus	Keine Stromversorgung.
STATUS	grün	an	Nach dem Einschalten: Das Gerät wird gestartet. Während des Betriebs: Es ist ein Fehler aufgetreten.
	grün	blinkend	Das Gerät ist aktiv.
	grün	aus	Während des Betriebs: Es ist ein Fehler aufgetreten.
BRI	orange	an	D-Kanal ist aktiv.
		blinkend	Mindestens 1 B-Kanal ist aktiv.
2 x SFP	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
	grün	blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
	orange	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.
ETH 1 bis 8	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
	grün	blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
	orange	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und	blinkend	Datenverkehr mit 10 Mbit/s.

LED	Farbe	Status	Information
	orange		

Anhand der Status-LED können Sie feststellen, in welchem Zustand sich der Router bei BRRP-Betrieb befindet.

LED	Farbe	Status	Information
STATUS	grün	leuchtet	Das Gerät agiert als Master-Router.
STATUS	grün	aus	Das Gerät agiert als Backup-Router.
STATUS	grün	blinkend	Das Gerät wird initialisiert.

1.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Lieferumfang	bintec RXL12x00	bintec PSU XL
Kabelsätze/Sonstiges	Ethernet-Kabel (rot) ISDN-BRI-Kabel (schwarz) Serielles Kabel (grau) USB Console Kabel (grau) Netzkabel Blindstopfen für SFP 19-Zoll-Montagesatz 4x Gummifuß - selbstklebend	2 x Verbindungskabel Netzkabel
Software	Companion DVD, **Dime Manager** auf DVD	Companion DVD
Dokumentation	Kurzanleitung und Sicherheitshinweise (gedruckt)	Kurzanleitung und Sicherheitshinweise (gedruckt)
Online-Dokumentation	Benutzerhandbuch (auf DVD) Workshops Release Notes, falls erforderlich	-

1.5 Allgemeine Produktmerkmale

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

Allgemeine Produktmerkmale

Eigenschaft	bintec RXL12x00	bintec PSU XL
Maße und Gewicht:		
Gerätemaße ohne Kabel (B x H x T)	19" Gehäuse (482,6 mm x 220 mm x 45 mm, mit Winkeln)	19" Gehäuse (482,6 mm x 220 mm x 45 mm, mit Winkeln)
Gewicht	ca. 2,7 kg	ca. 2,6 kg
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 4 kg	ca. 3 kg
Speicher	1 GB RAM, 128 MB Flash-ROM	-
Flash Card Slot	unterstützt SD-Flash-Karten bis zu 32 GB (SD 2.0)	-
LEDs	24 (1x Power, 1x Status, 1x2 BRI, 8x2 Ethernet, 2x2 SFP-Funktion)	2 x Power (Power 1 und Power 2)
Leistungsaufnahme Gerät	Leerlauf 15 Watt, Last 30 Watt, max. 40 Watt	max. 2x 40 Watt, typ. 2x 15 Watt
Spannungsversorgung	1) Kaltgeräteanschluss Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 % 2) 12V-XLR-Anschluss (männlich) zum Anschluss an **bintec PSU XL**	1) 1 x Kaltgeräteanschluss Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 %
Umweltanforderungen:		
Lagertemperatur	-25 °C bis +70 °C	-25 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C	0 °C bis +40 °C

Eigenschaft	bintec RXL12x00	bintec PSU XL
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:		
Ethernet IEEE 802.3 LAN (8-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	-
ISDN-BRI	Euro-ISDN (Mehrgeräte- und Anlagenanschluss, für In-Haus-Verkabelung) Nur TE-Modus	-
SFP LAN Port	SFP Slot für gängige optische 10/100/1000 Mbit/s Ethernet SFP Module, nicht hotswap-fähig	-
Console/RS232	Baudraten: 1200 - 115200 Baud, Standard: 115200 Baud	-
USB Console (Type B)	Baudraten: 1200 - 115200 Baud, Standard: 115200 Baud	-
USB (Type A)	Buchse zum Anschluss eines UMTS-Sticks.	-
Vorhandene Buchsen:		
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse	-
USB Console	Standard USB-Type-B-Buchse	-
USB	Standard USB-Type-A-Buchse	-
Ethernet-Schnittstellen	RJ45-Buchse	-
ISDN-BRI-Schnittstelle	RJ45-Buchse	-

Eigenschaft	bintec RXL12x00	bintec PSU XL
Spannungsversorgung	1) 1x Kaltgeräteanschluss zur primären Stromversorgung 2) 1 x XLR-Buchse (Eingang) zur redundanten Stromversorgung, 12V DC	1) 1x Kaltgeräteanschluss zur primären Stromversorgung 2) 2 x XLR-Buchse (Ausgang) zur redundanten Stromversorgung, 12V DC
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder

1.6 Reset

Ein Reset des Gerätes ermöglicht es Ihnen, Ihr Gerät wieder in einen definierten Ausgangszustand zu bringen. Dieses kann nötig sein, wenn unerwünschte Konfigurationen zurückgenommen werden sollen oder das Gerät neu programmiert werden soll.

Manueller Reset des Gerätes

Sie können das Gerät mit der **RESET**-Taste in den Auslieferungszustand zurücksetzen. Die **RESET**-Taste führt, je nachdem, wie lange sie gedrückt wird, zwei unterschiedliche Funktionen aus:

- Nach einmaligem kurzem Drücken führt das Gerät einen Neustart durch.
- Halten Sie die **RESET**-Taste so lang gedrückt bis die **STATUS** -LED anfängt zu blinken. Das Gerät führt einen Factory Reset durch. Dies bedeutet, dass das Gerät in den Auslieferungszustand zurückversetzt wird. Die Boot-Konfiguration wird gelöscht und alle Passwörter werden zurückgesetzt.

1.7 Reinigen

Sie können Ihr Gerät problemlos reinigen. Verwenden Sie dazu ein leicht feuchtes Tuch oder ein Antistatiktuch.

Achtung

Benutzen Sie keine Lösungsmittel! Verwenden Sie niemals ein trockenes Tuch; elektrostatische Aufladung könnte zu Defekten in der Elektronik führen. Achten Sie auf jeden Fall darauf, dass keine Feuchtigkeit eindringen kann und Ihr Gerät dadurch Schaden nimmt.

1.8 Support Information

Falls Sie zu Ihrem neuen Produkt Fragen haben, wenden Sie sich für prompte technische Unterstützung bitte an einen zertifizierten Fachhändler in Ihrer Nähe. Fachhändler sind von uns geschult und erhalten bevorzugt Support.

Weitere Informationen zu unseren Support- und Serviceangeboten entnehmen Sie bitte unseren Webseiten unter *www.bintec-elmeg.com*.

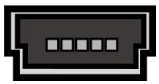
1.9 Pin-Belegungen

1.9.1 Serielle Schnittstelle

Zum Anschluss einer Konsole verfügen die Geräte über eine serielle Schnittstelle. Diese unterstützt Baudraten von 1200 bis 115200 Bit/s.

Die Schnittstelle ist als 5-polige Mini-USB-Buchse ausgeführt.

1 5



Die Pin-Belegung ist wie folgt:

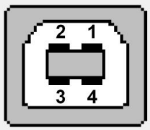
Pin-Belegung der Mini-USB-Buchse

Pin	Funktion
1	Nicht genutzt
2	TxD
3	RxD
4	Nicht genutzt
5	GND

Sie benötigen einen Seriell-USB-Treiber für den Baustein CP210x. Diesen können Sie von *www.bintec-elmeg.com* herunterladen.

1.9.2 USB-Console-Schnittstelle

Zum Anschluss einer Konsole verfügen die Geräte über einen USB-Konsolenanschluss. Dieser unterstützt Baudraten von 1200 bis 115200 Bit/s.



Die Schnittstelle ist als Standard-USB-Type-B-Buchse ausgeführt.

Die Pin-Belegung ist wie folgt:

Pin-Belegung der USB-Type-B-Buchse

Pin	Funktion
1	Vbus
2	D-
3	D+
4	GND
Shell	Shield

Hinweis

Sie benötigen einen Seriell-USB-Treiber für den Baustein CP210x. Diesen können Sie von *www.bintec-elmeg.com* herunterladen.

1.9.3 USB-Schnittstelle

Zum Anschluss eines UMTS-Sticks verfügen die Geräte über einen USB-Anschluss.

Die Schnittstelle ist als Standard-USB-Type-A-Buchse ausgeführt.

Die Pin-Belegung ist wie folgt:

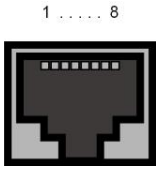
Pin-Belegung der USB-Type-A-Buchse

Pin	Funktion
1	Vbus
2	D-
3	D+
4	GND
Shell	Shield

1.9.4 Ethernet-Schnittstellen

Die Geräte verfügen über eine Ethernet-Schnittstelle mit integriertem 8-Port Switch (ETH1 - ETH8).

Der 8-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 -

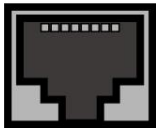
1.9.5 ISDN-BRI-Schnittstelle

Der **bintec RXL12x00** verfügt über eine ISDN-BRI-Schnittstelle, die z. B. zur Fernwartung genutzt werden kann.

Das Gerät können ausschließlich im TE-Modus betrieben werden, die Schnittstelle verfügt nicht über eine 100-Ohm-Terminierung.

Der Anschluss erfolgt über eine RJ45-Buchse:

1 8



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

RJ45-Buchse für ISDN-Anschluss im TE-Modus

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

1.9.6 XLR-Einbaubuchse am bintec RXL12x00

Der **bintec RXL12x00** verfügt über eine XLR-Einbaubuchse (männlich) für eine redundante Stromversorgung.

Die Pin-Belegung der Neutrik-Buchse /Stecker-Kombination ist wie folgt:

Dreipolige XLR-Buchse (männlich)

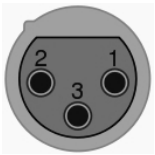
Pin	Funktion
1	+12 V
2	-12 V
3	nicht genutzt

- Eingang zweite/redundante Stromversorgung

- 11,5 V DC 3 A
- Toleranzbereich +/-2 %
- Es dürfen nur die hierfür vorgesehenen bintec elmeg-Stromversorgungsgeräte angeschlossen werden!
- Es dürfen nur die hierfür vorgesehenen Kabel verwendet werden!

1.9.7 XLR-Einbaubuchsen am bintec PSU XL

Der **bintec PSU XL** verfügt über zwei XLR-Einbaubuchsen für elektrische Steckverbindungen.



Die Pin-Belegung der Neutrik-Buchse /Stecker-Kombination ist wie folgt:

Dreipolige XLR-Buchse (weiblich)

Pin	Funktion
1	+12 V
2	-12 V
3	nicht genutzt

- Zwei unabhängige Ausgänge zur redundanten Stromversorgung
- 11,5 V DC 3 A +/-2 %, je 5 A
- Kurzschlußfest
- Es dürfen nur die hierfür vorgesehenen bintec elmeg-Geräte angeschlossen werden!
- Es dürfen nur die hierfür vorgesehenen Kabel verwendet werden!

2 Grundkonfiguration

Die Konfiguration Ihres Geräts wird mit dem **GUI** (Graphical User Interface) durchgeführt.

Der Weg zur Basiskonfiguration wird Ihnen im Folgenden Schritt für Schritt erläutert. Tiefergehende Netzwerkkenntnisse sind dabei nicht erforderlich. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

Die mitgelieferte **Companion DVD** enthält alle Tools, die Sie für Konfiguration und Management Ihres Geräts benötigen.

2.1 Voreinstellungen

2.1.1 Vorkonfigurierte Daten

Ihr Gerät wird mit einer vordefinierten IP-Konfiguration ausgeliefert:

- **IP-Adresse**: *192.168.0.254*
- **Netzmaske**: *255.255.255.0*

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

- **Benutzername**: *admin*
- **Passwort**: *admin*

Hinweis

Alle bintec elmeg-Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert werden. Ändern Sie unbedingt die Passwörter, um unberechtigten Zugriff auf Ihr Gerät zu verhindern!

Die Vorgehensweise bei der Änderung von Passwörtern finden Sie unter *Systempasswort ändern* auf Seite 20.

2.2 System-Voraussetzungen

Ihr bintec elmeg Gateway bietet eine umfangreiche Ausstattung für den verschlüsselten Datentransfer und den Zugang zum Internet für den Unternehmenseinsatz.

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

- Betriebssystem Microsoft Windows ab Windows XP
- Internet Explorer 8 oder 9, Mozilla Firefox ab Version 3.
- Installierte Netzwerkkarte (Ethernet)
- DVD-Laufwerk
- Installiertes TCP/IP-Protokoll (siehe *PC einrichten* auf Seite 18)

2.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration und den Internet-Anschluss bereitlegen
- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.

Darüber hinaus können Sie ...

- die **Dime Manager**-Software installieren, die Ihnen weitere Werkzeuge zur Arbeit mit Ihrem Gerät zur Verfügung stellt. Die Installation ist optional und für die Konfiguration oder den Betrieb des Geräts nicht zwingend erforderlich.

2.3.1 Daten sammeln

Die wesentlichen Daten für die Konfiguration mit dem **GUI** haben Sie schnell gesammelt, denn es sind keine Informationen erforderlich, die vertiefte Netzwerkkenntnisse voraussetzen.

Gegebenenfalls können Sie die Beispielwerte übernehmen.

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

- Grundkonfiguration (sofern sich Ihr Gerät im Auslieferungszustand befindet)
- Internetzugang (optional)

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.

Sollten Sie ein neues Netzwerk einrichten, dann können Sie die angegebenen Beispielwerte für IP-Adressen und Netzmasken übernehmen. Fragen Sie im Zweifelsfall Ihren System-

Administrator.

Grundkonfiguration

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

Basisinformationen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	*192.168.0.254*	
Netzmaske Ihres Gateways	*255.255.255.0*	

Internetzugang über ADSL

Wenn Sie einen Internetzugang einrichten wollen, brauchen Sie einen Internet-Service-Provider (kurz ISP). Von Ihrem ISP bekommen Sie Ihre persönlichen Zugangsdaten mitgeteilt. Die Bezeichnungen der benötigten Zugangsdaten können unter Umständen von ISP zu ISP variieren. Grundsätzlich jedoch handelt es sich um die gleiche Art von Information, die Sie zur Einwahl benötigen.

In der nachfolgenden Tabelle sind die Zugangsdaten zusammengestellt, die Ihr Gerät für eine DSL-Internet-Verbindung benötigt:

Daten für den Internetzugang über ADSL

Zugangsdaten	Beispielwert	Ihre Werte
Provider-Name	*GoInternet*	
Protokoll	*PPP over Ethernet (PPPoE)*	
Ihr Benutzername	*MyName*	
Passwort	*TopSecret*	

Einige ISPs, wie z. B. T-Online, benötigen zusätzlich Informationen:

Zusätzliche Informationen für T-Online

Zugangsdaten	Beispielwert	Ihre Werte
Anschlusskennung (12stellig)	*000123456789*	
T-Online-Nummer (meist 12stellig)	*06112345678*	
Mitbenutzerkennung	*0001*	

Hinweis

Geben Sie bei der Konfiguration eines T-Online-Internetzugangs in das Feld **Benutzername** nacheinander und ohne Leerzeichen folgende Nummern ein:

Anschlusskennung (12-stellig) + T-Online Nummer (meist 12-stellig) + Mitbenutzernummer (für den Hauptnutzer immer 0001)

Sollte Ihre T-Online Nummer weniger als 12 Stellen enthalten, muss zwischen der T-Online Nummer und der Mitbenutzernummer das Zeichen "#" stehen.

Wenn Sie T-DSL nutzen, müssen Sie dieser Zahlenfolge noch die Endung "@t-online.de" hinzufügen.

Ihr Benutzername könnte dann so aussehen:

000123456789061123456 78#0001@t-online.d

Daten für den Internetzugang über UMTS/LTE

Zugangsdaten	Beispielwert	Ihre Werte
UMTS/LTE PIN	*vom Anbieter erhalten*	
Zugriffspunkt (APN)	*UMTS/LTE*	
Benutzername	*MyName*	
Passwort	*TopSecret*	

2.3.2 PC einrichten

Um Ihr Gerät über das Netzwerk erreichen und eine Konfiguration mittels des **GUI** 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.
- Weisen Sie Ihrem PC eine feste IP-Adresse zu.

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.

PC IP-Adresse zuweisen

Weisen Sie Ihrem PC wie folgt eine IP-Adresse zu:

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

(2) Wählen Sie **Folgende IP-Adresse verwenden** und geben Sie eine geeignete IP-Adresse ein.

Gateway IP-Adresse im PC eintragen

Fahren Sie dann fort, indem Sie wie folgt die IP-Adresse des Gateways in die Konfiguration Ihres PCs eintragen:

(1) Geben Sie in **Internetprotokoll (TCP/IP)** -> **Eigenschaften** unter **Standardgateway** die IP-Adresse Ihres Gateways ein.

(2) Tragen Sie unter **Folgende DNS-Serveradressen verwenden** die IP-Adresse Ihres Geräts ein.

(3) Klicken Sie auf **OK**.

(4) Schließen Sie das Statusfenster mit **OK**.

Der Rechner verfügt nun über eine IP-Konfiguration.

Hinweis

Zur Konfiguration können Sie nun das **GUI** aufrufen, indem Sie in einem unterstützten Browser (Internet Explorer ab Version 8, Mozilla Firefox ab Version 3) die IP-Adresse Ihres Gerätes eingeben (192.168.0.254) und sich mit den voreingestellten Anmeldedaten (**User**: `admin`, **Password**: `admin`) anmelden.

2.3.3 Systempasswort ändern

Alle bintec elmeg-Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert werden. Ändern Sie unbedingt die Passwörter, um unberechtigten Zugriff auf Ihr Gerät zu verhindern!

Gehen Sie dazu vor wie folgt:

(a) Gehen Sie in das Menü **Systemverwaltung**->**Globale Einstellungen**->**Passwörter**.

(b) Geben Sie für **Systemadministrator-Passwort** ein neues Passwort ein.

(c) Geben Sie das neue Passwort noch einmal unter **Systemadministrator-Passwort bestätigen** ein.

(d) Klicken Sie auf **OK**.

(e) Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

Beachten Sie folgende Regeln zum Passwortgebrauch:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. sollten deshalb nicht als Passwörter gewählt werden.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).
- Das Passwort sollte mindestens 8 Zeichen lang sein.
- Wechseln Sie regelmäßig das Passwort, z. B. alle 90 Tage.

2.4 Internetverbindung einrichten

Sie können Ihr Gerät über ein externes Modem mit dem Internet verbinden (z. B. ein Kabelmodem) oder hierfür ein externes Gateway verwenden. Bei dieser Art von Konfigurationen unterstützt Sie der entsprechende Assistent des **GUI**. Sie finden den Internet-Assistenten neben weiteren Assistenten zur vereinfachten Konfiguration unterschiedlicher Anwendungen an oberster Stelle des Menübaums unter **Assistenten**.

2.4.1 Internetverbindung über UMTS/LTE

Der Aufbau einer Internetverbindung über UMTS/LTE erfordert eine aktivierte SIM-Karte Ihres UMTS/LTE-Anbieters.

(1) Gehen Sie im **GUI** in das Menü **Assistenten**->**Internetzugang**.

(2) Legen Sie mit **Neu** einen neuen Eintrag an und wählen Sie als **Verbindungstyp** *UMTS/LTE*.

(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 dem Button **Konfiguration speichern** oberhalb der Menünavigation.

2.4.2 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 zum Gerät. Klicken Sie im Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihrer Anlage ein (z. B. *192.168.0.254*). Es erscheint ein Fenster mit dem Hinweis `"Antwort von..."`.

(2) Testen Sie den Internetzugang, indem Sie im Internet Browser *www.bintec-elmeg.com* eingeben. Auf den Internet-Seiten der bintec elmeg GmbH finden Sie Neuigkeiten, Updates und weiterführende Dokumentation.

Hinweis

Durch eine Fehlkonfiguration der Geräte im LAN 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 (Leuchtanzeige ISDN und die Ethernet-Schnittstellen, an denen Sie ein oder mehrere WANs angeschlossen haben).

2.5 Softwareaktualisierung

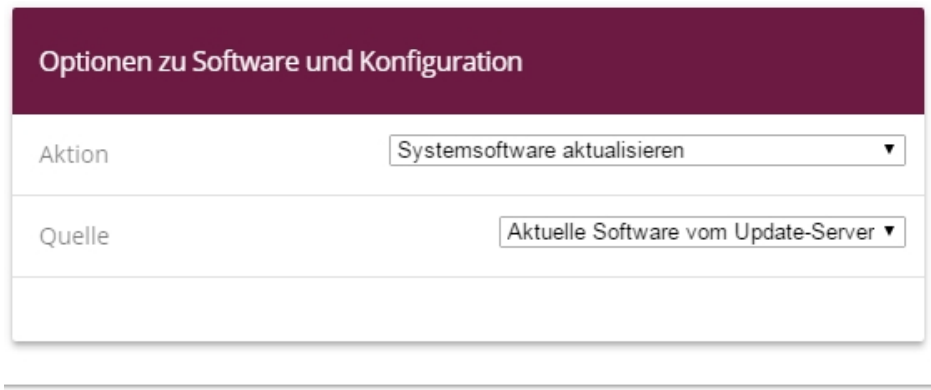
Die Funktionsvielfalt von bintec elmeg-Geräten wird permanent erweitert. Diese Erweiterungen stellt Ihnen bintec elmeg GmbH kostenlos zur Verfügung. Die Überprüfung auf neue Software-Versionen und die Aktualisierung können einfach über das **GUI** vorgenommen werden. Voraussetzung für ein automatisches Update ist eine bestehende Internetverbindung.

Gehen Sie folgendermaßen vor:

(1) Gehen Sie in das Menü **Wartung**->**Software &Konfiguration**.

(2) Wählen Sie unter **Aktion** *Systemsoftware aktualisieren* und unter **Quelle** *Aktuelle Software vom Update-Server*

(3) Bestätigen Sie mit **Los**.



Das Gerät verbindet sich nun mit dem Download-Server der bintec elmeg GmbH und überprüft, ob eine aktualisierte Version der Systemsoftware verfügbar ist. Ist dies der Fall, wird die Aktualisierung Ihres Geräts automatisch vorgenommen. Nach der Installation der neuen Software werden Sie zum Neustart des Geräts aufgefordert.

Achtung

Die Aktualisierung kann nach dem Bestätigen mit **LOS** 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.

3 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

3.1 Zugangsmöglichkeiten

Im Folgenden werden die verschiedenen Zugangsmöglichkeiten vorgestellt. Wählen Sie das für Ihre Bedürfnisse geeignete Vorgehen.

Für den Zugriff auf Ihr Gerät zur Konfiguration gibt es verschiedene Möglichkeiten:

- Über Ihr LAN
- Über die serielle Schnittstelle
- Über eine ISDN-Verbindung

3.1.1 Zugang über LAN

Der Zugang über eine der Ethernet-Schnittstellen Ihres Geräts ermöglicht es Ihnen, zur Konfiguration das **GUI** in einem Web-Browser zu öffnen und über Telnet oder SSH auf Ihr Gerät zuzugreifen.

Achtung

Falls Sie die initiale Konfiguration mit dem **GUI** vornehmen, kann es zu Inkonsistenzen oder Fehlfunktionen führen, sobald Sie weitere Einstellungen über andere Konfigurationsmöglichkeiten vornehmen. Daher wird empfohlen, die Konfiguration mit dem **GUI** fortzuführen. Sollten Sie SNMP-Shell-Kommandos verwenden, behalten Sie auch diese Konfigurationsmethode bei.

3.1.1.1 HTTP/HTTPS

Mit einem aktuellen Web-Browser können Sie die HTML-Oberflächen zur Konfiguration Ihres Geräts verwenden. Geben Sie dazu Folgendes in das Adressfeld Ihres Web-Browsers ein:

- *http://192.168.0.254*

  oder

- *https://192.168.0.254*

3.1.1.2 Telnet

Abgesehen von der Konfiguration über einen Web-Browser können Sie mit einer Telnet-Verbindung auf die SNMP-Shell zugreifen und weitere Konfigurationsmöglichkeiten nutzen.

Um eine Telnet-Verbindung zu Ihrem Gerät aufzubauen, benötigen Sie keine zusätzliche Software auf Ihrem PC: Telnet steht auf allen Betriebssystemen zur Verfügung.

Gehen Sie folgendermaßen vor:

Windows

(1) Klicken Sie im Windows-Startmenü auf **Ausführen...**.

(2) Geben Sie `telnet <IP-Adresse Ihres Geräts>` ein.

(3) Klicken Sie auf **OK**.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.

(4) Fahren Sie fort mit *Anmelden zur Konfiguration* auf Seite 30.

Unix

Auch unter UNIX und Linux können Sie ohne weiteres eine Telnet-Verbindung herstellen:

(1) Geben Sie `telnet <IP-Adresse Ihres Geräts>` in ein Terminal ein.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.

(2) Fahren Sie fort mit *Anmelden zur Konfiguration* auf Seite 30.

3.1.1.3 SSH

Zusätzlich zur unverschlüsselten und potentiell einsehbaren Telnet-Session können Sie sich auch über eine SSH-Verbindung mit Ihrem Gerät verbinden. Diese ist verschlüsselt und ermöglicht es, alle Optionen der Fernwartung sicher auszuführen.

Um sich über SSH mit dem Gerät zu verbinden, müssen folgende Voraussetzungen erfüllt sein:

- Auf dem Gerät müssen für den Vorgang benötigte Verschlüsselungsschlüssel vorhanden sein.
- Auf Ihrem PC muss ein SSH Client installiert sein.

Schlüssel zur Verschlüsselung

Stellen Sie zunächst sicher, dass die Schlüssel zur Verschlüsselung der Verbindung auf Ihrem Gerät vorhanden sind:

(1) Loggen Sie sich auf eine der bereits verfügbaren Arten auf Ihrem Gerät ein (z. B. über Telnet - zum Login siehe *Anmelden* auf Seite 29).

(2) Am Eingabe-Prompt geben Sie `update -i` ein. Sie befinden sich auf der Flash Management Shell.

(3) Rufen Sie eine Liste aller auf dem Gerät gespeicherten Dateien auf: `ls -al`.

Wenn Sie eine Anzeige wie die Folgende sehen, sind die notwendigen Schlüssel bereits vorhanden, und Sie können sich über SSH mit dem Gerät verbinden:

```
Flash-Sh > ls -al

Flags Version Length Date Name ...

Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860

Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub

Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key

Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub

Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```

Hinweis

Das Gerät erstellt für jeden der sog. Algorithmen (RSA und DSA) ein Schlüsselpaar, d. h. es müssen je Algorithmus zwei Dateien im Flash gespeichert sein (siehe Abbildung oben).

Sollten keine Schlüssel vorhanden sein, müssen Sie diese zunächst erstellen. Gehen Sie folgendermaßen vor:

(1) Verlassen Sie die Flash Management Shell mit `exit`.

(2) Rufen Sie das **GUI** auf und melden Sie sich an Ihrem Gerät an (siehe *Das GUI aufrufen* auf Seite 32.

(3) Stellen Sie sicher, dass als Sprache *Deutsch* gewählt ist.

(4) Kontrollieren Sie den Schlüsselstatus im Menü **Systemverwaltung**->**Administrativer Zugriff**->**SSH**. Wenn beide Schlüssel verfügbar sind, sehen Sie in den beiden Feldern **RSA-Schlüsselstatus** und **DSA-Schlüsselstatus** den Wert *Generiert*.

(5) Wenn Sie in einem der beiden Felder oder in beiden Feldern den Wert *Nicht generiert* sehen, so müssen Sie den entsprechenden Schlüssel erzeugen lassen. Um die Schlüssel vom Gerät erzeugen zu lassen, klicken Sie auf **Generieren**.
Das Gerät erzeugt den entsprechenden Schlüssel und speichert ihn im FlashROM.

Generiert zeigt die erfolgreiche Generierung an.

(6) Stellen Sie sicher, dass beide Schlüssel erfolgreich erzeugt worden sind. Wiederholen Sie dazu gegebenenfalls die oben beschriebene Prozedur.

Login über SSH

Um sich auf dem Gerät über SSH einzuloggen, gehen Sie folgendermaßen vor:

Wenn Sie sichergestellt haben, dass alle benötigten Schlüssel auf dem Gerät vorhanden sind, sollten Sie feststellen, ob ein SSH Client auf Ihrem PC installiert ist. Die meisten UNIX- und Linux-Distributionen installieren standardmäßig einen SSH Client, auf einem Windows PC muss in der Regel zusätzliche Software installiert werden, z. B. PuTTY.

Um sich über SSH auf Ihrem Gerät einzuloggen, gehen Sie folgendermaßen vor:

UNIX

(1) Geben Sie `ssh <IP-Adresse des Geräts>` in einem Terminal ein.
Das Login-Prompt-Fenster wird angezeigt, sie befinden sich auf der SNMP Shell des Geräts.

(2) Fahren Sie mit *Anmelden* auf Seite 29 fort.

Windows

(1) Wie eine SSH-Verbindung aufgebaut wird, hängt stark von der verwendeten Software ab. Beachten Sie die Dokumentation des von Ihnen verwendeten Programms.
Sobald Sie sich mit dem Gerät verbunden haben, wird das Login-Prompt-Fenster angezeigt. Sie befinden sich auf der SNMP Shell des Geräts.

(2) Fahren Sie mit *Anmelden* auf Seite 29 fort.

Hinweis

PuTTY benötigt für eine Verbindung mit einem bintec elmeg-Gerät ggf. bestimmte Einstellungen. Auf den Support-Seiten von *http://www.bintec-elmeg.com* finden Sie eine FAQ, welche die notwendigen Einstellungen ausführt.

3.1.2 Zugang über die serielle Schnittstelle

Jedes bintec elmeg-Gateway verfügt über eine serielle Schnittstelle, mit der eine direkte Verbindung von einem PC aus möglich ist. Das folgende Kapitel beschreibt, was beim Aufbau einer seriellen Verbindung zu beachten ist und wie Sie vorgehen können, um Ihr Gerät auf diesem Weg zu konfigurieren.

Der Zugang über die serielle Schnittstelle ist gut geeignet, wenn Sie bei Ihrem Gerät eine

Erstkonfiguration durchführen und ein LAN-Zugang über die vorkonfigurierte IP-Adresse (192.168.0.254/255.255.255.0) nicht möglich ist.

Windows

Wenn Sie einen Windows-PC benutzen, benötigen Sie für die serielle Verbindung ein Terminal-Programm, z. B. HyperTerminal. Stellen Sie sicher, dass HyperTerminal bei der Windows-Installation auf dem PC mitinstalliert wurde. Sie können allerdings auch ein beliebiges anderes Terminal-Programm verwenden, das sich auf die entsprechenden Parameter (siehe unten) einstellen lässt.

Gehen Sie folgendermaßen vor, um über die serielle Schnittstelle auf Ihr Gerät zuzugreifen:

(1) Klicken Sie im Windows-Startmenü auf **Programme** -> **Zubehör** -> **Kommunikation** -> **HyperTerminal** -> **Gerät an COM1** (bzw. **Gerät an COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um HyperTerminal zu starten.

(2) Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das HyperTerminal-Fenster geöffnet hat.

Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts. Sie können sich nun auf Ihrem Gerät einloggen und mit der Konfiguration beginnen.

Überprüfen

Falls der Login-Prompt auch nach mehrmaligem Betätigen der **Eingabetaste** nicht erscheint, konnte die Verbindung zu Ihrem Gerät nicht hergestellt werden.

Überprüfen Sie daher die Einstellungen von COM1 bzw. COM2 Ihres Rechners:

(1) Klicken Sie auf **Datei** -> **Eigenschaften**.

(2) Klicken Sie im Register **Verbinden mit** auf **Konfigurieren**
Folgende Einstellungen sind erforderlich:
- Bits pro Sekunde: *9600*
- Datenbits: *8*
- Parität: *Keiner*
- Stopbits: *1*
- Flusssteuerung: *Keiner*

(3) Tragen Sie die Werte ein und klicken Sie auf **OK**.

(4) Stellen Sie im Register **Einstellungen** ein:
- Emulation: *VT100*

(5) Klicken Sie auf **OK**.

Damit Änderungen an den Terminal-Programmeinstellungen wirksam werden, müssen Sie die Verbindung zu Ihrem Gerät trennen und wieder neu herstellen.

Wenn Sie HyperTerminal verwenden, kann es zu Problemen mit der Darstellung von Umlauten und anderen Sonderzeichen kommen. Stellen Sie daher HyperTerminal ggf. auf *Automatische Erkennung* anstatt auf *VT 100*.

Unix

Sie benötigen ein Terminal-Programm wie z. B. `cu` (unter System V), `tip` (unter BSD) oder `minicom` (unter Linux). Die Einstellungen für diese Programme entsprechen den oben aufgelisteten.

Beispiel für eine Befehlszeile, um `cu` zu nutzen: `cu -s 9600 -c/dev/ttyS1`

Beispiel für eine Befehlszeile, um `tip` zu nutzen: `tip -9600 /dev/ttyS1`

3.1.3 Zugang über ISDN

Alle Geräte, die über eine ISDN-Schnittstelle verfügen, können von einem anderen Gerät aus mittels eines ISDN-Rufs erreicht und konfiguriert werden.

Der Zugang über ISDN mit ISDN-Login empfiehlt sich vor allem dann, wenn Ihr Gerät aus der Ferne konfiguriert oder gewartet werden soll. Dies ist auch dann möglich, wenn Ihr Gerät sich noch im Auslieferungszustand befindet. Der Zugang erfolgt dann mit Hilfe eines bereits konfigurierten Geräts oder eines Rechners mit ISDN-Karte im Remote-LAN. Das zu konfigurierende Gerät im eigenen LAN wird über eine Rufnummer des ISDN-Anschlusses (z. B. 1234) erreicht. So kann z. B. der Administrator im Remote-LAN Ihr Gerät konfigurieren, ohne vor Ort zu sein.

Hinweis

Wenn Sie ein unkonfiguriertes Gerät parallel zu einer Telefonanlage an einen ISDN-Anschluss anschließen, kann die Telefonanlage solange keine Rufe annehmen, bis auf dem Gerät eine ISDN-Nummer konfiguriert ist.

Der Zugang über ISDN verursacht Kosten. Wenn Ihr Gerät und Ihr Rechner im gleichen LAN sind, ist es günstiger, auf Ihr Gerät über das LAN oder über die serielle Schnittstelle zuzugreifen.

Ihr Gerät in Ihrem LAN muss lediglich mit dem ISDN-Anschluss verbunden und eingeschaltet sein.

Gehen Sie folgendermaßen vor, um Ihr Gerät über ISDN-Login zu erreichen:

(1) Schließen Sie Ihr Gerät an das ISDN an.

(2) Loggen Sie sich wie gewohnt als Administrator auf dem Gerät im Remote-LAN ein.

(3) Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer des ISDN-Anschlusses Ihres Geräts>` ein, z. B. `isdnlogin 1234`.

(4) Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.

Fahren Sie fort mit *Anmelden zur Konfiguration* auf Seite 30.

3.2 Anmelden

Mittels bestimmer Zugangsdaten können Sie sich auf Ihrem Gerät anmelden und unterschiedliche Aktionen ausführen. Dabei hängt der Umfang der verfügbaren Aktionen von den Berechtigungen des entsprechenden Benutzers ab.

Unabhängig davon, über welchen Weg Sie auf Ihr Gerät zugreifen, erscheint zunächst ein Login-Prompt. Ohne Authentifizierung können Sie auf dem Gerät keinerlei Informationen einsehen und die Konfiguration nicht ändern.

3.2.1 Benutzernamen und Passwörter im Auslieferungszustand

Im Auslieferungszustand ist Ihr Gerät mit folgenden Benutzernamen und Passwörtern versehen:

Benutzernamen und Passwörter im Auslieferungszustand

Benutzername	Passwort	Befugnisse
`admin`	`admin`	Systemvariablen lesen und ändern, Konfigurationen speichern; **GUI** benutzen.
`write`	`public`	Systemvariablen (außer Passwörter) lesen und schreiben (Änderungen gehen bei Ausschalten Ihres Geräts verloren).
`read`	`public`	Systemvariablen (außer Passwörter) lesen.

Um Konfigurationsänderungen vorzunehmen und zu speichern, müssen Sie sich mit dem Benutzernamen `admin` einloggen. Auch die Zugangsdaten (Benutzernamen und Passwörter) können geändert werden, wenn sich der Benutzer mit dem Benutzernamen `admin` eingloggt. Aus Sicherheitsgründen sind Passwörter nicht im Klartext, sondern nur als Sternchen am Bildschirm sichtbar. Die Benutzernamen erscheinen hingegen im Klartext.

Ein Sicherheitskonzept Ihres Geräts besteht darin, dass Sie mit dem Benutzernamen `read` alle anderen Konfigurationseinstellungen lesen können, nicht aber die Zugangsdaten. Es

ist also nicht möglich, sich mit `read` einzuloggen, das Passwort des Benutzers `admin` auszulesen und sich dann anschließend mit `admin` einzuloggen, um Konfigurationsänderungen vorzunehmen.

Achtung

Alle bintec elmeg-Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert werden. Die Vorgehensweise bei der Änderung von Passwörtern ist unter *Passwörter* auf Seite 48 beschrieben.

Ändern Sie unbedingt die Passwörter, um unberechtigten Zugriff auf Ihr Gerät zu verhindern!

Haben Sie Ihr Passwort vergessen, dann müssen Sie Ihr Gerät in den Auslieferungszustand zurückversetzen und Ihre Konfiguration geht verloren!

3.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 23 beschrieben.

GUI(Graphical User Interface)

So loggen Sie sich über die HTML-Oberfläche ein:

(1) Geben Sie Ihren Benutzernamen in das Feld **User** des Eingabefensters ein.

(2) Geben Sie Ihr Passwort in das Feld **Password** des Eingabefensters ein und bestätigen Sie mit der **Eingabetaste** oder klicken Sie auf die **Login** Schaltfläche.

Im Browser öffnet sich die Status-Seite des **GUI**.

SNMP-Shell

So loggen Sie sich auf der SNMP-Shell ein:

(1) Geben Sie Ihren Benutzernamen ein, z. B. `admin`, und bestätigen Sie mit der **Eingabetaste**.

(2) Geben Sie Ihr Passwort ein, z. B. `admin`, und bestätigen Sie mit der **Eingabetaste**.

Ihr Gerät meldet sich mit dem Eingabeprompt, z. B. `RXL12500:>`. Das Einloggen war erfolgreich. Sie befinden sich auf der SNMP-Shell.

Um die SNMP-Shell nach Beenden der Konfiguration zu verlassen, geben Sie `exit` ein und bestätigen mit der **Eingabetaste**.

3.3 Konfigurationsmöglichkeiten

Dieses Kapitel bietet zunächst eine Übersicht über die verschiedenen Tools, die Sie zur Konfiguration Ihres Geräts verwenden können.

Sie haben folgende Möglichkeiten, Ihr Gerät zu konfigurieren:

- **GUI**
- Assistent
- SNMP-Shell-Kommandos

Hinweis

Das ausführliche Hilfesystem des Assistenten hilft Ihnen, offene Fragen zu klären. Deshalb wird auf den Assistenten in diesem Dokument nicht näher eingegangen.

Welche Konfigurationsmöglichkeiten Ihnen zur Verfügung stehen, hängt von der Art der Verbindung zu Ihrem Gerät ab:

Verbindungs- und Konfigurationsarten

Verbindungsart	Mögliche Konfigurationsarten
LAN	Assistent, **GUI**, Shell-Kommandos
Serielle Verbindung	Shell-Kommandos

Im Folgenden wird die Konfiguration anhand des **GUI** beschrieben.

Hinweis

Um die Konfiguration des Geräts zu ändern, müssen Sie sich mit dem Benutzernamen `admin` einloggen! Wenn Sie das entsprechende Passwort nicht kennen, können Sie keine Konfiguration vornehmen. Dies gilt für alle Konfigurationsarten.

3.3.1 GUI (Graphical User Interface)

Das **GUI** ist eine web-basierte grafische Benutzeroberfläche, die Sie von jedem PC aus mit einem aktuellen Web-Browser über eine HTTP- oder HTTPS-Verbindung bedienen können.

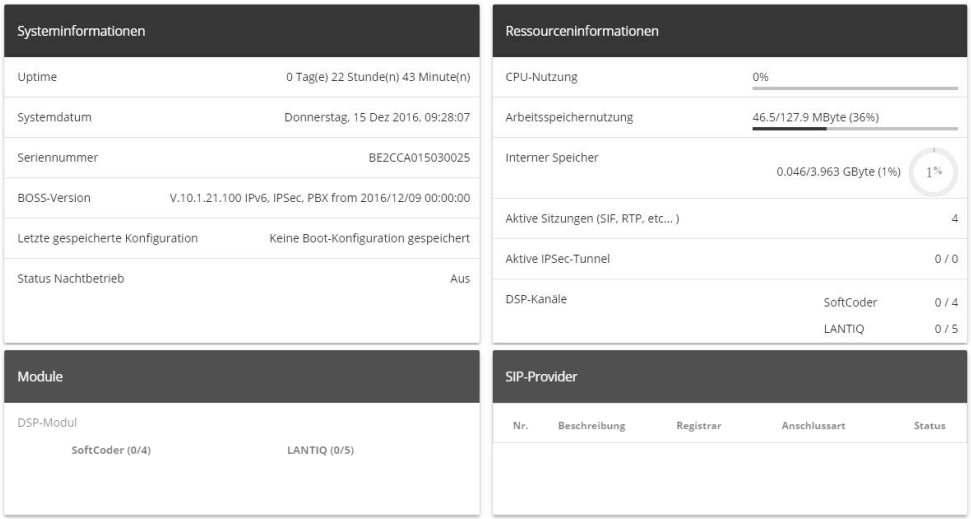
Mit dem **GUI** können Sie alle Konfigurationsaufgaben einfach und komfortabel durchführen.

Es ist in Ihr Gerät integriert und steht in Englisch zur Verfügung. Weitere Sprachen können, falls erwünscht, im Download-Bereich *Software &Konfiguration* auf Seite 461 auf *www.bintec-elmeg.com* heruntergeladen und auf dem Gerät installiert werden. Gehen Sie hierzu vor wie in *Optionen* auf Seite 461 beschrieben.

Die Einstellungsänderungen, die Sie mit dem **GUI** vornehmen, werden mit der **OK** bzw. **Übernehmen**-Schaltfläche des jeweiligen Menüs übernommen, ohne dass das Gerät neu gestartet werden muss.

Wenn Sie die Konfiguration abschließen und so speichern möchten, dass sie beim nächsten Neustart des Geräts als Boot-Konfiguration geladen wird, speichern Sie diese, indem Sie auf die Schaltfläche **Konfiguration speichern** klicken.

Mit dem **GUI** können Sie ebenfalls die wichtigsten Funktionsparameter Ihres Geräts überwachen.



Konfigurationsoberfläche Startseite

3.3.1.1 Das GUI aufrufen

(1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe *Aufstellen und Anschließen* auf Seite 1).

(2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe *PC einrichten* auf Seite 18).

(3) Öffnen Sie einen Webbrowser.

(4) Geben Sie `http://192.168.0.254` in das Adressfeld des Webbrowsers ein.

(5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein und klicken Sie auf **LOGIN**.

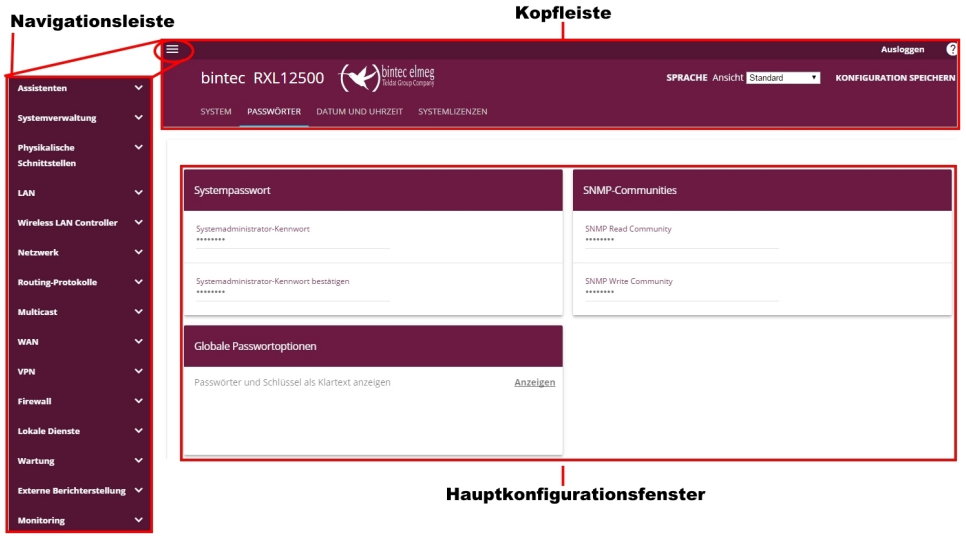
Sie befinden sich nun im Statusmenü des **GUI** Ihres Geräts (siehe *Status* auf Seite 43).

3.3.1.2 Bedienelemente

GUI Fenster

Das **GUI** Fenster ist in drei Bereiche geteilt:

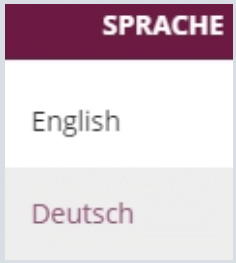
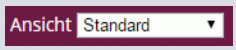
- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster



Kopfleiste

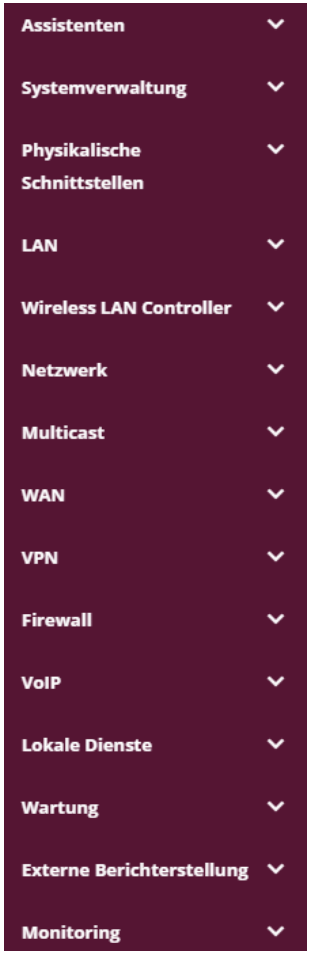
Konfigurationsoberfläche Kopfleiste

Menü	Funktion
	Öffnet die Navigationsleiste, über die Sie Zugriff auf die Menüs zur Konfiguration haben.
	**Ausloggen**: Wenn Sie die Konfiguration beenden möchten, klicken Sie auf diese Schaltfläche, um sich von Ihrem Gerät abzumelden. Es wird ein Fenster geöffnet, in dem Ihnen folgende

Menü	Funktion
	Optionen angeboten werden: • Konfiguration speichern, vorherige Konfiguration sichern, dann verlassen: Ihre Änderungen werden gespeichert, aber die zuvor aktive Konfiguration wird so gesichert, so dass Sie ggf. später wieder darauf zurückgreifen können. Erst dann erfolgt die Abmeldung vom Gerät. • Konfiguration speichern, dann verlassen: Ihre Änderungen werden gespeichert. Dabei wird die zuvor aktive Konfiguration ersetzt. Erst dann erfolgt die Abmeldung vom Gerät. • Ohne zu speichern verlassen: Ihre Änderungen sind zwar aktiv, werden aber nicht gespeichert. Nach einem Neustart sind wieder die zuvor gültigen Einstellungen aktiv.
	**Online-Hilfe**: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Eine Beschreibung des Untermenüs mit den wichtigsten Informationen zu den verfügbaren Optionen wird angezeigt.
	**Sprache**: Wählen Sie in dem Aufklappmenü die gewünschte Sprache aus, in der die Konfigurationsoberfläche angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen *Deutsch* und *English*. Der Standardwert ist *Deutsch*.
	**Ansicht**: Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl steht Standard und SNMP-Browser.
	Die Schaltfäche **Konfiguration speichern**. Wenn Sie Änderungen an der Konfiguration vorgenommen haben, können Sie diese auf zwei Arten speichern: • Konfiguration speichern - Ihre Änderungen werden in die aktuelle Startkonfiguration (die Konfiguration, mit der Ihr Gerät nach jedem Start aktiv wird) übernommen und gespeichert. Die zuvor aktive Konfiguration wird dabei ersetzt. • Konfiguration speichern und vorhergehende Boot-Konfiguration sichern: Ihre Änderungen werden wie oben gespeichert, aber die zuvor aktive Konfiguration wird so gesi-

Menü	Funktion
	chert, so dass Sie ggf. später wieder darauf zurückgreifen können. Es kann immer nur eine Sicherungsdatei erzeugt werden.

Navigationsleiste



Die Navigationsleiste enthält die Hauptkonfigurationsmenüs und deren Untermenüs. Klicken Sie auf das gewünschte Hauptmenü. Es öffnet sich das jeweilige Untermenü. Wenn Sie auf das gewünschte Untermenü gehen, wird der gewählte Eintrag farbig unterlegt angezeigt. Nach der Wahl des Untermenüs wird die Navigationsleiste geschlossen.

Hauptkonfigurationsfenster

Die Untermenüs enthalten im Allgemeinen mehrere Registerkarten. Diese werden über die

im Hauptfenster oben stehenden Reiter aufgerufen. Durch Klicken auf einen Reiter öffnet sich das Fenster mit den Basis-Parametern, welches durch Klicken auf die Schaltfläche **Erweiterte Einstellungen** erweiterbar ist und dann Zusatzoptionen anzeigt.

Konfigurationselemente

Die verschiedenen Aktionen, die Sie bei der Konfiguration Ihres Geräts in der Konfigurationsoberfläche ausführen können, werden mithilfe folgender Schaltflächen ausgelöst:

Schaltflächen

Schaltfläche	Funktion
	Aktualisiert die Ansicht.
	Wenn Sie einen neu konfigurierten Listeneintrag nicht sichern wollen, machen Sie diesen und die evtl. getätigten Einstellungen durch **Abbrechen** rückgängig.
	Bestätigt die Einstellungen eines neuen Eintrags und die Parameteränderungen in einer Liste.
	Startet die konfigurierte Aktion sofort.
	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.
	Fügt einen Eintrag zu einer internen Liste hinzu.

Schaltflächen für spezielle Funktionen

Schaltfläche	Funktion
	Im Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** und im Menü **Systemverwaltung**->**Zertifikate**->**CRLs** werden mit dieser Schaltfläche die Untermenüs für die Konfiguration des Zertifikate- bzw. CRL-Imports aufgerufen.
	Im Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** wird mit dieser Schaltfläche das Untermenü für die Konfiguration der Zertifikatsanforderung aufgerufen.
	Im Menü **Monitoring**->**ISDN/Modem**->**Aktuelle Anrufe** werden durch Drücken dieser Schaltfläche die in der Spalte  ausgewählten aktiven Rufe beendet.

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

Symbole

Symbol	Funktion
	Löscht den entsprechenden Listeneintrag.
	Zeigt das Menü zur Änderung der Einstellungen eines Eintrags an.
	Zeigt die Details eines Eintrags an.
	Voice-Mail-Nachricht kann abgehört werden.
	Nachrichten werden gespeichert.
	Mit diesem Symbol gelangen Sie auf die Benutzeroberfläche eines **elmeg** IP1x0-Telefons.
	Verschiebt einen Eintrag. Es öffnet sich eine Combobox, in der Sie auswählen können, vor / hinter welchen Listeneintrag der ausgewählte Eintrag verschoben werden soll.
	Legt einen weiteren Listeneintrag vorher an und öffnet das Konfigurationsmenü.
	Setzt den Status des Eintrags auf `Inaktiv`.
	Setzt den Status des Eintrags auf `Aktiv`.
	Kennzeichnet den Status "Ruhend" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Aktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Inaktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Blockiert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-Bandscan aus.
	Zeigt die nächste Seite einer Liste an.

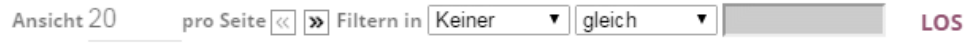
Symbol	Funktion
«	Zeigt die vorherige Seite einer Liste an.

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

Listenoptionen

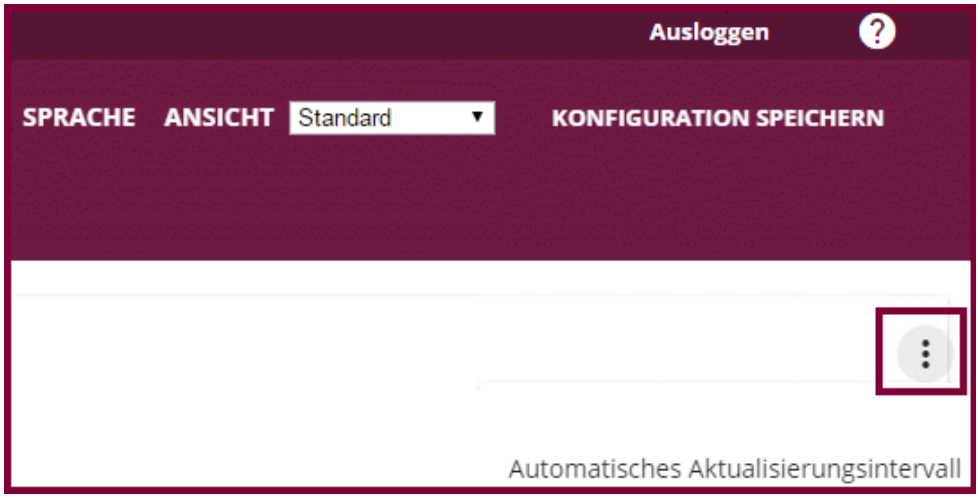
Menü	Funktion
Aktualisierungsintervall	Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll. Geben Sie dazu einen Zeitraum in Sekunden in das Eingabefeld ein und bestätigen Sie mit ÜBERNEHMEN.
Filter	Sie haben die Möglichkeit, die Einträge einer Liste nach bestimmten Kriterien filtern und entsprechend anzeigen zu lassen. Sie können die Anzahl der pro Seite angezeigten Einträge bestimmen, indem Sie in **Ansicht** x **pro Seite** die gewünschte Zahl eingeben. Mit den Tasten « und » blättern Sie eine Seite vor bzw. eine Seite zurück. Sie können nach bestimmten Stichwörtern innerhalb der Konfigurationsparameter filtern, indem Sie bei **Filtern in x <Option> y** die gewünschte Filterregel auswählen und das Suchwort in das Eingabefeld eingeben. LOS startet den Filtervorgang.
Konfigurationselemente	Einige Listen enthalten Konfigurationselemente. So können Sie direkt in der Liste die Konfiguration des entsprechenden Listeneintrags ändern.

Konfiguration des Aktualisierungsintervalls



Liste filtern

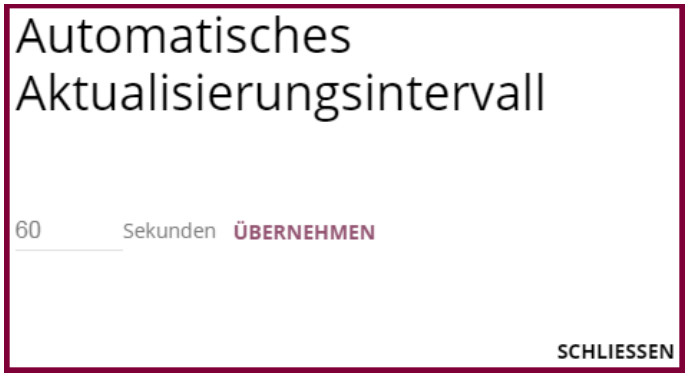
Auf der **Statusseite** können Sie über den Button ⋮ die Option **Automatisches Aktualisierungsintervall** öffnen.



Automatische Aktualisierungsintervall öffnen

Klicken Sie auf **Automatisches Aktualisierungsintervall**.

Geben Sie die Zeit in Sekunden ein und klicken Sie auf ÜBERNEHMEN.



Konfiguration des Aktualisierungsintervalls

Struktur der Konfigurationsmenüs

Die Menüs enthalten folgende Grundstrukturen:

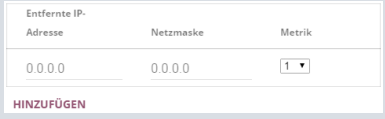
Menüstruktur

Menü	Funktion
Basis-Konfigurationsmenü / Liste	Bei Auswahl eines Menüs der Navigationsleiste wird zunächst das Menü mit den Basisparametern angezeigt. Bei einem Untermenü mit mehreren Seiten wird jeweils das Menü mit den Basisparametern der ersten Seite angezeigt.

Menü	Funktion
	Das Menü enthält entweder eine Liste aller konfigurierten Einträge oder die Grundeinstellungen für die jeweilige Funktion.
Untermenü 	Die Schaltfläche **Neu** ist in jedem Menü vorhanden, in dem eine Liste aller konfigurierten Einträgen angezeigt wird. Klicken Sie diese Schaltfläche, um das Konfigurationsmenü für das Anlegen eines neuen Listeneintrags aufzurufen.
Untermenü 	Klicken Sie auf diese Schaltfläche, um den bestehenden Listeneintrag zu bearbeiten. Sie gelangen in das Konfigurationsmenü.
Menü 	Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.

Für die Konfiguration stehen folgende Optionen zur Verfügung:

Konfigurationselemente

Menü	Funktion
Eingabefelder	z. B. leeres Textfeld  Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.
Radiobuttons	z. B.  Wählen Sie die entsprechende Option aus.
Checkbox	z. B. Aktivieren durch Auswahl der Checkbox 
Dropdown-Menüs	z. B.  Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.
Interne Listen	z. B.  Klicken Sie auf die Schaltfläche HINZUFÜGEN. Ein neuer Listen-

Menü	Funktion
	eintrag wird angelegt. Geben Sie die entsprechenden Daten ein. Bleiben die Felder des Listeneintrags leer, wird dieser bei Bestätigen mit **OK** nicht gespeichert. Löschen Sie Einträge, indem Sie auf das -Symbol klicken.

Darstellung von Optionen, die nicht zur Verfügung stehen

Optionen, die abhängig von der Wahl anderer Einstelloptionen nicht zur Verfügung stehen, sind grundsätzlich ausgeblendet. Falls die Nennung solcher Optionen bei der Konfigurationsentscheidung behilflich sein könnte, werden sie stattdessen grau dargestellt und sind nicht auswählbar.

Wichtig

Bitte beachten Sie die eingeblendeten Hinweise in den Untermenüs! Diese geben Auskunft über eventuelle Fehlkonfigurationen.

3.3.1.3 Menüs

Die Konfigurationsoptionen Ihres Geräts sind in die Untermenüs gruppiert, die in der Navigationsleiste im linken Fensterbereich angezeigt werden.

Hinweis

Beachten Sie, dass nicht alle Geräte über den maximal möglichen Funktionsumfang verfügen. Prüfen Sie die Software-Ausstattung Ihres Geräts auf der jeweiligen Produktseite unter *www.bintec-elmeg.com* .

3.3.2 SNMP Shell

SNMP (Simple Network Management) ist ein Protokoll, über das definiert wird, wie Sie auf die Konfigurationseinstellungen zugreifen können.

Alle Konfigurationseinstellungen sind in der sog. MIB (Management Information Base) in Form von MIB-Tabellen und MIB-Variablen hinterlegt. Auf diese können Sie mittels SNMP-Kommandos direkt von der SNMP-Shell zugreifen. Diese Art der Konfiguration erfordert ein vertieftes Verständnis unserer Geräte.

4 Assistenten

Das Menü **Assistenten** bietet Schritt-für-Schritt-Anleitungen für folgende Grundkonfigurationsaufgaben:

- **Erste Schritte**
- **Internetzugang**
- **VPN**
- **VoIP PBX im LAN**

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

5 Systemverwaltung

Das Menü **Systemverwaltung** enthält allgemeine System-Informationen 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.

5.1 Status

Wenn Sie sich in das **GUI** einloggen, erscheint die Status-Seite Ihres Geräts, auf der die wichtigsten System-Informationen angezeigt werden.

Sie erhalten einen Überblick über folgende Daten:

- System-Status
- Aktivitäten Ihres Geräts: Ressourcenauslastung, aktive Sessions und Tunnel
- Status und die Grundkonfiguration der LAN-, WAN-, ISDN- und ADSL-Schnittstellen
- Informationen über gegebenenfalls gesteckte Zusatzmodule

Sie können das Aktualisierungsintervall der Status-Seite individuell anpassen, indem Sie für **Automatisches Aktualisierungsintervall** den gewünschten Zeitraum in Sekunden angeben und auf die **Übernehmen**-Schaltfläche klicken.

Achtung

Geben Sie für **Automatisches Aktualisierungsintervall** keinen Wert unter *5* Sekunden ein, da sich der Bildschirm dann in zu kurzen Intervallen aktualisiert, um weitere Änderungen vornehmen zu können!

Das Menü **Systemverwaltung**->**Status** besteht aus folgenden Feldern:

Felder im Menü Systeminformationen

Feld	Wert
Uptime	Zeigt die Zeit an, die vergangen ist, seit das Gerät neu gestartet wurde.
Systemdatum	Zeigt das aktuelle Systemdatum und die Systemuhrzeit an.
Seriennummer	Zeigt die Geräte-Seriennummer an.

Feld	Wert
BOSS-Version	Zeigt die aktuell geladene Version der Systemsoftware an.
Back-up der Konfiguration auf SD Karte	Nur bei gesteckter SD-Karte sichtbar. Zeigt an, ob ein Back-up der Konfiguration auf der SD-Karte verfügbar ist oder nicht.
Letzte gespeicherte Konfiguration	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.

Felder im Menü Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtarbeitsspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
Speicherkarte	Zeigt den Status einer gegebenenfalls gesteckten optionalen externen Speicherkarte und die Speichergröße in GByte oder MByte an.
ISDN Verwendung Extern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl der zur Verfügung stehenden B-Kanäle für ausgehende Verbindungen an.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF-, TDRC- und IP-Lastverteilung-Sessions an.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü Physikalische Schnittstellen

Feld	Wert
Schnittstelle - **Verbindungsinformation** - **Link**	Hier sind alle physikalischen Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle angeschlossen bzw. aktiv ist. Schnittstellendetails für Ethernet-Schnittstellen: • IP-Adresse • Netzmaske • Nicht konfiguriert

Feld	Wert
	Schnittstellendetails für ISDN-Schnittstellen: • Konfiguriert • Nicht konfiguriert Schnittstellendetails für xDSL-Schnittstellen: • Leitungsgeschwindigkeit Downstream/Upstream Schnittstellendetails für LTE-Verbindung: • Aktuelle Qualität der UMTS/LTE-Verbindung

Felder im Menü WAN-Schnittstellen

Feld	Wert
Beschreibung - **Verbindungsinformation** - **Link**	Hier sind alle WAN-Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle aktiv ist.

5.2 Globale Einstellungen

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

5.2.1 System

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird auch als PPP-Host-Name benutzt. Möglich ist eine Zeichenkette mit maximal 255 Zeichen. Als Standardwert ist der Gerätetyp voreingestellt.
Standort	Geben Sie an, wo sich Ihr Gerät befindet.

Feld	Wert
Kontakt	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Möglich ist eine Zeichenkette mit maximal 255 Zeichen.
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. • *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.

Feld	Wert
	• *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*.
Kommunikation mit dem Cloud NetManager	Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen. Aktivieren oder deaktivieren Sie die Option **Kommunikation mit dem Cloud NetManager**. Im Auslieferungszustand ist die Option *Aktiviert*.
IP-Adresse des Cloud NetManagers	Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen. Hier ist die Adresse des bintec elmeg Cloud NetManagers bereits vorkonfiguriert. Sollten Sie einen eigenen Manager betreiben wollen, müssen Sie hier die Adresse Ihres Servers eintragen.
LED-Modus	Nur für WLAN-Geräte Wählen Sie das Leuchtverhalten der LEDs. Mögliche Werte: • *Status* (Standardwert): Die LEDs zeigen ihr Standardverhalten. • *Blinkend*: Nur die Status-LED blinkt einmal in der Sekunde. • *Aus*: Alle LEDs sind deaktiviert.
Manuelle IP-Adresse des WLAN-Controller	Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar. Geben Sie die IP-Adresse des WLAN-Controllers an. Der Wert kann nur verändert werden, wenn die WLAN-Controller-Funktion aktiviert ist.
Herstellernamen anzeigen	Hier können Sie die Anzeige des Herstellers in der MAC-Adresse ein- oder ausschalten. Für den Herstellernamen (meist

Feld	Wert
	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. Im Syslog (Syslog-Level = *debug*) erscheint die Meldung *new config state: modified*. 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. Im Syslog erscheint die Meldung *new config state: confirmed*.

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. Im Syslog erscheint zunächst eine Meldung zur Beendigung der aktiven Session (z. B. *delete httpSessionStat entry admin at Fri Apr 21 11:04:34 2017 (keep alive timeout)*), danach erfolgt die Speicherung: *auto save on session termination*.

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

5.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

Hinweis

Alle bintec elmeg-Geräte werden mit gleichem Benutzernamen und Passwort ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert wurden.

Ändern Sie unbedingt die Passwörter, um unberechtigten Zugriff auf das Gerät zu verhindern.

Solange das Passwort nicht verändert wird, erscheint unter **Systemverwaltung**->**Status** der Warnhinweis: "Systempasswort nicht geändert!".

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

Felder im Menü Systempasswort

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

Felder im Menü SNMP-Communities

Feld	Wert
SNMP Read Community	Geben Sie das Passwort für den Benutzernamen `read` ein.
SNMP Write Community	Geben Sie das Passwort für den Benutzernamen `write` ein.

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

Feld	Wert
	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. Bei Drücken von **OK** oder erneutem Aufruf des Menüs werden sie als Sternchen angezeigt.

5.2.3 Datum und Uhrzeit

Die Systemzeit benötigen Sie u. a. für korrekte Zeitstempel bei Systemmeldungen, Gebührenerfassung oder IPSec-Zertifikaten.

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

ISDN/Manuell

Die Systemzeit kann bei Geräten mit ISDN-Schnittstelle über ISDN aktualisiert werden, d. h. beim ersten ausgehenden Ruf werden Datum und Uhrzeit aus dem ISDN entnommen. Alternativ kann die Zeit auch manuell auf dem Gerät eingestellt werden.

Wenn für die **Zeitzone** der korrekt Standort des Geräts (Land/Stadt) eingestellt ist, erfolgt die Umschaltung der Uhrzeit von Sommer- auf Winterzeit (und zurück) 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.

Wenn für die **Zeitzone** ein Wert abweichend von der Universal Time Coordinated (UTC), also die Option *UTC+-x*, gewählt wurde, muss die Sommer-Winterzeitumstellung entsprechend den Anforderungen manuell durchgeführt werden.

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. Die Umschaltung der auf diese Weise bezogenen Uhrzeit von Sommer- auf Winterzeit (und zurück) muss manuell durchgeführt werden, indem der Wert im Feld **Zeitzone** mit einer Option UTC+ oder UTC- entsprechend angepasst wird.

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 Grundeinstellungen

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, z. B. *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.

Feld	Beschreibung
	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 aktiviert. 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. • *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.

Feld	Beschreibung
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 nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • *Endlos*: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver zuerst 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 nicht aktiv. Zeitanfragen eines Clients werden nicht beantwortet.

Felder im Menü Zeiteinstellungen (GPS) (nur für Geräte mit GPS)

Feld	Beschreibung
Zeitaktualisierungsintervall	Wählen Sie aus, ob das Gerät die Systemzeit über GPS empfangen soll. Geben Sie ggf. die Zeit (in Sekunden) für die Aktualisierung der Systemzeit über GPS ein. Der Wert 0 (Standardwert) bedeutet, dass die Systemzeit bei jedem GPS Fix aktualisiert wird. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

5.2.4 Systemlizenzen

In diesem Kapitel wird beschrieben, wie Sie die Funktionen einer gegebenenfalls erworbenen Software-Lizenz freischalten.

Es sind generell folgende Lizenztypen zu unterscheiden:

- Lizenzen, die im Auslieferungszustand des Geräts bereits vorhanden sind
- kostenfreie Zusatzlizenzen
- kostenpflichtige Zusatzlizenzen

Welche Lizenzen im Auslieferungszustand zur Verfügung stehen und welche zusätzlich kostenlos bzw. kostenpflichtig für Ihr Gerät erworben werden können, erfahren Sie auf dem Datenblatt zu Ihrem Gerät, das Sie unter *www.bintec-elmeg.com* abrufen können.

Lizenzdaten eintragen

Die Lizenzdaten der Zusatzlizenzen erhalten Sie über die Online-Lizenzierungs-Seiten im Support-Bereich auf *www.bintec-elmeg.com* . Bitte folgen Sie den Anweisungen der Online-Lizenzierung. (Bei kostenpflichtigen Lizenzen beachten Sie bitte auch die Hinweise auf dem Lizenzblatt.) Daraufhin erhalten Sie eine E-Mail mit folgenden Daten:

- **Lizenzschlüssel** und
- **Lizenzseriennummer**.

Diese Daten tragen Sie im Menü **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**->**Neu** ein.

Im Menü **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**->**Neu** wird eine Liste aller eingetragenen Lizenzen angezeigt (**Beschreibung**, **Lizenztyp**, **Lizenzseriennummer**, **Status**).

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 Gerät nicht unterstützt.

Außerdem wird die zur Online-Lizenzierung notwendige **Systemlizenz-ID** oberhalb der Liste angezeigt.

Hinweis

Um die Standardlizenzen eines Geräts wiederherstellen zu können, klicken Sie die Schaltfläche **Stdrd. Lizenzen** (Standardlizenzen).

5.2.4.1 Bearbeiten oder Neu

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

Freischalten von Zusatzlizenzen

Die entsprechenden Zusatzlizenzen schalten Sie frei, indem Sie die erhaltenen Lizenzinformationen im Menü **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**->**Neu** hinzufügen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

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**->**Neu**.

(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.

5.3 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 zum 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 des Bridge-Links setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Funkmoduls, auf dem der Bridge-Link konfiguriert ist

(c) Nummer des Bridge-Link

Beispiel: *wds1-0* (erster Bridge-Link auf dem ersten Funkmodul)

Der Name des Client-Links setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Funkmoduls, auf dem der Client-Link konfiguriert ist

(c) Nummer des Client-Links

Beispiel: *sta1-0* (erster Client-Link 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)

5.3.1 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.

Standardmäßig sind alle bestehenden Schnittstellen im Routing-Modus. Bei Auswahl der Option *Neue Bridge-Gruppe* für **Modus / Bridge-Gruppe**, wird automatisch eine Bridge-Gruppe, also *br0*, *br1* usw., angelegt und die Schnittstelle im Bridging-Modus betrieben.

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.

5.3.1.1 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.

Bearbeiten für Geräte der WIxxxxn und RS-Serie

Für WLAN-Clients im Bridge-Modus (sog. MAC-Bridge) können sie über das Symbol weitere Einstellungen bearbeiten.

Sie können mit der Funktion MAC-Bridge Bridging für Geräte hinter Access Clients realisieren. Zusätzlich kann in einem Wildcard-Modus festgelegt werden, wie Unicast nicht-IP-Frames bzw. nicht-ARP Frames verarbeitet werden sollen. Um die Funktion MAC-Bridge zu nutzen, müssen Sie Konfigurationsschritte in mehreren Menüs vornehmen.

(1) Wählen Sie das **GUI** Menü **Wireless LAN**->**WLAN**->**Einstellungen Funkmodul** und klicken Sie auf das Symbol zur Änderung eines Eintrags.

(2) Wählen Sie **Betriebsmodus** = *Access Client* und speichern Sie die Einstellungen mit **OK**.

(3) Wählen Sie das Menü **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**. Die zusätzliche Schnittstelle **sta1-0** wird angezeigt.

(4) Wählen Sie für die Schnittstelle **sta1-0** Modus / Bridge-Gruppe = *br0 (<IPAdresse>)* sowie **Konfigurationsschnittstelle** = *en1-0* und speichern Sie die Einstellungen mit **OK**.

(5) Klicken Sie auf die Schaltfläche **Konfiguration speichern**, um alle Konfigurationseinstellungen zu speichern. Sie können die MAC-Bridge verwenden.

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

Felder im Menü Layer 2.5-Optionen

Feld	Wert
Schnittstelle	Zeigt die Schnittstelle an, die gerade bearbeitet wird.
Wildcard-Modus	Wählen Sie aus, welchen Wilrdcard-Modus Sie auf der Schnittstelle nutzen wollen. Mögliche Werte: • *Keiner* (Standardwert): Es wird kein Wildcard-Modus verwendet. • *statisch*: Mit dieser Einstellung müssen Sie bei **Wildcard-MAC-Adresse** die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist. Jedes Paket ohne IP und ohne ARP wird an dieses Gerät weitergereicht. Dieses Vorgehen wird auch dann beibehalten, wenn das entsprechende Gerät nicht mehr angeschlossen ist. • *zuerst*: Mit dieser Einstellung wird die MAC-Adresse des ersten Nicht-IP-Unicast-Frame bzw Nicht-

Feld	Wert
	ARP-Unicast-Frame, der an irgendeiner der Ethernet-Schnittstellen ankommt, als Wildcard-MAC-Adresse benutzt. Diese Wildcard-MAC-Adresse kann nur durch einen Neustart des Geräts oder die Auswahl eines anderen Wildcard-Modus zurückgesetzt werden. • *letzte*: Mit dieser Einstellung wird die eigene WLAN-MAC-Adresse benutzt, um die Verbindung zum Access Point herzustellen. Sobald ein Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame auftaucht, wird er an diejenige MAC-Adresse weitergeleitet, von welcher der letzte Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame bei einer Ethernet-Schnittstelle des Geräts eingetroffen ist. Diese Wildcard-MAC-Adresse wird mit jedem Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame erneuert.
Wildcard-MAC-Adresse	Nur für **Wildcard-Modus** = *statisch* Geben Sie die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist.
Transparente MAC-Adresse	Nur für **Wildcard-Modus** = *statisch*, *zuerst* Wählen Sie aus, ob die **Wildcard-MAC-Adresse** zusätzlich als WLAN-MAC-Adresse benutzt werden, um damit die Verbindung zum Access Point herzustellen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

5.4 Administrativer Zugriff

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

5.4.1 Zugriff

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

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

Hinweis

Nicht alle Optionen sind für alle bintec elmeg-Geräte verfügbar. Informieren Sie sich im Datenblatt Ihres Geräts, welche Verbindungstypen unterstützt werden!

Nur für Telefonanlagen: Weiterhin können Sie Ihr Gerät für Wartungsarbeiten durch den bintec elmeg-Kundenservice freischalten. Hierzu aktivieren Sie je nach angeforderter Service-Leistung die Option **Service Login (ISDN Web-Access)** oder **Service Call Ticket (SSH Web-Access)** und wählen die Schaltfläche **OK**. Folgen Sie den Anweisungen des bintec elmeg-Kundenservice!

Service Login (ISDN Web-Access) ist standardmäßig nicht aktiv. Wenn die Option aktiviert ist, wird sie nach ca. 30 Minuten automatisch wieder deaktiviert.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Standardeinstellungen wiederherstellen	Erst wenn Sie Änderungen an der Konfiguration des administrativen Zugangs vornehmen, werden entsprechende Zugangsregeln eingerichtet und aktiviert. Mithilfe des Symbols 🗑 können Sie die Standardeinstellungen wiederherstellen.

5.4.1.1 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.

5.4.2 SSH

Ihr Gerät bietet einen verschlüsselten Zugang zur Shell. Diesen Zugang können Sie im Menü **Systemverwaltung**->**Administrativer Zugriff**->**SSH** aktivieren (**Aktiviert**, Standardwert) oder deaktivieren. Ferner können Sie auf die Optionen zur Konfiguration des SSH-Login zugreifen.

Um den SSH Daemon ansprechen zu können, wird eine SSH-Client-Anwendung, z. B.

PuTTY, benötigt.

Wenn Sie SSH Login zusammen mit dem PuTTY-Client verwenden wollen, müssen Sie u. U. einige Besonderheiten bei der Konfiguration beachten. Wir haben diesbezüglich eine FAQ erstellt. Sie finden diese im Bereich Dienste/Support auf *www.bintec-elmeg.com*.

Um die Shell Ihres Geräts über einen SSH Client erreichen zu können, stellen Sie sicher, dass die Einstellungen beim SSH Daemon und dem SSH Client übereinstimmen.

Hinweis

Sollte nach der Konfiguration eine SSH-Verbindung nicht möglich sein, starten Sie das Gerät neu, um den SSH Daemon korrekt zu initialisieren.

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

Felder im Menü SSH-Parameter (Secure Shell)

Feld	Wert
SSH-Dienst aktiv	Wählen Sie aus, ob der SSH-Daemon aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
SSH-Port	Hier können Sie den Port eingeben, über den die SSH-Verbindung aufgebaut werden soll. Der Standardwert ist *22*.
Maximale Anzahl gleichzeitiger Verbindungen	Tragen Sie die maximale Anzahl gleichzeitig aktiver SSH-Verbindungen ein. Der Standardwert ist *1*.

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

Feld	Wert
Verschlüsselungsalgorithmen	Wählen Sie die Algorithmen, die für die Verschlüsselung der SSH-Verbindung verwendet werden sollen. Mögliche Optionen: • *3DES*

Feld	Wert
	• *Blowfish* • *AES-128* • *AES-256* Standardmäßig sind *3DES*, *Blowfish* und *AES-128* aktiv.
Hashing-Algorithmen	Wählen Sie die Algorithmen, die zur Message-Authentisierung der SSH-Verbindung verwendet werden sollen. Mögliche Optionen: • *MD5* • *SHA-1* • *RipeMD 160* Standardmäßig sind *MD5*, *SHA-1* und *RipeMD 160* aktiv.

Felder im Menü Schlüsselstatus

Feld	Wert
RSA-Schlüsselstatus	Zeigt den Status des RSA-Schlüssels an. Wenn bisher kein RSA-Schlüssel generiert wurde, wird *Nicht generiert* und ein Link *Generieren* angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status *Wird generiert* angezeigt. Wenn die Generierung erfolgreich abgeschlossen wurde, ändert sich der Status von *Wird generiert* auf *Generiert*. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut *Nicht generiert* mit Link *Generieren* angezeigt. Sie können die Generierung wiederholen. Wird der Status *Unbekannt* angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.
ECDSA-Schlüsselstatus	Zeigt den Status des ECDSA-Schlüssels an. Wenn bisher kein ECDSA-Schlüssel generiert wurde, wird *Nicht generiert* und ein Link *Generieren* angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status *Wird generiert* angezeigt. Wenn die Generierung erfolg-

Feld	Wert
	reich abgeschlossen wurde, ändert sich der Status von *Wird generiert* auf *Generiert*. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut *Nicht generiert* mit Link *Generieren* angezeigt. Sie können die Generierung wiederholen. Wird der Status *Unbekannt* angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.
ED25519-Schlüsselstatus	Zeigt den Status des ED25519-Schlüssels an. Wenn bisher kein ED25519-Schlüssel generiert wurde, wird *Nicht generiert* und ein Link *Generieren* angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status *Wird generiert* angezeigt. Wenn die Generierung erfolgreich abgeschlossen wurde, ändert sich der Status von *Wird generiert* auf *Generiert*. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut *Nicht generiert* mit Link *Generieren* angezeigt. Sie können die Generierung wiederholen. Wird der Status *Unbekannt* angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.

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

Felder im Menü Erweiterte Einstellungen

Feld	Wert
Toleranzzeit beim Login	Geben Sie die Zeit (in Sekunden) ein, die für den Verbindungsaufbau zur Verfügung steht. Wenn ein Client innerhalb dieser Zeit nicht erfolgreich authentifiziert werden kann, wird die Verbindung getrennt. Der Standardwert ist *600* Sekunden.
Komprimierung	Wählen Sie aus, ob Datenkompression verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
TCP-Keepalives	Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Protokollierungslevel	Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus. Zur Verfügung stehen: • *Information* (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. • *Fatal*: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. • *Fehler*: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. • *Debug*: Es werden alle Meldungen aufgezeichnet.

5.4.3 SNMP

SNMP (Simple Network Management Protocol) ist ein Netzwerkprotokoll, mittels dessen Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwacht und gesteuert werden können. SNMP regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Das Protokoll beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf.

Die Datenobjekte, die per SNMP abgefragt werden können, sind in Tabellen und Variablen strukturiert und in der sogenannten MIB (Management Information Base) definiert. Sie enthält alle Konfigurations- und Statusvariablen des Geräts.

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

- Überwachung von Netzwerkkomponenten
- Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten
- Fehlererkennung und Fehlerbenachrichtigung.

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

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

Felder im Menü Grundeinstellungen

Feld	Wert
SNMP-Version	Wählen Sie aus, welche SNMP-Version Ihr Gerät für externe SNMP-Zugriffe verwenden soll. Mögliche Werte: • *v1*: SNMP-Version 1 • *v2c*: Community-Based SNMP-Version 2 • *v3*: SNMP-Version 3 Standardmäßig sind *v1*, *v2c* und *v3* aktiv. Ist keine Option ausgewählt, ist die Funktion nicht aktiv.
SNMP-Listen-UDP-Port	Zeigt den UDP-Port (*161*) an, an dem das Gerät SNMP-Requests annimmt. Der Wert kann nicht verändert werden.
SNMP multicast discovery	Aktivieren oder deaktivieren Sie die Funktion **SNMP multicast discovery**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Tipp

Wenn Ihr SNMP-Manager SNMPv3 unterstützt, sollten Sie nach Möglichkeit diese Version verwenden, da ältere Versionen alle Daten unverschlüsselt übertragen.

5.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

5.5.1 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 Verbindungs-

Feld	Wert
	aufbau 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 Ablehung 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.

5.5.1.1 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.

Feld	Wert
	• *Accounting* (nur für PPP-Verbindungen): Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet. • *Login-Authentifizierung*: Der RADIUS-Server wird verwendet, um den Zugang zur SNMP Shell Ihres Geräts zu kontrollieren. • *IPSec-Authentifizierung*: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. • *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* Wählen Sie in Hotspot-Anwendungen den Modus aus, der vom Anbieter definiert ist. In Standardanwendungen belassen Sie den Wert bei *Standard*. Mögliche Werte für Hotspot-Anwendungen: • *France Telecom*: Für Hotspot-Anwendungen der France Telecom. • *bintec HotSpot Server*: Für Hotspot-Anwendungen.
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.

Feld	Wert
	Mögliche Werte von *0* (höchste Priorität) bis *7* (niedrigste Priorität). Der Standardwert ist *0*. Siehe auch **Richtlinie** in den erweiterten Einstellungen.
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, wie z. B. Hotspot-Server-Konfiguration, aus. • *<Gruppenname>*: Wählen Sie aus der Liste eine schon definierte Gruppe aus.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Wert
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. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit *inaktiv* ist. 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.

Feld	Wert
	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 *IPSec-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. 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.

5.5.2 TACACS+

TACACS+ ermöglicht die Zugriffssteuerung von Ihrem Gerät, Netzzugangsservern (NAS) und anderen Netzwerkkomponenten über einen oder mehrere zentrale Server.

TACACS+ ist wie RADIUS ein AAA-Protokoll und bietet Authentifizierungs-, Autorisierungs- und Abrechnungsdienste (TACACS+-Gebührenerfassung wird derzeit von bintec elmeg-Geräten nicht unterstützt).

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

- Authentifizierung für Login Shell
- Kommando-Autorisierung auf der Shell (z. B. telnet, show)

TACACS+ verwendet TCP Port 49 und stellt eine gesicherte und verschlüsselte Verbindung her.

Im Menü **Systemverwaltung**->**Remote Authentifizierung**->**TACACS+** wird eine Liste al-

ler eingetragenen TACACS+-Server angezeigt.

5.5.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Authentifizierungstyp	Zeigt an, welche TACACS+-Funktion genutzt werden soll. Der Wert kann nicht verändert werden. Mögliche Werte: • *Login-Authentifizierung*: Hier können Sie festlegen, ob der aktuelle TACACS+-Server für die Login-Authentifizierung zu Ihrem Gerät benutzt werden soll.
Server-IP-Adresse	Geben Sie die IP-Adresse des TACACS+-Servers ein, der für eine Login-Authentifizierung abgefragt werden soll.
TACACS+-Passwort	Geben Sie das Passwort ein, welches benutzt werden soll, um den Datenaustausch zwischen dem TACACS+-Server und dem Netzzugangsserver (Ihrem Gerät) zu authentifizieren und (falls zutreffend) zu verschlüsseln. Die maximale Länge des Eintrags ist 32 Zeichen.
Priorität	Weisen Sie dem aktuellen TACACS+-Server eine Priorität zu. Der Server mit dem niedrigsten Wert ist der erste, der für die TACACS+-Login-Authentifizierung benutzt wird. Falls er keine Antwort liefert oder der Zugriff verweigert wurde (nur für **Richtlinie** = *Nicht verbindlich*), wird der Eintrag mit der nächstniedrigeren Priorität genutzt. Verfügbare Werte sind *0* bis *9*, der Standardwert ist *0*.
Eintrag aktiv	Wählen Sie aus, ob dieser Server für die Login-Authentifizierung verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Richtlinie	Wählen Sie die Interpretation der TACACS+-Antwort aus. Mögliche Werte: • *Nicht verbindlich* (Standardwert): Die TACACS+-Server werden gemäß ihrer Priorität (siehe **Priorität**) abgefragt, bis eine positive Antwort oder von einem authoritativen Server eine negative Antwort empfangen wurde. • *Verbindlich*: Eine negative Antwort auf eine Anfrage wird akzeptiert, d. h. es wird kein weiterer TACACS+-Server abgefragt. Die Geräte-interne Benutzerverwaltung wird durch TACACS+ nicht ausgeschaltet. Sie wird geprüft, nachdem alle TACACS+Server abgefragt wurden.
TCP-Port	Zeigt den für das TACACS+-Protokoll verwendeten Standard-TCP-Port (*49*) an. Der Wert kann nicht verändert werden.
Timeout	Geben Sie die Zeit in Sekunden ein, die der NAS auf eine Antwort von TACACS+ warten soll. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+-Server abgefragt (nur für **Richtlinie** = *Nicht verbindlich*) und der aktuelle Server in einen *blockiert*-Status versetzt. Mögliche Werte sind *1* bis *60*, der Standardwert ist *3*.
Blockzeit	Geben Sie die Zeit in Sekunden ein, die der aktuelle Server in einem blockierten Status verbleiben soll. Nach Ende der Blockierung wird der Server in den Status versetzt, der im Feld **Eintrag aktiv** angegeben ist. Mögliche Werte sind *0* bis *3600*, der Standardwert ist *60*. Der Wert *0* bedeutet, dass der Server nie in einen *blockiert*-Status versetzt wird und somit keine weiteren Server angefragt werden.
Verschlüsselung	Wählen Sie aus, ob der Datenaustausch zwischen dem TA-

Feld	Beschreibung
	CACS+-Server und dem NAS mit MD5 verschlüsselt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Ist die Funktion nicht aktiv, werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung sondern nur für Debug-Zwecke empfohlen.

5.5.3 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*

Feld	Beschreibung
	deaktiviert.

5.6 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.

5.6.1 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 die Zugriffsprofile *Mini-Callcenter*, *Kosten*, *Telefonbuch*, *Benutzerzugang zur Telefonanlage*, *Schnellstart*, *Experte*, *Benutzer* bereits angelegt. Diese können Sie mithilfe des Symbols ändern sowie über das Symbol auf die Standardeinstellungen zurücksetzen.

5.6.1.1 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** und **Zum SNMP Browser wechseln** verwenden. Sie können maximal 29 Zugriffsprofile anlegen.

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

Felder im Menü Grundeinstellungen

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.
Zum SNMP Browser wechseln	Wenn Sie die Schaltfläche **Zum SNMP Browser wechseln** aktivieren, kann der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und alle dort angezeigten Einstellungen ändern. **Achtung** Beachten Sie, dass die Berechtigung für **Zum SNMP Browser wechseln** bedeutet, dass der Benutzer auf die gesamte MIB zugreifen kann, da in dieser Ansicht kein individuelles Zugangsprofil angelegt werden kann. Mit der Berechtigung für **Konfiguration speichern** kann er die geänderte MIB speichern. Mit der Berechtigung für **Zum SNMP Browser wechseln** heben Sie die konfigurierten GUI- Einschränkungen auf der MIB-Ebene wieder auf. Aktivieren oder deaktivieren Sie **Zum SNMP Browser wechseln**. 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. Untergeordnete 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.

5.6.2 Benutzer

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

Es sind keine Benutzer vorkonfiguriert.

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.

5.6.2.1 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 Grundeinstellungen

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. Die Auswahl **Nur lesen** ist nur möglich, wenn die Option **Zum SNMP Browser wechseln** im Menü **Zugriffsprofile** nicht aktiv ist. Ist die Option **Zum SNMP Browser wechseln** aktiv, so wird ein Warnhinweis angezeigt, weil der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und beliebige Änderungen vornehmen kann. Die Option **Nur lesen** ist in der SNMP-Browser-Ansicht nicht verfügbar. Werden einem Benutzer sich überschneidende Zugriffsprofile

Feld	Beschreibung
	zugeordnet, so hat Lesen und Schreiben eine höhere Priorität als **Nur lesen**. Schaltflächen können nicht auf die Einstellung **Nur lesen** gesetzt werden.

5.7 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 Unterschrift 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.

5.7.1 Zertifikatsliste

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

5.7.1.1 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

Feld	Beschreibung
	dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im 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.

5.7.1.2 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. • *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.

Feld	Beschreibung
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-*

Feld	Beschreibung
	Zertifikat verwenden -- 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.

Feld	Beschreibung
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. 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.

5.7.1.3 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 **Durchsuchen...** 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. • *Base64* • *Binär*

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

5.7.2 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.

5.7.2.1 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 **Durchsuchen...** 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 Kodiererken-

Feld	Beschreibung
	nung. 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.

5.7.3 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.

5.7.3.1 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 Physikalische Schnittstellen

In diesem Menü konfigurieren Sie die physikalischen Schnittstellen, die Sie beim Anschließen Ihres Gateways verwendet haben. Die Konfigurationsoberfläche zeigt ausschließlich diejenigen Schnittstellen an, die auf Ihrem Gerät zur Verfügung stehen. Sie sehen im Menü **Systemverwaltung**->**Status** eine Liste aller physikalischen Schnittstellen und Informationen darüber, ob die Schnittstellen angeschlossen bzw. aktiv sind und ob sie bereits konfiguriert sind.

6.1 Ethernet-Ports

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

Die Ethernet-Ports **ETH1** bis **ETH4** sowie **SFP1** sind im Auslieferungszustand der logischen Ethernet-Schnittstelle *en1-0* zugewiesen und mit **IP-Adresse** *192.168.0.254* und **Netzmaske** *255.255.255.0* konfiguriert.

Die Ports **ETH5 bis ETH8** sowie **SFP2** sind der logischen Ethernet-Schnittstelle *en1-5* zugewiesen und nicht vorkonfiguriert.

Hinweis

Um die Erreichbarkeit Ihres Geräts 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. Führen Sie im Zweifelsfall die Konfiguration per serieller Verbindung über die **Console**-Schnittstelle durch.

ETH 1 - 8

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.

SFP 1 und 2

Die Konfigurationsoptionen sind identisch mit denen der Ports **1** - **8**.

Hinweis

Wenn Sie diese Ports mit einem SFP-Modul betreiben wollen, muss dieses vor dem Systemstart gesteckt sein!

Unterstützt werden folgende SFP-Module mit SERDES-Interface für FTTH-Verbindungen:

- AT-SPBD10-13: 1000LX Single Mode BiDi SFP (1310 Tx, 1490 Rx) 10 km
- AT-SPBD10-14: 1000LX Single Mode BiDi SFP (1490 Tx, 1310 Rx) 10 km
- AT-SPLX40: 1000LX (LC) SFP, 40 km

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.

6.1.1 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 Switch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Anschlussseite des Geräts. Den beiden SFP-Ports entsprechen die Switch-Ports 9 und 10.
Ethernet-Schnittstellenauswahl	Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-Schnittstelle zu. Zur Auswahl stehen die Schnittstellen *en1-0* bis *en1-9*. In der Grundeinstellung ist **Switch Port 1**-**4** und **9** die Schnittstelle *en1-0*, **Switch Port 5**-**8** und **10** die Schnittstelle *en1-5* 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*

Feld	Beschreibung
	• *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.

6.2 ISDN-Ports

In diesem Menü konfigurieren Sie die ISDN-Schnittstellen Ihres Geräts. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluss Ihr Gateway angeschlossen ist. Die ISDN-Schnittstellen Ihres Gateways können Sie für verschiedene Nutzungstypen einsetzen.

Um die ISDN-Schnittstellen zu konfigurieren, müssen Sie zwei Schritte durchführen:

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

6.2.1 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.

6.2.1.1 Bearbeiten mit

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

ISDN-BRI-Schnittstelle

Die ISDN-BRI-Schnittstellen Ihres Gateways können Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen.

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.
Automatische Konfiguration beim Start	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 aktiv.
Ergebnis der automatischen Konfiguration	Zeigt den Status der ISDN-Autokonfiguration an. Die automatische D-Kanal-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter **Port-Verwendung** manuell ausgewählt ist. Das Feld kann nicht editiert werden. Angezeigt wird das Ergebnis der automatischen Konfiguration für die **Port-Verwendung** und den **ISDN-Konfigurationstyp**. Mögliche Werte: • Alle möglichen Werte für die **Port-Verwendung** und den **ISDN-Konfigurationstyp**. • *Wird ausgeführt*: Erkennung läuft noch.
Port-Verwendung	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist.

Feld	Beschreibung
	Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll. Mögliche Werte: • *Nicht verwendet*: Der ISDN-Anschluss wird nicht genutzt. • *Dialup (Euro-ISDN)* • *Standleitung*
ISDN-Konfigurationstyp	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist und für **Port-Verwendung** = *Dialup (Euro-ISDN)* Wählen Sie die ISDN-Anschlussart aus. Mögliche Werte: • *Punkt-zu-Mehrpunkt* (Standardwert): Mehrgeräteanschluss. • *Punkt-zu-Punkt*: Anlagenanschluss.
ISDN-Switch-Typ	Nur für **Port-Verwendung** = *Standleitung* Wählen Sie das ISDN-Protokoll, das Ihnen Ihr Provider zur Verfügung stellt: Mögliche Werte: • *Standleitung B1 64S*: Festverbindung über B-Kanal 1 (64 kbit/s) • *Standleitung B1+B2 64S2*: Festverbindung über beide B-Kanäle (128 kbit/s) • *Standleitung D+B1+B2 TS02*: Festverbindung über D-Kanal und beide B-Kanäle (144 kbit/s) • *Standleitung B1+B2 Unterschiedliche Endpunkte*: Festverbindung zu zwei verschiedenen Endpunkten. • *Standleitung B1+D TS01*: Festverbindung über B-Kanal 1 und D-Kanal (80 kbit/s) • *Standleitung B2+D TS01*: Festverbindung über B-Kanal 2 und D-Kanal (80 kbit/s) • *Standleitung B2 64S*: Festverbindung über B-Kanal 2 (64 kbit/s)

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.

6.2.2 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 bintec elmeg-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 bintec elmeg-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 nichtpaketorientierte 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.

6.2.2.1 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*. • *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

Feld	Beschreibung
	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)

6.3 UMTS/LTE

6.3.1 UMTS/LTE

Im Menü **UMTS/LTE** konfigurieren Sie die Anbindung eines optional steckbaren UMTS/LTE-USB-Sticks. Ihr Gerät unterstützt USB-Sticks ab USB 2.0.

Eine Liste der unterstützten UMTS/LTE-USB-Sticks finden Sie unter *www.bintec-elmeg.com* im Bereich **Produkte**.

Hinweis

Wenn Sie einen Internetzugang über UMTS einrichten und den SMS-Benachrichtigungsdienst verwenden, wird die Verbindung kurz unterbrochen, sobald eine SMS versendet wird.

Hinweis

LTE kann aktuell nicht für eingehende Verbindungen über ISDN-Login verwendet werden.

LTE kann aktuell nicht zusammen mit dem SMS-Benachrichtigungsdienst verwendet werden.

6.3.1.1 Bearbeiten

Wählen Sie das Symbol , um den jeweiligen Eintrag für das gesteckten UMTS/LTE-USB-Stick zu bearbeiten.

Hinweis

Beachten Sie, dass die verwendete Technologie nicht nur von der Verfügbarkeit und von der Einstellung im Feld **Bevorzugter Netzwerktyp** abhängt sondern auch von der Signalstärke und von der Signalqualität.

Das Menü **Physikalische Schnittstellen**->**UMTS/LTE**->**UMTS/LTE**-> besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
UMTS/LTE-Status	Wählen Sie aus, ob das gewählte UMTS/LTE-Modem aktiviert werden soll oder nicht. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Modem-Status	Nur für **UMTS/LTE-Status** = *Aktiviert* Zeigt den Status des UMTS/LTE-Modems an.

Feld	Beschreibung
	Mögliche Werte: • *Aktiv* • *Inaktiv* • *Init* • *Gerufen* • *Rufend* • *Verbinden* • *SIM Einlegen erforderlich* • *PIN Eingabe erforderlich* • *Fehler* • *Nicht verbunden*
Aktuelles Netzwerk	Nur für **UMTS/LTE-Status** = *Aktiviert* Zeigt das aktuelle Netzwerk an, z. B. GSM oder UMTS.
Mobilfunk-Anbieter	Nur für **UMTS/LTE-Status** = *Aktiviert* Wird nur angezeigt, wenn sich das Modem im Zustand "up" befindet. Zeigt den aktuell verbundenen **Mobilfunk-Anbieter** an.
Netzwerkqualität	Nur für **UMTS/LTE-Status** = *Aktiviert* Zeigt die aktuelle Qualität der UMTS/LTE-Verbindung an. Der Wert kann nicht verändert werden.
Bevorzugter Netzwerktyp	Nur für **UMTS/LTE-Status** = *Aktiviert* Wählen Sie aus, welcher Netzwerktyp bevorzugt verwendet werden soll. Mögliche Werte: • *Automatisch* (Standardwert): Für die Verbindung wird automatisch GPRS, UMTS oder LTE gewählt, je nachdem welcher Netzwerktyp örtlich zur Verfügung steht. • *Nur GPRS*: Nur GPRS wird verwendet, sollte GPRS nicht verfügbar sein, kommt keine Verbindung zustande.

Feld	Beschreibung
	• *Nur UMTS*: Nur UMTS wird verwendet, sollte UMTS nicht verfügbar sein, kommt keine Verbindung zustande. • *Bevorzugt GPRS*: Es wird bevorzugt GPRS verwendet, sollte GPRS nicht verfügbar sein, wird UMTS verwendet. • *Bevorzugt UMTS*: Es wird bevorzugt UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet. • *Nur LTE*: Nur LTE wird verwendet, sollte LTE nicht verfügbar sein, kommt keine Verbindung zustande • *LTE preferred (Priorität 4G/3G/2G)*: Es wird bevorzugt LTE verwendet, sollte LTE nicht verfügbar sein, wird UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet • *LTE/UMTS (Priorität 4G/3G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet. • *LTE/GPRS (Priorität 4G/2G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet. • *LTE/GPRS/UMTS (Priorität 4G/2G/3G)*: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird UMTS verwendet. • *UMTS/LTE (Priorität 3G/4G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet. • *UMTS/GPRS (Priorität 3G/2G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird GPRS verwendet. • *UMTS/LTE/GPRS (Priorität 3G/4G/2G)*: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet.. • *GPRS/LTE (Priorität 2G/4G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet. • *GPRS/UMTS (Priorität 2G/3G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von

Feld	Beschreibung
	GPRS wird UMTS verwendet. • *GPRS/LTE/UMTS (Priorität 2G/4G/3G)*: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet. **Hinweis** Ein eingehender Datenruf (PPP-Einwahl oder ISDN-Login über V.110) kann in der Regel nur über GSM aufgebaut werden. Für UMTS/LTE ist ein Aufbau nur möglich, wenn der Provider diese Funktionalität auf Antrag freigeschaltet hat. Wenn sich ein Modem im Zustand "up" befindet und **Bevorzugter Netzwerktyp** nicht *Nur UMTS* ist, registriert sich das Modem normalerweise im GSM-Netz, damit eingehende Daten-Rufe signalisiert werden können. Wird danach eine Verbindung zum Internet hergestellt, wird in das UMTS-Netz umgeschaltet, sofern UMTS aktuell verfügbar ist.
Eingehender Diensttyp	Nur für **UMTS/LTE-Status** = *Aktiviert* Wählen Sie aus, welchem Subsystem des Gateways ein über das Modem eingehender Ruf zugewiesen werden soll. Mögliche Werte: • *Deaktiviert*: Es erfolgt keine Rufannahme (Standardwert für LTE-Verbindungen). • *ISDN-Login* : Der Ruf wird dem ISDN-Login-Subsystem zugewiesen (Standardwert für UMTS-Verbindungen). • *PPP-Einwahl*: Der Ruf wird dem PPP-Subsystem zugewiesen. • *IPSec*: Der Ruf erfolgt über IPSec. Beachten Sie für die Einstellung **Eingehender Diensttyp** *IPSec* Folgendes: IPSec-Callback wird dazu verwendet, einen IPSec-Peer zu veranlassen, eine Internetverbindung aufzubauen, um so einen IP-

Feld	Beschreibung
	Sec-Tunnel über das Internet zu ermöglichen. Mit Hilfe eines direkten Anrufs über das UMTS/LTE-Mobilfunknetz kann dem Peer 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 Anruf über Mobilfunk veranlasst, eine Verbindung aufzubauen. Im Menü **VPN**->**IPSec**->**IPSec-Peers**->->**Erweiterte Einstellungen** können Sie unter **Eigene IP-Adresse per ISDN/GSM übertragen** zudem auswählen, ob die IP-Adresse zum IPSec-Tunnelaufbau in dem Callback-UMTS/LTE-Ruf mitgesendet werden soll. Dieses verkürzt und erleichtert unter Umständen den Tunnelaufbau.
PUK	Wird nur angezeigt, wenn das Gerät dreimal vergeblich versucht hat, eine Verbindung aufzubauen, z. B. wenn die PIN der SIM-Karte (siehe das Feld **SIM-Karte verwendet PIN**) dreimal falsch eingegeben wurde. Geben Sie den PUK (Personal Unblocking Key) Ihrer SIM-Karte ein, um die SIM-Karte zu entsperren.
SIM-Karte verwendet PIN	Nur für **UMTS/LTE-Status** = *Aktiviert* Geben Sie die PIN Ihrer UMTS/LTE-Modemkarte ein.  **Hinweis** Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.  **Hinweis** Wenn das Gerät dreimal vergeblich versucht hat eine Verbindung aufzubauen, z. B. weil dreimal die falsche PIN eingegeben wurde, so müssen Sie zum Entsperren der SIM-Karte den **PUK** eingeben.
Fallback-Nummer	Nur für **UMTS/LTE-Status** = *Aktiviert*

Feld	Beschreibung
	Tragen Sie die Rufnummer für die Funktion GSM Fallback ein. Wenn ein Sprachruf auf diese Nummer eingeht, wird eine ggf. aktive Verbindung sofort getrennt und der Betriebsmodus des Modems auf GSM zurückgesetzt, in welchem das Modem so lange bleibt, bis wieder ein Datenruf (PPP, ISDN-Login, IPSec-Callback) erfolgt. Ist für die WAN-Verbindung der Flatrate-Modus aktiviert (Option **Immer aktiv** aktiviert in **WAN**->**Internet + Einwählen**->**UMTS/LTE**->), führt dies zu sofortigem Verbindungswiederaufbau. **Hinweis** Beachten Sie, dass die SIM-Karte diese Funktion unterstützen muss und nicht alle Mobilfunk-Anbieter Sprachrufe auf Daten-SIM-Karten weiterleiten.
APN (Access Point Name)	Nur für **UMTS/LTE-Status** = *Aktiviert* Wenn GPRS/UMTS/LTE benutzt werden soll, müssen Sie hier den sogenannten Access Point Name eintragen, den Sie von Ihrem Provider erhalten haben. Maximal können 80 Zeichen eingegeben werden. Wird hier nichts oder ein falscher APN angegeben, so funktioniert eine konfigurierte GPRS/UMTS/LTE-Verbindung nicht.

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

Felder im Menü Roaming/PLMN-Auswahl

Feld	Beschreibung
Roaming-Modus	Wählen Sie aus, ob Sie Roaming verwenden wollen. Mögliche Werte: • *Deaktiviert* (Standardeinstellung): Roaming ist ausgeschaltet. Das Home PLMN (Public Land Mobile Network) wird verwendet, d.h. der Anbieter, bei dem die SIM-Karte registriert ist. • *Auto*: Verwenden Sie diesen Modus, wenn weder **Roaming-Modus** = *Deaktiviert* noch **Roaming-Modus** = *Fest*

Feld	Beschreibung
	eingestellt Ihren Anforderungen entspricht. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. • *Uneingeschränkt*: Dieser Modus ist für spezielle Anforderungen vorgesehen. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. • *International*: Dieser Modus ist für spezielle Anforderungen vorgesehen. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. • *National*: Dieser Modus ist in vielen Ländern, z. B. in Deutschland, nicht verfügbar. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. • *Fest eingestellt*: Wenn das Feld **Lokale Umgebung** nicht *Aktiviert* ist, können Sie mit **Roaming-Modus** = *Fest eingestellt* eine **Region** und ein **Land** innerhalb dieser **Region** auswählen. Innerhalb dieses Landes können Sie einen **Mobilnetzbetreiber** festlegen. Wenn das Feld **Lokale Umgebung** *Aktiviert* ist, können Sie mit **Roaming-Modus** = *Fest eingestellt* einen **Mobilnetzbetreiber** in Ihrer Nähe auswählen.
Lokale Umgebung	Nur für **Roaming-Modus** = *Fest eingestellt* Legen Sie fest, ob Sie einen **Mobilnetzbetreiber** in Ihrer Nähe auswählen wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Mobilnetzbetreiber	Nur für **Roaming-Modus** = *Fest eingestellt* Wählen Sie einen **Mobilnetzbetreiber** aus der Liste aus. Mit **Lokale Umgebung** *Aktiviert* können Sie einen einen **Mobilnetzbetreiber** in Ihrer Umgebung wählen. Außerhalb Ihrer Umgebung wählen Sie zuerst eine **Region** aus, danach ein **Land** und zuletzt einen **Mobilnetzbetreiber**, der dort zur Verfügung steht.

Feld	Beschreibung
Region	Nur für **Roaming-Modus** = *Fest eingestellt* und **Lokale Umgebung** nicht *Aktiviert* Wählen Sie die gewünschte **Region** aus der Liste aus.
Land	Nur für **Roaming-Modus** = *Fest eingestellt* und **Lokale Umgebung** nicht *Aktiviert* Wählen Sie abhängig von der gewählten **Region** das gewünschte **Land** aus der Liste aus.

Felder im Menü Geschlossene Benutzergruppe

Feld	Beschreibung
Authentifizierungs-APN	Tragen Sie hier den Authentifizierungs Access Point Namen für die **Geschlossene Benutzergruppe** ein, den Sie von Ihrem Provider erhalten haben.
Authentifizierungsmethode	Wählen Sie das Authentifizierungsprotokoll für die **Geschlossene Benutzergruppe** aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option. • *pap*: 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* (Standardwert): Vorrangig CHAP, sonst PAP ausführen.
Benutzername	Geben Sie den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben.
Passwort	Geben Sie das Passwort ein, das Sie von Ihrem Provider erhalten haben.
Feste IP-Adresse	Geben Sie die IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.

Durch Klicken auf die -Schaltfläche wird eine ausführliche Statistik zu der jeweiligen UMTS/LTE-Verbindung angezeigt.

Werte in der Liste Status des Mobilgerätes

Feld	Beschreibung
Gerät	Zeigt die Bezeichnung des internen Modemanschlusses an.
Modemmodell	Zeigt die Bezeichnung des Modems an.
IMEI	Die IMEI (International Mobile Station Equipment Identity) zeigt die 15-stellige Sereinnummer des Modems an.
Oper Status	Zeigt den Betriebszustand des Modems an.
ICC ID	Zeigt die Karten-ID an, die auf der SIM-Karte hinterlegt ist.
Rufnummer	Zeigt die Rufnummer an, die auf der SIM-Karte hinterlegt ist.
Adresse des Service-Centers	Zeigt die Adresse des Provider Service-Centers an, die auf der SIM-Karte hinterlegt ist.
Home PLMN	Zeigt das Home PLMN (Public Land Mobile Network) an, d.h. den Anbieter, bei dem die SIM-Karte registriert ist.
Ausgewähltes PLMN	Zeigt ein eventuell ausgewähltes PLMN an. Falls kein PLMN ausgewählt wurde, wird das Home PLNM angezeigt.
Aktuelles Netzwerk	Zeigt an, welches Netz aktuell verwendet wird (z. B. UMTS oder GSM).
Netzwerkqualität	Zeigt die aktuelle Qualität der Verbindung an.
Funkzellen Code	Zeigt den Funkzellen Code der Funkzelle an, in der das Modem aktuell registriert ist.
Cell ID	Zeigt die Cell ID der Funkzelle an, in der das Modem aktuell registriert ist.
Letzer Befehl	Zeigt den letzten Befehl an, der vom System an das Modem geschickt wurde.
Letzte Antwort	Zeigt die letzte Antwort an, die vom Modem gegeben wurde.

Werte in der Liste Netzbetreiber

Feld	Beschreibung
PLMN	Zeigt das PLMN des Netzbetreibers an.
Name	Zeigt den Namen des Netzbetreibers an.
Zugangstyp	Zeigt das aktuell verfügbare Netzwerk an (z. B. UMTS oder GSM).
Status	Zeigt den Registrierungsstatus an.

7 LAN

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

7.1 IP-Konfiguration

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

7.1.1 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

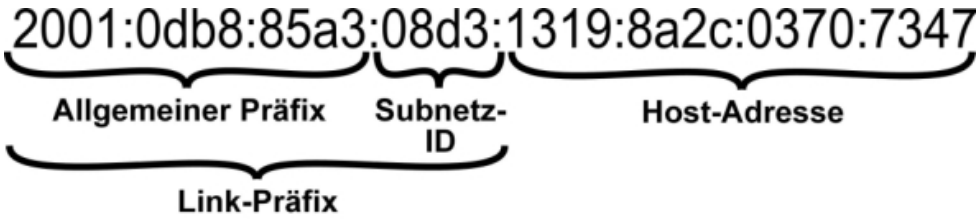
Falls Ihr Gerät an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie für das zweite Teilnetz eine zweite **IP-Adresse / Netzmaske** eintragen.

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*.

7.1.1.1 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.

Feld	Beschreibung
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. • *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 350 konfigurieren.
Adressmodus	Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.

Feld	Beschreibung
	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.

Feld	Beschreibung
	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 350 konfigurieren.
IPv6-Modus	Nur für **IPv6** = *Aktiviert* 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): Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle gesendet werden sollen. Mithilfe der Router Advertisements wird z.B. die Präfix Liste übertragen und der Router propagiert sich als Standard-Gateway. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. • *Host*: Die Schnittstelle wird im Host-Modus betrieben.
DHCP-Server	Nur für **IPv6** = *Aktiviert* und **IPv6-Modus** = *Router (Router-Advertisement übermitteln)* 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

Feld	Beschreibung
	SLAAC erzeugen sollen. 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)*, und **DHCP-Server** *Aktiviert*), so müssen Sie hier seine IPv6-Adressen konfigurieren.
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.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

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

Felder im Menü Basisparameter

Feld	Beschreibung
Ankündigen	Nur für **IPv6-Modus** = *Router (Router-Advertisement übermitteln)* 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.

Feld	Beschreibung
	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.

Feld	Beschreibung
	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

Feld	Beschreibung
	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*

Feld	Beschreibung
	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 (Router-Advertisement übermitteln)* und **Router Advertisement übertragen** = *Aktiviert*

Feld	Beschreibung
	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 (Router-Advertisement übermitteln)* 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 (Router-Advertisement übermitteln)* 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.

Feld	Beschreibung
	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 (Router-Advertisement übermitteln)* 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:
	
	• *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.

7.2 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**.

7.2.1 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.

7.2.1.1 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 -

Feld	Beschreibung
	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. 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.

7.2.2 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 aus-

Feld	Beschreibung
	gewählte Port nicht Mitglied ist.

7.2.3 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:

Feld 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.

8 Wireless LAN Controller

Mit dem Wireless LAN Controller können Sie eine WLAN-Infrastruktur aufbauen und verwalten. Die Vernetzung erfolgt dabei nach dem Master-Slave-Prinzip. Das System nutzt das CAPWAP-Protokoll (Control and Provisioning of Wireless Access Points Protocol) für die Kommunikation zwischen Master und Slaves. In größeren WLAN-Netzen übernimmt ein Gateway die Master-Funktion und verwaltet die Access Points (APs). In kleineren WLAN-Infrastrukturen mit bis zu sechs APs dient ein AP als Master. Der WLAN Controller kann ab Systemsoftwareversion 10.1.7 auch dazu verwendet werden, ein WLAN ausschließlich mit dem internen Funkmodul des Geräts zu realisieren.

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

Der WLAN Controller verfügt über einen Assistenten, der Sie bei der Konfiguration unterstützt. Sobald der Controller alle APs in seinem System "gefunden" hat, bekommen diese jeweils ein neues Passwort und eine neue Konfiguration. Sie werden über den WLAN Controller verwaltet und sind nicht mehr " von außen" manipulierbar; der Zugriff auf den jeweiligen AP ist gesperrt.

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

- APs erkennen und vernetzen

  Sie können mit dem Assistenten fabrikneue Geräte automatisch erkennen und zu einem WLAN vernetzen.

- APs überwachen

  Der WLAN Controller überwacht den Access-Point-Betrieb und die Client-Aktivitäten. Benachbarte APs außerhalb des eigenen WLANs werden ebenfalls erkannt und angezeigt. Bei Ausfall eines APs in Ihrem WLAN können Sie sich per E-Mail benachrichtigen lassen.

  Unauthorisierte Verbindungsversuche zu einem AP von außen werden vom WLAN Controller verworfen.

  Die Sicherung der Netzwerkschlüssel und Passwörter erfolgt nicht auf den APs selbst. Daher stellen APs, die an öffentlich zugänglichen Stellen installiert sind, im Falle eines Diebstahls kein Sicherheitsrisiko dar.

- APs verwalten

  Software und Konfiguration lassen sich schnell und einfach ändern und an alle APs verteilen. Die Konfiguration ist zentral gespeichert und wird bei Bedarf (z. B. Stromausfall) automatisch erneut an alle APs übertragen. Updates der Systemsoftware erfolgen eben-

falls automatisiert.

Darüber hinaus werden unter anderem folgende Funktionen unterstützt:

- Automatische Kanalplanung für überlappungsfreie Frequenzvergabe
- VLAN und Multi-SSID
- IEEE 802.11 a/b/g/n/ac
- Optimiertes Roaming für Voice over WLAN (VoWLAN)
- Programm-gesteuerte Aktionen (z. B. WLAN ausschalten während der Nacht).

Sie können mit dem WLAN Controller zum Beispiel folgende Szenarien realisieren:

- Mehrere Standorte

  Bei einem Unternehmen mit mehreren Standorten können Sie mit dem WLAN Controller alle Standorte mit WLAN ausstatten und untereinander vernetzen. Sie können für alle Mitarbeiter einen Zugang zum Intranet der Firma und zum Internet zur Verfügung stellen.
- Gäste-WLAN

  Der WLAN Controller hilft Ihnen, einen WLAN-Zugang zu Ihrem lokalen Netzwerk anzulegen und ein Gäste-WLAN einzurichten. Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum Internet haben aber keinen Zugriff auf das Intranet der Firma.

Hinweis

Wenn Sie mit dem WLAN Controller das interne WLAN-Funkmodul eines bintec-elmeg-Geräts konfigurieren und verwalten wollen, muss folgendeVoraussetzung erfüllt sein:

Die WLAN-Schnittstelle muss sich in einer Bridge-Gruppe mit der Ethernet-Schnittstelle befinden, über die das Gerät an das LAN angeschlossen ist. Dieses ist nicht bei allen Produkten in der Standardkonfiguration der Fall. Überprüfen Sie ggf. zunächst die Einstellung der Schnittstellen.

8.1 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.

8.1.1 Wireless LAN Controller Wizard

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

8.1.1.1 Grundeinstellungen

Der Wireless LAN Controller verwendet folgende Einstellungen:

Regulierungsbereich

Wählen Sie hier den Regulierungsbereich. Durch die Auswahl ergeben sich die Länder, die Sie im Anschluss für die Option **Region** auswählen können. Der Stadardwert ist hier *ETSI* (European Telecommunications Standards Institute).

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 bintec elmeg 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.

8.1.1.2 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.

8.1.1.3 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.

8.1.1.3.1 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. Mit Auswahl von *Aktiviert* 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 eine Kombination von WPA, WPA 2 bzw. WPA 3 oder eine spezifische WPA-Version 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

Bei der Verwendung von WPA-Enterprise können Sie 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.

8.1.1.4 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 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.

8.1.2 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.

8.1.2.1 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 Netzwerkkonfiguration

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 be-

Feld	Beschreibung
	treiben 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 Controller-Konfiguration

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

8.2.1 Allgemein

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Status	Aktivieren Sie die Option **Status** um die Grundeinstellungen für den Wireless LAN Controller zu konfigurieren. Standarmäßig ist die Funktion nicht aktiv.
Die gesamte Konfiguration des WLAN Controllers löschen	Nur für **Status** = nicht aktiviert. Mithilfe des Symbols 🗑 können Sie eine Konfiguration löschen.

Feld	Beschreibung
Regulierungsbereich	Wählen Sie hier den Regulierungsbereich. Durch die Auswahl ergeben sich die Länder, die Sie im Anschluss für die Option **Region** auswählen können. Der Stadardwert ist hier *ETSI* (European Telecommunications Standards Institute).
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. ein bintec elmeg Gateway als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste**->**DHCP-Server**->**DHCP Pool**->**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.

Feld	Beschreibung
	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.
Standort des verwalteten Access Points	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. Danach bootet er und anschließend synchronisieren sich Controller und AP erneut.
LED-Modus des verwalteten Access Points	Wählen Sie das Leuchtverhalten der Access Point-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 Autoprofil für Access Points

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.

8.2.2.1 Bearbeiten oder Neu

Das Menü **Wireless LAN Controller**->**Controller-Konfiguration**->**Access Point-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 Funkmodul 2

Feld	Beschreibung
Betriebsmodus	Wählen Sie aus, ob Access Points, denen das Autoprofil zugewiesen wird, das entsprechende Radiomodul aktivieren sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Aktives Funkmodul-	Nur für **Betriebsmodus** = *Aktiviert*

Feld	Beschreibung
profil	Wählen Sie ein Funkmodulprofil aus. Mögliche Werte: • *2.4 GHz Radio Profile* • *5 GHz Radio Profile*
Zugewiesene Drahtlosnetzwerke (VSS)	Nur für **Betriebsmodus** = *Aktiviert* Fügen Sie mit **Hinzufügen** ein Drahtlosnetzwerk hinzu.

8.3 Access-Point-Konfiguration

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

8.3.1 Access Points

Im Menü **Wireless LAN Controller**->**Access Point-Konfiguration**->**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

Status	Bedeutung
	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.

8.3.1.1 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**->**Access Point-Konfiguration**->**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

Feld	Beschreibung
Gerätetyp	Hier werden Ihnen verschiedene relevante Informationen zu´diesem Access Point angezeigt wie ...der Typ des verwalteten Access Points.
Seriennummer	... die Seriennummer des verwalteten Gerätes.
LAN-MAC-Adresse	... die MAC-Adresse der LAN-Schnittstelle des verwalteten Geräts.
Funkmodul 1 unterstützte Funktionen	Informationen zu den vom Access Point unterstützten Funktionen: • Frequenzbänder • Bandbreite

Feld	Beschreibung
	• Drahtloser Modus • Spatial Streams • Data-Rate Trimming • WPA 3

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.
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

Feld	Beschreibung
	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 je nach Einstellung des Modulprofils *36*, *40*, *44*, *48* und *Auto* (Standardwert)
Verwendeter Kanal	Nur für Managed APs. Zeigt den aktuell benutzten Kanal.
Sendeleistung	Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen. Mögliche Werte:

Feld	Beschreibung
	• *Max.* (Standardwert): Die maximale Antennenleistung wird verwendet. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*
Zugewiesene Drahtlosnetzwerke (VSS)	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

8.3.2 Funkmodulprofile

Im Menü **Wireless LAN Controller**->**Access Point-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**).

8.3.2.1 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**->**Access Point-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:

Feld	Beschreibung
	• *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 innerhalb oder außerhalb von Gebäuden betrieben. • *5 GHz Indoor*: Ihr Gerät wird mit 5 GHz innerhalb von Gebäuden betrieben. • *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. • *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 das **Frequenzband** = *2,4 GHz In/Outdoor* stehen Ihnen alle Modi von *802.11b* bis zum aktuellen *802.11ax* (ohne 802.11ac, das nur im 5-GHz-Modus sinnvoll ist) sowie Kombinationen davon zur Verfügung. Bedenken Sie, dass nicht alle Access Points und auch nicht alle Clients immer die neusten Modi unterstützen. Für **Frequenzband** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* oder *5,8 GHz Outdoor* stehen Ihnen alle alle Modi von *802.11a* bis zum aktuellen *802.11ax* (ohne 802.11b und g, die für 5-GHz nicht spezifiziert sind) sowie Kombinationen davon zur Verfügung. Bedenken Sie, dass nicht alle Access Points und auch nicht alle Clients immer die neusten

Feld	Beschreibung
	Modi unterstützen.
Bandbreite	Nur für **Frequenzband** = *5 GHz* und nicht **Drahtloser Modus** *802.11a*. Wählen Sie aus, wie viele Kanäle verwendet werden sollen. Mögliche Werte: • *20 MHz*: Ein Kanal mit 20 MHz Bandbreite wird verwendet. • *40 MHz*: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Haupt-Kanal und der andere als Erweiterungs-Kanal. • *80 MHz*: Vier Kanäle mit je 20 MHz Bandbreite werden verwendet. Somit steht eine Bandbreite von 80 MHz zur Verfügung.
Anzahl der Spatial Streams	Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen. Mögliche Werte: *1* bis *4*. Die verfügbaren Optionen hängen von der Kombination des Frequenzbands und des Drahtlosen Modus ebenso ab wie vom Access-Point-Modell.
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

Feld	Beschreibung
	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 sogenannte 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 mindestens 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. • *World Mode* (für **Frequenzband** = *2,4 GHz*, Standardwert): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle *1*, *6*, *11* . • *ETSI-Modus* (für **Frequenzband** = *2,4 GHz*): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle *1*, *5*, *9*, *13* . • *Keine Wetterradarkanäle* (für **Frequenzband** = *5 GHz*, Standardwert): Die Wetterradarkanäle sind von der Kanalwahl ausgeschlossen. Mögliche Werte: *36*, *40*, *44*, *48*, *52*, *56*, *60*, *64*, *100*, *104*, *108*, *112*, *116*, *132*, *136*, *140*.

Feld	Beschreibung
	• *Indoors No DFS/TPC* (für **Frequenzband** = *5 GHz*): Diese Kanäle können innerhalb von Gebäuden verwendet werden. DFS (Dynamic Frequency Selection) und TPC (Transmitter Power Control) kommen dabei nicht zum Einsatz. Mögliche Werte: *36*, *40*, *44*, *48*. • *Keine Outdoor-Kanäle* (für **Frequenzband** = *5 GHz*): In diesem Kanalplan sind die nur für Indoor-Anwendungen freigegebenen Kanäle 36 bis 64 zusammengefasst. Mit diesem Kanalplan können insbesondere 5GHz-WLAN-fähige Multimedia-Geräte wie Smart TVs optimal in das WLAN-Netz eingebunden werden, die häufig die 5GHz-Outdoor-Kanäle (ab Kanal 100) nicht unterstützen. • *Benutzerdefiniert*: Wählen Sie die gewünschten Kanäle selbst aus.
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.
Bei Störung Kanal wechseln	Aktivieren Sie diese Option, wenn der Access Point den Funkkanal ändern soll, sobald die Verbindung durch Störungen beeinträchtigt wird.
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**,

Feld	Beschreibung
	Anzahl der Spatial Streams und **Drahtloser Modus** stehen verschiedene feste Werte in MBit/s zur Auswahl.
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 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. 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.

Feld	Beschreibung
	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*.

8.3.3 Drahtlosnetzwerke (VSS)

Im Menü **Wireless LAN Controller**->**Access Point-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.

8.3.3.1 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**->**Access Point-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.

Feld	Beschreibung
	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.
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: • *OWE-Transition*

Feld	Beschreibung
	Die Einstellung *OWE-Transition* erfordert keine Eingabe eines **Preshared Key** und ist für offene Gästenetze geeignet. Es bietet sich für Netze an, die von WPA3-fähigen Clients, aber auch von älteren, nicht WPA3-fähigen, Clients genutzt werden sollen.Bei Clients, die **WPA3** unterstützen, erfolgt die Datenübertragung zwischen Access Point und Client verschlüsselt. Bei Clients, die kein **WPA3** unterstützen, erfolgt die Datenübertragung unverschlüsselt. • *OWE*
	Hinweis OWE funktioniert nur mit Endgeräten, die WPA3 und OWE unterstützen.
	Die Einstellung *OWE* erfordert keine Eingabe eines **Preshared Key** und ist für offene Gästenetze geeignet. Die Datenübertragung zwischen Access Point und Client ist dennoch verschlüsselt. • *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 Zei-

Feld	Beschreibung
	chen.
WPA-Modus	Für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* Mögliche Werte: • *WPA*: WLAN Clients, die **WPA** unterstützen, können sich verbinden. • *WPA2*: WLAN Clients, die **WPA2** unterstützen, können sich verbinden. • *WPA3*: Nur WLAN Clients, die **WPA3** unterstützen, können sich verbinden. • *WPA und WPA2* : WLAN Clients, die **WPA1** oder **WPA2** unterstützen, können sich verbinden. • *WPA2 und WPA3* (Standardwert): WLAN Clients, die **WPA2** oder **WPA3** unterstützen, können sich verbinden.
WPA Cipher	Für **Sicherheitsmodus** = *WPA-PSK* oder *WPA-Enterprise* und für **WPA-Modus** = *WPA* oder *WPA und WPA2* . Wählen Sie aus, welche Verschlüsselung Sie anwenden wollen. Mögliche Werte: • *AES* : AES wird angewendet. • *TKIP*: TKIP wird angewendet • *AES und TKIP* (Standardwert): AES oder TKIP werden angewendet.
WPA2 Cipher	Für **Sicherheitsmodus** = *WPA-PSK* oder *WPA-Enterprise* und für **WPA-Modus** = *WPA2* oder *WPA und WPA2* Wählen Sie aus, welche Verschlüsselung Sie anwenden wollen. Mögliche Werte: • *AES* : AES wird angewendet. • *AES und TKIP* (Standardwert): AES oder TKIP werden angewendet.
WPA2/3 Cipher	Für **Sicherheitsmodus** = *WPA-PSK* oder

Feld	Beschreibung
	und für **WPA-Modus** = *WPA2 und WPA3* wird lediglich eine Verschlüsselung mit AES unterstützt. Weitere Einstellungen sind nicht erforderlich.
WPA3 Cipher	Für **Sicherheitsmodus** = *WPA-PSK* oder *WPA-Enterprise* und für **WPA-Modus** = *WPA3* wird eine Verschlüsselung mit AES in folgenden Varianten unterstützt: • AES • AES-GCMP • AES-256 • AES-GCMP-256.
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!
RADIUS-Server	Nur für **Sicherheitsmodus** = *WPA-Enterprise*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.

Feld	Beschreibung
	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	Wählen Sie aus, ob das 5-GHz-Band bevorzugt verwendet werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming*: das 5-GHz-Band wird nicht bevorzugt verwendet, Fast Roaming kommt zum Einsatz. • *5-GHz-Band bevorzugt*: Das 5-GHz-Band soll - wenn möglich - bevorzugt verwendet werden.  **Hinweis** Wenn Sie die Einstellung *5GHz-Band bevorzugt* verwenden, müssen Sie in beiden Client-Bändern denselben Netzwerknamen (SSID) konfigurieren. • *AP Steering* (Access Point Steering): Beim Access Point Steering wird ein WLAN Client ggf. nicht nur in ein anderes Frequenzband, sondern auch an einen anderen Access Point verwiesen. Voraussetzung hierfür ist die Aktivierung von 802.11k/v.
Schneller BSS-Übergang (802.11r)	802.11r ermöglicht auch bei stark verschlüsselten WLAN-Netzen eine unterbrechungsfreie Verbindung, wenn der WLAN-Client von einem zum einen anderen Access Point wechselt.
Verwaltung der Funkressourcen (802.11k) und **Netzwerkunterstütztes Roaming (802.11v)**	802.11k/v tauscht Informationen zwischen WLAN Clients und WLAN Access Points aus und steuert auf Basis dieser Informationen die Lastverteilung zwischen mehreren Access Points effizienter. Diese beiden Optionen werden in der Regel zusammen aktiviert, lassen sich aber auch getrennt voneinander konfigurieren. Dabei regelt 802.11v den Austausch der Informationen über die aktuelle Netzwerktopologie, während 802.11k das intelligente Client Roaming auf Basis der Topologiedaten regelt.

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.

Feld	Beschreibung
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) • *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 Data-Rate Trimming

Feld	Beschreibung
Geschwindigkeitsprofil im 2,4-GHz-Band	Mit Data-Rate Trimming können Sie bei Bedarf die WLAN-Leistung verbessern. Sie können niedrige Datenübertragungsraten blockieren und damit erzwingen, dass ausschließlich höhere Datenraten verwendet werden. Clients, die mit niedrigeren Übertragungsgeschwindigkeiten andere Clients behindern, werden vom Access Point abgemeldet. Wählen Sie das Profil mit den Geschwindigkeiten aus, das für die Clients freigegeben werden soll. Mögliche Werte: • *Alle (Min. 1 MBit/s)* - Alle Clients, die eine Übertragungsgeschwindigkeit von 1 MBit/s aufrecht erhalten können, können sich am Access Point anmelden.

Feld	Beschreibung
	• *Min. 6 MBit/s (keine 802.11b-Geräte)* - s.o. für Clients mit 6 Mbit/s Mindestgeschwindigkeit; Clients, die nach dem veralteten Standard 802.11b arbeiten, werden nicht zugelassen. • *Min. 12 MBit/s (keine 802.11b-Geräte)* - s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit • *Min. 24 MBit/s (keine 802.11b-Geräte)* - s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit
Geschwindigkeitsprofil im 5-GHz-Band	Mögliche Werte: • *Alle (Min. 6 MBit/s)* - Alle Clients, die eine Übertragungsgeschwindigkeit von 6 MBit/s aufrecht erhalten können, können sich am Access Point anmelden. • *Ab 12 MBit/s* - s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit • *Ab 24 MBit/s* - s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit

Felder im Menü Unteren RSSI-Schwellwert verwalten

Feld	Beschreibung
RSSI-Schwellwert	Mithilfe des Parameters RSSI Schwellwert können Sie einen Grenzwert für den Signalpegel definieren. Wenn ein Access Point „sieht“, dass einer seiner Clients länger als unter der Toleranzzeit angegeben diesen Signalpegel unterschreitet, stellt er die Kommunikation zu ihm ein. Der Client wird dadurch gezwungen, sich einen neuen Access Point zu suchen, d. h. zu prüfen, welcher Access Point das beste Signal liefert und sich mit ihm zu verbinden. Geben Sie den unteren RSSI-Schwellwert in dBm an. Wenn dieser Wert länger als unter der Toleranzzeit angegeben unterschritten wird, so stellt der Access Point die Kommunikation zum betroffenen Client ein. Der Standardwert ist *-110* dBm.
Toleranzzeit	Geben Sie die Zeit in Sekunden ein, während der die Datenübertragungsrate unter den RSSI-Schwellwert sinken darf, ohne dass der Client mit Konsequenzen rechnen muss.

Feld	Beschreibung
	Der Standardwert ist *5* Sekunden.

8.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

Hinweis

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

8.4.1 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.
Access Points, die mit der aktuell installierten Lizenz verwaltet werden können	bintec-elmeg-Geräte verfügen ab Werk über eine freie Lizenz zur Verwaltung von Access Points. Der Anzahl der verwaltbaren Access Points ist dabei von Gerätetyp zu Gerätetyp unterschiedlich.
Maximal Anzahl an Access Points, die von diesem Gerät mit einer vollen Lizenz verwaltet werden können	Aufgrund unterschiedlicher Hardwareausstattung können bintec-elmeg-Geräte eine bestimmte Anzahl von Access Points verwalten.
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/	Zeigt die Anzahl der verbundenen Clients pro Drahtlosnetzwerk

Status	Bedeutung
VSS	(VSS) zeitabhängig an.

8.4.2 Access Points

Im Menü **Wireless LAN Controller**->**Monitoring**->**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 **Access Points**.

8.4.2.1 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.

8.4.2.2 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.

8.4.3 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 Access Points, **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.
Anmeldung	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.

8.4.4 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 Access Points**, **VSS**, **MAC-Adresse (VSS)**, **Kanal**, **Status**).

8.4.5 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.

8.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Acces Points und Clients.

8.5.1 Eigene Access Points

Dieses Menü zeigt Informationen über die vom Controller verwalteten Access Points an, wie sie sich gegenseitig "sehen". Dies liefert nützliche Informationen über das von den verwalteten Access Points gebildete Netzwerk und hilft Ihnen bei der Identifizierung potenzieller WLAN-Probleme.

Das Menü enthält Informationen wie den Namen des Access Points, den Kanal, auf dem er arbeitet, seine Signalstärke und wann er von welchem Access Point und auf welchem Kanal zuletzt gesehen wurde.

8.5.2 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** , **Summe der Erkennungen**.

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.

8.5.3 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.

8.5.4 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**->**Access Point-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	Zeigt den betroffenen AP an.

Status	Bedeutung
Point	
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 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.

8.5.4.1 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.

8.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

8.6.1 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. 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** =

Feld	Beschreibung
	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.

9 Netzwerk

9.1 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.

9.1.1 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** = *192.168.0.0*, **Netzmaske** = *255.255.255.0*,**Gateway** = *192.168.0.250*, **Schnittstelle** = *LAN_EN1-0*, **Routentyp** = *Netzwerkroute via Schnittstelle* angezeigt,

9.1.1.1 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 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-Infor-

Feld	Beschreibung
	mationen 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.

Feld	Beschreibung
	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* 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.

Feld	Beschreibung
	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: • *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.

Feld	Beschreibung
	• *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 benutz-

Feld	Beschreibung
	bar, 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" 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.

9.1.2 Konfiguration von IPv6-Routen

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

9.1.2.1 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.

Feld	Beschreibung
	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. 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.

Feld	Beschreibung
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*.

9.1.3 IPv4-Routing-Tabelle

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

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = *192.168.0.0*, **Netzmaske** = *255.255.255.0*,**Gateway** = *192.168.0.250*, **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*)

Feld	Beschreibung
	oder über eins der verfügbaren Protokolle.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

9.1.4 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 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.

9.1.5 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.

9.2 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 110 sowie die für IPv6 relevanten Parameter im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**.

9.2.1 Konfiguration eines Allgemeinen Präfixes

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

9.2.1.1 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

Feld	Beschreibung
	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*. • **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.
Präfixlänge	Für einen dynamisch bezogenen Präfix müssen Sie hier lediglich die Präfixlänge eingeben. Sie können die Länge des zugewiesenen Präfixes ggf. bei Ihrem Dienstanbieter erfragen. Standardmäßig ist hier eine Länge von *56* vorgegeben.

9.3 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 182).

Konkrete Hinweise für die Konfiguration von NAT finden Sie am Ende des Kapitels unter *NAT - Konfigurationsbeispiel* auf Seite 188.

9.3.1 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.

9.3.2 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.

9.3.2.1 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-

Feld	Beschreibung
	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 wer-

Feld	Beschreibung
	den. 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*

Feld	Beschreibung
	• *IPv6* • *IPX in IP* • *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.

Feld	Beschreibung
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-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)* bzw. *ausgehend (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:

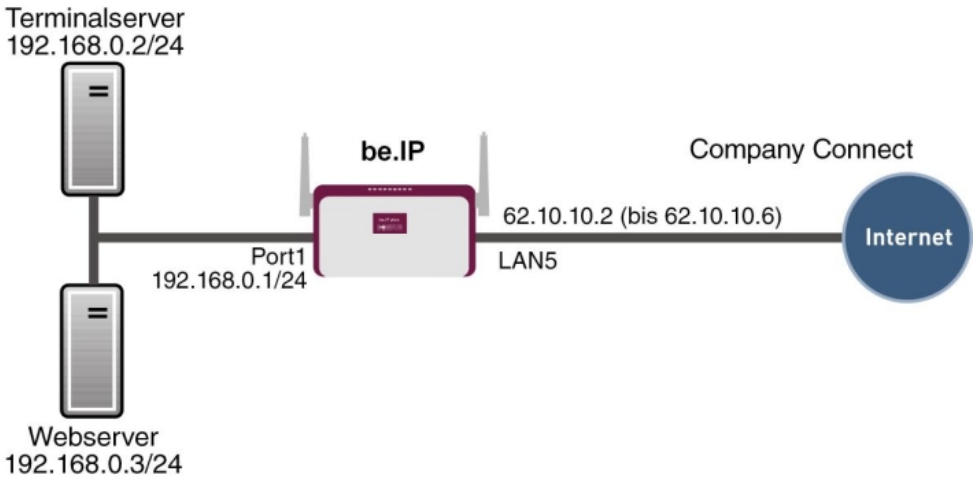
Feld	Beschreibung
	• *Original Quell-Port/Bereich verwenden*: Der in **Original Quell-Port/Bereich** angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten. • *Verwende Port/Bereich beginnend bei*: Es erscheint ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

9.3.3 NAT - Konfigurationsbeispiel

Voraussetzungen

- Grundkonfiguration des Gateways
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang, hier als Beispiel **Company Connect** mit acht IP-Adressen.
- Die Ethernet-Schnittstelle **LAN5** Ihres Geräts ist an den Zugangsrouter zum Internet (IP-Adresse *62.10.10.1/29*) angeschlossen.
- Die IP-Adressen *62.10.10.2* bis *62.10.10.6* sind auf der Ethernet-Schnittstelle **LAN5** eingetragen.

Beispielszenario



Konfigurationsziel

- Sie konfigurieren NAT-Freigaben, damit Sie per HTTP auf Ihr Gateway zugreifen können.
- Sie wollen auf Ihren Terminalserver und auf den Firmen-Webserver über das Internet zugreifen können.

Konfigurationsschritte im Überblick

NAT einschalten

Feld	Menü	Wert
NAT aktiv	**Netzwerk->NAT->NAT-Schnittstellen**	Aktiviert für *LAN_EN5-0*
Verwerfen ohne Rückmeldung	**Netzwerk->NAT->NAT-Schnittstellen**	Aktiviert für *LAN_EN5-0*

NAT-Freigabe für GUI

Feld	Menü	Wert
Beschreibung	**Netzwerk->NAT->NAT-Konfiguration->Neu**	z. B. *GUI*
Schnittstelle	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*LAN_EN5-0*
Art des Datenverkehrs	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*eingehend (Ziel-NAT)*
Dienst	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Benutzerdefiniert*
Protokoll	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*TCP*
Quell IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Beliebig*
Original Ziel-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Host*, z. B. *62.10.10.2*
Original Ziel-Port/Bereich	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Port angeben* , *80*
Neue Ziel-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Host*, z. B. *127.0.0.1*
Neuer Ziel-Port	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Original* deaktiviert, *80*

Webserver

Feld	Menü	Wert
Beschreibung	**Netzwerk->NAT->NAT-**	z. B. *Webserver*

Feld	Menü	Wert
	Konfiguration->Neu	
Schnittstelle	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*LAN_EN5-0*
Art des Datenverkehrs	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*eingehend (Ziel-NAT)*
Dienst	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*http*
Quell-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Beliebig*
Original Ziel-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Host*, z. B. *62.10.10.3*
Neue Ziel-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Host*, z. B. *192.168.0.3*
Neuer Ziel-Port	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Original*

Terminal Server

Feld	Menü	Wert
Beschreibung	**Netzwerk->NAT->NAT-Konfiguration->Neu**	z. B. *Terminal-Server*
Schnittstelle	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*LAN_EN5-0*
Art des Datenverkehrs	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*eingehend (Ziel-NAT)*
Dienst	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Benutzerdefiniert*
Protokoll	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*TCP*
Quell-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Beliebig*
Original Ziel-IP-Adresse/Netzmaske	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Host*, z. B. *62.10.10.4*
Original Ziel-Port/Bereich	**Netzwerk->NAT->NAT-Konfiguration->Neu**	*Port angeben*, *3389*
Neue Ziel-	**Netzwerk->NAT->NAT-**	*Host*, z. B.

Feld	Menü	Wert
IP-Adresse/Netzmaske	**Konfiguration**->**Neu**	*192.168.0.2*
Neuer Ziel-Port	**Netzwerk**->**NAT**->**NAT-Konfiguration**->**Neu**	*Original*

9.4 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.

Konkrete Hinweise für die Konfiguration von Lastverteilung finden Sie unter *Lastverteilung - Konfigurationsbeispiel* auf Seite 198.

9.4.1 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.

9.4.1.1 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 Datenrate, 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.

Feld	Beschreibung
	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

Feld	Beschreibung
	Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen 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

Feld	Beschreibung
	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*) .

9.4.2 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.

9.4.2.1 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)

Feld	Beschreibung
	• *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 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.

Feld	Beschreibung
	Der Standardwert ist *900* Sekunden.

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

Felder im Menü Erweiterte Einstellungen

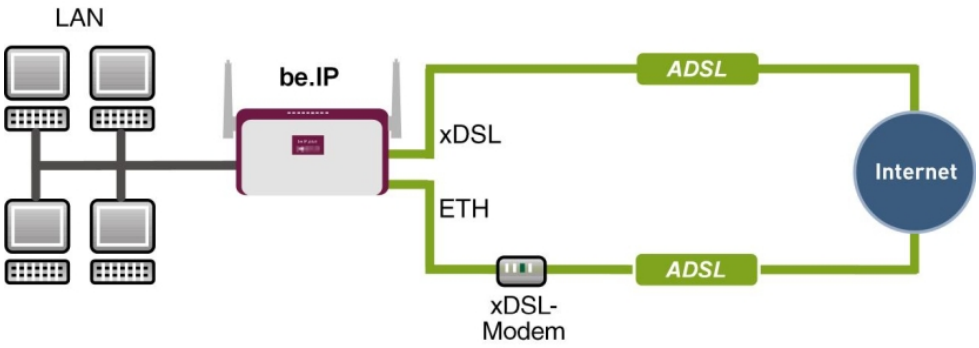
Feld	Beschreibung
Unveränderliche Parameter	Legen Sie fest, ob die beiden Parameter **Zieladresse** und **Zielport** bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d. h. ob die nachfolgenden Datenpakete über denselben **Zielport** zur selben **Zieladresse** 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.

9.4.3 Lastverteilung - Konfigurationsbeispiel

Voraussetzungen

- Gateway mit integriertem xDSL-Modem
- Externes xDSL-Modem
- Zwei unabhängige xDSL-Internetverbindungen

Beispielszenario



Konfigurationsziel

- Der Datenverkehr wird auf Basis von IP-Sitzungen jeweils zur Hälfte auf die beiden ADSL-Leitungen verteilt.
- Wie Verbindungsabbrüche vermieden werden, welche durch die Verteilung auf verschiedene Internetzugänge auftreten können, zeigen wir Ihnen am Beispiel von verschlüsselten HTTP-Verbindungen (HTTPS).

Hinweis

Beim Aufbau der ADSL-Verbindungen bezieht das Gateway neben der öffentlichen IP-Adresse auch die IP-Adressen der DNS-Server zur Namensauflösung von dem konfigurierten Internet-Provider. Vor allem bei der Verwendung von unterschiedlichen Internet-Providern müssen die DNS-Server verbindungsspezifisch verwendet werden. Die Konfiguration der DNS-Server wird beim Anlegen der ADSL-Verbindungen automatisch erstellt und kann im Menü **Lokale Dienste**->**DNS**->**DNS-Server** eingesehen werden.

Konfigurationsschritte im Überblick

Erste Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	**Assistenten**->**Internetzugang**->**Internetverbindungen**->**Neu**	*Internes ADSL-Modem*
Beschreibung	**Assistenten**->**Internetzugang**->**Internetverbindunge**->**Neu**->**Weiter**	z. B. *ADSL-1*
Typ	**Assistenten**->**Internetzugang**->**Internetverbindunge**->**Neu**->**Weiter**	*Benutzerdefiniert über PPPoE (PPP über Ethernet)*

Feld	Menü	Wert
Benutzername	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	z. B. *fester_ip@provider.de*
Passwort	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	z. B. *test12345*

Hinweis

Der Hinweis beim Anlegen der zweiten ADSL-Verbindung kann ignoriert werden. Routingkonflikte aufgrund mehrerer Standardrouten werden durch IP-Lastverteilung verhindert.

Zweite Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	**Assistenten->Internetzugang->Internetverbindungen->Neu**	*Externes xDSL-Modem*
Beschreibung	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	z. B. *ADSL-2*
Physischer Ethernet-Port	**Assistenten -> Internetzugang->Internetverbindungen->Neu->Weiter**	z. B. *ETH5*
Typ	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	*Benutzerdefiniert*
Benutzername	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	z. B. *#0001@t-online.de*
Passwort	**Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter**	z. B. *test12345*

Lastverteilungsgruppe anlegen

Feld	Menü	Wert
Gruppenbeschreibung	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**	z. B. *Internetzugang*
Verteilungsrichtlinie	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**	*Sitzungs-Round-Robin*
Verteilungsmodus	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**	*Immer*
Schnittstelle	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen**	*WAN_ADSL-1*
Verteilungsverhält-	**Netzwerk->Lastverteilung->Lastvertei-**	*50*

Feld	Menü	Wert
nis	**lungsgruppen->Neu->Hinzufügen**	
Schnittstelle	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen**	*WAN_ADSL-2*
Verteilungsverhältnis	**Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen**	*50*

Special Session Handling

Feld	Menü	Wert
Beschreibung	**Netzwerk->Lastverteilung->Special Session Handling->Neu**	z. B. *HTTPS*
Dienst	**Netzwerk->Lastverteilung->Special Session Handling->Neu**	*http (SSL)*
Special Handling Timer	**Netzwerk->Lastverteilung->Special Session Handling->Neu**	*900* Sekunden

9.5 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

9.5.1 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**.

9.5.1.1 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. Mögliche Werte: • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-

Feld	Beschreibung
	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

Feld	Beschreibung
	sind nicht näher spezifiziert. • *Host*: Geben Sie die Quell-IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Quell-Netzwerk-Adresse und die zugehörige Netzmaske 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* 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

Feld	Beschreibung
	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*.

9.5.2 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.

9.5.2.1 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. • *<Name des Klassenplans>*: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können.

Feld	Beschreibung
	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**->**QoS-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.

Feld	Beschreibung
	 **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 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.
Setze 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*

Feld	Beschreibung
	Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.

9.5.3 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.

9.5.3.1 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.

Feld	Beschreibung
Priorisierungsalgorithmus	Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten 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

Feld	Beschreibung
	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* • *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 Con-	Nur für **Traffic Shaping** = aktiviert

Feld	Beschreibung
trol	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 ge-

Feld	Beschreibung
	wählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und 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*

Feld	Beschreibung
	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.
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.

Feld	Beschreibung
	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 Pa-

Feld	Beschreibung
	ket 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 Datenstau (RED)	Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen. 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*.

9.6 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 Zu-

gangsentscheidung 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 ein bintec elmeg-Gateway 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 über die serielle Konsolen-Schnittstelle (nicht für alle Geräte verfügbar) oder mit ISDN-Login auf Ihr Gateway zu.

9.6.1 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.

9.6.1.1 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*

Feld	Beschreibung
	• *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 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-

Feld	Beschreibung
	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: • *-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

Feld	Beschreibung
	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 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 For-

Feld	Beschreibung
	mat 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*. Der Standardwert ist *Nicht beachten*.

9.6.2 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.

9.6.2.1 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.

Feld	Beschreibung
	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 zutrifft*: 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.

9.6.3 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.

9.6.3.1 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.

9.7 Drop-In

Mit dem Drop-In-Modus können Sie ein Netzwerk in mehrere Segmente aufteilen, ohne das IP-Netzwerk in Subnetze teilen zu müssen. Dazu können mehrere Schnittstellen in einer Drop-In-Gruppe zusammengefasst und einem Netzwerk zugeordnet werden. Alle Schnittstellen sind dann mit der gleichen IP-Adresse konfiguriert.

Die Netzwerkkomponenten eines Segments, die an einem Anschluss angeschlossen sind, können dann gemeinsam z. B. mit einer Firewall geschützt werden. Der Datenverkehr von Netzwerkkomponenten zwischen einzelnen Segmenten, die unterschiedlichen Ports zugeordnet sind, wird dann entsprechend der konfigurierten Firewall-Regeln kontrolliert.

9.7.1 Drop-In-Gruppen

Im Menü **Netzwerk**->**Drop-In**->**Drop-In-Gruppen** wird eine Liste aller konfigurierten **Drop-In-Gruppen** angezeigt. Eine **Drop-In**-Gruppe repräsentiert jeweils ein Netzwerk.

9.7.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere **Drop-In-Gruppen** einzurichten.

Das Menü **Netzwerk**->**Drop-In**->**Drop-In-Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine eindeutige Bezeichnung für die **Drop-In**-Gruppe ein.
Modus	Wählen Sie, welcher Modus für die Übermittlung der MAC-Adressen von Netzwerkkomponenten verwendet werden soll. Mögliche Werte: • *Transparent* (Standardwert): ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet. • *Proxy*: ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden mit der MAC-Adresse der entsprechenden Schnittstelle weitergeleitet.
Vom NAT ausnehmen (DMZ)	Hier können Sie Datenverkehr von NAT ausnehmen. Verwenden Sie diese Funktion, um zum Beispiel die Erreichbarkeit bestimmter Web-Server in einer DMZ sicherzustellen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Netzwerkkonfiguration	Wählen Sie aus, auf welche Weise dem **Drop-In**-Netzwerk eine IP-Adresse/Netzmaske zugewiesen wird. Mögliche Werte: • *Statisch* (Standardwert) • *DHCP*
Netzwerkadresse	Nur für **Netzwerkkonfiguration** = *Statisch* Geben Sie die Netzwerkadresse des **Drop-In**-Netzwerks ein.

Feld	Beschreibung
Netzmaske	Nur für **Netzwerkkonfiguration** = *Statisch* Geben Sie die zugehörige Netzmaske ein.
Lokale IP-Adresse	Nur für **Netzwerkkonfiguration** = *Statisch* Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss für alle Ethernet-Ports eines Netzwerks identisch sein.
DHCP Client an Schnittstelle	Nur für **Netzwerkkonfiguration** = *DHCP* Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wählen, die als DHCP-Client agieren soll. Diese Einstellung benötigen Sie zum Beispiel, wenn der Router Ihres Providers als DHCP-Server dient. Sie können unter den Schnittstellen wählen, welche Ihr Gerät zur Verfügung stellt, die Schnittstelle muss jedoch Mitglied der Drop-In-Gruppe sein.
ARP Lifetime	Legt die Zeitspanne fest, während derer ARP-Einträge im Cache gehalten werden. Der Standardwert ist *3600* Sekunden.
DNS-Zuweisung über DHCP	Das Gateway kann DHCP-Pakete, die die Drop-In-Gruppe durchlaufen, modifizieren und sich selbst als angebotenen DNS-Server eintragen. Mögliche Werte: • *Unverändert* (Standardwert) • *Eigene IP-Adresse*
Schnittstellenauswahl	Wählen Sie alle Ports aus, die in der **Drop-In**-Gruppe (im Netzwerk) enthalten sein sollen. Fügen Sie mit **Hinzufügen** weitere Einträge hinzu.

10 Routing-Protokolle

10.1 RIP

Die Einträge in der Routing-Tabelle können entweder statisch festgelegt werden oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Geräten. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol). Standardmäßig ungefähr alle 30 Sekunden (dieser Wert kann in **Aktualisierungstimer** verändert werden) sendet ein Gerät Meldungen zu entfernten Netzwerken, wobei es Informationen aus seiner eigenen aktuellen Routing-Tabelle verwendet. Dabei wird immer die gesamte Routing-Tabelle ausgetauscht. Mit Triggered RIP findet nur ein Austausch statt, wenn sich Routing Informationen geändert haben. In diesem Fall werden nur die geänderten Informationen versendet.

Durch Beobachtung der Informationen, die von anderen Geräten verschickt werden, werden neue Routen und kürzere Wege für bestehende Routen in der Routing-Tabelle gespeichert. Da Routen zwischen Netzwerken unerreichbar werden können, entfernt RIP Routen, die älter als 5 Minuten sind (d. h Routen, die in den letzten 300 Sekunden - **Garbage Collection Timer** + **Routentimeout** - nicht verifiziert wurden). Mit Triggered RIP gelernte Routen werden jedoch nicht gelöscht.

Ihr Gerät unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

10.1.1 RIP-Schnittstellen

Im Menü **Routing-Protokolle**->**RIP**->**RIP-Schnittstellen** wird eine Liste aller RIP-Schnittstellen angezeigt.

10.1.1.1 Bearbeiten

Für jede RIP-Schnittstelle sind über das -Menü die Optionen *Version in Senderichtung*, *Version in Empfangsrichtung* und *Routenankündigung* auswählbar.

Das Menü **Netzwerk**->**RIP**->**RIP-Schnittstellen**-> besteht aus folgenden Feldern:

Felder im Menü RIP-Parameter für

Feld	Beschreibung
Version in Senderich-	Entscheiden Sie, ob über RIP Routen propagiert werden sollen,

Feld	Beschreibung
tung	und wenn ja, wählen Sie die RIP-Version für das Senden von RIP-Paketen über die Schnittstelle in Senderichtung aus. Mögliche Werte: • *Keine* (Standardwert): RIP ist nicht aktiv. • *RIP V1*: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • *RIP V2*: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • *RIP V1/V2*: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • *RIP V2 Multicast*: Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9. • *RIP V1 Triggered*: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • *RIP V2 Triggered*: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP).
Version in Empfangs-richtung	Entscheiden Sie, ob über RIP Routen importiert werden sollen und wenn ja, wählen Sie die RIP-Version für das Empfangen von RIP-Paketen über die Schnittstelle in Empfangsrichtung aus. Mögliche Werte: • *Keine* (Standardwert): RIP ist nicht aktiv. • *RIP V1*: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • *RIP V2*: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • *RIP V1/V2*: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • *RIP V1 Triggered*: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • *RIP V2 Triggered*: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet

Feld	Beschreibung
	(Triggered RIP).
Routenankündigung	Wählen Sie aus, wann ggf. aktivierte Routing-Protokolle (z. B. RIP) die für diese Schnittstelle definierten IP-Routen propagieren sollen. Beachten Sie: Diese Einstellung hat keinen Einfluss auf die oben erwähnte Schnittstellen-spezifische RIP-Konfiguration. Mögliche Werte: • *Aktiv oder Ruhend* (nicht für LAN-Schnittstellen, Schnittstellen im Bridge-Modus und Schnittstellen für Standleitungen): Routen werden propagiert, wenn der Status der Schnittstelle auf aktiv oder bereit steht. • *Nur aktiv* (Standardwert): Routen werden nur propagiert, wenn der Status der Schnittstelle auf aktiv steht. • *Immer*: Routen werden immer propagiert unabhängig vom Betriebsstatus.

10.1.2 RIP-Filter

Im diesem Menü können Sie exakt festlegen, welche Routen exportiert oder importiert werden sollen oder nicht.

Hierbei können Sie nach folgenden Strategien vorgehen:

- Sie deaktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Der Import bzw. Export aller anderen Routen, die nicht aufgeführt werden, bleibt erlaubt.
- Sie aktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Dann müssen Sie den Import bzw. Export aller anderen Routen auch explizit deaktivieren. Dieses erreichen Sie mittels eines Filters für **IP-Adresse/Netzmaske** = kein Eintrag (dies entspricht der IP-Adresse 0.0.0.0 mit der Netzmaske 0.0.0.0). Damit dieses Filter als letztes angewendet wird, muss es an der niedrigsten Position eingeordnet werden.

Ein Filter für eine Standard-Route konfigurieren Sie mit folgenden Werten:

- **IP-Adresse/Netzmaske** = für IP-Adresse keine Eintrag (dies entspricht der IP-Adresse 0.0.0.0), für Netzmaske = 255.255.255.255

Im Menü **Routing-Protokolle**->**RIP**->**RIP-Filter** wird eine Liste aller RIP-Filter angezeigt.

Mit der Schaltfläche ≡+ können Sie vor dem Listeneintrag ein weiteres Filter einfügen. Es

öffnet sich das Konfigurationsmenü zum Erstellen eines neuen Filters.

Mit der Schaltfläche ↑↓ können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position das Filter verschoben werden soll.

10.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere RIP-Filter einzurichten.

Das Menü **Routing-Protokolle**->**RIP**->**RIP-Filter**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie aus, für welche Schnittstelle die zu konfigurierende Regel gilt.
IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske ein, auf welche die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen. Die Regeln für eingehende und ausgehende RIP-Pakete (Importieren oder Exportieren) müssen für dieselbe IP-Adresse getrennt konfiguriert werden. Sie können einzelne Host-Adressen ebenso angeben wie Netzadressen.
Richtung	Wählen Sie aus, ob das Filter für das Exportieren oder das Importieren von Routen gilt. Mögliche Werte: • *Importieren* (Standardwert) • *Exportieren*
Metrik-Offset für Aktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Aktiv" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Aktiv" ist. Mögliche Werte sind *-16* bis *16*. Der Standardwert ist *0*.
Metrik-Offset für Inakti-	Wählen Sie den Wert aus, der der Metrik der Route beim Import

Feld	Beschreibung
ve Schnittstellen	hinzugefügt werden soll, wenn der Status der Schnittstelle "Ruhend" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Ruhend" ist. Mögliche Werte sind *-16* bis *16*. Der Standardwert ist *0*.

10.1.3 RIP-Optionen

Das Menü **Routing-Protokolle**->**RIP**->**RIP-Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale RIP-Parameter

Feld	Beschreibung
RIP-UDP-Port	Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass Ihr Gerät auf einem Port sendet und lauscht, den keine weiteren Geräte benutzen. Der Standardwert *520* sollte eingestellt bleiben.
Standardmäßige Routenverteilung	Wählen Sie aus, ob die Standard-Route Ihres Geräts über RIP-Updates propagiert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Poisoned Reverse	Wählen Sie das Verfahren zur Verhinderung von Routing-Schleifen. Bei Standard RIP werden die gelernten Routen über alle Schnittstellen mit aktiviertem RIP SENDEN propagiert. Bei **Poisoned Reverse** propagiert Ihr Gerät jedoch über die Schnittstelle, über die es die Routen gelernt hat, diese mit der Metrik (Next Hop Count) 16 (="Netz ist nicht erreichbar"). Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
RFC 2453-Variabler Ti-	Wählen Sie aus, ob für die in RFC 2453 beschriebenen Timer

Feld	Beschreibung
mer	diejenigen Werte verwendet werden sollen, die Sie im Menü **Timer für RIP V2 (RFC 2453)** konfigurieren können. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn Sie die Funktion deaktivieren, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.
RFC 2091-Variabler Timer	Wählen Sie aus, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü **Timer für Triggered RIP (RFC 2091)** konfigurieren können. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Felder im Menü Timer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	Nur für **RFC 2453-Variabler Timer** = *Aktiviert* Nach Ablauf dieses Zeitraums wird eine RIP-Aktualisierung gesendet. Der Standardwert ist *30* (Sekunden).
Routentimeout	Nur für **RFC 2453-Variabler Timer** = *Aktiviert* Nach der letzten Aktualisierung einer Route wird der Routentimeout aktiv. Nach dessen Ablauf wird die Route deaktiviert und der Garbage Collection Timer gestartet. Der Standardwert ist *180* (Sekunden).
Garbage Collection Timer	Nur für **RFC 2453-Variabler Timer** = *Aktiviert* Der Garbage Collection Timer wird gestartet, sobald der Routentimeout abgelaufen ist.

Feld	Beschreibung
	Nach Ablauf dieses Zeitraums wird die ungültige Route aus der IPROUTETABLE gelöscht, sofern keine Aktualisierung für die Route erfolgt. Der Standardwert ist *120* (Sekunden).

Felder im Menü Timer für Triggered RIP (RFC 2091)

Feld	Beschreibung
Hold Down Timer	Nur für **RFC 2091-Variabler Timer** = *Aktiviert* Der Hold Down Timer wird aktiv, sobald Ihr Gerät eine unerreichbare Route (Metric 16) erhält. Nach Ablauf dieses Zeitraums wird die Route ggf. gelöscht. Der Standardwert ist 120 (in Sekunden).
Retransmission Timer	Nur für **RFC 2091-Variabler Timer** = *Aktiviert* Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft. Der Standardwert ist 5 (in Sekunden).

10.2 OSPF

Open Shortest Path First (OSPF) ist ein dynamisches Routing-Protokoll, das häufig in größeren Netzwerken als Alternative zu RIP angewendet wird. Es wurde ursprünglich dazu entwickelt, einige Einschränkungen des RIP zu umgehen (wenn es in größeren Netzwerken verwendet wird).

Einige Probleme (mit RIP), die OSPF umgeht sind:

- Verringerte Netzwerklast: Nach einer kurzen Initialisierungsphase werden Routing Informationen nicht wie mit RIP periodisch übertragen, sondern nur geänderte Routing Informationen.
- Authentifizierung: Zur Erhöhung der Sicherheit beim Austausch von Routing Informationen kann eine Gateway-Authentifizierung konfiguriert werden.
- Routing Traffic Kontrolle: Um den Traffic, der durch Austausch von Routing Informationen entsteht, zu begrenzen, können Gateways zu Areas zusammengefasst werden.
- Verbindungskosten: Im Unterschied zu RIP wird für die Kalkulation der Verbindungskos-

ten nicht die Anzahl der Next Hops berücksichtigt, sondern die Bandbreite des jeweiligen Transportmediums.

- Keine Einschränkung der Hop-Anzahl: Die Einschränkung der maximalen Hop-Anzahl 16 bei RIP besteht für OSPF nicht.

Obwohl das OSPF-Protokoll wesentlich komplexer ist als RIP, ist das Grundkonzept dasselbe, d.h. auch OSPF ermittelt zur Weiterleitung der Pakete den jeweils besten Weg.

OSPF ist ein Interior Gateway Protocol, das verwendet wird um Routing Informationen innerhalb eines autonomen Systems (Autonomous System, AS) zu verteilen. Durch Fluten werden Link State Updates zwischen den Gateways ausgetauscht. Jede Änderung der Routing Informationen wird an alle Gateways im Netzwerk weitergegeben. OSPF-Bereiche (Areas) werden definiert, um die Anzahl an Link State Updates einzugrenzen. Alle Gateways einer Area haben eine übereinstimmende Link State Datenbank.

Eine Area ist interface-spezifisch. Gateways, deren Interfaces zu mehreren Areas gehören und diese an den Backbone anbinden werden Area Border Router (ABR) genannt. ABRs enthalten daher die Informationen der Backbone Area und aller angebunden Areas. Ein Gateway, dessen Interfaces alle in einer Area eingebunden sind, werden Internal Router (IR) genannt.

Man unterscheidet vier Arten von Link State Paketen: Router Links geben den Status der Interfaces eines Gateways an, die zu einer bestimmt Area gehören. Summary Links werden vom ABR generiert und definiert, wie die Informationen zur Erreichbarkeit im Netzwerk zwischen Areas ausgetauscht werden. In der Regel werden alle Informationen in die Backbone-Area gesendet, welche dann die Informationen an die anderen Areas weiterleitet. Network Links werden vom Designated Router (DS) innerhalb eines Segments verschickt und propagieren alle Gateways, die an ein bestimmtes Multi-Access Segment wie Ethernet, Token Ring und FDDI (auch NBMA) angebunden sind. External Links weisen auf Netzwerke ausserhalb des AS. Diese Netzwerke werden in das OSPF mittels Redistribution eingebunden. Ein Autonomous System Border Router (ASBR) hat in diesem Falle die Aufgabe, diese externen Routen in das AS einzubinden.

Zur Erhöhung der Sicherheit ist es möglich, die OSPF Pakete authentifizieren zu lassen, so dass die Gateways mittels vorgegebener Passwörter an Routing Domänen teilnehmen können.

In grösseren Netzwerken wird empfohlen, mehrere Areas zu definieren. Wenn mehr als eine Area angelegt wird, muss eine dieser Areas die Area ID 0.0.0.0 besitzen, die die Backbone Area definiert. Diese muss zentraler Punkt aller Areas sein, d.h. alle Areas müssen physikalisch mit der Backbone Area verbunden sein. In seltenen Fällen können Gateways nicht direkt physikalisch an die Backbone Area angebunden werden. Dann müssen virtuelle Links eingerichtet werden.

Der Verwendungszweck von Virtuellen Links ist die Anbindung von Areas, bei denen keine physikalische Anbindung an den Backbone möglich ist und das Aufrechterhalten der Ver-

bindung des Backbone im Falle eines Ausfalls der 0.0.0.0 Area.

Summarizing wird die Konsolidierung verschiedener Routen zu einem einzigen Advertisment (Summary Link) genannt. Dieses geschieht in der Regel an den Area-Grenzen durch den ABR.

Im OSPF können bestimmte Areas als sogenannte Stub Areas definiert werden. Dadurch wird verhindert, dass externe Netzwerke, wie z.B. solche, die aus anderen Protokollen durch Redistribution in OSPF propagiert werden, in die Stub Area hinein propagiert werden. Das Routing solcher Areas nach aussen hin wird mit einer Default Route propagiert. Die Konfiguration einer Stub Area reduziert die Datenbankgrösse innerhalb der Area und verringert die Grösse an benötigtem Speicherplatz auf den Gateways, die in die Area eingebunden sind.

10.2.1 Bereiche

Bevor die Gateway-Schnittstelle einem Bereich zugeordnet werden kann, müssen zunächst OSPF-Bereiche definiert werden.

Im Menü **Routing-Protokolle**->**OSPF**->**Bereiche** wird eine Liste aller konfigurierten OSPF-Bereiche angezeigt.

10.2.1.1 Bearbeiten oder Neu

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

Das Menü **Routing-Protokolle**->**OSPF**->**Bereiche**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Bereichs-ID	Geben Sie die ID ein, die den OSPF-Bereich identifiziert. Der Backbone-Bereich ist *0.0.0.0*.
Externe Routen importieren	Spezifizieren Sie, ob das Gateway Routing-Informationen, welche aus externen autonomen Systemen (nicht Areas) generiert wurden, importieren soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiviert.
Importiere Summary-Routen	Nur für **Externe Routen importieren** = *Deaktiviert* Definieren Sie, ob Summary LSAs (vom Area Border Gateway

Feld	Beschreibung
	generierte Routing-Informationen) in die Stub Area gesendet werden sollen. Mögliche Werte: • *Aktiviert* (Standardwert): Aktiviert den Import. • *Deaktiviert*: Deaktiviert den Import.
Standardroute für Bereich eintragen (nur ABR)	Nur für **Externe Routen importieren** = *Deaktiviert* Wählen Sie aus, ob das Area Border Gateway keine LSAs in die Stub Area senden, sondern nur eine Default Route propagieren soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiviert.

Felder im Menü Route Aggregation

Feld	Beschreibung
IP-Adresse	Definieren Sie den OSPF-Bereich. • *IP-Adresse*: Geben Sie hier die IP-Adresse des Bereichs ein, der zusammengefasst werden soll. • *Netzmaske*: Geben Sie hier die Netzmaske ein. • *Ankündigen*: Subnetze, die zu Bereichen zusammengefasst sind, lösen entweder das Propagieren des angegebenen Verbunds aus (*Ja*, Standardwert), oder führen dazu, dass das Subnetz gar nicht außerhalb des Bereichs propagiert wird (*Nein*), d.h. weder die eigentlichen Subnetze noch das zusammengefasste Gesamtsubnetz werden propagiert. Fügen Sie mit **Hinzufügen** neue Einträge hinzu.

10.2.2 Schnittstellen

Im Menü **Routing-Protokolle**->**OSPF**->**Schnittstellen** wird eine Liste aller Schnittstellen angezeigt.

Achtung

Wenn Ihre Schnittstelle nicht nur der Backbone Area 0.0.0.0 zugewiesen werden sollen, müssen Sie im Menü **Routing-Protokolle**->**OSPF**->**Bereiche** zunächst OSPF-Bereiche (Areas) definieren.

10.2.2.1 Bearbeiten

Wählen Sie das Symbol , um die OSPF-Einstellungen für die Schnittstellen zu verändern.

Das Menü **Routing-Protokolle**->**OSPF**->**Schnittstellen**-> besteht aus folgenden Feldern:

Felder im Menü OSPF-Schnittstellenkonfiguration

Feld	Beschreibung
Admin-Status	Der Status einer OSPF-Schnittstelle definiert, ob über die Schnittstelle Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden. Wenn OSPF noch nicht aktiviert wurde, wird nur das Admin-Status-Feld angezeigt (in diesem Fall sind Änderungen irrelevant). Mögliche Werte: • *Aktiv*: OSPF ist für diese Schnittstelle aktiviert, d.h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • *Passiv*: OSPF ist nicht für diese Schnittstelle aktiviert, 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 Schnittstelle propagiert. • *Inaktiv*: OSPF ist für diese Schnittstelle komplett deaktiviert.
Bereichs-ID	Wählen Sie die ID des Bereichs aus, dem diese Schnittstelle zugeordnet werden soll. Wenn Ihre Schnittstelle nicht nur der Backbone Area 0.0.0.0 zugewiesen werden sollen, müssen Sie im Menü **Routing-Protokolle**->**OSPF**->**Bereiche** zunächst OSPF-Bereiche definieren.

Feld	Beschreibung
Metrikbestimmung	Legen Sie fest, wie die Metrik dieser Schnittstelle berechnet wird. Mögliche Werte: • *Auto (Schnittstellengeschwindigkeit)* (Standardwert): Die Metrik wir anhand der Geschwindigkeit der Schnittstelle automatisch festgelegt. • *Fest eingestellt*: Geben Sie eine festen Wert in **Metrik (Direkte Routen)** ein.
Metrik (Direkte Routen)	Geben Sie den Basismetrikwert an. Die tatsächlich für eine Route verwendete Metrik beruht auf einem Base Metric Value, der sich aus der Bandbreite der Schnittstelle errechnet: BMV = 100.000.000 / Bandbreite in bps. Für **Metrikbestimmung** *Auto (Schnittstellengeschwindigkeit)* wird hier der automatisch ermittelte Wert angezeigt und kann nicht verändert werden. Der Basismetrikwert ist für Bandbreiten >= 100.000.000 bps immer *1*. Der Basismetrikwert von Gigabit-Schnittstellen und 100-MBit-Schnittstellen ist somit identisch. Um dies zu ändern müssen Sie einen festen Wert in **Metrikbestimmung** einstellen.
Authentifizierungstyp	Wählen Sie die Art der Authentifizierung aus, die angewendet wird, wenn OSPF-Pakete über diese OSPF-Schnittstelle verschickt (oder eingehende geprüft) werden. Diese legt fest, wie der Schlüssel im Feld **Schlüssel zur Authentisierung** verwendet wird. Standardmäßig ist der Wert auf *Keiner* gesetzt. Bei *Klartext* wird der Schlüssel als Textfolge in jedem Paket verschickt. Bei *MD5* wird der Schlüssel verwendet, um einen Hash zu erstellen, der in jedem Paket mitgeschickt wird.
Schlüssel zur Authentisierung	Geben Sie eine Textfolge ein, die in Verbindung mit dem definierten **Authentifizierungstyp** verwendet wird.
Indirekte, statische Routen exportieren	Wenn dieser Wert auf *Deaktiviert* (Standardwert) gesetzt ist, werden nur direkte Routen (d.h. Routen zu direkt über diese Schnittstelle erreichbaren Netzen) über aktive OSPF-Schnittstellen propagiert (siehe **Admin-Status**). Wenn der Wert auf *Aktiviert* gesetzt ist, werden auch indirekte statische

Feld	Beschreibung
	Routen über aktive Schnittstellen propagiert.
Demand Circuit Options	Legen Sie fest, ob auf dieser Schnittstelle Demand OSPF Prozeduren (Hello Unterdrückung an FULL Neighbors und das Setzen des DoNotAge Flags auf der propagierten LSA) durchgeführt werden sollen (*Aktiviert*, Standardwert) oder nicht (*Deaktiviert*). Diese Option sollte insbesondere bei Verbindungen deren Kosten zeitabhängig berechnet werden (z.B. ISDN-Wählverbindungen, Internetverbindungen ohne Flatrate) aktiviert werden.

10.2.3 Globale Einstellungen

Das Menü **Routing-Protokolle**->**OSPF**->**Globale Einstellungen** beinhaltet globale OSPF-Parameter. Hier wird u.a. OSPF auf dem Gateway aktiviert.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Globale OSPF-Einstellungen

Feld	Beschreibung
OSPF-Status	Aktivieren oder deaktivieren Sie OSPF. Standardmäßig ist die Funktion nicht aktiv.
Standardroute für AS eintragen	Wenn diese Option aktiviert ist, propagiert das Gateway eine Default Route über alle aktiven OSPF Schnittstellen. Standardmäßig ist die Funktion nicht aktiv.
Auf Discard/Refuse-Schnittstelle gebundene Routen propagieren	Die logischen Schnittstellen REFUSE und IGNORE haben folgende Bedeutung: REFUSE bedeutet (wenn eine Route darauf existiert), dass Pakete von dieser Schnittstelle verworfen werden und ein ICMP Unreachable Reply generiert wird. IGNORE bedeutet (wenn eine Route darauf existiert), dass Pakete von dieser Schnittstelle kommentarlos verworfen werden. Wenn die Option aktiviert ist, werden Routen, die an die beiden discard/refuse Schnittstellen gebunden sind, vom OSPF in seine Datenbank übernommen. Ist die Option deaktiviert werden diese Routen ignoriert.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Dynamic LS Update Compression	Nur für **RXL1250** / **RXL12100** Aktivieren oder deaktivieren Sie die Funktion. Standardmäßig ist die Funktion nicht aktiv.

11 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.

11.1 Allgemein

11.1.1 Allgemein

Im Menü **Multicast**->**Allgemein**->**Allgemein** können Sie die Multicast-Funktionalität aus- bzw. einschalten.

Das Menü besteht aus den folgenden Feldern:

Felder im Menü Grundeinstellungen

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.

11.2 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.

11.2.1 IGMP

In diesem Menü konfigurieren Sie die Schnittstellen, auf denen IGMP aktiv sein soll.

11.2.1.1 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. 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).

Feld	Beschreibung
	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

Mit IGMP Proxy können mehrere lokal angeschlossene Schnittstellen als ein Subnetz zu einem benachbarten Router simuliert werden. Auf der IGMP-Proxy-Schnittstelle eingehende Queries werden in die lokalen Subnetze weitergeleitet. Lokale Reports werden auf der IPGM-Proxy-Schnittstelle weitergeleitet.

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.

Feld	Beschreibung
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.
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.

11.2.2 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 Grundeinstellungen

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.

Feld	Beschreibung
	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.

11.3 Weiterleiten

11.3.1 Weiterleiten

In diesem Menü legen Sie fest, welche Multicast-Gruppen zwischen den Schnittstellen Ihres Geräts immer weitergeleitet werden.

11.3.1.1 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.

11.4 PIM

Protocol Independent Multicast (PIM) ist ein Multicast-Routingverfahren, das dynamisches Routing von Multicast-Paketen ermöglicht. Bei PIM wird die Informationsverteilung über einen zentralen Punkt geregelt, der als Rendezvous Point bezeichnet wird. Dorthin werden die Datenpakete initial geleitet und auf Anfrage anderer Router den Empfängern zur Verfügung gestellt.

Bei Multicast-Routing-Protokollen unterscheidet man grundsätzlich zwischen Sparse Mode und Dense Mode. Beim Dense Mode werden alle Pakete weitergeleitet und nur die Pakete an Gruppen verworfen, die explizit abbestellt wurden. Beim Sparse Mode werden nur Pa-

kete an Gruppen weitergeleitet, die von diesen bestellt wurden. Ihr Gerät verwendet PIM im Sparse Mode.

11.4.1 PIM-Schnittstellen

Im Menü **Multicast**->**PIM**->**PIM-Schnittstellen** wird eine Liste aller PIM-Schnittstellen angezeigt.

11.4.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um PIM-Schnittstellen zu konfigurieren.

Das Menü **Multicast**->**PIM**->**PIM-Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü PIM-Schnittstelleneinstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle, die für PIM benutzt werden soll, d.h. über die Multicast Routing betrieben werden soll.
PIM-Modus	Zeigt den Modus an, der für PIM benutzt wird. Ihr Gerät verwendet den PIM Sparse Mode. Der Eintrag kann nicht verändert werden.
Stub Interface Mode	Bestimmen Sie, ob die Schnittstelle für PIM-Datenpakete genutzt werden soll. Mit diesem Parameter können Sie z. B. eine Schnittstelle für IGMP benutzen, aber vor (gefälschten) PIM-Nachrichten schützen. Ist diese Funktion deaktiviert (Standardwert), werden die PIM-Datenpakete für diese Schnittstelle blockiert. Wenn die Funktion aktiv ist, ist die Schnittstelle für die PIM-Datenpakete freigegeben.
Designated-Router-Priorität	Bestimmen Sie den Wert der Designated Router Priority, der in die Option **Designated-Router-Priorität** eingefügt wird. Je höher dieser Wert ist, desto größer ist die Wahrscheinlichkeit, dass der entsprechende Router als Designated Router verwendet wird. Der Standardwert ist *1*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Hello-Intervall	Bestimmen Sie, in welchen Zeitabständen (in Sekunden) PIM Hello Messages über diese Schnittstelle gesendet werden. Der Wert *0* bedeutet, dass auf dieser Schnittstelle keine PIM Hello Mesages gesendet werden. Wertebereich: *0* bis *18000* Sekunden. Der Standardwert ist *30*.
Triggered-Hello-Intervall	Bestimmen Sie, wie lange maximal gewartet werden darf, bis eine PIM Hello Message nach einem Sytemstart oder nach einem Neustart eines Nachbarn gesendet wird. Der Wert *0* bedeutet, dass PIM Hello Mesages immer sofort gesendet werden. Wertebereich: *0* bis *60* Sekunden. Der Standardwert ist *5*.
Hello Hold Time	Bestimmen Sie den Wert des Holdtime Feldes in einer PIM Hello Message. Daraus ergibt sich, wie lange ein PIM-Router als verfügbar gilt. Sobald die **Hello Hold Time** abgelaufen ist und und keine weitere Hello Message empfangen wurde, wird dieser PIM-Router als nicht erreichbar betrachtet. Wertebereich: *0* bis *65535* Sekunden. Der Standardwert ist *105*.
Join/Prune-Intervall	Bestimmen Sie die Häufigkeit, mit der PIM Join/Prune Messages auf der Schnittstelle gesendet werden sollen. Der Wert *0* bedeutet, dass auf dieser Schnittstelle keine periodischen PIM Join/Prune Mesages gesendet werden. Wertebereich: *0* bis *18000* Sekunden. Der Standardwert ist *60*.
Join/Prune Hold Time	Bestimmen Sie den Wert, der in das Holdtime Feld einer PIM

Feld	Beschreibung
	Join/Prune Message eingefügt wird. Dies ist die Zeitspanne, die ein Empfänger den Join/Prune State halten muss. Wertebereich: *0* bis *65535* Sekunden. Der Standardwert ist *210*.
Propagation Delay	Bestimmen Sie den Wert, der in das Propagation Delay Feld eingefügt wird. Dieses Feld ist ein Bestandteil der LAN Prune Delay Option in den PIM Hello Messages, die auf dieser Schnittstelle gesendet werden. Propagation Delay und Override Interval stellen die sogenannten LAN-Prune-Delay-Einstellungen dar. Sie bewirken eine verzögerte Verarbeitung von Prune-Messages bei Upstream Routern. Wenn **Propagation Delay** zu klein ist, kann es zum Abbruch der Übertragung von Multicast-Paketen kommen, bevor ein Downstream Router eine Prune Override Message geschickt hat. Wertebereich: *0* bis *32* Sekunden. Der Standardwert ist *1*.
Override Interval	Bestimmen Sie den Wert, den das Gateway in das Feld Override Interval der LAN Prune Delay Option einfügt. **Override Interval** bestimmt, wie lange ein Downstream Router höchstens warten darf, bis er eine Prune Override Message schickt. Wertebereich: *0* bis *65* Sekunden. Der Standardwert ist *3*.

11.4.2 PIM-Rendezvous-Punkte

Im Menü **Multicast**->**PIM**->**PIM-Rendezvous-Punkte** können Sie festlegen, welcher Rendezvous Point für welche Gruppen zuständig sein soll.

Es wird eine Liste aller PIM Rendezvous Points angezeigt.

11.4.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um PIM Rendezvous Points zu konfigurieren.

Das Menü **Multicast**->**PIM**->**PIM-Rendezvous-Punkte**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen für PIM-Rendezvous-Punkt

Feld	Beschreibung
Multicast-Gruppenbereich	Wählen Sie die Multicast-Gruppen für den PIM Rendevouz Point aus. Sie können • `Alle Gruppen` (Standardwert) angeben oder mit Auswahl von • `Bestimmter Bereich` ein Multicast-Netzwerksegment spezifizieren.
Multicast-Gruppen-Adresse	Nur bei **Multicast-Gruppenbereich** = `Bestimmter Bereich` Geben Sie hier die IP-Adresse des Multicast-Netzwerksegments ein.
Präfixlänge der Multicast-Gruppe	Nur bei **Multicast-Gruppenbereich** = `Bestimmter Bereich` Geben Sie hier die Netzmaskenlänge des Multicast-Netzwerksegments ein. 224.0.0.0/4 bezeichnet das komplette Multicast Class D Segment. Wertebereich: `4` (Standardwert) bis `32`.
Rendezvous Point IP-Adresse	Geben Sie die IP-Adresse oder den Hostnamen des Rendezvous Points ein.
Vorrang	Geben Sie den Wert für pimGroupMappingPrecedence ein, der für statische RP Konfigurationen verwendet werden soll. Dieses erlaubt die genaue Kontrolle darüber, welche Konfiguration durch diese statische Konfiguration ersetzt werden soll. Wenn die Funktion aktiviert ist, wird pimStaticRPOverrideDyna-

Feld	Beschreibung
	mic ignoriert. Die absoluten Werte dieses Objekts haben nur Bedeutung auf dem lokalen Router und müssen nicht mit anderen Routern abgestimmt werden. Die Funktion ist mit dem Standardwert *0* deaktiviert. Wenn die Funktion durch Setzen eines Wertes nicht 0 aktiviert wird, kann das verschiedene Auswirkungen auf andere Router haben. Verwenden Sie daher diese Funktion nicht, wenn eine genaue Kontrolle des Verhaltens des statischen RP nicht benötigt wird.

11.4.3 PIM-Optionen

Das Menü **Multicast**->**PIM**->**PIM-Optionen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
PIM-Status	Wählen Sie aus ob PIM aktiviert werden soll. Mit Auswahl von *Aktivieren* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Keepalive-Periode	Geben Sie die Zeitspanne in Sekunden ein, in der eine Keepalive Nachricht gesendet werden muss. Mögliche Werte: *0* bis *65535*. Der Standardwert ist *210*.
Register Suppression Timer	Geben Sie die Zeit in Sekunden an, nach der ein PIM Designated Router (DR) keine register-encapsulated Daten mehr zum Rendevouz Point (RP) schicken soll, nachdem die Register-Stop-Nachricht empfangen wurde. Dieses Objekt wird verwendet, um sowohl am DR als auch am RP Timer zu nutzen. Dieser Zeitraum wird in der PIM-SM Spezifikation Register_Suppression_Time genannt. Mögliche Werte: *0* bis *65535*. Der Standardwert ist *60*.

12 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.

12.1 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

Feld	Beschreibung
	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 durchfüh-

ren, 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

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.

12.1.1 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.

12.1.1.1 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 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.

Feld	Beschreibung
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.

Feld	Beschreibung
	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. 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 350 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.

Feld	Beschreibung
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.

Feld	Beschreibung
Sicherheitsrichtlinie	Nur für **IPv6** = *Aktiviert* 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 350 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 Prefix-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.

Feld	Beschreibung
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**

Feld	Beschreibung
	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-

Feld	Beschreibung
	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:

Feld	Beschreibung
	• *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. 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*.

12.1.2 Dual Stack Lite (DS-Lite)

Dual Stack Lite ermöglicht die Nutzung von IPv4-Verbindungen, auch wenn der zur Verfügung stehende Internetanschluss ausschließlich mit IPv6 betrieben wird. Das ist z. B. dann der Fall, wenn Sie weiterhin IPv4-Verbindungen benötigen, der Internetanbieter allerdings aufgrund knapper IPv4-Adressen nur eine IPv6-Adresse zur Verfügung stellt.

Bei DS-Lite werden IPv4-Pakete in IPv6-Pakete "eingepackt". Die so getunnelten Pakete werden zum AFTR-Server (Address Family Transition Router) des Internetanbieters gesendet, der die IPv4-Packete "auspackt" und in den IPv4-Bereich des Internet weiterleitet.

Im Menü **WAN**->**Internet + Einwählen**->**Dual Stack Lite** wird eine Liste aller Dual-Stack-Lite-Schnittstellen angezeigt.

12.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Dual-Stack-Lite-Schnittstellen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**Dual Stack Lite**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Weisen Sie Ihrer Dual-Stack-Lite-Verbindung einen Namen zu.
IPv6-Schnittstelle	Wählen Sie die IPv6-Schnittstelle aus, die für die DS-Lite-Verbindung verwendet wird. Dies ist normalerweise die

Feld	Beschreibung
	Schnittstelle Ihrer Internetverbindung. Über diese Schnittstelle gesendete IPv4-Pakete werden in IPv6-Pakete verpackt.
AFTR	Geben Sie die IPv6-Adresse oder den Domänennamen Ihres AFTR (Address Family Transition Router) ein. Sie erhalten die Adresse vom Anbieter Ihrer IPv6-Internetverbindung.
Standardroute	Wählen Sie aus, ob Sie diese Verbindung als Standardroute verwenden wollen. Die Einstellung ist sinnvoll, um den gesamten IPv4-Datenverkehr, der über das Internet gehen soll, auch wirklich über die IPv6-Verbindung senden zu können. Andernfalls müssen Sie entsprechende Einstellungen im Routing vornehmen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

12.1.3 PPTP

Im Menü **WAN**->**Internet + Einwählen**->**PPTP** wird eine Liste aller PPTP-Schnittstellen angezeigt.

In diesem Menü konfigurieren Sie eine Internet-Verbindung, die zum Verbindungsaufbau das Point-to-Point Tunneling Protocol (PPTP) verwendet. Dies ist z. B. in Österreich notwendig.

12.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere PPTP-Schnittstellen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**PPTP**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um die Internetverbindung eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPTP-Ether-	Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-

Feld	Beschreibung
net-Schnittstelle	Gegenstelle transportiert werden. 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 **Physikalische Schnittstellen**->**ATM**->**Profile**->**Neu** für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. *ethoa50-0*, aus.
Benutzername	Geben Sie den Benutzernamen 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 sind *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. 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:

Feld	Beschreibung
	• *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 350 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 temporär gültige IP-Adresse vom Provider. • *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 für **IP-Adressmodus** = *Statisch* Weisen Sie der PPTP-Schnittstelle eine 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 PPTP-Partner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu.

Feld	Beschreibung
	• *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*.

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 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

Feld	Beschreibung
	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.
PPTP-Adressmodus	Zeigt den Adressmodus an. Der Wert kann nicht verändert werden. Mögliche Werte: • *Statisch*: Die **Lokale PPTP-IP-Adresse** wird dem ausgewählten Ethernet-Port zugewiesen.
Lokale PPTP-IP-Adresse	Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird. Der Standardwert ist *10.0.0.140*.
Entfernte PPTP-IP-Adresse	Geben Sie die IP-Adresse des PPTP-Partners ein. Der Standardwert ist *10.0.0.138*.
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.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

12.1.4 ISDN

Im Menü **WAN**->**Internet + Einwählen**->**ISDN** wird eine Liste aller ISDN-Schnittstellen im TE-Modus (externes ISDN) 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

12.1.4.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere ISDN-Schnittstellen einzurichten.

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

Feld	Beschreibung
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 ab-*

Feld	Beschreibung
	rufen 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 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 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.

Feld	Beschreibung
	• *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:

Feld	Beschreibung
	• *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 Sicherheitsgründen 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

Feld	Beschreibung
	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. 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.
Anzahl Verwendeter Ports	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.

12.1.5 UMTS/LTE

Hinweis

Beachten Sie, dass das Menü **UMTS/LTE** nur bei Geräten mit integriertem UMTS/HSDPA-Modem bzw. bei Geräten mit Unterstützung für die Verwendung eines UMTS/HSDPA/LTE-USB-Sticks verfügbar ist!

Im Menü **WAN**->**Internet + Einwählen**->**UMTS/LTE** wird eine Liste aller konfigurierten GPRS/UMTS/LTE-Verbindungen angezeigt.

Mit den Mobilfunkstandards GPRS, UMTS und LTE kann eine Internet-Verbindung über das Mobilfunknetz aufgebaut werden.

12.1.5.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Verbindungen einzurichten.

Das Menü **WAN**->**Internet + Einwählen**->**UMTS/LTE**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um die Internet-Verbindung eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
UMTS/ LTE-Schnittstelle	Wählen Sie die UMTS/LTE-Schnittstelle aus. Für **RS120wu** ist das integrierte Modem mit Slot 6 Einheit 0 UMTS vorausgewählt, für Geräte mit optional gestecktem UMTS/LTE-Stick der USB-Port des Geräts.
Benutzername	Geben Sie den Benutzernamen 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.

Feld	Beschreibung
	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, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte sind *0* bis *3600* (Sekunden). *0* deaktiviert den Short-Hold. Der Standardwert ist *300*.

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: • *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.

Feld	Beschreibung
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*.

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 von *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.

Feld	Beschreibung
	• *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 **DNS-Server Primär** und **DNS-Server Sekundär** 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. 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.

12.1.6 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 Adapte angeschlossen sein (als Zubehör erhältlich).

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 zunächst 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.

12.1.6.1 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, bevor-

Feld	Beschreibung
	zugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

12.2 Standleitung

Eine Standleitung ist eine permanente (stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetzwerk. Im Gegensatz zu einer Wählleitung steht der gesamte Übertragungsweg immer zur Verfügung. Die Standleitung kann nicht vom Teilnehmer über ein Wählverfahren aufgebaut werden und hat daher keine Rufnummer. Die Verbindung muss vom Netzbetreiber hergestellt werden.

12.2.1 Schnittstellen

Im Menü **WAN**->**Standleitung**->**Schnittstellen** wird eine Liste aller automatisch generierten Standleitungsverbindungen angezeigt. Zur automatischen Generierung ist die Konfiguration der entsprechenden ISDN-Schnittstelle nötig.

12.2.1.1 Bearbeiten

Wählen Sie die Schaltfläche um die Konfiguration der entsprechenden Standleitung für eine BRI-Schnittstelle zu bearbeiten.

Das Menü **WAN**->**Standleitung**->**Schnittstellen**->**Automatisch generiert von BRI (ISDN-S0)**-> besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung für die Verbindung ein.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
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 nicht aktiv.
Lokale IP-Adresse	Tragen Sie hier die IP-Adresse ein, die Sie von Ihrem Netzbe-

Feld	Beschreibung
	treiber erhalten haben.
Routeneinträge	Definieren Sie weitere Routeneinträge für diesen Verbindungsparten. Fügen Sie mit **Hinzufügen** neue Einträge hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll. 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. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Komprimierung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner* (Standardwert): Es wird keine Verschlüsselung angewendet. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden.

Feld	Beschreibung
	Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine 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 OSPFProtokoll- Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie die ARP-Requests für diesen 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.

Wählen Sie die Schaltfläche um die Konfiguration der entsprechenden Standleitung für eine PRI-Schnittstelle zu bearbeiten.

Das Menü **WAN**->**Standleitung**->**Schnittstellen**->**Automatisch generiert von PRI (ISDN-S2M)**-> besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung für die Verbindung ein.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
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 nicht aktiv.
Lokale IP-Adresse	Tragen Sie hier die IP-Adresse ein, die Sie von Ihrem Netzbetreiber erhalten haben.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbindungsparten. Fügen Sie mit **Hinzufügen** neue Einträge hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll. 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. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Komprimierung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner* (Standardwert): Es wird keine Verschlüsselung angewendet. • *STAC* • *MS-STAC*

Feld	Beschreibung
	• *MPPC*: Microsoft Point-to-Point Compression

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine 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 OSPFProtokoll- Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie die ARP-Requests für diesen 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.

12.3 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.

12.3.1 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.

12.3.1.1 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 Grundeinstellungen

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

Feld	Beschreibung
	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.

13 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.

Zum Aufbau eines VPN-Tunnels stehen verschiedene Protokolle zur Verfügung, wie z. B. IPSec oder PPTP.

Die Authentifizierung der Verbindungspartner erfolgt über ein Passwort, mithilfe von Preshared Keys oder über Zertifikate.

Bei IPSec wird die Verschlüsselung der Daten z. B. mit Hilfe von AES oder 3DES erledigt, bei PPTP kann MPPE benutzt werden.

13.1 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 81) 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

bintec elmeg Gateways unterstützen 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 IP-Sec-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.

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 sich die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten entsprechen muss.

13.1.1 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 konfigurierten 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 480.

13.1.1.1 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*

Feld	Beschreibung
	• *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. 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 Me-

Feld	Beschreibung
	nü **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.
IP-Version des Tunnelnetzwerks	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 350 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.

Feld	Beschreibung
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-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*.

Feld	Beschreibung
	• *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 IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert 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. Ausnahmen für die gewählte Einstellung können Sie im Menü *Firewall* auf Seite 350 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

Feld	Beschreibung
	niederiger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.

Zusätzlicher Filter des Datenverkehrs

bintec elmeg Gateways unterstützen 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-Profil	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.
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:

Feld	Beschreibung
	• *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 Peers mit IKEv2. 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

Feld	Beschreibung
	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 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	Nur wenn unter **Öffentliche Schnittstelle** eine Schnittstelle ausgewählt ist. Legen Sie fest, wie strikt die Einstellung 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.

Feld	Beschreibung
	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.
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

Feld	Beschreibung
	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. • *Nie einwählen*: 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	Nur verfügbar, wenn auf dem Gerät Zertifikate verwendet werden. Wenn Sie die Option **Folgenden CA-Zertifikaten vertrauen** aktivieren, können Sie 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 bintec elmeg-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 308 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

Feld	Beschreibung
	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: • *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-*

Feld	Beschreibung
	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.

13.1.2 Phase-1-Profile

Im Menü **VPN**->**IPSec**->**Phase-1-Profile** wird eine Liste aller konfigurierten IPSec-Phase-1-Profile angezeigt.

In der Spalte **Standard** können Sie das Profil markieren, das als Standard-Profil verwendet werden soll.

13.1.2.1 Neu

Wählen Sie die Schaltfläche **Neues IKEv1-Profil erstellen** bzw. **Neues IKEv2-Profil erstellen**, um weitere Profile einzurichten.

Das Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neues IKEv1-Profil erstellen** 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 Propo-

Feld	Beschreibung
	sal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden. 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. • *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 Geschwindig-

Feld	Beschreibung
	keit 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.
DH-Gruppe	Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec elmeg-Geräten unterstützt wird, steht für "modular exponentiation". Folgende Gruppen und zugehörige Bit-Werte der Exponentiation stehen zur Verfügung: • *1 (768 Bit)* • *2 (1024 Bit)* • *5 (1536 Bit)* • *14(2048 Bit)*

Feld	Beschreibung
	• *15(3072 Bit)* • *16(4096 Bit)* Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.
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)**

Feld	Beschreibung
	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.
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)*

Feld	Beschreibung
	• *Schlüsse-ID*
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-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 er-

Feld	Beschreibung
	kennt 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.

Feld	Beschreibung
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.
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*

Feld	Beschreibung
	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.

13.1.3 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.

13.1.3.1 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 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.

Feld	Beschreibung
	• *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)

Feld	Beschreibung
	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. 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. Folgende Gruppen und zugehörige Bit-Werte der Exponentiation stehen zur Verfügung: • *1 (768 Bit)* • *2 (1024 Bit)* • *5 (1536 Bit)* • *14(2048 Bit)* • *15(3072 Bit)* • *16(4096 Bit)* Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.
Lebensdauer	Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablau-

Feld	Beschreibung
	fen 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 der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	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 bintec elmeg 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 ein bintec elmeg-Gerät ist. Wenn ja, wird *Heartbeats (Senden &Erwarten)* (bei Gegenstelle mit bintec elmeg) oder *Inaktiv* (bei Gegenstelle ohne bintec elmeg) 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 Ma-

Feld	Beschreibung
	ximum Transfer Unit) propagiert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

13.1.4 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.

13.1.4.1 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.
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. • *Lokal*: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	Nur für **Rolle** = *Client* Geben Sie den Authentifizierungsnamen des Clients ein.

Feld	Beschreibung
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.

13.1.5 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools für Ihre konfigurierten IPSec-Verbindungen angezeigt.

Wenn Sie bei einem IPSec-Peer für **IPv4-Adressenvergabe** *Server im IKE-Konfigurationsmodus* eingestellt haben, müssen Sie hier die IP-Pools, aus denen die IP-Adressen vergeben werden, definieren.

13.1.5.1 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)

Feld	Beschreibung
	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.

13.1.6 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*

Feld	Beschreibung
	• *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 bintec elmeg-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 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	Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich

Feld	Beschreibung
synchronisieren	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.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
Zertifikatsketten senden	Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen. 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.

13.2 L2TP

Das Layer-2-Tunnelprotokoll (L2TP) ermöglicht das Tunneling von PPP-Verbindungen über eine UDP-Verbindung.

Ihr bintec elmeg-Gerät unterstützt die folgenden zwei Modi:

- L2TP-LNS-Modus (L2TP Network Server): nur für eingehende Verbindungen
- L2TP-LAC-Modus (L2TP Access Concentrator): nur für ausgehende Verbindungen.

Folgendes ist bei der Konfiguration von Server und Client zu beachten: Auf beiden Seiten (LAC und LNS) muss jeweils ein L2TP-Tunnelprofil angelegt werden. Auf der Auslöserseite (LAC) wird das entsprechende L2TP-Tunnelprofil für den Verbindungsaufbau verwendet. Auf der Responderseite (LNS) wird das L2TP-Tunnelprofil für die Verbindungsannahme

benötigt.

13.2.1 Tunnelprofile

Im Menü **VPN**->**L2TP**->**Tunnelprofile** wird eine Liste aller konfigurierten Tunnelprofile angezeigt.

13.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Tunnelprofile einzurichten.

Das Menü **VPN**->**L2TP**->**Tunnelprofile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das aktuelle Profil ein. Ihr Gerät benennt die Profile automatisch mit *L2TP* und nummeriert diese, der Wert kann jedoch geändert werden.
Lokaler Hostname	Geben Sie den Hostnamen für LNS bzw. LAC ein. • *LAC*: Der lokale Hostname wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem entfernten Hostnamen eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Reply). • *LNS*: Entspricht dem Wert für **Entfernter Hostname** der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	Geben Sie den Hostnamen des LNS bzw. LAC ein: • *LAC*: Definiert den Wert für **Lokaler Hostname** des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Ein im LAC konfigurierter **Lokaler Hostname** muss zu **Entfernter Hostname**n passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • *LNS*: Definiert den **Lokaler Hostname**n des LAC. Falls das Feld **Entfernter Hostname** auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für al-

Feld	Beschreibung
	le ankommenden Rufe benutzt wird, für die kein Profil mit passendem entfernten Hostnamen gefunden werden kann.
Passwort	Geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den **Lokaler Hostname**n und das **Passwort**, die in der SCCRQ des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS. Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.

Felder im Menü Parameter des LAC-Modus

Feld	Beschreibung
Entfernte IP-Adresse	Geben Sie die feste IP-Adresse des LNS ein, die als Zieladresse für Verbindungen genutzt wird, die auf diesem Profil aufbauen. Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.
UDP-Quellport	Geben Sie an, wie die Portnummer ermittelt werden soll, die als Quellport für alle abgehenden L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen. Standardmäßig ist die Option **Fest eingestellt** deaktiviert, was bedeutet, dass den Verbindungen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden. Wenn Sie einen fixen Port eingeben möchten, aktivieren Sie die Option *Fest eingestellt*. Wenn Sie Probleme mit der Firewall bzw. NAT feststellen, wählen Sie diese Option. Verfügbare Werte sind dann *0* bis *65535*.
UDP-Zielport	Geben Sie die Zielportnummer ein, die für alle Rufe genutzt wird, die auf diesem Profil aufbauen. Der entfernte LNS, der den Ruf empfängt, muss diesen Port auf L2TP-Verbindungen überwachen.

Feld	Beschreibung
	Mögliche Werte sind *0* bis *65535*. Der Standardwert ist *1701* (RFC 2661).

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Lokale IP-Adresse	Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen. Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel die entfernte IP-Adresse erreicht.
Hello-Intervall	Geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten. Verfügbare Werte sind *0* bis *255*, der Standardwert ist *30*. Der Wert *0* bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.
Minimale Zeit zwischen Versuchen	Geben Sie die Mindestzeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Die Wartezeit wird dynamisch verlängert, bis sie die **Maximale Zeit zwischen Versuchen** erreicht hat. Verfügbare Werte sind *1* bis *255*, der Standardwert ist *1*.
Maximale Zeit zwischen Versuchen	Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *16*.
Maximale Anzahl Wiederholungen	Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *5*.

Feld	Beschreibung
Sequenznummern der Datenpakete	Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folgenummern benutzen soll oder nicht. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

13.2.2 Benutzer

Im Menü **VPN**->**L2TP**->**Benutzer** wird eine Liste aller konfigurierten L2TP-Partner angezeigt.

13.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere L2TP-Partner einzurichten.

Das Menü **VPN**->**L2TP**->**Benutzer**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.
Verbindungstyp	Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkservers (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll. Mögliche Werte: • *LNS* (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • *LAC*: Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.

Feld	Beschreibung
Tunnelprofil	Nur für **Verbindungstyp** = *LAC* Wählen Sie ein im Menü **Tunnelprofil** erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.
Benutzername	Geben Sie die Kennung Ihres Geräts 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.
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, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Zur Verfügung stehen Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Short Hold. Der Standardwert ist *300*.

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*: Nur für **Verbindungstyp** = *LNS*. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Nur für **Verbindungstyp** = *LAC*. Ihr Gerät erhält dynamisch eine IP-Adresse.
IP-Zuordnungspool (IPCP)	Nur für **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP**

Feld	Beschreibung
	Pools konfigurierten IP Pool aus.
Standardroute	Nur für **IP-Adressmodus** = *IP-Adresse abrufen* und *Statisch* 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 nicht aktiv .
NAT-Eintrag erstellen	Nur für **IP-Adressmodus** = *IP-Adresse abrufen* und *Statisch* Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur für **IP-Adressmodus** = *Statisch* Geben Sie die WAN-IP-Adresse Ihres Geräts ein.
Routeneinträge	Nur für **IP-Adressmodus** = *Statisch* Geben Sie **Entfernte IP-Adresse** und **Netzmaske** des LANs des L2TP-Partners und die dazugehörige **Metrik** ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

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 einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *300*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus.

Feld	Beschreibung
	Mögliche Werte: • *PAP/CHAP/MS-CHAP* (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *PAP*: 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. • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn **Verschlüsselung** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner*: Es wird keine MPP-Verschlüsselung angewendet. • *Aktiviert* (Standardwert): 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.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Feld	Beschreibung
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 aktiv.

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, 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 aktiviert, 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 Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner *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 L2TP-Partner

Feld	Beschreibung
	(aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner 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 L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

13.2.3 Optionen

Das Menü **VPN**->**L2TP**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Optionen

Feld	Beschreibung
UDP-Zielport	Geben Sie den Port ein, der vom LNS auf ankommende L2TP-Tunnelverbindungen überwacht werden soll. Verfügbare Werte sind alle ganzen Zahlen von *1* bis *65535*, der Standardwert ist *1701*, wie es in RFC 2661 vorgegeben ist.
UDP-Quellportauswahl	Wählen Sie aus, ob der LNS nur den überwachten Port (**UDP-Zielport**) als lokalen Quellport für die L2TP-Verbindung nutzen soll. Mit *Fest eingestellt* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

13.3 PPTP

Zur Absicherung des Datenverkehrs über eine vorhandene IP-Verbindung kann mittels Point-to-Point-Tunneling-Protokoll (=PPTP) ein verschlüsselter PPTP-Tunnel aufgebaut werden.

Zunächst wird an beiden Standorten eine Verbindung zu einem ISP (=Internet Service Provider) aufgebaut. Wenn diese Verbindungen stehen, wird über das Internet ein Tunnel zum PPTP Partner, hier dann mit PPTP, aufgebaut.

Für diesen Vorgang baut das PPTP-Subsystem eine Kontrollverbindung zwischen den Tunnelendpunkten auf. Diese übermittelt Steuerungsdaten, welche die Verbindung zwischen den zwei PPTP-Tunnelendpunkten aufbauen, aufrechterhalten und beenden. Sobald diese Kontrollverbindung aufgebaut ist, überträgt das PPTP die in GRE-Pakete (GRE = Generic Routing Encapsulation) eingepackten Nutzdaten.

13.3.1 PPTP-Tunnel

Im Menü **PPTP-Tunnel** wird eine Liste aller PPTP-Tunnels angezeigt.

13.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu** um weitere PPTP-Partner einzurichten.

Das Menü **VPN**->**PPTP**->**PPTP-Tunnel**->**Neu** besteht aus folgenden Feldern:

Felder im Menü PPTP Partner Parameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Namen ein, um den Tunnel eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPTP-Modus	Geben Sie die Rollenverteilung der PPTP-Schnittstelle an. Mögliche Werte: • *PNS* (Standardwert): Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Servers zu. • *Windows-Client-Modus*: Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Clients zu.
Benutzername	Geben Sie den Benutzernamen 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.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist.

Feld	Beschreibung
	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 *300*. Beispiel: *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.
Entfernte PPTP-IP-Adresse	Nur für **PPTP-Modus** = *PNS* Geben Sie die IP-Adresse des PPTP-Partners ein.
Entfernte PPTP-IP-Adresse / Hostname	Nur für **PPTP-Modus** = *Windows-Client-Modus* Geben Sie die IP-Adresse des PPTP-Partners ein.

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*: Nur für **PPTP-Modus** = *PNS*. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Nur für **PPTP-Modus** = *Windows-Client-Modus*. Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	Nur bei **IP-Adressmodus** = *Statisch* 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 nicht aktiv.

Feld	Beschreibung
NAT-Eintrag erstellen	Nur bei **IP-Adressmodus** = *Statisch* Wenn eine PPTP-Verbindung 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 für **IP-Adressmodus** = *Statisch* Weisen Sie der PPTP-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur für **IP-Adressmodus** = *Statisch* 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*.
IP-Zuordnungspool (IPCP)	Nur bei **PPTP-Modus** = *PNS*, **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie hier einen im Menü **VPN**->**PPTP**->**IP Pools** konfigurierten IP-Pool aus.

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*.
Nutzungsart	Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.

Feld	Beschreibung
	Mögliche Werte: • *Standard* (Standardwert): Kein spezieller Typ ist ausgewählt. • *Mehrfacheinwahl (Nur Einwahl)*: Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP-Partner aus. Mögliche Werte: • *PAP*: 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 PPTP-Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2* (Standardwert): Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn **Verschlüsselung** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner*: Es wird keine MPP-Verschlüsselung angewendet. • *Aktiviert* (Standardwert): Die MPP-Verschlüsselung V2

Feld	Beschreibung
	mit 128 bit wird nach RFC 3078 angewendet. • *Windows-kompatibel*: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.
Komprimierung	Wählen Sie ggf. die Art der Komprimierung aus, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner* (Standardwert): Es wird keine Verschlüsselung angewendet. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, 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 aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-

Feld	Beschreibung
	Protokoll-Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen PPTP-Partner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen PPTP-Partner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner *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 PPTP-Partner *Aktiv* (aktiv) ist, wenn also bereits eine Verbindung zum PPTP-Partner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü PPTP-Callback

Feld	Beschreibung
Callback	Ermöglicht den Aufbau eines PPTP-Tunnels über das Internet mit einem PPTP-Partner, selbst wenn dieser momentan nicht online ist. In der Regel wird mittels ISDN-Ruf der PPTP-Partner aufgefordert, online zu gehen und eine PPTP-Verbindung aufzubauen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
	Beachten Sie, dass Sie die entsprechende Option auf den Gateways beider Partner aktivieren müssen. Für diese Funktion wird in der Regel ein ISDN-Anschluss benötigt. Ohne ISDN ist Callback nur in Spezialanwendungen zu aktivieren.
Eingehende ISDN-Nummer	Nur wenn **Callback** aktiviert ist. Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number).
Ausgehende ISDN-Nummer	Nur wenn **Callback** aktiviert ist. Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number).

Felder im Menü Auswahl des Wählports (nur wenn Callback = aktiviert)

Feld	Beschreibung
Ausgewählte Ports	Geben Sie die ISDN-Ports an, über die der Callback ausgeführt werden soll. Mögliche Werte: • *Alle Ports*: Der Callback wird über einen der verfügbaren ISDN-Ports ausgeführt. • *Port angeben*: In **Spezifische Ports** können Sie die gewünschten ISDN-Ports auswählen.
Spezifische Ports	Nur für **Ausgewählte Ports** = *Port angeben* können Sie mit **Hinzufügen** weitere Ports auswählen.

13.3.2 Optionen

In diesem Menü können Sie allgemeine Einstellungen des globalen PPTP Profils vornehmen.

Das Menü **VPN**->**PPTP**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Optionen

Feld	Beschreibung
GRE-Window-Anpassung	Wählen Sie, ob Sie GRE Window Adaption aktivieren wollen. Diese Anpassung ist erst notwendig, wenn Sie unter Microsoft Windows XP das Service Pack 1 installiert haben. Da Microsoft

Feld	Beschreibung
	mit dem SP1 den Bestätigungalgorithmus innerhalb des GRE-Protokolls geändert hat, muss bei bintec elmeg-Geräten die automatische Window-Anpassung für GRE abgeschaltet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
GRE-Window-Größe	Geben Sie die maximale Anzahl an GRE-Paketen ein, die ohne Bestätigung geschickt werden kann. Windows verwendet seit der Version XP ein höheres initiales Empfangs-Window im GRE, weshalb die maximale Sende-Window-Größe über den Wert **GRE-Window-Größe** angepasst werden sollte. Mögliche Werte sind *0* bis *256*. Der Standardwert ist *0*.
Max. eingehende Kontrollverbindungen über entfernte IP-Adresse	Geben Sie die maximale Anzahl der Kontrollverbindungen ein.

13.3.3 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools für PPTP-Verbindungen angezeigt.

Ihr Gerät kann als dynamischer IP-Adress-Server für PPTP-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 zunächst 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.

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere IP Pools einzurichten.

13.3.3.1 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.

13.4 GRE

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das dazu dient, andere Protokolle einzukapseln und so in Form von IP-Tunneln zu den spezifizierten Empfänger zu transportieren.

Die Spezifikation des GRE-Protokolls liegt in zwei Versionen vor:

- GRE V.1 zur Verwendung in PPTP-Verbindungen (RFC 2637, Konfiguration im Menü **PPTP**)
- GRE V.0 (RFC 2784) zur allgemeinen Enkapsulierung mittels GRE

Im diesem Menü können Sie ein virtuelles Interface zur Nutzung von GRE V.0 konfigurieren. Der Datenverkehr, der über dieses Interface geroutet wird, wird dann mittels GRE enkapsuliert und an den spezifizierten Empfänger gesendet.

13.4.1 GRE-Tunnel

Im Menü **VPN**->**GRE**->**GRE-Tunnel** wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.

13.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere GRE-Tunnel einzurichten.

Das Menü **VPN**->**GRE**->**GRE-Tunnel**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	Wenn Sie die **Standardroute** aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihre Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	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 Standard-Netzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.
MTU	Geben Sie die maximale Paketgröße (Maximum Transfer Unit,

Feld	Beschreibung
	MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf. Mögliche Werte sind *1* bis *8192*. Der Standardwert ist *1500*.
Schlüssel verwenden	Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701). Mit *Aktiviert* wird die Kennung aktiviert. Standardmäßig ist die Funktion nicht aktiv.
Schlüsselwert	Nur wenn **Schlüssel verwenden** aktiviert ist. Geben Sie die GRE-Verbindungskennung ein. Mögliche Werte sind *0* bis *2147483647*. Der Standardwert ist *0*.

14 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen bintec elmeg Gateways 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 bintec elmeg-Geräte 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 ein-

zelnen 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).

Konkrete Hinweise für die Konfiguration einer Stateful Inspection Firewall (SIF) finden Sie am Ende des Kapitels unter *Konfiguration* auf Seite 365.

14.1 Richtlinien

14.1.1 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 Dia-

log, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

14.1.1.1 Neu

Hinweis

Informationen zur Auswahl der Vertrauenswürdige Schnittstellen finden Sie hier: *IPv4-Filterregeln* auf Seite 352.

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:

Feld	Beschreibung
	• *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.

14.1.2 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 vertrau-

enswürdigen 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 konfigurierten 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.

14.1.2.1 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

Feld	Beschreibung
	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.
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.

Feld	Beschreibung
	• *Verweigern* : Die Pakete werden abgewiesen. • *Zurückweisen* : Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

14.1.3 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.
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

Feld	Beschreibung
	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).

Feld	Beschreibung
	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 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.

14.2 Schnittstellen

14.2.1 IPv4-Gruppen

Im Menü **Firewall**->**Schnittstellen**->**IPv4-Gruppen** wird eine Liste aller konfigurierten IPv4-Schnittstellen-Gruppen angezeigt.

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

14.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv4-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 IPv4-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**.

14.2.2 IPv6-Gruppen

Im Menü **Firewall**->**Schnittstellen**->**IPv6-Gruppen** wird eine Liste aller konfigurierten IPv6-Schnittstellen-Gruppen angezeigt.

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dies vereinfacht die Konfiguration von Firewall-Regeln.

14.2.2.1 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.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

14.3 Adressen

14.3.1 Adressliste

Im Menü **Firewall**->**Adressen**->**Adressliste** wird eine Liste aller konfigurierten Adressen angezeigt.

14.3.1.1 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.

Feld	Beschreibung
Adresse/Präfix	Nur für **IPv6** = *Aktiviert* Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.

14.3.2 Gruppen

Im Menü **Firewall**->**Adressen**->**Gruppen** wird eine Liste aller konfigurierten Adressgruppen angezeigt.

Sie können Adressen zu Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

14.3.2.1 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**.

14.4 Dienste

14.4.1 Diensteliste

Im Menü **Firewall**->**Dienste**->**Diensteliste** wird eine Liste aller zur Verfügung stehender Dienste angezeigt. Wählen Sie das Symbol , um vorhanden Einträge zu bearbeiten. Mithilfe des -Symbols können Sie Einträge löschen.

Hinweis

Dienst wird auch aus der Liste der NAT-Dienste gelöscht! Wiederherstellung nur durch Factory Reset möglich.

14.4.1.1 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

Feld	Beschreibung
	an. 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*

Feld	Beschreibung
	• *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

14.4.2 Gruppen

Im Menü **Firewall**->**Dienste**->**Gruppen** wird eine Liste aller konfigurierten Service-Gruppen angezeigt.

Sie können Dienste in Gruppen zusammenfassen. Dieses vereinfacht die Konfiguration von Firewall-Regeln.

14.4.2.1 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**.

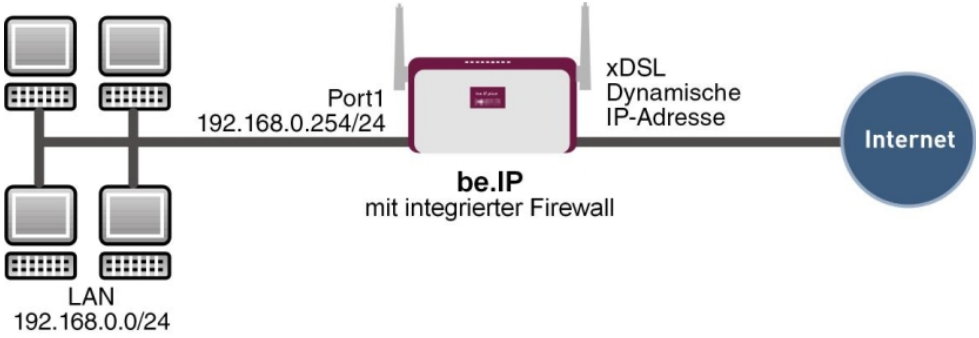
14.5 Konfiguration

14.5.1 SIF - Konfigurationsbeispiel

Voraussetzungen

- Verbindung zum Internet
- Ihr LAN muss mit dem Port 1, 2, 3 oder 4 Ihres Gateways (z. B. RS232bw) verbunden sein

Beispielszenario



Konfigurationsziel

- Den Mitarbeitern eines Unternehmens sollen nur bestimmte Dienste im Internet zur Verfügung stehen (HTTP, HTTPS, FTP, DNS).
- Das Gateway soll als DNS-Proxy arbeiten, das heißt, die Clients verwenden die als DNS-Server.
- Nur der Systemadministrator und der Geschäftsführer sollen eine HTTP- und eine Telnetverbindung zum Gateway herstellen können.
- Der Geschäftsführer soll alle Dienste im Internet nutzen können.
- Jeglicher anderer Datenverkehr soll geblockt werden.

Wichtig

Bei einer Fehlkonfiguration der Firewall kann die Funktionalität des Routers bzw. der Verbindungen mitunter stark beeinträchtigt oder sogar unterbrochen werden.

Es gilt der bei Firewalls übliche Grundsatz: Was nicht explizit erlaubt ist, ist verboten.

Daher ist eine genaue Planung der Filterregeln und der Filterregelkette erforderlich um eine korrekte Arbeitsweise sicherzustellen.

Konfigurationsschritte im Überblick

Aliasnamen für IP-Adressen und Netzadressen

Feld	Menü	Wert
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Administrator*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.2* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Geschäftsführer*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.3* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *be.IP*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.254* mit *255.255.255.255*
Beschreibung	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *Netzwerk-Intern*
Adresstyp	**Firewall -> Adressen -> Adressliste -> Neu**	*Adresse/Subnetz*
Adresse/Subnetz	**Firewall -> Adressen -> Adressliste -> Neu**	z. B. *192.168.0.0* mit *255.255.255.0*

Adressgruppen

Feld	Menü	Wert
Beschreibung	**Firewall->Adressen->Gruppen->Neu**	z. B. *be.IP*
IP-Version	**Firewall->Adressen->Gruppen->Neu**	*IPv4*
Auswahl	**Firewall->Adressen->Gruppen->Neu**	z. B. *Administrator* und *Geschäftsführer*

Dienstgruppen

Feld	Menü	Wert
Beschreibung	**Firewall->Dienste->Gruppen->Neu**	z. B. *Internetports*
Mitglieder	**Firewall->Dienste->Gruppen->Neu**	z. B. *http*, *http (SSL)* und *ftp*
Beschreibung	**Firewall->Dienste->Gruppen->Neu**	z. B. *Administrationsports*
Mitglieder	**Firewall->Dienste->Gruppen->Neu**	z. B. *http* und *telnet*

Filterregel 1: Gateway verwalten (Systemadministrator)

Feld	Menü	Wert
Quelle	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*be.IP*
Ziel	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*be.IP*
Dienst	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*Administrationsports*
Aktion	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*Zugriff*

Filterregel 2: Gateway als DNS-Proxy verwenden

Feld	Menü	Wert
Quelle	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*LOCAL*
Ziel	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*ANY*
Dienst	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*dns*
Aktion	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*Zugriff*
Quelle	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*Netzwerk_Intern*
Ziel	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*be.IP*
Dienst	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*dns*
Aktion	**Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu**	*Zugriff*

Filterregel 3: Zugriff von außen auf das Gateway verweigern

Feld	Menü	Wert
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*ANY*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*be.IP*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Verweigern*

Filterregel 4: Zugriff auf alle Dienste im Internet erlauben (Geschäftsführer)

Feld	Menü	Wert
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Geschäftsführer*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*any*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*

Filterregel 5: Zugriff auf das Internet erlauben (Mitarbeiter)

Feld	Menü	Wert
Quelle	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Netzwerk_Intern*
Ziel	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*ANY*
Dienst	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Internetports*
Aktion	**Firewall** -> **Richtlinien** -> **IPv4-Filterregeln** -> **Neu**	*Zugriff*

15 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)
- Zugriffsbeschränkung auf das Internet (Web-Filter)
- Zuordnung von eingehenden und ausgehenden Daten- und Sprachrufen zu authorisierten Benutzern (CAPI-Server)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Schutz des Benutzer-LAN (Diebstahlsicherung)
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)
- Bereitstellung öffentlicher Internetzugänge (Hotspot).
- Ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten (Wake-On-LAN)

15.1 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.

15.1.1 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. 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

Feld	Beschreibung
	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.

Feld	Beschreibung
	• *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.

15.1.2 DNS-Server

Im Menü **Lokale Dienste**->**DNS**->**DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

15.1.2.1 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.

Feld	Beschreibung
	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** = *Statisch* Mit der Einstellung *Beliebig* wird ein DNS-Server für alle Schnittstellen konfiguriert.
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte:

Feld	Beschreibung
	• *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.

15.1.3 Statische Hosts

Im Menü **Lokale Dienste**->**DNS**->**Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

15.1.3.1 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 BasisparameterStandarddomäne

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-

Feld	Beschreibung
	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. automatisch 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.

15.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung** wird eine Liste aller konfigurierten Weiterleitungen für definierte Domänen angezeigt.

15.1.4.1 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* 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

Feld	Beschreibung
	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 konifgurierten Schnittstelle weitergeleitet. • *DNS-Server*: Anfragen werden an einen 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 die 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.

15.1.5 Dynamische Hosts

Im Menü **Lokale Dienste**->**DNS**->**Dynamische Hosts** sehen Sie die relevanten Angaben zu den Dynamischen DNS-Einträgen.

15.1.6 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.

15.1.7 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.

Feld	Beschreibung
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

15.2 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.

15.2.1 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.

15.3 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.

15.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

15.3.1.1 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 genau so ein, wie er beim DynDNS-Provider registriert ist.

Feld	Beschreibung
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internetanbieters).
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 die eingegebenen Daten registriert sind. Es 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 und die aktuelle IP-Adresse der ausgewählten Schnitttelle an den Anbieter übermittelt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
HTTPS/SSL	Diese Option steht nur zur Verfügung, wenn der von Ihnen ausgewählte DynDNS-Anbieter SSL unterstützt. Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider** können Sie ggf. selbst einen Anbieter mit dieser Option einrichten. Aktivieren Sie die Option, um zwischen Ihrem Gerät und dem DynDNS-Anbieter eine verschlüsselte Verbindung mittels SSL aufzubauen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsüberprüfung	Aktivieren Sie diese Funktion, um das SSL-Zertifikat des Ser-

Feld	Beschreibung
	vers zu überprüfen.
IP-Version	Diese Option steht nur zur Verfügung, wenn der von Ihnen ausgewählte DynDNS-Anbieter für beide IP-Versionen über entsprechende Server-Adressen verfügt. Wählen Sie die IP-Version der Adresse, die Sie beim DynDNS-Anbieter aktualisieren wollen. Mögliche Werte: IPv4 IPv6. Um ggf. sowohl eine IPv4- als auch die IPv6-Adresse einer Schnittstelle zu aktualisieren, legen sie zwei Einträge mit ansonsten gleichen Einstellungen an.Informieren Sie sich bei Ihrem Anbieter, ob dieser Mehrfachaktualisierungen unterstützt!

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.

15.3.2 DynDNS-Provider

Im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

15.3.2.1 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. Welches Protokoll Ihr Anbiter verwendet, erfahren Sie in dessen Anleitung. Mögliche Werte: • *DynDNS* (Standardwert) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*

Feld	Beschreibung
	• *dyndnss* • *dyndns2*
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.
IPv6-Server	Geben Sie den Host-Namen oder die IPv6-Adresse des DynDNS-Servers ein, wenn Sie IPv6-Adressen aktualisieren wollen.
Supports SSL	Aktivieren Sie diese Option, wenn Ihr DynDNS-Anbieter SSL zur Absicherung der Datenübertragung unterstützt. Standardmäßig ist die Option deaktiviert.
Homepage	Hier können Sie eine Web-Adresse angeben, mit der Sie direkt auf die Seite des Anbieters gelangen.

15.4 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.

Konkrete Hinweise für die Konfiguration eines DHCP-Servers, eines DHCP-Clients oder eines DHCP-Relay-Servers (siehe auch *DHCP-Relay-Einstellungen* auf Seite 393) finden Sie am Ende des Kapitels unter *DHCP - Konfigurationsbeispiel* auf Seite 394.

15.4.1 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.

15.4.1.1 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 ein.

15.4.2 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 konfigurierten 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 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

15.4.2.1 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 die **Schnittstelle** angeschlossenen Ethernet verwendet werden soll oder für DHCP-Anfragen, die aus einem über Gateways erreichbaren 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 die **Schnittstelle** angeschlossenen Ethernet verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-

Feld	Beschreibung
	Anfragen aus einem über Gateways erreichbaren Ethernet verwendet. • *Lokal/Relais*: Der DHCP-Pool kann für lokale und für weitergeleitete DHCP-Anfragen aus direkt angeschlossenen bzw. über Gateways erreichbaren 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

Feld	Beschreibung
	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.

Feld	Beschreibung
	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* 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.

15.4.3 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.

15.4.3.1 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.

15.4.4 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

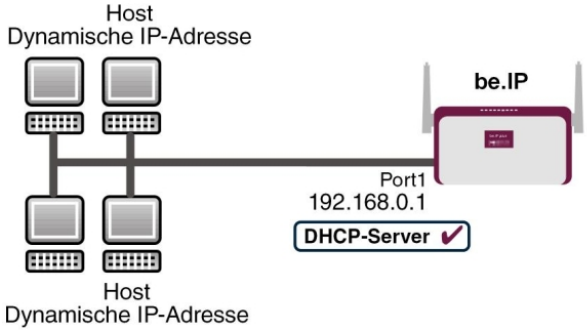
Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen. Der Standardwert ist `0.0.0.0`.
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein. Der Standardwert ist `0.0.0.0`.

15.4.5 DHCP - Konfigurationsbeispiel

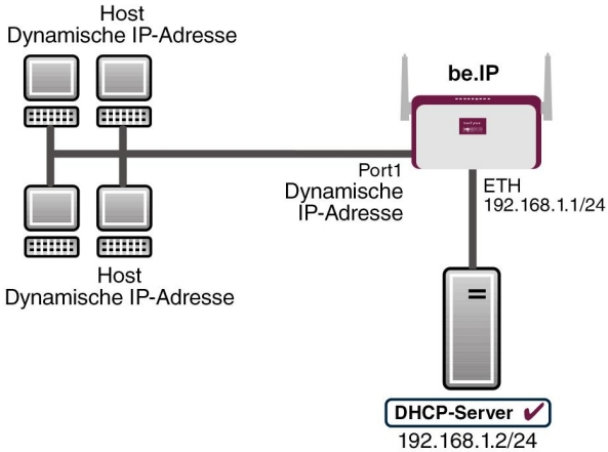
Voraussetzungen

- Optional ein DHCP-Server

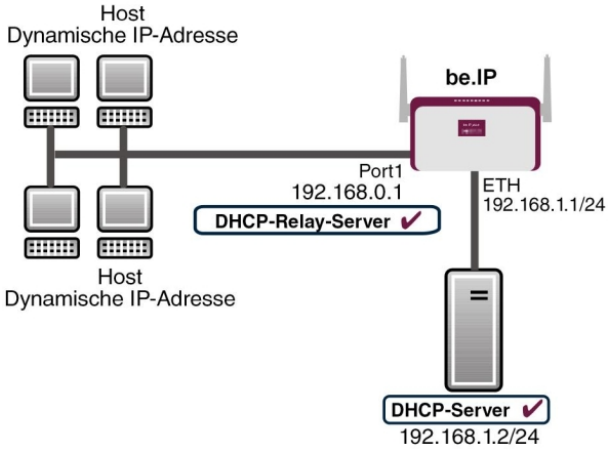
Beispiel-Szenarien



Beispielszenario als DHCP-Server



Beispielszenario als DHCP-Client



Beispielszenario als DHCP-Relay-Server

Konfigurationsziel

Sie können Ihr Gerät als DHCP-Server, als DHCP-Client oder als DHCP-Relay-Server einsetzen.

Konfigurationsschritte im Überblick

DHCP-Server

Feld	Menü	Wert
IP-Poolname	**Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration->Neu**	z. B. *IP-Pool-1*
IP-Adressbereich	**Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration->Neu**	z. B. *192.168.0.2* und *192.168.0.10*
Schnittstelle	**Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**	z. B. *en1-0*
IP-Poolname	**Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**	*IP-Pool-1*
Pool-Verwendung	**Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**	*Lokal*
Gateway	**Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen**	*Router als Gateway verwenden*

Feld	Menü	Wert
Lease Time	**Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen**	z. B. *120*
Für DNS- / WINS-Serverzuordnung zu verwendende IP-Adresse	**Lokale Dienste->DNS->Globale Einstellungen->Erweiterte Einstellungen**	z. B. *Eigene IP-Adresse*

DHCP-Client

Feld	Menü	Wert
Adressmodus	**LAN->IP-Konfiguration->Schnittstellen-> <en1-4>->** ✎	*DHCP*
DHCP-MAC-Adresse (optional)	**LAN->IP-Konfiguration->Schnittstellen-> <en1-4> ->** ✎ **->Erweiterte Einstellungen**	MAC-Adresse eines bestimmten DHCP-Servers

DHCP-Relay-Server

Feld	Menü	Wert
Primärer DHCP-Server	**Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen**	z. B. *192.168.1.2*
Sekundärer DHCP-Server (optional)	**Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen**	falls vorhanden

15.5 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**->**Erweitert**

15.5.1 DHCPv6-Server

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.

15.5.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um ein Option Set anzulegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Das Menü **Neu** 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.
Address assignment	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.

Feld	Beschreibung
	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.

15.5.2 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

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 Server-Priorität

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-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.

15.5.3 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

15.5.4 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

15.5.4.1 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.

15.6 CAPI-Server

Mit der Funktion CAPI-Server können Sie an Nutzer der CAPI-Anwendungen Ihres Geräts Benutzernamen und Passwörter vergeben. So stellen Sie sicher, dass nur authorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen über CAPI aufbauen können.

Der Dienst CAPI ermöglicht eingehenden und ausgehenden Daten- und Sprachrufen die Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Entfernte CAPI-Schnittstelle Ihres Geräts zugreifen. So können beispielsweise mit Ihrem Gerät verbundene Hosts Faxe empfangen und senden.

Hinweis

Alle eingehenden Rufe an die CAPI werden allen registrierten und "lauschenden" CAPI-Applikationen im LAN angeboten.

Im Auslieferungszustand ist für das Subsystem CAPI ein Benutzer mit dem Benutzernamen `default` ohne Passwort eingetragen.

Wenn Sie Ihre gewünschten Benutzer mit Passwort angelegt haben, sollten Sie den Benutzer *default* ohne Passwort löschen.

15.6.1 Benutzer

Im Menü **Lokale Dienste**->**CAPI-Server**->**Benutzer** wird eine Liste aller konfigurierten CAPI Benutzer angezeigt.

15.6.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

Das Menü **Lokale Dienste**->**CAPI-Server**->**Benutzer**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
Passwort	Geben Sie das Passwort ein, mit dem sich der Benutzer **Benutzername** identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
Zugriff	Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

15.6.2 Optionen

Das Menü **Lokale Dienste**->**CAPI-Server**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Server aktivieren	Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Faxkopfzeile	Wählen Sie aus, ob am oberen Seitenrand von ausgehenden Faxen die Faxkopfzeile gedruckt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Port des CAPI-Servers	Das Feld ist nur editierbar, wenn **Server aktivieren** aktiviert ist. Geben Sie die TCP-Port-Nummer für Remote-CA-PI-Verbindungen ein. Der Standardwert ist *2662*.

15.7 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.

Konkrete Hinweise für die Konfiguration des Aufgabenplaners finden Sie am Ende des Kapitels unter *Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)* auf Seite 424.

Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der bintec elmeg Gateways. 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.

15.7.1 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.

15.7.1.1 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.

Feld	Beschreibung
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* (nicht für alle Geräte verfügbar): 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. • *Status der GEO-Zone* : Die in **Aktionen** konfigurierten

Feld	Beschreibung
	und zugewiesenene Aktionen werden ausgelöst, wenn die definierten **GEO-Zonen** einen bestimmten Status annehmen.
Überwachte GEO-Zone	Nur für **Ereignistyp** *Status der GEO-Zone* Wählen Sie eine konfigurierte GEO-Zone aus.
GEO Zone Status	Nur für **Ereignistyp** *Status der GEO-Zone* Wählen Sie den **GEO Zone Status** aus. Mögliche Werte: • *Wahr*: Die aktuelle Position liegt innerhalb der definierten Zone. • *Falsch*: Die aktuelle Position liegt außerhalb der definierten Zone.
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 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

Feld	Beschreibung
	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*.

Feld	Beschreibung
Ziel-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden 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.
Erfolgreiche Versuche	Nur für **Ereignistyp** *Ping-Test* 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 Ver-	Nur für **Ereignistyp** *Ping-Test*

Feld	Beschreibung
suche	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*.
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

Feld	Beschreibung
	Wochentag 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.

15.7.2 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.

15.7.2.1 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 verändert. • *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. • *5,8 GHz-WLAN-Bandscan*: Nur für Geräte mit Wireless LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt.

Feld	Beschreibung
	• *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*

Feld	Beschreibung
	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 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.

Feld	Beschreibung
	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.
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*

Feld	Beschreibung
	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:

Feld	Beschreibung
	• *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. 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*

Feld	Beschreibung
	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. 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.

Feld	Beschreibung
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*

Feld	Beschreibung
	Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll. 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.

Feld	Beschreibung
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. 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

Feld	Beschreibung
	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*, *5,8 GHz-WLAN-Bandscan* und *Betriebsmodus*

Feld	Beschreibung
	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 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 Gerät abweichen.

15.7.3 Optionen

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

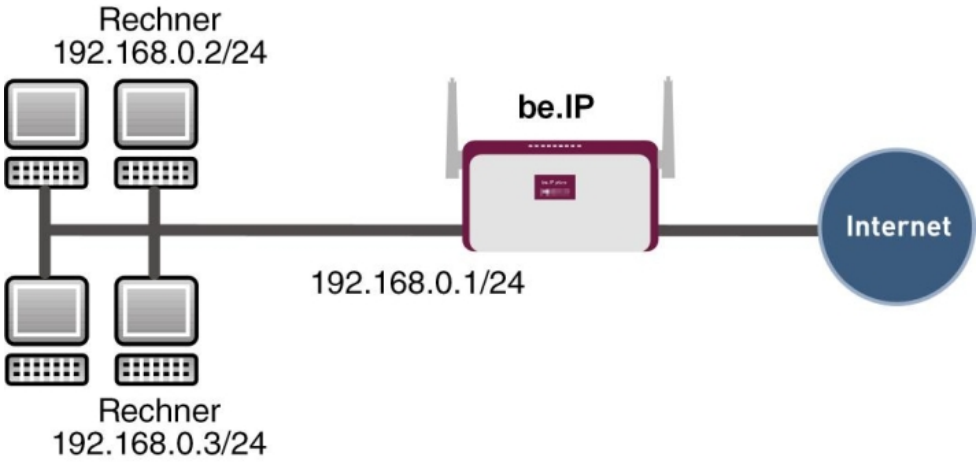
Feld	Beschreibung
Schedule-Intervall	Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll. Standardmäßig ist das Schedule-Intervall nicht aktiv. Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind. Möglich sind Werte zwischen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

15.7.4 Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)

Voraussetzungen

- Grundkonfiguration des Gateways

Beispielszenario



Beispielszenario Zeitgesteuerte Aufgaben

Konfigurationsziel

- Das Gateway soll täglich während der Nacht neu starten.
- Am Wochenende soll die WLAN-Schnittstelle abgeschaltet werden.
- Einmal im Monat soll die Konfiguration automatisch auf einen TFTP-Server gesichert werden.

Konfigurationsschritte im Überblick

Täglicher Neustart

Feld	Menü	Wert
Ereignisliste	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Neu*
Beschreibung	**Lokale Dienste->Scheduling->Aus-**	z. B. *Neustart aus-*

Feld	Menü	Wert
	löser->Neu	*lösen*
Ereignistyp	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Zeit*
Zeitbedingung	**Lokale Dienste->Scheduling->Auslöser->Neu**	Bedingungstyp = *Perioden*, Bedingungseinstellungen = *Täglich*
Startzeit	**Lokale Dienste->Scheduling->Auslöser->Neu**	Stunde *02* Minute *00*
Beschreibung	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *Neustart des Geräts*
Befehlstyp	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Neustart*
Ereignisliste	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Neustart auslösen*
Bedingung für Ereignisliste	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Alle*
Neustart des Geräts nach	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *60* Sekunden
Schedule-Intervall	**Lokale Dienste->Scheduling->Optionen**	*Aktiviert*, *55* sec

WLAN-Schnittstelle abschalten

Feld	Menü	Wert
Ereignisliste	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Neu*
Beschreibung	**Lokale Dienste->Scheduling->Auslöser->Neu**	z. B. *WLAN-Schnittstelle abschalten auslösen*
Ereignistyp	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Zeit*
Zeitbedingung	**Lokale Dienste->Scheduling->Auslöser->Neu**	Bedingungstyp = *Perioden*, Bedingungseinstellungen = *Samstag Sonntag*
Startzeit	**Lokale Dienste->Scheduling->Auslöser->Neu**	Stunde *00* Minute *00*
Stoppzeit	**Lokale Dienste->Scheduling->Auslöser->Neu**	Stunde *23* Minute *59*

Feld	Menü	Wert
Beschreibung	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *WLAN-Schnittstelle abschalten*
Befehlstyp	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Schnittstellenstatus*
Ereignisliste	**Lokale Dienste->Scheduling->Aktionen->Neu**	*WLAN-Schnittstelle abschalten auslösen*
Bedingung für Ereignisliste	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Alle*
Schnittstelle	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *vss1-0*
Schnittstellenstatus festlegen	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Inaktiv*
Schedule-Intervall	**Lokale Dienste->Scheduling->Optionen**	*Aktiviert*, *55* sec

Konfiguration monatlich sichern

Feld	Menü	Wert
Ereignisliste	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Neu*
Beschreibung	**Lokale Dienste->Scheduling->Auslöser->Neu**	z. B. *Konfigurationssicherung auslösen*
Ereignistyp	**Lokale Dienste->Scheduling->Auslöser->Neu**	*Zeit*
Zeitbedingung	**Lokale Dienste->Scheduling->Auslöser->Neu**	Bedingungstyp = *Tag des Monats*, Bedingungseinstellungen = *1*
Startzeit	**Lokale Dienste->Scheduling->Auslöser->Neu**	Stunde *03* Minute *00*
Beschreibung	**Lokale Dienste->Scheduling->Aktionen->Neu**	Konfiguration sichern
Befehlstyp	**Lokale Dienste->Scheduling->Aktionen->Neu**	Konfigurationsmanagement
Ereignisliste	**Lokale Dienste->Scheduling->Aktionen->Neu**	Konfigurationssicherung auslösen
Bedingung für Ereig-	**Lokale Dienste->Scheduling->Ak-**	Alle

Feld	Menü	Wert
nisliste	**tionen->Neu**	
Aktion	**Lokale Dienste->Scheduling->Aktionen->Neu**	Konfiguration exportieren
Server-URL	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *tftp://192.168.2.5*
CSV-Dateiformat	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Aktiviert*
Dateiname auf Server	**Lokale Dienste->Scheduling->Aktionen->Neu**	z. B. *monthly-backup.cf*
Dateiname in Flash	**Lokale Dienste->Scheduling->Aktionen->Neu**	*boot*
Konfiguration enthält Zertifikate/Schlüssel	**Lokale Dienste->Scheduling->Aktionen->Neu**	*Aktiviert*
Schedule-Intervall	**Lokale Dienste->Scheduling->Optionen**	*Aktiviert*, *55* sec

15.8 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Bei Geräten der **bintec WI**-Serie können Sie die Temperatur überwachen lassen.

Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

15.8.1 Hosts

Im Menü **Lokale Dienste**->**Überwachung**->**Hosts** wird eine Liste aller überwachten Hosts angezeigt.

15.8.1.1 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-Adresse ein.

Feld	Beschreibung
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 unzugänglich 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.

Feld	Beschreibung
	Die **Aktionen** *Aktivieren* und *Deaktivieren* werden ebenfalls abgebrochen, wenn die Hosts wieder als zugänglich 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 beim IP-Lastverteilung verwendet wird.

15.8.2 Schnittstellen

Im Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

15.8.2.1 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) Schnitt-

Feld	Beschreibung
	stelle(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*.

15.8.3 Ping-Generator

Im Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

15.8.3.1 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. • *Spezifisch* (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.

Feld	Beschreibung
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*.

15.9 ISDN-Diebstahlsicherung

Mit der Funktion ISDN-Diebstahlsicherung können Sie verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn unter **WAN**->**Internet + Einwählen**->**ISDN**-> das Feld **Immer aktiv** aktiviert ist.)

15.9.1 Optionen

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet, und die Schnittstellen werden administrativ auf "up" gesetzt.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.

Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

Das Menü **Lokale Dienste**->**ISDN-Diebstahlsicherung**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
ISDN-Diebstahlsicherungs-dienst	Aktivieren oder deaktivieren Sie die Funktion ISDN-Diebstahlsicherung. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Wählnummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die das Gateway wählt, wenn es sich selbst anruft.
Eingehende Nummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die mit der aktuellen Calling Party Number verglichen werden soll.
Ausgehende Nummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die als Calling Party Number gesetzt wird.
Überwachte Schnittstellen	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Fügen Sie mit **Hinzufügen** eine neue Schnittstelle hinzu. Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, auf welche die Funktion ISDN-Diebstahlsicherung angewendet werden soll.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Anzahl der Wählversuche	Geben Sie die Anzahl der Wählversuche ein, die das Gateway unternehmen soll, um sich nach einem Neustart über ISDN selbst anzurufen. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *3*.
Timeout	Geben Sie die Zeitspanne ein, die das Gateway warten soll, bis es sich nach einem erfolglosen Versuch erneut selbst anruft.

Feld	Beschreibung
	Mögliche Werte sind *2* bis *20*. Der Standardwert ist *5*.

15.10 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* .

15.10.1 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 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.

15.10.2 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.

Feld	Beschreibung
	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*.

15.11 Hotspot-Gateway

Wichtig

Das Hotspot-Gateway darf nicht mit aktiviertem IPv6 betrieben werden, da IPv6-Datenverkehr vom Hotspot-Gateway nicht erfasst wird und daher nicht kontrolliert werden kann.

Die **Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **Hotspot Solution** besteht aus einem vor Ort installierten bintec elmeg Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.

- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec elmeg Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS**->**Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec elmeg Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

  Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

  - Gehen Sie auf *www.bintec-elmeg.com* zu **Service/Support** -> **Services** -> **Online Services**.

  - Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

  - Sie erhalten daraufhin die Login-Daten des Hotspot Servers.

Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von bintec elmeg GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler

	festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Wird durch bintec elmeg individuell festgelegt
Password	Wird durch bintec elmeg individuell festgelegt

Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf *www.bintec-elmeg.com* zum Download zur Verfügung steht.

15.11.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec elmeg Gateway für die **Hotspot Solution**.

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller konfigurierten Hotspot Netzwerke angezeigt.

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktieren.

15.11.1.1 Bearbeiten oder Neu

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**-> konfigurien Sie die Hotspot Netzwerke. Wählen Sie die Schaltfläche **Neu**, um weitere Hotspot Netzwerke einzurichten.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, an der das Hotspot LAN oder WLAN angeschlossen ist. Bei Betrieb über LAN tragen Sie hier die Ethernet-Schnittstelle ein (z. B. die en1-0). Bei Betrieb über WLAN muss die WLAN-Schnittstelle ausgewählt werden, an der

Feld	Beschreibung
	der Access Point angeschlossen ist. **Achtung** Die Konfiguration Ihres Gerätes ist aus Sicherheitsgründen nicht über eine Schnittstelle möglich, die für den Hotspot konfiguriert ist. Wählen Sie hier daher sorgfältig die Schnittstelle aus, die Sie für den Hotspot nutzen wollen! Wenn Sie hier die Schnittstelle auswählen, über die die aktuelle Konfigurationssitzung stattfindet, geht die aktuelle Verbindung verloren. Sie müssen sich dann über eine erreichbare, nicht für den Hotspot konfigurierte Schnittstelle zur weiteren Konfiguration Ihres Geräts erneut anmelden.
Domäne am Hotspot-Server	Geben Sie den Domänennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.
Walled Garden	Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen. Standardmäßig ist die Funktion deaktiviert.
Walled Network / **Netzmaske**	Nur wenn **Walled Garden** aktiviert ist. Geben Sie die Netzadresse des **Walled Network** und die entsprechende **Netzmaske** des Intranet-Servers ein. Für den aus **Walled Network** / **Netzmaske** resultierenden Adressraum benötigen die Clients keine Authentifizierung. Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.
Walled Garden URL	Nur wenn **Walled Garden** aktiviert ist. Geben Sie die **Walled Garden URL** des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse er-

Feld	Beschreibung
	reichbar sein.
Geschäftsbedingungen	Nur wenn **Walled Garden** aktiviert ist. Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB´s auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. http://www.webserver.de/agb.htm. Die Seite muss im Adressraum des Walled Garden-Networks liegen.
Zusätzliche, frei zugängliche Domänennamen	Nur wenn **Walled Garden** aktiviert ist. Fügen Sie mit **Hinzufügen** weitere URLs oder IP-Adressen hinzu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
Aufzurufende Seite nach Login	Hier können Sie eine URL angeben, zu der ein Benutzer umgeleitet wrd, wenn er sich bei der Hotspot-Lösung angemeldet hat.
Sprache für Anmeldefenster	Hier können Sie die Sprache für die Start/Login-Seite auswählen. Folgende Sprachen werden unterstützt: *English*, *Deutsch*, *Italiano*, *Français*, *Español*, *Português* und *Nederlands* . Die Sprache kann auf der Start/Login-Seite selbst jederzeit umgeschaltet werden.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Tickettyp	Wählen Sie den Tickettyp aus. Mögliche Werte: • *Voucher*: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort. • *Benutzername/Passwort* (Standardwert): Benutzername und Passwort müssen eingegeben werden.
Zulässiger Hotspot-Client	Hier legen Sie fest, welche Art von Benutzern sich am Hotspot

Feld	Beschreibung
	anmelden dürfen. Mögliche Werte: • *Alle*: Alle Clients werden zugelassen. • *DHCP-Client*: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
Geräte pro Ticket	Geben Sie die maxmímale Anzahl Geräte pro Ticket an.
Anmeldefenster	Aktivieren oder deaktivieren Sie das Anmeldefenster. Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames. Wenn die Funktion aktiviert ist, wird auf der linken Seite das Anmelde-Formular angezeigt. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt. Standardmäßig ist die Funktion aktiv.
Pop-Up-Fenster für Statusanzeige	Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet. Standardmäßig ist die Funktion aktiv.
Standard-Timeout bei Inaktivität	Aktivieren oder deaktivieren Sie den **Standard-Timeout bei Inaktivität** Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet. Standardmäßig ist die Funktion aktiv. Der Standardwert ist *600* Sekunden.

15.11.2 Optionen

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Host für mehrere Standorte	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.

15.12 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**.

15.12.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

15.12.1.1 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 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*

Feld	Beschreibung
	• *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.

Feld	Beschreibung
	• *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 Ziel-IP-Adresse/Länge sind

Feld	Beschreibung
	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 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	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Ser-

Feld	Beschreibung
(802.1p/Layer 2)	vice, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Wertebereich *0* bis *7*. Der Standardwert ist *Nicht beachten*.

15.12.2 WOL-Regeln

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** wird eine Liste aller konfigurierten WOL-Regeln angezeigt.

15.12.2.1 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

Feld	Beschreibung
	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. • *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

Feld	Beschreibung
	Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.

15.12.3 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.

15.12.3.1 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.

15.13 BRRP

Im Menü **BRRP** können Sie eine Redundanz für Ihr Gateway konfigurieren.

Hinweis

Für Geräte der R23x-Serie und der RS-Serie benötigen Sie eine Lizenz.

BRRP (Bintec Router Redundancy Protocol) ist eine bintec elmeg-spezifische Implementierung des VRRP (Virtual Router Redundancy Protocol). Ein Router-Redundanzverfahren dient hauptsächlich dazu, die Verfügbarkeit eines physikalischen Gateways im LAN oder WAN sicherzustellen.

Begriffe und Definitionen

Zur Beschreibung der Funktion werden einige spezielle Begriffe verwendet. Folgende Begriffe werden im entsprechenden RFC und im Internet-Entwurf definiert.

BRRP Begriffe

Feld	Beschreibung
VRRP-Router	"Ein Router, der das Virtual Router Redundancy Protocol benutzt. Er kann in einen oder in mehrere "virtuelle Router" integriert sein."
Virtueller Router	"Ein abstraktes, von VRRP gesteuertes Objekt, das als Standard-Router für Hosts eines LAN verwendet wird. Es besteht aus einem Virtual Router Identifier (**ID des virtuellen Routers**) und einer IP-Adresse bzw. einer Gruppe zugehöriger IP-Adressen innerhalb eines gemeinsamen LAN. Ein VRRP-Router kann den Datenverkehr eines einzelnen virtuellen Routers oder mehrerer virtueller Router absichern."
IP Address Owner	"Der VRRP-Router, der die IP-Adresse(n) des virtuellen Routers als echte Schnittstellen- Adresse(n) besitzt. Es handelt sich um den Router, der, wenn er aktiv ist, auf Pakete für ICMP-Pings, TCP-Verbindungen etc. an eine dieser IP-Adressen antwortet."
Primary IP Address	"Eine IP-Adresse, die aus der Gruppe der echten Schnittstellenadressen gewählt wird. Eine mögliche Algorithmusoption ist die Auswahl der ersten Adresse. VRRP Advertisements werden immer mit der Primary IP-Adresse als Quelle des IP-Pakets verschickt."
VRRP Advertisement	Ein Keepalive, das der Master zu den Backup-Gateways schickt, um seine Erreichbarkeit zu signalisieren.
Virtual Router Master	"Der VRRP-Router, der das Weiterleiten der Pakete übernimmt, die an die mit dem "virtuellen Router" verbundenen IP-Adressen geschickt wurden, und der für die Beantwortung von ARP (Address Resolution Protocol) Requests an diese IP-Adressen zuständig ist."
Virtual Router Backup	"Die Gruppe der VRRP-Router, welche die Verantwortung für das Weiterleiten übernehmen, falls der Master ausfallen sollte." Im Backup-Status sind diese VRRP-Router inaktiv, d.h. beantworten keine ARP-Requests."

15.13.1 Virtuelle Router

Bei der Verwendung eines Router-Redundanzprotokolls werden mehrere Router zu einer logischen Einheit zusammengefasst. Das Router-Redundanzprotokoll BRRP verwaltet die beteiligten Router und organisiert im einzelnen Folgendes:

Es stellt sicher, dass jeweils nur ein Router innerhalb des logischen Verbunds aktiv ist.

Es gewährleistet, dass bei Ausfall des aktiven Routers ein anderer Router die Funktion des ausgefallenen Geräts übernimmt. Wann welcher Router aktiv ist, wird über eine dem Router zugeordnete Priorität bestimmt.

Nehmen wir als Beispiel ein einfaches Szenario, in dem Gateway A den Internetzugang der Hosts in einem LAN ermöglicht. Wenn dieses Gateway ausfällt, haben alle Hosts keinen Zugang zum Internet, deren Routen statisch konfiguriert sind. Um den Hosts weiterhin Zugang zum Internet zu ermöglichen, bietet Gateway B allen Hosts im LAN den Dienst an, den vorher Gateway A durchgeführt hat. Alle Aufgaben eines virtuellen Routers und das Umschalten von Diensten von einem Gateway auf das andere werden von dem BRRP-Redundanzprotokoll gesteuert.

Das BRRP folgt den Spezifikationen in RFC 2338 und dem entsprechenden Internet- Entwurf (siehe *www.ietf.org*).

Die Konfiguration des Router-Redundanzverfahrens wird in folgenden Schritten durchgeführt:

- Konfiguration der Schnittstelle, über welche die BRRP-Advertisement-Datenpakete geschickt werden.

Hinweis

Diese Schnittstelle wird zur Übertragung der BRRP-Advertisement-Datenpakete sowie eventuell zur Übertragung von Keepalive-Monitoring-Datenpaketen verwendet. Zur Übertragung der Nutzdaten muss eine andere Schnittstelle im nächsten Schritt konfiguriert werden.

Die Konfiguration der Advertisement-Schnittstelle wird im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu** unter **BRRP Advertisement-Schnittstelle** vorgenommen.

Nur der aktive Router des Routerverbunds sendet Advertisement-Datenpakete. Die IPv4-Multicast-Adresse 224.0.0.18 dient als Zieladresse für alle Router, die Bestandteil des Routerverbundes sind. Alle passiven Router des Verbundes müssen diese Adresse überwachen, damit sie bei Ausbleiben der Advertisement-Datenpakete entsprechend ihrer Priorität und der sonstigen BRRP-Konfiguration reagieren können.

- Konfiguration der Schnittstelle zur Übertragung von Nutzdaten (Konfiguration der virtuellen Schnittstelle).

  Eine virtuelle Schnittstelle wird über die Zuweisung zu einem virtuellen Router über das BRRP-Router-Redundanzprotokoll aktiviert bzw. deaktiviert.

  Die Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu**->**Ethernet-Schnittstelle** vorgenommen.

  In diesem Schritt konfigurieren Sie die IP-Adresseinstellungen und ordnen die Schnittstelle einem virtuellen Router zu. Darüber hinaus werden die Eigenschaften des virtuellen Routers (z. B. die Priorität) festgelegt.

Hinweis

Das System vergibt die MAC-Adresse der virtuellen Schnittstelle nach folgendem Schema automatisch: 00:00:5E:00:01:<ID des virtuellen Routers>. Die ID des virtuellen Routers bestimmt somit die MAC-Adresse der Schnittstelle, die zur Übertragung der Nutzdaten verwendet wird.

Die Konfiguration der virtuellen Schnittstelle (MAC-Adresse, IP-Adresse) sowie die Konfiguration des virtuellen Routers (Sendeintervall für Advertisements, Umschalttoleranz) muss innerhalb des logischen Verbundes auf allen Routern mit derselben Virtual Router ID identisch sein.

Sie müssen IP-Adressen aus unterschiedlichen Subnetzen für die Advertisement-Schnittstelle und für die virtuelle Schnittstelle verwenden.

Alle virtuellen Schnittstellen auf einem physikalischen Router sollten normalerweise dieselbe Priorität haben.

- Konfiguration der Synchronisation zwischen den virtuellen Routern, sowie Konfiguration der Ereignisse, die zu einem Umschalten des Betriebszustandes der virtuellen Router führen.

  Über die Steuerung des Betriebszustandes eines virtuellen Routers wird implizit auch der Betriebszustand der Schnittstelle gesteuert, die mit dem virtuellen Router verknüpft ist. Da im Fehlerfall alle Schnittstellen eines Geräts deaktiviert werden müssen, muss der Betriebszustand aller Schnittstellen eines Geräts synchronisiert werden. Die Synchronisation ist notwendig, wenn mehrere Schnittstellen auf einem Gerät überwacht werden. Diese Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**VR-Synchronisation**->**Neu** vorgenommen.
- Einschalten des Redundanzverfahrens. Diese Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**Optionen** vorgenommen.

Im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu** konfigurieren Sie die Advertisement-Schnittstelle und die virtuelle(n) Schnittstelle(n). Sie müssen auf allen physikalischen Routern, die am Redundanzverfahren teilnehmen, dieselben virtuellen Router mit denselben Schnittstellen konfigurieren. (Die virtuellen Router haben jedoch auf den verschiedenen physikalischen Routern unterschiedliche Priorität.)

15.13.1.1 Neu

Wählen Sie die Schaltfläche **Neu** um weitere Virtuelle Router zu konfigurieren.

Das Menü **Lokale Dienste**->**BRRP**->**Virtuelle Router**->**Neu** besteht aus folgenden Feldern:

Felder im Menü BRRP Advertisement-Schnittstelle

Feld	Beschreibung
Ethernet-Schnittstelle	Wählen Sie die Schnittstelle aus, über die BRRP-Advertisement-Pakete versendet und erwartet werden. Wenn Sie einen virtuellen Router bearbeiten, wird die Ethernet-Schnittstelle angezeigt und kann nicht verändert werden. Hinweis: Die Ethernet-Schnittstelle zur Versendung der Advertisements ist immer up and running und kann daher nicht als **Schnittstelle des virtuellen Routers** verwendet werden.
IP-Adresse	Zeigt die IP-Adresse(n) der Schnittstelle an, über die BRRP-Advertisement-Pakete versendet und erwartet werden.

Felder im Menü BRRP Überwachte Schnittstelle

Feld	Beschreibung
Schnittstelle des virtuellen Routers	Zeigt an, auf welcher physikalischen Schnittstelle die virtuelle Schnittstelle basiert, wenn eine neue virtuelle Schnittstelle angelegt wird. Die Bezeichnung der virtuellen Schnittstelle wird beim Anlegen automatisch vergeben. Zeigt die Bezeichnung der virtuellen Schnittstelle an, wenn eine bereits angelegte virtuelle Schnittstelle bearbeitet wird.
IP-Adresse des virtuellen Routers	Geben Sie die IP-Adresse und die Netzmaske des virtuellen Routers ein. Hier geben Sie die IP-Adresse ein, die Sie im lokalen Netz als eigentliche Gateway-IP-Adresse verwenden wollen.

Feld	Beschreibung
	Hinweis Um Probleme im LAN zu vermeiden, dürfen die **IP-Adresse** für Advertisements und die **IP-Adresse des virtuellen Routers** nicht aus demselben Subnetz stammen.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers. Diese ID identifiziert den "virtuellen Router" innerhalb des LAN und ist Bestandteil jedes BRRP-Advertisement-Pakets, das vom aktuellen Master gesendet wird. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*.
Priorität der virtuellen Schnittstelle	Setzen Sie die gesendete BRRP-Priorität der Schnittstelle für den virtuellen Router fest. Höhere Prioritäten bestimmen die Schnittstellen des Masters in der Initialisierungs-Phase und bei aktivem **Pre-Empt-Modus (zurück in Master-Status)**. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *100*. Eine Priorität von 255 wird für Router genutzt, deren IP-Adresse mit der IP-Adresse des virtuellen Routers übereinstimmt.

Im Menü **Erweiterte Einstellungen** müssen Sie alle Parameter für alle virtuellen Router auf allen Geräten, die am Routerverbund teilnehmen, identisch konfigurieren. Wir empfehlen Ihnen, die Voreinstellungen zu belassen.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Sendeintervall für Advertisements	Legen Sie fest, wie oft ein BRRP-Advertisement-Paket gesendet wird, wenn der virtuelle Router als Master definiert ist. Nur der aktuelle Master sendet über Multicast BRRP-Advertisements, welche auch die ID und die Priorität des Masters enthalten. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*. Der Wert wird in Sekunden angegeben, der Standardwert ist *1*.

Feld	Beschreibung
	Basierend auf diesem Sendeintervall für Advertisements läuft routerintern ein Advertisement Timer, nach dessen Ablauf ein Advertisement-Paket gesendet wird.
Umschalttoleranz	Legen Sie die Anzahl der BRRP Advertisements fest, die aufeinanderfolgend fehlen dürfen, bevor der Backup Router mit dem höchsten Prioritätswert annimmt, dass der Master inaktiv ist und er die Rolle des Masters übernimmt. Basierend auf dem Parameter **Master down trials** läuft routerintern ein Master Down Timer, nach dessen Ablauf vom Backup Router angenommen wird, dass der Master nicht erreichbar ist, falls kein Advertisment empfangen wurde. Das effektive Master Down Intervall entspricht der Zeit errechnet aus der Anzahl erwarteter, aber ausgelassener BRRP Advertisements, dem Advertisement Interval und der sogenannten Skew Time, welche einen minimalen Zeitraum abhängig von der Priorität hinzufügt. Je höher die Priorität, desto kürzer ist die hinzugefügte Zeit, so dass ein Backup-Router mit höherer Priorität früher reagiert als einer mit niedrigerer Priorität). Mögliche Werte sind *1* bis *255*, der Standardwert ist *10*.
Pre-Empt-Modus (zurück in Master-Status)	Legen Sie fest, ob ein Backup-Router mit höherer Priorität Vorrang hat vor einem Master-Router mit niedriger Priorität. Der Pre-Empt-Modus dient dazu, unnötige Umschaltvorgänge zu verhindern. Mit *Aktiviert* wird die Funktion aktiv. Der Router mit der höheren Priorität hat immer Vorrang. Das heißt, bei Wiedererreichbarkeit des eigentlichen Master-Routers wird dieser auch immer aktiv. Wenn die Funktion nicht aktiv ist, bleibt der aktuell aktive Backup-Router auch nach Wiedererreichbarkeit des eigentlichen Master-Routers weiterhin aktiv, obwohl die Priorität des Master-Routers höher ist als die Priorität des derzeitig aktiven Backup-Routers. Standardmäßig ist die Funktion aktiv. Beachten Sie eine Ausnahme: Wird als **Priorität der virtuellen Schnittstelle** *255* ausgewählt, erhält das Gateway mit dieser Priorität auf jeden Fall die Masterrolle, d.h. die Einstellung in

Feld	Beschreibung
	Pre-Empt-Modus (zurück in Master-Status) wird nicht berücksichtigt. Wählen Sie daher zur Nutzung von Pre-Empt-Modus eine **Priorität der virtuellen Schnittstelle** kleiner *255*.
Authentisierung aktivieren	Aktivieren oder deaktivieren Sie die Authentisierung. Mit *Aktiviert* wird die Funktion aktiv. Wenn die Funktion aktiv ist, wird ein Eingabefeld angezeigt. Hier geben Sie den Authentisierungsschlüssel ein. Hinweis: Beachten Sie, dass der Authentisierungsschlüssel für alle am Routerverbund teilnehmenden virtuellen Router gleich sein muss. Standardmäßig ist die Funktion nicht aktiv.

15.13.2 VR-Synchronisation

Im Menü **Lokale Dienste**->**BRRP**->**VR-Synchronisation** wird der Watchdog Daemon konfiguriert, d. h. Sie legen fest, wie Statusänderungen gehandhabt werden.

Nach Öffnen des Menüs **Lokale Dienste**->**BRRP**->**VR-Synchronisation** wird eine Liste aller Synchronisationen angezeigt. Sie können entweder virtuelle Router untereinander synchronisieren oder Schnittstellen. Neue Synchronisationen können im Menü **Neu** hinzugefügt werden.

Sie können z. B. die beiden virtuellen Router R1 und R2 über BRRP synchronisieren. Dazu müssen Sie zwei Einträge anlegen. Für den ersten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R1 und als **Synchronisations-VR/Schnittstelle** R2 verwenden. Für den zweiten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R2 und als **Synchronisations-VR/Schnittstelle** R1 konfigurieren.

15.13.2.1 Neu

Wählen Sie die Schaltfläche **Neu** um neue Synchronisationen hinzuzufügen.

Das Menü **Lokale Dienste**->**BRRP**->**VR-Synchronisation**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Monitoring-VR/Schnittstelle

Feld	Beschreibung
Monitoring-Modus	Zeigt an, welcher Mechanismus für die Überwachung eines vir-

Feld	Beschreibung
	tuellen Routers angewendet wird. Mögliche Werte: • *BRRP*: Die BRRP-spezifischen Status-Advertisements werden zur Statusermittlung des Masters verwendet. (Der Master sendet Advertisements gemäß seiner Konfiguration im Menü **Lokale Dienste**->**BRRP**->**Virtuelle Router**->**Neu**->**Erweiterte Einstellungen**.)
ID des virtuellen Routers	Wählen Sie einen virtuellen Router über die **ID des virtuellen Routers** und legen Sie durch die Auswahl fest, welche Schnittstelle kontrolliert werden soll. Wählbar sind die vorher definierten IDs (siehe **ID des virtuellen Routers** im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu** im Bereich **BRRP Überwachte Schnittstelle**). Der Watchdog Daemon fragt die in **Virtuelle Router** festgelegten Detailinformationen ab.

Felder im Menü Synchronisations-VR/Schnittstelle

Feld	Beschreibung
Sychronisationsmodus	Zeigt an, mit welchem Mechanismus virtuelle Router bzw. Schnittstellen synchronisiert werden: Mögliche Werte: • *BRRP*: BRRP wird für die Synchronisierung der virtuellen Router verwendet.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers, der synchronisiert werden soll. Über die Synchronisation des virtuellen Routers wird implizit die mit dem virtuellen Router verbundene virtuelle Schnittstelle synchronisiert.

15.13.3 Optionen

Im Menü **Lokale Dienste**->**BRRP**->**Optionen** können Sie die Funktion BRRP ein- oder ausschalten.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
BRRP aktivieren	Aktivieren oder deaktivieren Sie die Funktion BRRP. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

15.14 Trace

15.14.1 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, dass 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.

15.14.2 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.

16 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.

16.1 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.

16.1.1 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.

16.1.1.1 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.

16.2 Diagnose

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

16.2.1 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.

16.2.2 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.

16.2.3 Traceroute-Test

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

16.3 Software &Konfiguration

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

16.3.1 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 unter *www.bintec-elmeg.com* . Hier finden Sie auch aktuelle Dokumentationen.

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.

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden"

Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.

Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` 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 die **Los**-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.

Feld	Beschreibung
	• *Konfiguration importieren*: Wählen Sie in **Dateiname** eine 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. Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben! • *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. • *Konfigurationssicherung 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 *www.bintec-elmeg.com* 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. Folgende Optionen erfordern, dass eine MMC/SD-Karte gesteckt ist (sofern von Ihrem Gerät unterstützt) oder dass Ihr Ge-

Feld	Beschreibung
	rät über einen zusätzlichen internen Speicher verfügt: • *Voice Mail Wave-Dateien importieren* (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist, sofern von Ihren Gerät unterstützt): Wählen Sie in **Dateiname** die Datei *vms_wavfiles.zip* aus, die Sie importieren wollen. • *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. • *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 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.

Feld	Beschreibung
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 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 Sys-

tem- Dateien angezeigt.

16.4 Neustart

16.4.1 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.

16.5 Factory Reset

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

17 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.

17.1 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.

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter *www.bintec-elmeg.com*).

17.1.1 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.

17.1.1.1 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)

Feld	Beschreibung
	local0.
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*

17.2 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.

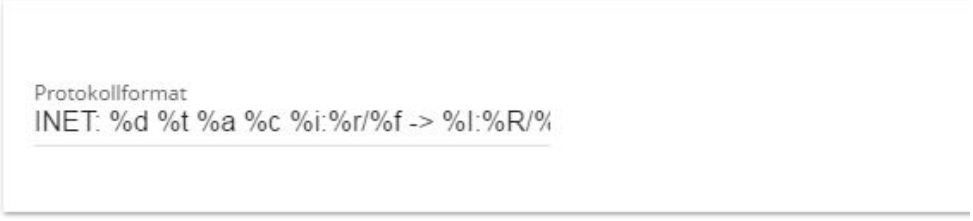
17.2.1 Schnittstellen

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.

17.2.2 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

Feld	Beschreibung
%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]

17.3 Benachrichtigungsdienst

Bisher war es schon 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.

17.3.1 Benachrichtigungsempfänger

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

17.3.1.1 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

Feld	Beschreibung
	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 Rogue AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • *Neuer Access Point (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 Sys-

Feld	Beschreibung
	log-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*
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*.

17.3.2 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.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Maximale 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 Mailadresse 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 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.

Feld	Beschreibung
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.

Felder im Menü SMS Parameter (nur für Geräte mit UMTS)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS. Die Aktivierung von *Uneingeschränkt* erlaubt eine beliebige Anzahl an versendeten SMS. Der Standardwert beträgt 10 SMS pro Tag. Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von *Uneingeschränkt*.

17.4 SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll in der IP-Protokollfamilie für den Transport von Managementinformationen über Netzwerkkomponenten.

Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine MIB. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren,

zu kontrollieren und zu überwachen. Mit Ihrem Gerät haben Sie ein solches SNMP-Werkzeug erhalten, den Konfigurationsmanager. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HPOpenView verwenden.

Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

17.4.1 SNMP-Trap-Optionen

Zur Überwachung des Systems wird im Fehlerfall unaufgefordert eine Nachricht gesendet, ein sogenanntes Trap-Paket.

Im Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Optionen** können Sie das Senden von Traps konfigurieren.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
SNMP Trap Broadcasting	Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll. Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
SNMP-Trap-UDP-Port	Nur wenn **SNMP Trap Broadcasting** aktiviert ist. Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll. Möglich ist jeder ganzzahlige Wert. Der Standardwert ist *162*.
SNMP-	Nur wenn **SNMP Trap Broadcasting** aktiviert ist.

Feld	Beschreibung
Trap-Community	Geben Sie eine SNMP-Kennung ein. Diese muss vom SNMP-Manager mit jeder SNMP-Anforderung übergeben werden, damit sie von Ihrem Gerät akzeptiert wird. Möglich ist eine Zeichenkette mit *0* bis *255* Zeichen. Der Standardwert ist *snmp-Trap*.

17.4.2 SNMP-Trap-Hosts

In diesem Menü geben Sie an, an welche IP-Adressen Ihr Gerät die SNMP-Traps schicken soll.

Im Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts** wird eine Liste aller konfigurierten SNMP-Trap-Hosts angezeigt.

17.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Das Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

17.5 SIA

17.5.1 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.

18 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.

18.1 Internes Protokoll

18.1.1 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.

18.2 IPSec

18.2.1 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.

Feld	Beschreibung
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)	Zeigt die Parameter der IKE (Phase 1) SAs an.

Feld	Beschreibung
Rolle / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	
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.

18.2.2 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.

18.3 ISDN/Modem

18.3.1 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*.
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.

Feld	Beschreibung
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*.

18.3.2 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*, *IPSec*, *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.

18.4 Schnittstellen

18.4.1 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 v -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.
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 Q -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.

18.4.2 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.

18.5 Bridges

18.5.1 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.

18.6 Hotspot-Gateway

18.6.1 Hotspot-Gateway

Im Menü **Monitoring**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Werte in der Liste Hotspot-Gateway

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

18.7 QoS

Im Menü **Monitoring**->**QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

18.7.1 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.

18.8 OSPF

Im Menü **Monitoring**->**OSPF** werden Informationen zu OSPF überwacht. Der OSPF-Monitor ist horizontal in drei Bereiche gegliedert und zeigt Informationen zu OSPF-Schnittstellen, den erkannten Nachbarn sowie die Link State Database Einträge.

18.8.1 Status

Im Menü **Monitoring**->**OSPF**->**Status** wird eine Liste aller Schnittstellen angezeigt, für die OSPF konfiguriert wurde.

Werte in der Liste Status

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: *Alle*, *OSPF-Schnittstellen*, *OSPF-Nachbarn* und *OSPF Link State Database*

Im Bereich **OSPF-Schnittstellen** sind alle aktivierten OSPF-Interfaces aufgelistet:

Werte in der Liste OSPF-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die OSPF konfiguriert wurde.
Designated Router (DR)	Zeigt die IP-Adresse des Designated Routers an. Der Designated Router generiert Network Links und verteilt diese an alle Gateways innerhalb des BMA-Netzwerkes (BMA = Broadcast Multi Access Network, z.B. Ethernet, FDDI, Token-ring). Ein Designated Router wird bei None BMA-Netzwerken, z.B. X.25, Frame Relay, ATM, nicht angezeigt.
Backup Designated Router (BDR)	Zeigt die IP-Adresse des Backup Designated Routers an.
Admin-Status	Zeigt den OSPF-Admin-Status (*Aktiviert* oder *Deaktiviert*) der Schnittstelle an.
Status	Der hier angezeigte OSPF-Status der Schnittstelle kann folgende Werte annehmen: • *Inaktiv*: OSPF läuft nicht auf dieser Schnittstelle. • *Wartend*: Die Initialphase des OSPF, in der DR und BDR bestimmt werden. • *Punkt-zu-Punkt*: Die Schnittstelle ist eine Point-To-Point-Schnittstelle. DR oder BDR werden nicht angezeigt.

Feld	Beschreibung
	• *Designated Router*: Das Gateway ist der Designated Router innerhalb des BMA-Netzwerkes. • *Designated Router Backup*: Das Gateway ist der Backup Designated Router innerhalb des BMA-Netzwerkes. • *Anderer Designated Router*: Ein anderes Gateway ist Designated Router oder Backup Designated Router innerhalb des BMA-Netzwerkes.

Im Bereich **Nachbar** werden die Nachbar-Gateways aufgelistet, die über das HELLO Protokoll identifiziert wurden:

Werte in der Liste OSPF-Nachbarn

Feld	Beschreibung
Nachbar	Zeigt die IP-Adresse des Nachbar-Gateways an.
Router-ID	Zeigt die systemweite Router-ID des Nachbar-Gateways an.
Schnittstelle	Zeigt die Schnittstelle an, über das dieses Nachbar-Gateway identifiziert wurde.
Status	Der OSPF-Status mit diesem Nachbar-Gateway kann folgende Werte annehmen: • *Inaktiv*: Die Verbindung zu diesem OSPF-Nachbarn ist inaktiv. • *Init*: Die Initialphase. Ein HELLO Paket wird vom Nachbarn empfangen. • *Bidirectional*: Bidirektionale Kommunikation mit dem Nachbarn. Die übermittelten HELLO Pakete sind vom Nachbar-Gateway angenommen worden (mit korrekten Parametern). • *Austausch starten*: Der Austausch von Database Description Paketen zwischen den Gateways hat begonnen. • *Austausch*: Aktiver Austausch von Database Description Paketen mit dem Nachbarn. • *Laden*: Das Gateway tauscht nun Link State Advertisements mit dem Nachbarn aus. • *Fertig*: Die Link State Datenbanken des Gateways und seines Nachbarn sind nun synchronisiert.

Im Bereich für die Link State Database werden die Header aller Link State Advertisements (LSA) aufgelistet.

Werte in der Liste OSPF Link State Database

Feld	Beschreibung
Bereich	Zeigt die Bereichsdatenbank an, der das LSA zugeordnet ist.
Typ	Zeigt den LSA-Typ an. Es gibt fünf LSA-Typen: Router Link, Network Link, Summary Link, Summary ASBR, und AS External.
Link-Status-ID	Zeigt die Link State ID des LSA an. Die Bedeutung der Link State ID hängt vom Typ des Advertisments ab.
Router-ID	Identifiziert das Gateway, das dieses LSA generiert hat.
Sequence Age	Zeigt das Alter des LSA (in Sekunden) an.

18.8.2 Statistik

Im Menü **Monitoring**->**OSPF**->**Statistik** werden die aktuellen Werte und Aktivitäten angezeigt.

Werte in der Liste Statistik

Feld	Beschreibung
Empfangene Hello Nachrichten	Zeigt die Anzahl der empfangenen Hello-Pakete an.
Gesendete Hello Nachrichten	Zeigt die Anzahl der gesendeten Hello-Pakete an.
Empfangene Database Description Pakets	Zeigt die Anzahl der empfangenen Datenbankeinträge.
Gesendete Database Description Pakets	Zeigt die Anzahl der gesendeten Datenbankeinträge.
Empfangene Link State Acknowledge Pakets	Zeigt die Anzahl der empfangenen Link State Acknowledge Pakete.
Gesendete Link State Acknowledge Pakets	Zeigt die Anzahl der gesendeten Link State Acknowledge Pakete.
Empfangene Link State Request Pakets	Zeigt die Anzahl der empfangenen Link State Request Pakete.
Gesendete Link State Request Pakets	Zeigt die Anzahl der gesendeten Link State Request Pakete.
Empfangene Link State Update Pakets	Zeigt die Anzahl der empfangenen Link State Update Pakete.
Gesendete Link State	Zeigt die Anzahl der gesendeten Link State Update Pakete.

Feld	Beschreibung
Update Pakets	
Aktualisierung der Routing-Tabelle aufgrund von Summary Link Advertisements	Zeigt die Anzahl der inkrementellen Routing-Tabellen-Updates an, die durchgeführt wurden, wenn neue Summary Link Advertisements empfangen wurden.
Updates der Routing-Tabelle aufgrund von External Advertisements	Zeigt die Anzahl der inkrementellen Routing-Tabellen-Updates an, die durchgeführt wurden, wenn neue externe Advertisements empfangen wurden.

18.9 PIM

18.9.1 Allgemeine Statusangaben

Im Menü **Monitoring**->**PIM**->**Allgemeine Statusangaben** wird der Status aller konfigurierten PIM Komponenten angezeigt.

Werte in der Liste Allgemeine Statusangaben

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: *Alle*, *PIM-Schnittstellen*, *PIM-Nachbarn* und *Zuordnung Multicast-Gruppen zu RPs*

Werte in der Liste PIM-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der PIM-Schnittstelle an.
IP-Adresse	Zeigt die primäre IP-Adresse der PIM-Schnittstelle an.
Designated Router (DR)	Zeigt die primäre IP-Adresse des Designated Routers auf dieser PIM-Schnittstelle an.

Werte in der Liste PIM-Nachbarn

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, über die der PIM Neighbor erreicht wird.

Feld	Beschreibung
Generation ID	Zeigt die ID des Nachbar-Gateways an.
IP-Adresse	Zeigt die primäre IP-Adresse des PIM Neighbors an.
Uptime	Zeigt an, wie lange der letzte PIM Neighbor ein Nachbar des lokalen Routers ist.
Expiry Timer	Zeigt an, wann der PIM Neighbor nicht mehr als Nachbar eingetragen ist. Wird der Wert *0* angezeigt, bleibt der PIM Neighbor immer als Nachbar eingetragen.

Werte in der Liste Zuordnung Multicast-Gruppen zu RPs

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Präfixlänge der Multicast-Gruppe	Zeigt die dazugehörige Netzmaske an.
IP-Adresse des Rendezvous Points	Zeigt die IP-Adresse des Rendevous Points an.

18.9.2 Nicht-schnittstellen-spezifischer Status

Das Menü **Monitoring**->**PIM**->**Nicht-schnittstellen-spezifischer Status** enthält Status-Angaben für alle PIM-Schnittstellen.

Werte in der Liste Nicht-schnittstellen-spezifischer Status

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: *Alle*, *(*,*,RP) Status*, *(*,G) Status*, *(S,G) Status* und *(S,G,RPT) Status*

Werte in der Liste (*,*,RP) Status

Feld	Beschreibung
IP-Adresse des Rendezvous Point	Zeigt die IP-Adresse des Rendezvous Point (RP) der Gruppe an.
Upstream Join State	Der Upstream (*,*,RP) Join/Prune Status gibt den Status der Upstream (*,*,RP) State Machine in der PIM-SM Spezifikation wieder.
Upstream Nachbar-	Zeigt die primäre IP-Adresse des Upstream Neighbors, oder un-

Feld	Beschreibung
IP-Adresse	known(0), wenn die Upstream Neighbor IP-Adresse nicht bekannt ist oder es sich nicht um einen PIM Neighbor handelt.
Uptime	Zeigt den Zeitraum an, wie lange der RP besteht.
Upstream Join Timer	Der Join/Prune Timer wird verwendet, um periodisch Join(*,*,RP) Nachrichten zu senden, und um Prune(*,*,RP) Nachrichten von Peers auf einer Upstream LAN Schnittstelle zu korrigieren.

Werte in der Liste (*,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Upstream Nachbar-IP-Adresse	Zeit die primäre IP-Adresse des Neighbors auf pimStarGRPFIfIndex an, zu der der lokale Router periodisch (*,G) Join Nachrichten schickt. Der InetAddressTyp ist durch das Objekt pimStarGUpstreamNeighborType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF'(*,G) genannt.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der Next Hop nicht bekannt ist.
Upstream Join State	Zeigt an, ob der lokale Router dem RP Tree der Gruppe beitreten soll. Dieses entspricht dem Status der Upstream (*,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (*,G) Join Nachricht auf pimStarGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Upstream Join Timer genannt. Er hat den Wert `0`, wenn der Timer deaktiviert ist.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimSGAddressType definiert.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Neighbors auf pimSGRPFIfIndex an, zu dem der Router periodisch (S,G) Join Nachrichten schickt. Der Wert ist `0`, wenn der RPF Next Hop nicht bekannt

Feld	Beschreibung
	oder kein PIM Neighbor ist. InetAddressType wird im Objekt pimSGAddressType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF'(S,G) genannt.
Upstream Join State	Zeigt an, ob der lokale Router den Shortest-Path-Tree für die Quelle und die Gruppe, die durch diesen Eintrag dargestellt wird, beitreten soll. Dieses entspricht dem Status der Upstream (S,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (S,G) Join Nachricht auf pimSGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Upstream Join Timer genannt. Er hat den Wert *0*, wenn der Timer deaktiviert ist.
Shortest Path Tree	Zeigt an, ob das Shortest Path Tree Bit gesetzt ist, d.h. ob das Forwarding über den Shortest Path Tree stattfinden soll.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der RPF Next Hop nicht bekannt ist.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Override Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste Triggered (S,G,rpt) Join Nachricht auf pimStarGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Upstream Override Timer genannt. Er hat den Wert *0*, wenn der Timer deaktiviert ist.

18.9.3 Schnittstellenspezifische Zustände

Das Menü **Monitoring**->**PIM**->**Schnittstellenspezifische Zustände** enthält schnittstellenspezifische Status-Angaben.

Werte in der Liste Schnittstellenspezifische Zustände

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: `Alle`, `(*,G,I) Status`, `(S,G,I) Status` und `(S,G,RPT) Status`

Werte in der Liste (*,G,I) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (*,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieses entspricht dem Status der Downstream Per-Interface (*,G) State Machine in the PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (*,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Join Expiry Timer genannt. Er hat den Wert `0`, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich.
Assert-Status	Zeigt den (*,G) Assert State für diese Schnittstelle. Dieser entspricht dem Status der Per-Interface (*,G) Assert State Machine in der PIM-SM Spezifikation. Wenn pimStarGPimMode 'bidir' ist, muss dieses Objekt 'noInfo' lauten.
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner an, wenn pimStarGIAssertState 'iAmAssertLoser' lautet. InetAddressType wird durch das Objekt pimStarGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (S,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden.

Feld	Beschreibung
	Dieser entspricht dem Status der Downstream Per-Interface (S,G) State Machine in der PIM-SM und PIM-DM Spezifikation.
Uptime	Zeigt die Zeit an, die verbleibt, bevor der lokale Router auf eine (S,G) Prune Nachricht reagiert, die auf dieser Schnittstelle empfangen wird. Der Router wartet diese Zeit, um zu prüfen, ob ein anderer Downstream Router die Prune Nachricht korrigiert. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Prune-Pending Timer genannt. Er hat den Wert *0*, wenn der Timer deaktiviert ist.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Join Expiry Timer genannt. Er hat den Wert *0*, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.
Assert-Status	Zeigt den (S,G) Assert State für diese Schnittstelle an. Dieser entspricht dem Status der Per-Interface (S,G) Assert State Machine in der PIM-SM Spezifikation Siehe "I-D.ietf-pim-sm-v2-new section 4.6.1"
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner, wenn pimSGIAssertState 'iAmAssertLoser lautet. InetAddressType wird durch das Objekt pimSGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Join/Prune-Status	Zeigt an, ob der lokale Router die Quelle des RP Tree abschneiden soll. Dieses entspricht in der PIM-SM Spezifikation dem Status der Upstream (S,G,rpt) State Machine für Triggered Messages.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G,rpt) Prune State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Prune Expiry Timer genannt. Er hat

Feld	Beschreibung
	den Wert `0`, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.

Index

#

A

B

C