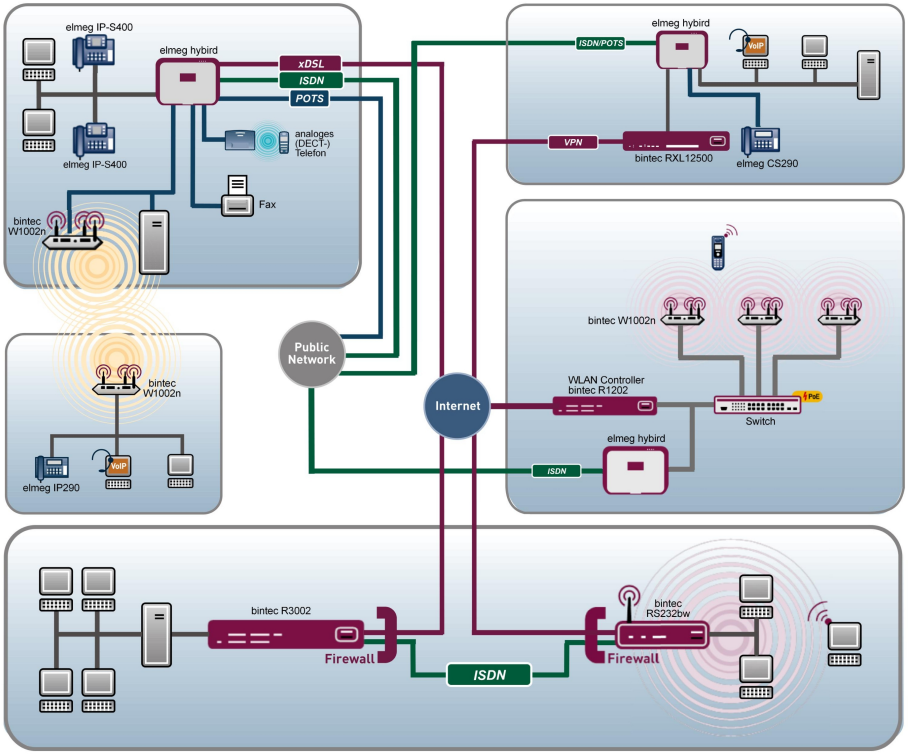


Benutzerhandbuch
bintec Next Generation WLAN

Referenz

Rechtlicher Hinweis

Ziel und Zweck
Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec elmeg-Geräten. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind zu finden unter *www.bintec-elmeg.com* .

Haftung
Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. bintec elmeg GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Release Notes für bintec elmeg-Gateways finden Sie unter *www.bintec-elmeg.com* .

bintec elmeg-Produkte bauen in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. bintec elmeg GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken
bintec elmeg und das bintec elmeg-Logo, bintec und das bintec-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der bintec elmeg GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter *www.bintec-elmeg.com* .

Wie Sie bintec elmeg GmbH erreichen
bintec elmeg GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25
Teldat France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, Frankreich, Telefon: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05
Internet: *www.teldat.fr*

Inhaltsverzeichnis

Kapitel 1 Einleitung

Die Access Points der neuen Generation sind umweltfreundlich hergestellt und entsprechen der RoHS-Richtlinie. Sie unterstützen die aktuellste WLAN-Technologie und sind insbesondere für den Einsatz im professionellen Umfeld konzipiert.

Sicherheitshinweise

Was Sie im Umgang mit Ihrem Access Point beachten müssen, erfahren Sie in der Broschüre **Sicherheitshinweise**, die im Lieferumfang Ihres Gerätes enthalten ist.

Installation

Wie Sie Ihr Gerät anschließen, erfahren Sie im Kapitel *Inbetriebnahme* auf Seite 6.

Konfiguration

Das Kapitel *Grundkonfiguration* auf Seite 17 sagt Ihnen, welche Vorbereitungen zur Konfiguration nötig sind. Anschließend zeigen wir Ihnen, wie Sie Ihr Gerät mit einem aktuellen Web-Browser von einem Windows-PC aus erreichen und grundlegende Einstellungen vornehmen können.

Passwort

Wenn Sie sich mit der Konfiguration von bintec elmeg-Geräten gut auskennen und gleich beginnen möchten, fehlen Ihnen eigentlich nur noch der werkseitig eingestellte Benutzername und das Passwort.

Benutzername: `admin`

Passwort: `admin`

Hinweis

Denken Sie daran, das Passwort sofort zu ändern, wenn Sie sich das erste Mal auf Ihrem Gerät einloggen. Alle bintec elmeg-Geräte werden mit gleichem Passwort ausgeliefert. Sie sind daher erst gegen einen unauthorisierten Zugriff geschützt, wenn Sie das Passwort ändern. Die Vorgehensweise bei der Änderung von Passwörtern ist im Kapitel *Systempasswort ändern* auf Seite 25 beschrieben.

Workshops

Anwendungsbezogene Schritt-für-Schritt-Anleitungen zu den wichtigsten Konfigurationsaufgaben finden Sie im separaten Handbuch **Anwendungs-Workshops**, das unter *www.bintec-elmeg.com* unter **Lösungen** zum Download bereitsteht.

Dime Manager

Die Geräte sind außerdem für den Einsatz des **Dime Manager** vorbereitet. Das Management Tool **Dime Manager** findet Ihre bintec-Geräte im Netz schnell und unkompliziert. Die .NET-basierte Anwendung, die für bis zu 50 Geräte konzipiert ist, zeichnet sich durch einfache Bedienung und übersichtliche Darstellung der Geräte, ihrer Parameter und Dateien aus.

Mittels SNMP-Multicast werden alle Geräte im lokalen Netz gefunden unabhängig von ihrer aktuellen IP-Adresse und zusätzlich auch entfernte Geräte, die über SNMP erreichbar sind. Eine neue IP-Adresse und das gewünschte Passwort können neben anderen Parametern zugewiesen werden. Über HTTP oder TELNET kann anschließend eine Konfiguration angestoßen werden. Bei Verwendung von HTTP erledigt der Dime Manager das Einloggen auf den Geräten für Sie.

Systemsoftware-Dateien und Konfigurationsdateien können auf Wunsch einzeln oder für gleichartige Geräte in logischen Gruppen verwaltet werden.

Sie finden den **Dime Manager** auf der beiliegenden Produkt-DVD.

Kapitel 2 Zum Handbuch

Dieses Dokument ist gültig für bintec elmeg-Geräte mit einer System-Software ab Software-Version 9.1.9.

Die Referenz, die Sie vor sich haben, enthält folgende Kapitel:

Benutzerhandbuch - Referenz

Kapitel	Beschreibung
Einleitung	Sie erhalten einen Überblick über das Gerät.
Zum Handbuch	Wir erklären Ihnen, aus welchen Bestandteilen sich das Handbuch zusammensetzt und wie sie damit umgehen.
Inbetriebnahme	Diese enthält Anweisungen, wie Sie Ihr Gerät aufstellen und anschließen.
Grundkonfiguration	Hier finden Sie Schritt-für-Schritt-Anleitungen zu Grundfunktionen Ihres Geräts.
Reset	Hier erfahren Sie, wie Sie Ihr Gerät in den Auslieferungszustand zurücksetzen.
Technische Daten	Dieser Abschnitt enthält eine Beschreibung aller technischen Eigenschaften der Geräte.
Zugang und Konfiguration	Hier werden die verschiedenen Zugangs- und Konfigurationsmöglichkeiten erläutert.
Assistenten **Systemverwaltung** **Physikalische Schnittstellen** **LAN** **Wireless LAN** **Wireless LAN Controller** **Netzwerk** **Routing-Protokolle** **Multicast**	In diesen Kapiteln werden alle Konfigurationsoptionen des **GUI** beschrieben. Die einzelnen Menüs werden in der Reihenfolge der Navigation beschrieben. In den einzelnen Kapiteln finden Sie auch weiterführende Erläuterungen zum jeweiligen Subsystem.

Kapitel	Beschreibung
WAN **VPN** **Firewall** **Lokale Dienste** **Wartung** **Externe Berichterstellung** **Monitoring**	
Glossar	Das Glossar enthält eine Referenz der wichtigsten technischen Begriffe der Netzwerktechnik.
Index	Im Index sind alle wichtigen Begriffe für die Bedienung des Geräts und alle Konfigurationsoptionen gesammelt und über die Seitenangabe leicht wiederzufinden.

Damit Sie wichtige Informationen in diesem Handbuch besser finden, werden folgende Symbole verwendet:

Symbolübersicht

Symbol	Verwendung
	Kennzeichnet praktische Informationen.
	Kennzeichnet allgemeine wichtige Hinweise.
	Kennzeichnet Warnhinweise in der Gefahrenstufe "Achtung" (weist auf mögliche Gefahr hin, die bei Nichtbeachten Sachschäden zur Folge haben kann).
	Kennzeichnet Warnhinweise in der Gefahrenstufe "Warnung" (weist auf mögliche Gefahr hin, die bei Nichtbeachten Körperverletzung oder Tod zur Folge haben kann).

Die folgende Auszeichnungselemente sollen Ihnen helfen, die Informationen in diesem Handbuch besser einordnen und interpretieren zu können:

Auszeichnungselemente

Auszeichnung	Verwendung
•	Kennzeichnet Listen.
Menü -> **Untermenü** **Datei** -> **Öffnen**	Kennzeichnet Menüs und Untermenüs.
nicht-proportional, z. B. `ping 192.168.0.252`	Kennzeichnet Kommandos die Sie wie dargestellt eingeben müssen.
fett, z. B. **Windows-Startmenü**	Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
fett, z. B. **Lizenzschlüssel**	Kennzeichnet Felder.
kursiv, z. B. *keiner*	Kennzeichnet Werte, die Sie eintragen bzw. die eingestellt werden können.
Online: blau und kursiv, z. B. *www.bintec-elmeg.com*	Kennzeichnet Hyperlinks.

Kapitel 3 Inbetriebnahme

Hinweis

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

3.1 bintec W1003n, W2003n, W2003n-ext und W2004n

3.1.1 Aufstellen und Anschließen

Hinweis

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

Die Geräte **bintec W1003n**, **bintec W2003n** und **bintec W2004n** besitzen integrierte Antennen, deren Abstrahlcharakteristik für die Deckenmontage optimiert ist.

Das Gerät **bintec W2003n-ext** verwendet externe Antennen, die im Lieferumfang enthalten sind.

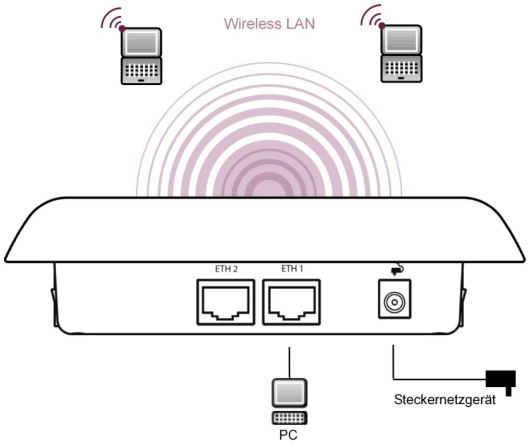


Abb. 2: Anschlussmöglichkeiten **bintec W2003n** *,* **bintec W2003n-ext**, **bintec W2004n**

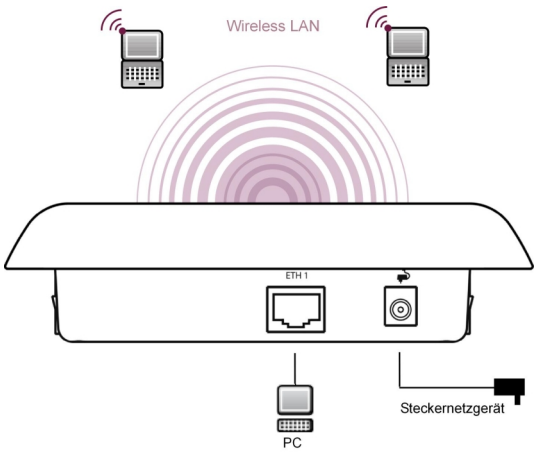


Abb. 3: Anschlussmöglichkeiten **bintec W1003n**

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

(1) Antennen

Bei **bintec W2003n-ext** schrauben Sie die mitgelieferten Standardantennen auf die dafür vorgesehenen Anschlüsse. Falls Sie andere Antennen verwenden, beachten Sie, dass SIMO-Antennen am Anschluss Ant1 und MIMO-Antennen an den Anschlüssen Ant1 und Ant2 anzuschließen sind.

(2) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. **bintec W1003n** hat nur einen Gigabit-Ethernet-Port, **ETH1**.

Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite Anschluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-Anschlüsse am selben Switch können sich Loops bilden.

Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss

Hinweis

Die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker (Artikelnummer 5500001254) ist als Zubehör erhältlich.

Schließen Sie das Gerät an eine Steckdose an. Nehmen Sie dazu das Steckernetzteil und stecken Sie es in die dafür vorgesehene Buchse Ihres Geräts. Stecken Sie

nun den Netzstecker in eine Steckdose (100–240 V). Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer 5530000082) erfolgen.

Montage

Die Access Points sind wahlweise an die Wand oder an die Decke zu montieren oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die vier selbstklebenden Füße auf der unteren Seite des Gerätes. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wand- / Deckenmontage

Um die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** oder **bintec W2004n** an der Wand bzw. Decke zu montieren, verwenden Sie die Halterung, die im Lieferumfang enthalten ist (Artikelnummer 5500001278).

Warnung

Vergewissern Sie sich vor dem Bohren, dass sich an der Bohrstelle keine Hausinstallationen befinden. Bei Beschädigung an Gas-, Strom-, Wasser- und Abwasserleitungen kann Lebensgefahr oder Sachschaden entstehen.

- Schrauben Sie die Halterung an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät ggf. mit einem Kensington-Schloss gegen Diebstahl.

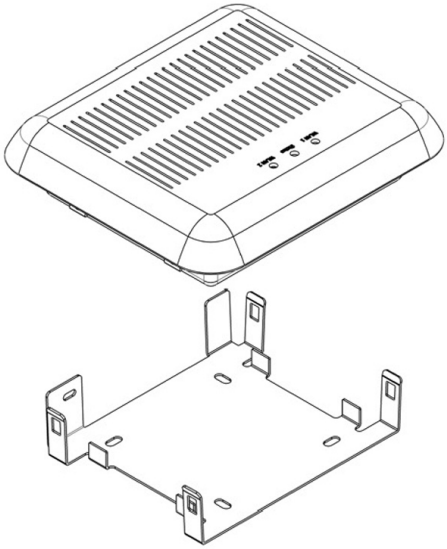


Abb. 4: Deckenmontage **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** *und* **bintec W2004n**

3.1.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec W1003n verfügt über einen Ethernet-Anschluss, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** verfügen über zwei Ethernet-Anschlüsse.

Die Anschlüsse sind folgendermaßen angeordnet:

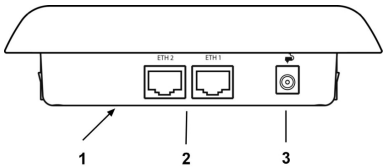


Abb. 5: Unterseite **bintec W2003n**, **bintec W2003n-ext** *und* **bintec W2004n**

bintec W2003n, bintec W2003n-ext und bintec W2004n Unterseite

1	RESET	Reset-Taste führt Neustart durch (an der Bodenplatte des Geräts)
2	ETH1/PoE und ETH2	10/100/1000 Base-T Ethernet-Schnittstelle

		Bei **bintec W1003n** ist nur ETH1 vorhanden!
3	POWER	Buchse für Steckernetzteil

3.1.3 LEDs

Anhand der LEDs können Sie Funkstatus und Funkaktivität Ihres Geräts erkennen.

Hinweis

Beachten Sie, dass die Anzahl der aktiven WLAN LEDs abhängig ist von der Anzahl der vorhandenen Radiomodule.

Die LEDs von **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** sind folgendermaßen angeordnet:

Abb. 6: LEDs von **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** *und* **bintec W2004n**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Status (grün)	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
	an (statisch)	Fehler
	an (blinkend)	Betriebsbereit
WLAN 1/2 (grün)	aus	Radiomodul oder alle zugeordneten VSS deaktiviert
	an (langsam blinkend)	VSS ist aktiv, kein Client angemeldet
	an (schnell blinkend)	VSS ist aktiv, mindestens 1 Client ist angemeldet
	an (flackernd)	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr

Das Leuchtverhalten der LEDs können Sie im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.

Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustands erhalten.

Status	Nur die Status-LED blinkt einmal in der Sekunde.
Blinkend	Die LEDs zeigen ihr Standardverhalten.
Aus	Alle LEDs sind deaktiviert.

3.1.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	**Software**	**Dokumentation**
bintec W1003n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2003n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2003n-ext	Ethernet-Kabel (RJ-45, STP) 4 externe RSMA-Standardantennen Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2004n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Informati-

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
	Wand- bzw. Deckenbefestigung		on (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise

3.1.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	ca. 162 x 145 x 45 mm
Gewicht	ca. 1000 g (mit WLAN-Modulen)
LEDs	Für **bintec W1003n**: 3 (1x Status, 1x WLAN, 1x Ethernet) Für **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n**: 4 (1x Status, 2x WLAN, 2x Ethernet)
Leistungsaufnahme Gerät	max. 12 W
Spannungsversorgung	9 V, 1.3 A (Das Steckernetzteil mit der Artikelnummer 5500001254 ist als Zubehör erhältlich) PoE an Ethernet 1 Class 0, gemäß 802.3af (max. 12,4 W). Der Gigabit PoE Injector mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Umweltanforderungen:	
Lagertemperatur	-40 °C bis +85 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 100 %
Verfügbare Schnittstellen:	
WLAN	**bintec W1003n**: 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2

Eigenschaft	Wert
	bintec W2003n: 1 Radiomodul 802.11bgn 2,4GHz Mimo 2x2; 1 Radiomodul 802.11an 5GHz Mimo 2x2 **bintec W2003n-ext**: 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2; 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2 **bintec W2004n**: 1 Radiomodul 802.11bgn 2,4GHz Mimo 3x3; 1 Radiomodul 802.11an 5GHz Mimo 3x3
Ethernet IEEE 802.3 LAN	10/100/1000 MBit/s
Vorhandene Buchsen:	
Ethernet-Schnittstelle	**bintec W1003n**: 1 RJ45-Buchse **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n**: 2 RJ45-Buchsen
Antennen:	
Antennenanschluss	**bintec W1003n**: 2 interne Antennen **bintec W2003n**: 4 interne Antennen **bintec W2003n-ext**: 4 externe Dualband-Antennen **bintec W2004n**: 6 interne Antennen
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Taster	Reset-Taster für Neustart oder Reset

3.1.6 Reset

Im Falle einer Fehlkonfiguration oder bei Nichterreichbarkeit Ihres Geräts können Sie das Gerät mit dem Reset-Knopf auf der Geräteunterseite mit den Standardeinstellungen des Auslieferungszustands starten lassen.

Dabei werden alle bestehenden Konfigurationsdaten gelöscht.

Bei **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** gehen Sie folgendermaßen vor:

(1) Drücken Sie die **Reset**-Taste Ihres Geräts.

(2) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt.

(3) Achten Sie auf die LEDs:
Die Status-LED leuchtet, das Gerät durchläuft die Boot-Sequenz.
Lassen Sie **Reset**-Taste los, wenn die Status-LED wieder zu blinken beginnt.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab *Grundkonfiguration* auf Seite 17 beschrieben.

Hinweis

Wenn Sie über das **GUI** die Boot-Konfiguration löschen, werden ebenfalls alle Passwörter zurückgesetzt und die aktuelle Boot-Konfiguration gelöscht. Beim nächsten Start startet das Gerät mit den Standardeinstellungen des Auslieferungszustands.

Hinweis

Wenn sie das LED-Verhalten im Menü **Globale Einstellungen** oder mit dem **WLAN Controller** auf einen anderen als den Standardwert gesetzt haben, bleibt diese Einstellung beim Zurücksetzen des Geräts erhalten.

3.2 Reinigen

Sie können Ihr Gerät problemlos reinigen. Verwenden Sie dazu ein leicht feuchtes Tuch oder ein Antistatiktuch. Benutzen Sie keine Lösungsmittel! Verwenden Sie niemals ein trockenes Tuch; die 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.

3.3 Pin-Belegung

3.3.1 Ethernet-Schnittstelle

Die Geräte **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** verfügen über zwei 10/100/1000 Ethernet-Schnittstellen, **bintec W1003n** hat eine 10/100/1000 Ethernet-Schnittstelle.

Der Anschluss erfolgt über eine RJ45-Buchse.

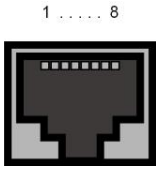


Abb. 7: 10/100/1000 Base-T Ethernet-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für LAN-Anschluss

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

3.4 Frequenzen und Kanäle

Weltweit gelten unterschiedliche Zulassungsbestimmungen. Im Wesentlichen gelten die ETSI Vorschriften (kommt hauptsächlich in Europa zur Anwendung). Für den Betrieb in Europa lesen Sie bitte die Hinweise in der R&TTE Compliance Information.

3.5 Support Information

Wenn Sie zu Ihrem neuen Produkt Fragen haben oder zusätzliche Informationen wünschen, erreichen Sie das Support Center von bintec elmeg GmbH montags bis freitags von 9:00 bis 17:00 Uhr. Folgende Kontaktmöglichkeiten stehen Ihnen zur Verfügung:

Internationale Supportkoordination	Telefon: +49 911 9673 0 Fax: +49 911 688 0725
Endkunden-Hotline	0900 1 38 65 93 (1,10 €/min aus dem deutschen Festnetz)

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

3.6 WEEE-Information

The waste container symbol with the »X« through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life.

Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist.

Le symbole se trouvant sur l'appareil et qui représente un conteneur à ordures barré signifie que l'appareil, une fois que sa durée d'utilisation a expiré, doit être éliminé dans des poubelles spéciales prévues à cet effet, de manière séparée des ordures ménagères courantes.

Il simbolo raffigurante il bidone della spazzatura barrato riportato sull'apparecchiatura significa che alla fine della durata in vita dell'apparecchiatura questa dovrà essere smaltita separatamente dai rifiuti domestici nei punti di raccolta previsti a tale scopo.

El símbolo del contenedor con la cruz, que se encuentra en el aparato, significa que cuando el equipo haya llegado al final de su vida útil, deberá ser llevado a los centros de recogida previstos, y que su tratamiento debe estar separado del de los residuos urbanos.

Symbolen som sitter på apparaten med den korsade avfallstunnan betyder att apparaten när den tjänat ut ska kasseras och lämnas till de förutsedda sortergårdarna och skiljas från normalt hushållsavfall.

Tegnet på apparatet som viser en avfallcontainer med et kyss over, betyr at apparatet må kastet på hertil egnet avfallssted og ikke sammen med vanlig avfall fra husholdningen.

Το σύμβολο που βρίσκεται στην συσκευή με το σταυρωμένο κοντέϊνερ απορριμμάτων σημαίνει, ότι η συσκευή στο τέλος της διάρκειας χρήσης της πρέπει να διατεθεί ξεχωριστά από τα κανονικά απορρίμματα στα γι' αυτό τον σκοπό προβλεπόμενα σημεία διάθεσης.

Symbolet med gennemkrydset affaldsbeholder på apparatet betyder, at apparatet, når det ikke kan bruges længere, skal bortskaffes adskilt fra normalt husholdningsaffald på et af de dertil beregnede bortskaffelsessteder.

Znajdujący się na urządzeniu symbol przekreślonego pojemnika na śmieci oznacza, że po upływie żywotności urządzenia należy go oddać do odpowiedniej placówki utylizacyjnej i nie wyrzucać go do normalnych śmieci domowych.

Het doorgehaalde symbool van de afvalcontainer op het apparaat betekent dat het apparaat op het einde van zijn levensduur niet bij het normale huisvuil mag worden verwijderd. Het moet bij een erkend inzamelpunt worden ingeleverd.

O símbolo com um caixote de lixo riscado, que se encontra no aparelho, significa, que o aparelho no fim da sua vida útil deve ser eliminado separadamente do lixo doméstico nos centros de recolha adequados.

Kapitel 4 Grundkonfiguration

Zur Grundkonfiguration Ihres Geräts stehen der **Dime Manager** (IP-Adressvergabe) und das **GUI** (weitere Konfigurationsschritte) zur Verfügung.

Der Weg zur Grundkonfiguration wird Ihnen im Folgenden Schritt für Schritt erläutert. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

Die Inhalte dieses Handbuches setzen die folgenden Basiskenntnisse voraus:

- Basiskenntnisse im Netzwerkaufbau,
- Kenntnisse über die grundlegende Netzwerkterminologie, wie beispielsweise Server, Client und IP-Adresse,
- Grundkenntnisse bei der Bedienung von Microsoft Windows Betriebssystemen.

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

Weitere nützliche Applikationen finden Sie im Internet unter *www.bintec-elmeg.com* .

4.1 Voreinstellungen

4.1.1 Vorkonfigurierte Daten

Sie haben drei Möglichkeiten, in Ihrem Netzwerk auf Ihr Gerät zur Konfiguration zuzugreifen:

(a) Dynamische IP-Adresse

Im Auslieferungszustand ist Ihr Gerät im DHCP-Client-Modus eingestellt, d.h. es erhält bei Anschluss an das Netzwerk automatisch eine IP-Adresse, sofern ein DHCP-Server betrieben wird. Ihr Gerät ist zur Konfiguration dann unter der vom DHCP-Server vergebenen IP-Adresse erreichbar. Zur Ermittlung der dynamisch vergebenen IP-Adresse lesen Sie bitte die Dokumentation Ihres DHCP-Servers.

(b) Fallback-IP-Adresse

Sollten Sie keinen DHCP-Server betreiben, können Sie Ihr Gerät direkt an Ihren Konfigurations-PC anschliessen und erreichen es dann unter folgender vordefinierter Fallback-IP-Konfiguration:

- **IP-Adresse**: `192.168.0.252`
- **Netzmaske**: `255.255.255.0`

Achten Sie darauf, dass der PC, von dem aus die Konfiguration durchgeführt wird, über eine geeignete IP-Konfiguration verfügt (siehe dazu *PC einrichten* auf Seite 21).

(c) Feste IP-Adresse zuweisen

Mit dem **Dime Manager** können Sie Ihrem Gerät eine neue IP-Adresse und das gewünschte Passwort zuweisen.

Hinweis

Beachten Sie bitte:

Hat Ihr Gerät bei der Erstkonfiguration dynamisch von einem in Ihrem Netzwerk betriebenen DHCP-Server eine IP-Adresse erhalten, wird die Fallback-IP-Adresse 192.168.0.252 automatisch gelöscht und Ihr Gerät ist darüber nicht mehr erreichbar.

Sollten sie dagegen bei der Erstkonfiguration eine Verbindung zum Gerät über die Fallback-IP-Adresse 192.168.0.252 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.

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 25.

4.1.2 Software-Update

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Eine Aktualisierung können Sie bequem mit dem **GUI** im Menü **Wartung**->**Software &Konfiguration** vornehmen.

Eine Beschreibung des Update-Vorgangs finden Sie unter *Softwareaktualisierung* auf Seite 27 .

4.2 System-Voraussetzungen

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

- Internet Explorer oder Mozilla Firefox
- Installierte Netzwerkkarte (Ethernet)
- DVD-Laufwerk
- Installiertes TCP/IP-Protokoll (siehe *PC einrichten* auf Seite 21)

4.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration bereitlegen.
- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.
- die **Dime Manager**-Software installieren, die Ihnen weitere Werkzeuge zur Arbeit mit Ihrem Gerät zur Verfügung stellt.

4.3.1 Daten sammeln

Die wesentlichen Daten für die Grundkonfiguration haben Sie schnell gesammelt, denn es sind keine Informationen erforderlich, die vertiefte Netzwerkkenntnisse voraussetzen. Ggf. können Sie die Beispielwerte übernehmen.

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

- IP-Konfiguration (obligatorisch sofern sich Ihr Gerät im Auslieferungszustand befindet)

Hinweis

Die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** unterstützen kein WDS und kein Bridgelink.

- optional: Konfiguration einer drahtlosen Netzwerkverbindung im Access-Point-Modus
- optional: Konfiguration von Client Links im Client Links-Modus

In der folgenden Tabelle haben wir jeweils Beispiele für die Werte der benötigten Daten 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:

IP-Konfiguration des Access Points

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Access Points	*192.168.0.252*	
Netzmaske Ihres Access Points	*255.255.255.0*	

Access-Point-Modus

Wenn Sie Ihr Gerät im Access-Point-Modus betreiben, können Sie die gewünschten Drahtlosnetzwerke einrichten. Hierzu benötigen Sie jeweils folgende Daten:

Konfiguration eines Drahtlosnetzwerks

Zugangsdaten	Beispielwert	Ihre Werte
Netzwerkname (SSID)	*default*	
Sicherheitsmodus	*WPA-PSK*	
Preshared Key	*supersecret*	

Access Client-Modus

Wenn Sie Ihr Gerät im Access Client-Modus betreiben, können Sie die gewünschten Client Links einrichten. Hierzu benötigen Sie jeweils folgende Daten:

IP-Konfiguration des Access Clients

Zugangsdaten	Beispielwert	Ihre Werte
Netzwerkname (SSID)	*default*	
Sicherheitsmodus	*WPA-PSK*	
Preshared Key	*supersecret*	

4.3.2 PC einrichten

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

- Stellen Sie sicher, dass das TCP/IP-Protokoll auf dem PC installiert ist.
- Wählen Sie die geeignete IP-Konfiguration für Ihren Konfigurations-PC.

  Der PC, über den Sie die IP-Adresse für Ihr Gerät konfigurieren möchten, muss sich im gleichen Netzwerk wie das zu konfigurierende Gerät befinden.

Windows 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)**.

Windows 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, die passende Netzmaske, Ihr Standardgateway und Ihren bevorzugten DNS-Server ein.

Wenn Sie in Ihrem Netzwerk einen DHCP-Server betreiben, können Sie die Windows-Standardeinstellung **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** belassen.

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

4.4 IP-Konfiguration

Im Auslieferungszustand ist Ihr Gerät im DHCP-Client-Modus eingestellt und erhält somit dynamisch eine IP-Adresse, sofern Sie einen DHCP-Server in Ihrem Netzwerk betreiben. Wenn das nicht der Fall ist, schliessen Sie Ihr Gerät direkt an den Konfigurations-PC an und verwenden die Fallback-IP-Adresse `192.168.0.252`.

Alternativ können Sie Ihrem Geräten die gewünschte feste IP-Adresse zuweisen, indem Sie den **Dime Manager** benutzen.

Installieren Sie dazu das Programm von der mitgelieferten DVD auf Ihren Konfigurations-PC.

Gehen Sie dazu vor wie folgt:

(a) Legen Sie die mitgelieferte DVD in das DVD-Laufwerk Ihres Konfigurations-PCs. Der Installationsassistent startet automatisch. Sollte das nicht der Fall sein, öffnen Sie auf der DVD über Ihren Dateibrowser die Datei `starter.exe`.

(b) Folgen Sie den Anweisungen des Installations-Assistenten.

Führen Sie anschliessend folgende Schritte aus, um eine IP-Adresse für Ihr Gerät zu konfigurieren:

(1) Starten Sie den **Dime Manager** aus dem Windows-Startmenü **Start** -> **Programme** -> -> **Dime Manager**.
Es erscheint folgendes Dialogfeld:

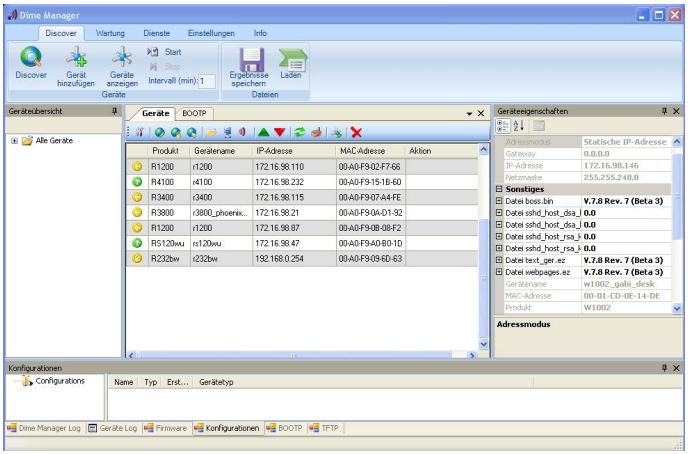


Abb. 9: **Dime Manager** *Startseite*

Der **Dime Manager** erkennt die im Netzwerk installierten Geräte.

(2) Doppelklicken Sie in der Liste das Gerätes, das konfiguriert werden soll.
Es erscheint folgendes Dialogfeld:

Abb. 10: IP-Adressvergabe mit dem **Dimet Manager**

(3) Geben Sie die Netzwerkparameter (**Gerätename**, **IP-Adresse**, **Netzmaske** und **Gateway**) ein und bestätigen Sie Ihre Angaben mit **OK**.

Hinweis

Der Parameter **Gerätename** darf maximal aus 32 Zeichen bestehen.

Der Parameter **Gerätename** darf nur aus Buchstaben „a“-“z“, „A“-“Z“, Ziffern „0“-“9“, Bindestrich „-“ und Punkt „.“ bestehen, um Fehler durch andere Systeme bei der Interpretation des Parameters **Gerätename** zu vermeiden. Das erste Zeichen muss ein Buchstabe sein, das letzte Zeichen darf kein Punkt „.“ und kein Minuszeichen „-“ sein, ein einzelnes Zeichen ist als Name nicht zulässig.

Ihr Gerät ist nun über das Ethernet mit seiner IP-Adresse über einen Web-Browser ansprechbar und kann jetzt konfiguriert werden.

GUI aufrufen

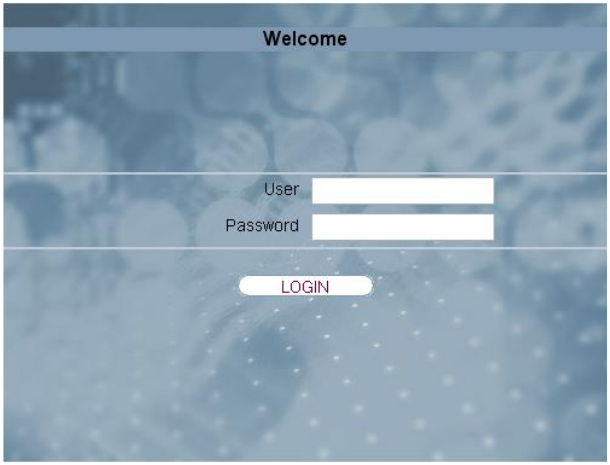


Abb. 11: **GUI** *Login*

Starten Sie die Konfigurationsoberfläche wie folgt:

(a) Geben Sie die IP-Adresse Ihres Geräts in die Adress-Zeile Ihres Web-Browsers ein.

Mit DHCP-Server:

- die IP-Adresse, die der DHCP-Server Ihrem Gerät vergeben hat

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse `192.168.0.252`
- Die über den **Dime Manager** vergebene feste IP-Adresse

Drücken Sie die **Eingabetaste**.

(b) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein.

4.5 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.

4.6 Drahtlosnetzwerk einrichten

Gehen Sie folgendermaßen vor, um ihr Gerät als Access Point zu nutzen:

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

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

(3) Speichern Sie die Konfiguration mit dem Button **Konfiguration speichern** oberhalb der Menünavigation.

WLAN-Adapter unter Windows XP konfigurieren

Windows XP hat nach der Installation der Treiber für Ihre WLAN-Karte eine neue Verbindung in der Netzwerkumgebung eingerichtet. Um diese Wireless-LAN-Verbindung zu konfi-

gurieren, gehen Sie bitte folgendermaßen vor:

(1) Klicken Sie auf **Start**-> **Systemsteuerung**. Dort doppelklicken Sie auf **Netzwerkverbindungen** -> **Drahtlose Netzwerkverbindung**.

(2) Wählen Sie anschließend auf der linken Seite **Erweiterte Einstellungen ändern** aus.

(3) Gehen Sie auf die Registerkarte **Drahtlosnetzwerke**.

(4) Klicken Sie auf **Hinzufügen**.

Fahren Sie folgendermaßen fort:

(1) Bei **Netzwerkname** geben Sie z. B. *Client-1* ein.

(2) Unter **Netzwerkauthentifizierung** wählen Sie *WPA2-PSK*.

(3) Bei **Datenverschlüsselung** konfigurieren Sie *AES*.

(4) Unter **Netzwerkschlüssel** und **Netzwerkschlüssel bestätigen** geben Sie den zuvor konfigurierten Preshared Key an.

(5) Verlassen Sie die Menüs jeweils mit **OK**.

Hinweis

Windows XP erlaubt die Anpassung vieler Menüs. Je nach Konfiguration kann der Pfad zu der Drahtlosnetzwerkverbindung, die Sie konfigurieren wollen, ein anderer sein als oben beschrieben.

WLAN-Adapter unter Windows 7 konfigurieren

Windows 7 erkennt vorhandene WLAN-Netzwerke automatisch. Sie müssen Ihre Verbindung nur noch konfigurieren.

(1) Klicken Sie zunächst auf das WLAN-Symbol im Infobereich der Taskleiste (Systemtray). Windows 7 zeigt Ihnen nun alle drahtlosen Netzwerke an, die sich in Ihrer Reichweite befinden.

(2) Wählen Sie das WLAN-Netz Ihres Geräts aus und klicken Sie auf **Verbinden**.

(3) Im sich anschließend öffnenden Fenster tragen Sie den zuvor konfigurierten Preshared Key ein und bestätigen mit **OK**.

4.7 Softwareaktualisierung

Die Funktionsvielfalt von bintec elmeg-Geräten wird permanent erweitert. Diese Erweiterungen stellt Ihnen bintec elmeg GmbH stets 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.

Kapitel 5 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

5.1 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

5.1.1 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.

5.1.1.1 HTTP/HTTPS

Mit einem aktuellen Web-Browser können Sie die HTML-Oberflächen zur Konfiguration Ihres Geräts verwenden.

Die Konfiguration lässt sich mit dem **GUI** durchführen. Geben Sie dazu die IP-Adresse Ihres Geräts in das Adressfeld Ihres Web-Browsers ein:

Mit DHCP-Server:

- die IP-Adresse, die Ihr DHCP-Server Ihrem Gerät vergeben hat

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse *192.168.0.252*
- Die über den **Dime Manager** vergebene feste IP-Adresse

Drücken Sie die **Eingabetaste**.

5.1.1.2 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 34.

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 34.

5.1.1.3 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 33).

(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 37).

(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 33 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 33 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.

5.1.2 Zugang über die serielle Schnittstelle

Ihr Gerät 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 (192.168.0.252/255.255.255.0) nicht möglich ist.

Windows

Um Ihr Gerät über die serielle Schnittstelle an Ihren Rechner anzuschließen, gehen Sie vor wie in der *Inbetriebnahme* **auf Seite 6** beschrieben.

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** -> **HyperTerminal**.

(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`

5.2 Anmelden

Mit Hilfe 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.

5.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

Benutzer-name	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` einloggt. Aus Sicherheitsgründen sind Passwörter im Setup Tool 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 auf Seite 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!

5.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 28 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. `w1002:>`. 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**.

5.3 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

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

Es stehen also für jede Verbindungsart mehrere Konfigurationsarten zur Verfügung.

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.

5.3.1 GUI (Graphical User Interface) für Fortgeschrittene

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 auf *www.bintec-elmeg.com* heruntergeladen und auf dem Gerät installiert werden.

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.

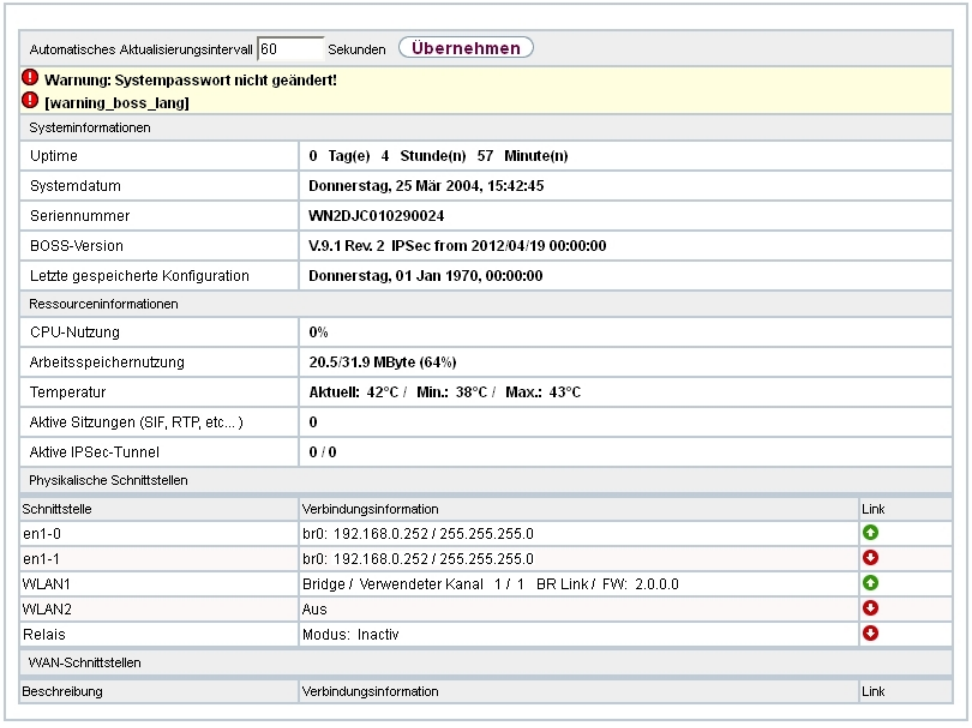


Abb. 12: **GUI** *Startseite*

5.3.1.1 Das GUI aufrufen

(1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind.

(2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe *PC einrichten* auf Seite 21).

(3) Öffnen Sie einen Web-Browser.

(4) Geben Sie `http://192.168.0.252` (oder die von Ihrem DHCP-Server dynamisch vergebene IP-Adresse oder die von Ihnen statisch mit dem **Dime Manager** vergebene IP-Adresse) in das Adressfeld des Web-Browsers 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 50).

5.3.1.2 Bedienelemente

GUI-Fenster

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

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

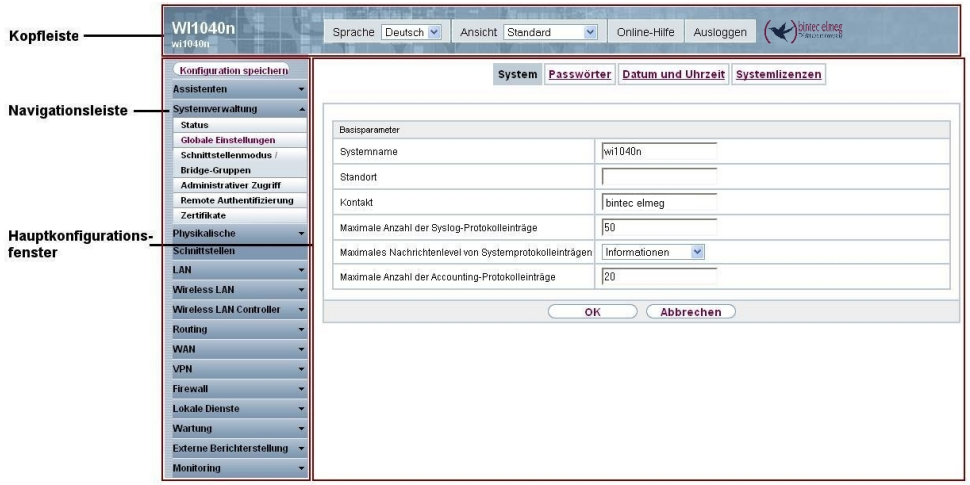


Abb. 13: Bereiche des **GUI**

Kopfleiste

Abb. 14: **GUI** *Kopfleiste*

GUI Kopfleiste

Menü	Funktion
Sprache Deutsch	**Sprache**: Wählen Sie in dem Dropdown-Menü die gewünschte Sprache aus, in der das **GUI** angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen Deutsch und Englisch.
Ansicht Standard	**Ansicht**: Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl steht Standard und SNMP-Browser.

Menü	Funktion
Online-Hilfe	**Online-Hilfe**: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Die Beschreibung des Untermenüs, in dem Sie sich gerade befinden, wird angezeigt.
Ausloggen	**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 Optionen angeboten werden: • Konfiguration speichern, vorherige Boot-Konfiguration sichern, dann verlassen. • Konfiguration speichern, dann verlassen. • Ohne zu speichern verlassen.

Navigationsleiste

Abb. 15: Konfiguration speichern Schaltfläche

Abb. 16: Menüs

Über der Navigationsleiste ist die Schaltfläche **Konfiguration speichern** zu finden.

Wenn Sie eine aktuelle Konfiguration speichern, können Sie diese als Boot-Konfiguration speichern oder Sie können zusätzlich die vorhergehende Boot-Konfiguration als Backup archivieren.

Wenn Sie im **GUI** auf die Schaltfläche **Konfiguration speichern** klicken, erscheint die Frage "Möchten Sie die aktuelle Konfiguration wirklich als Boot-Konfiguration speichern?"

Sie haben folgende zwei Wahlmöglichkeiten:

- *Konfiguration speichern*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern
- *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern und zusätzlich vor-

hergehende Boot-Konfiguration als Backup archivieren.

Wenn Sie die archivierte Boot-Konfiguration in Ihr Gerät laden wollen, gehen Sie in das Menü **Wartung**->**Software &Konfiguration**, wählen Sie **Aktion** = *Konfiguration importieren* und klicken Sie auf **Los**. Das archivierte Backup wird als aktuelle Boot-Konfiguration verwendet.

Die Navigationsleiste enthält weiterhin die Hauptkonfigurationsmenüs und deren Untermenüs.

Klicken Sie auf das gewünschte Hauptmenü. Es öffnet sich das jeweilige Untermenü.

Wenn Sie auf das gewünschte Untermenü klicken, wird der gewählte Eintrag in roter Schrift angezeigt. Alle anderen Untermenüs werden geschlossen. So können Sie stets mit einem Blick erkennen, in welchem Untermenü Sie sich befinden.

Statusseite

Wenn Sie das **GUI** aufrufen, erscheint nach der Anmeldung zunächst die Statusseite Ihres Geräts. Auf dieser werden die wichtigsten Daten Ihres Gerätes auf einen Blick sichtbar.

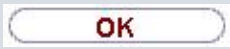
Hauptkonfigurationsfenster

Die Untermenüs enthalten im Allgemeinen mehrere Seiten. Diese werden über die im Hauptfenster oben stehenden Schalter aufgerufen. Durch Klicken auf einen Schalter öffnet sich das Fenster mit den Basis-Parametern, welches durch Klicken auf den Reiter **Erweiterte Einstellungen** erweiterbar ist und dann Zusatzoptionen anzeigt.

Konfigurationselemente

Die verschiedenen Aktionen, die Sie bei der Konfiguration Ihres Geräts im **GUI** ausführen können, werden mit Hilfe folgender Schaltflächen ausgelöst:

GUI 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.

Schaltfläche	Funktion
Hinzufügen	Fügt einen Eintrag zu einer internen Liste hinzu.

GUI Schaltflächen für spezielle Funktionen

Schaltfläche	Funktion
Importieren	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.
Anforderung	Im Menü **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** wird mit dieser Schaltfläche das Untermenü für die Konfiguration der Zertifikatsanforderung aufgerufen.

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

GUI Symbole

Symbol	Funktion
	Löscht den entsprechenden Listeneintrag.
	Zeigt das Menü zur Änderung der Einstellungen eines Eintrags an.
	Zeigt die Details eines Eintrags an.
	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.

Symbol	Funktion
	Kennzeichnet den Status "Wird aktiviert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-Bandscan aus.
	Zeigt die nächste Seite einer Liste an.
	Zeigt die vorherige Seite einer Liste an.

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

GUI 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.

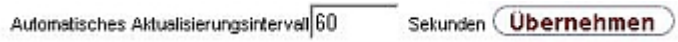


Abb. 17: Konfiguration des Aktualisierungsintervalls

Abb. 18: Liste filtern

Struktur der GUI Konfigurationsmenüs

Die Menüs des **GUI** enthalten folgende Grundstrukturen:

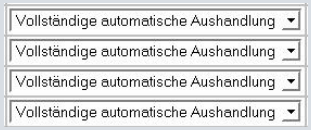
GUI Menüstruktur

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. 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:

GUI Konfigurationselemente

Menü	Funktion
Eingabefelder	z. B. leeres Textfeld  Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.
Radiobuttons	z. B.

Menü	Funktion
	 Wählen Sie die entsprechende Option aus.
Checkboxen	z. B. Aktivieren durch Auswahl der Checkbox  Auswahl verschiedener möglicher Optionen 
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  . Ein neuer Listeneintrag 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.

Warnsymbole

Symbol	Bedeutung
	Dieses Symbol erscheint in Meldungen, die Sie auf Einstellungen hinweisen, die mit dem Setup Tool vorgenommen wurden.
	Dieses Symbol erscheint in Meldungen, die Sie darauf hinweisen, dass Werte falsch eingegeben bzw. ausgewählt wurden.

Achten Sie besonders auf folgenden Hinweis:

"Warnung: Nicht unterstützte Änderungen durch das Setup-Tool!". Falls Sie sie mit dem **GUI** verändern, kann dies Inkonsistenzen oder Fehlfunktionen verursachen. Daher wird empfohlen, die Konfiguration mit dem Setup Tool fortzuführen.

5.3.1.3 GUI 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* .

5.3.2 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.

5.4 BOOTmonitor

Der BOOTmonitor ist nur über eine serielle Verbindung zum Gerät verfügbar.

Folgende Funktionen stellt der BOOTmonitor zur Verfügung, die Sie durch Eingabe der entsprechenden Ziffer auswählen:

(1) Boot System (Neustart des Systems):
Das Gerät lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.

(2) Software Update via TFTP (Softwareaktualisierung über TFTP):
Das Gerät führt ein Software-Update über einen TFTP-Server aus.

(3) Software Update via XMODEM (Softwareaktualisierung über XMODEM):
Das Gerät führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.

(4) Delete configuration (Konfiguration löschen):
Das Gerät wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsdateien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.

(5) Default BOOTmonitor Parameters (Standardeinstellungen des BOOTmonitors):
Sie können die Standard-Einstellungen des BOOTmonitors des Geräts verändern, z. B. die Baudrate für serielle Verbindungen.

(6) Show System Information (Systeminformationen anzeigen):
Zeigt nützliche Informationen des Geräts, wie z. B. SeriennummDer BOOTmonitor wird wie folgt gestartet.
er, MAC-Adresse und Software-Versionen.

Beim Hochfahren durchläuft das Gerät verschiedene Funktionszustände:

- Start-Modus
- BOOTmonitor-Modus
- Normaler Betriebsmodus

Nachdem im Start-Modus einige Selbsttests erfolgreich ausgeführt wurden, erreicht Ihr Gerät den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie seriell mit Ihrem Gerät verbunden sind.

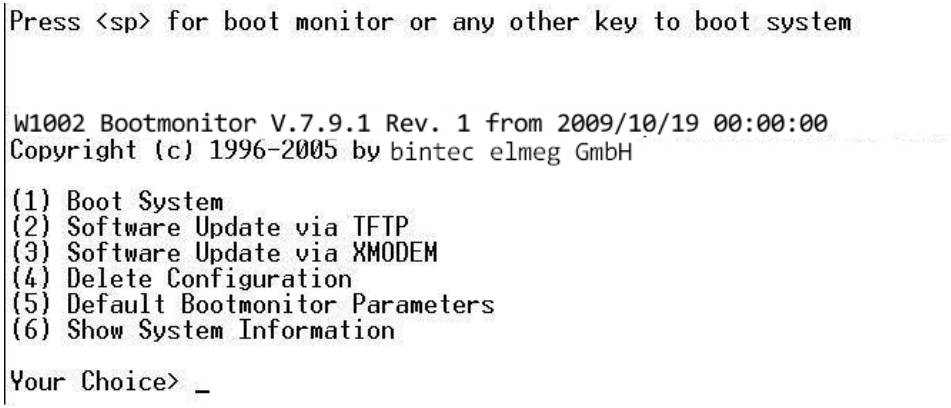


Abb. 19: BOOTmonitor

Betätigen Sie nach Anzeige des BOOTmonitor-Prompts innerhalb von vier Sekunden die Leertaste, um die Funktionen des BOOTmonitors zu nutzen. Wenn Sie keine Eingabe machen, wechselt das Gerät nach Ablauf der vier Sekunden in den normalen Betriebs-Modus.

Hinweis

Wenn Sie die Baudrate verändern (voreingestellt ist 9600 Baud), achten Sie darauf, dass das verwendete Terminalprogramm diese Baudrate verwendet. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zum Gerät herstellen!

Kapitel 6 Assistenten

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

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

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

Kapitel 7 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.

7.1 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- und WLAN-Schnittstellen

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!

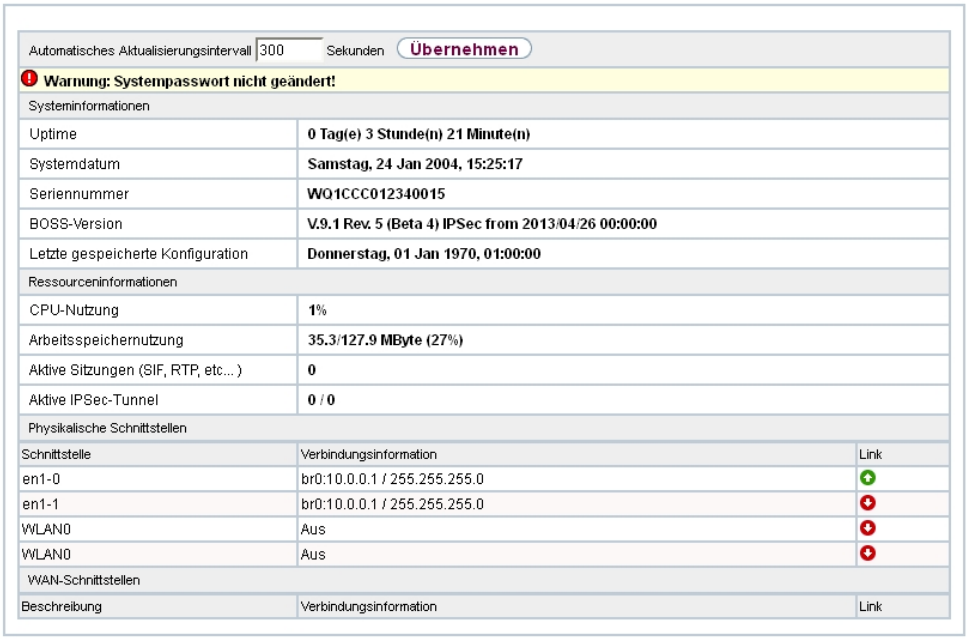


Abb. 20: **Systemverwaltung->Status**

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.
BOSS-Version	Zeigt die aktuell geladene Version der Systemsoftware an.
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.
Aktive Sitzungen (SIF,	Zeigt die Summe aller SIF-, TDRC- und IP-Lastverteilung Sessi-

Feld	Wert
RTP, etc...)	ons 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 Schnittstellendetails für serielle Schnittstellen / ISDN-Schnittstellen: • Konfiguriert • Nicht konfiguriert Schnittstellendetails für xDSL-Schnittstellen: • Leitungsgeschwindigkeit Downstream/Upstream Schnittstellendetails für WLAN-Schnittstellen: Access-Point-Modus: • Betriebsmodus: Access Point oder Aus • Der auf diesem Funkmodul verwendete Kanal • Anzahl der verbundenen Clients • Softwareversion der Funkkarte

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.

7.2 Globale Einstellungen

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

7.2.1 System

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

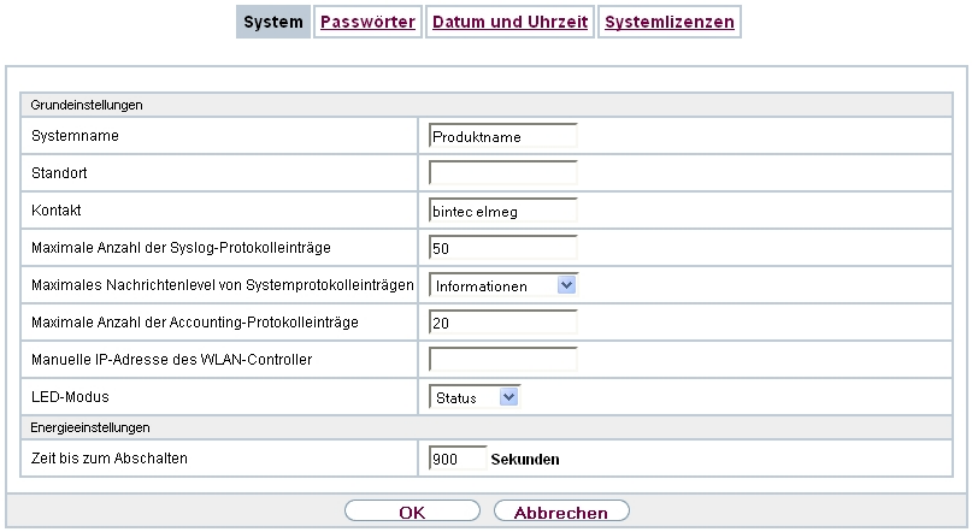


Abb. 21: **Systemverwaltung**->**Globale Einstellungen**->**System**

Das Menü **Systemverwaltung**->**Globale Einstellungen**->**System** 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*.
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.
LED-Modus	Diese Funktion ist nur für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** verfügbar. 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.

Felder im Menü Energieeinstellungen (nur für Geräte mit GPS)

Feld	Wert
Zeit bis zum Abschalten	Geben Sie die Zeit in Sekunden ein, wie lange das Gerät nach dem Abschalten des Motors noch eingeschaltet bleiben soll. Der Standardwert ist *900* Sekunden.

7.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

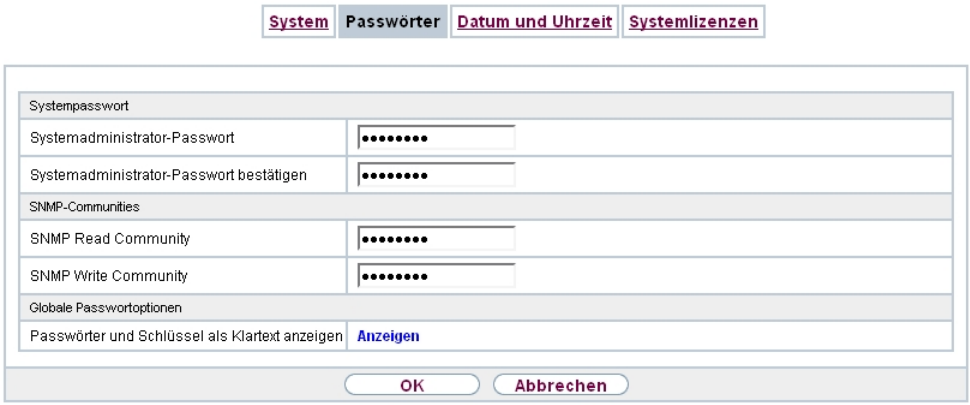


Abb. 22: **Systemverwaltung->Globale Einstellungen->Passwörter**

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.

Feld	Wert
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 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.

7.2.3 Datum und Uhrzeit

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

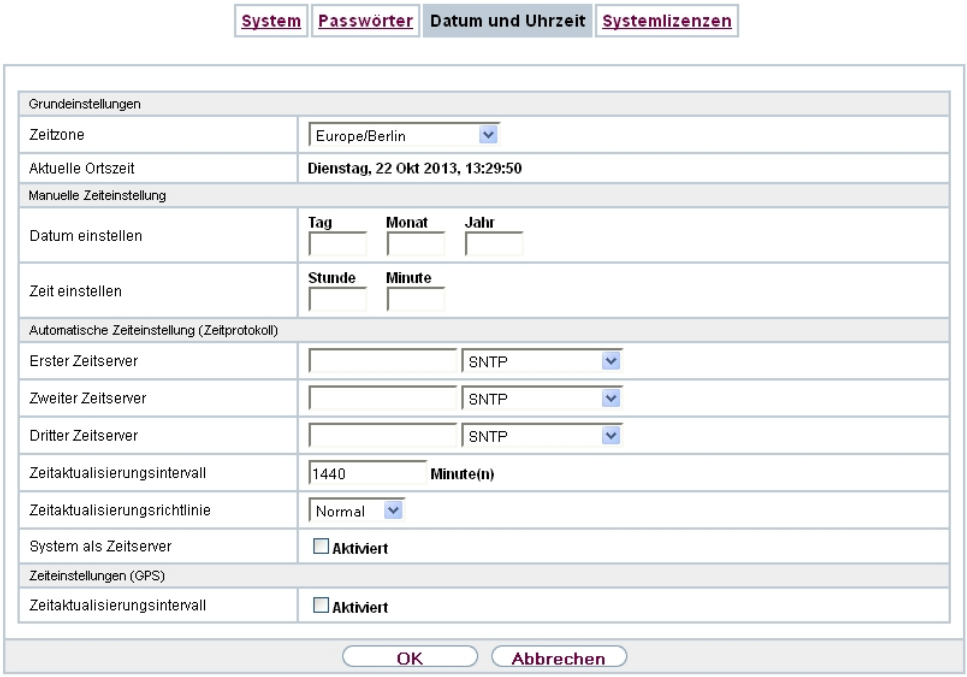


Abb. 23: **Systemverwaltung->Globale Einstellungen->Datum und Uhrzeit**

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	Geben Sie ein neues Datum ein. Format: • **Tag**: dd • **Monat**: mm • **Jahr**: yyyy
Zeit einstellen	Geben Sie eine neue Uhrzeit ein.

Feld	Beschreibung
	Format: • **Stunde**: hh • **Minute**: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	Nur für Geräte mit ISDN-Schnittstelle. Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll. Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeitserver empfangen wurde. Für den Zeitraum, in dem die Zeit über einen Zeitserver ermittelt wird, wird die Aktualisierung über ISDN außer Kraft gesetzt. Mit Auswahl von *Aktiviert* wird die Funktion 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.

Feld	Beschreibung
	Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Dritter Zeitserver	Geben Sie den dritten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird. Der Standardwert ist *1440*.
Zeitaktualisierungsrichtlinie	Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen. Mögliche Werte: • *Normal* (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minu-

Feld	Beschreibung
	ten 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*.
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.

7.2.4 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).

7.2.4.1 Bearbeiten oder Neu

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

Abb. 24: **Systemverwaltung->Globale Einstellungen->Systemlizenzen->Neu**

Freischalten von Zusatzlizenzen

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

Das Menü **Systemverwaltung->Globale Einstellungen->Systemlizenzen->Neu** 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.

7.3 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 WDS-Links bzw. Bridge-Links setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

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

(c) Nummer des WDS-Links bzw. Bridge-Link

Beispiel: *wds1-0* (erster WDS-Link bzw. 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)

7.3.1 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.

Abb. 25: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschrei-	Zeigt den Namen der Schnittstelle an.

Feld	Beschreibung
bung	
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.

7.3.1.1 Hinzufügen

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

Abb. 26: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**->**Hinzufügen**

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.

Abb. 27: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**->

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-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

Feld	Wert
	zum Access Point herzustellen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

7.4 Administrativer Zugriff

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

7.4.1 Zugriff

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

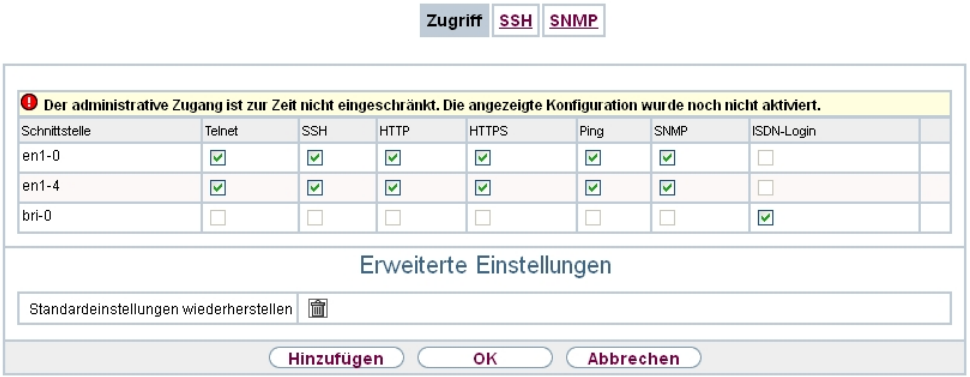


Abb. 28: **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff**

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

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.

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.

7.4.1.1 Hinzufügen

Wählen Sie die **Hinzufügen**-Schaltfläche, wenn Sie den administrativen Zugriff für weitere Schnittstellen konfigurieren wollen.

Abb. 29: **Systemverwaltung->Administrativer Zugriff->Zugriff->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.

7.4.2 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.

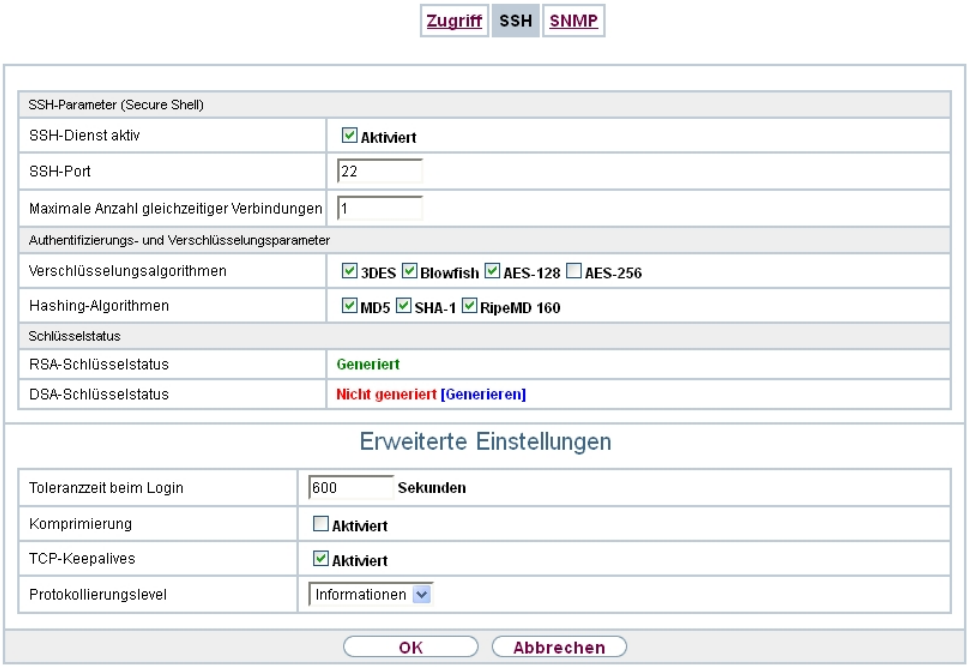


Abb. 30: **Systemverwaltung->Administrativer Zugriff->SSH**

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* • *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 in roter Schrift *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* in grüner Schrift 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. Standardmäßig ist der Status *Nicht generiert*.
DSA-Schlüsselstatus	Zeigt den Status des DSA-Schlüssels an. Wenn bisher kein DSA-Schlüssel generiert wurde, wird in roter Schrift *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* in grüner Schrift 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. Standardmäßig ist der Status *Nicht generiert*.

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 Verbindungs-

Feld	Wert
	aufbau 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.
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.

7.4.3 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 ent-

hält 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.

Abb. 31: **Systemverwaltung->Administrativer Zugriff->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.

Feld	Wert
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.

7.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

7.5.1 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 Verbindungsaufbau zu verwendenden Parametern.
ACCESS_REJECT	Server -> Client Wenn die im ACCESS_REQUEST enthaltenen Informationen nicht den Informationen in der Benutzerdatenbank des RADIUS-Servers entsprechen, sendet er ein ACCESS_REJECT zur 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.

7.5.1.1 Bearbeiten oder Neu

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

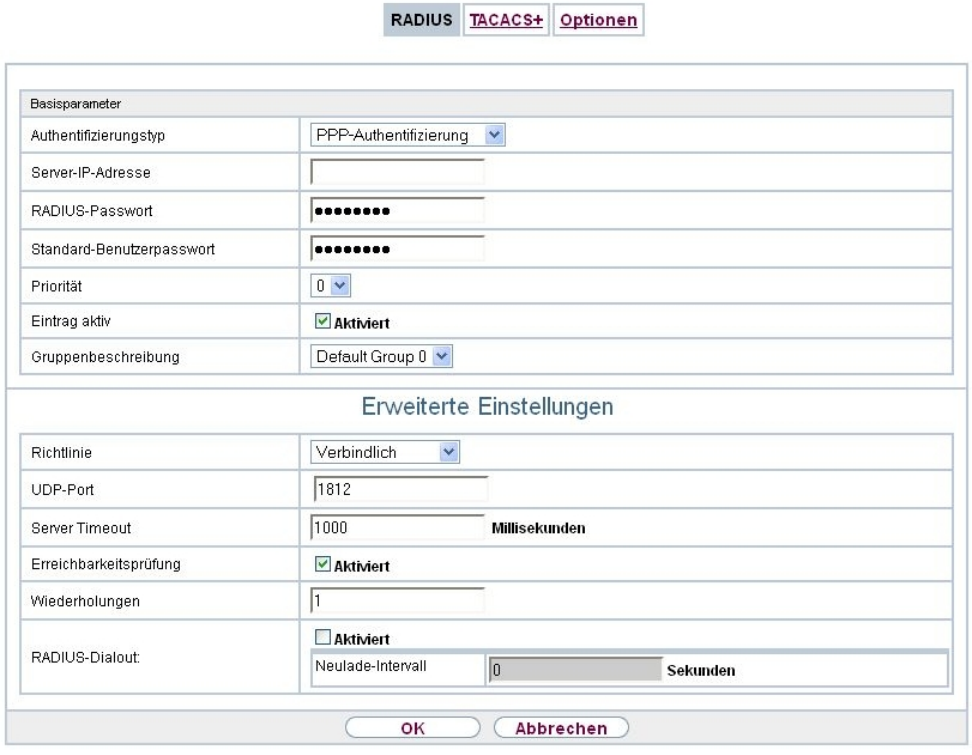


Abb. 32: **Systemverwaltung->Remote Authentifizierung->RADIUS->Neu**

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.

7.5.2 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.

7.5.2.1 Bearbeiten oder Neu

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

Abb. 33: **Systemverwaltung->Remote Authentifizierung->TACACS+ ->Neu**

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.

Feld	Beschreibung
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-

Feld	Beschreibung
	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 TACACS+-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.

7.5.3 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.

Abb. 34: **Systemverwaltung->Remote Authentifizierung->Optionen**

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

Felder im Menü Globale RADIUS-Optionen

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

7.6 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.

7.6.1 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 *TCC_ADMIN*, *HOTEL*, *CHARGES*, *PHONEBOOK*, *PBX_USER_ACCESS*bereits angelegt. Diese können Sie mithilfe des Symbols ändern sowie über das Symbol auf die Standardeinstellungen zurücksetzen.

Abb. 35: **Systemverwaltung**->**Konfigurationszugriff**->**Zugriffsprofile**

7.6.1.1 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.

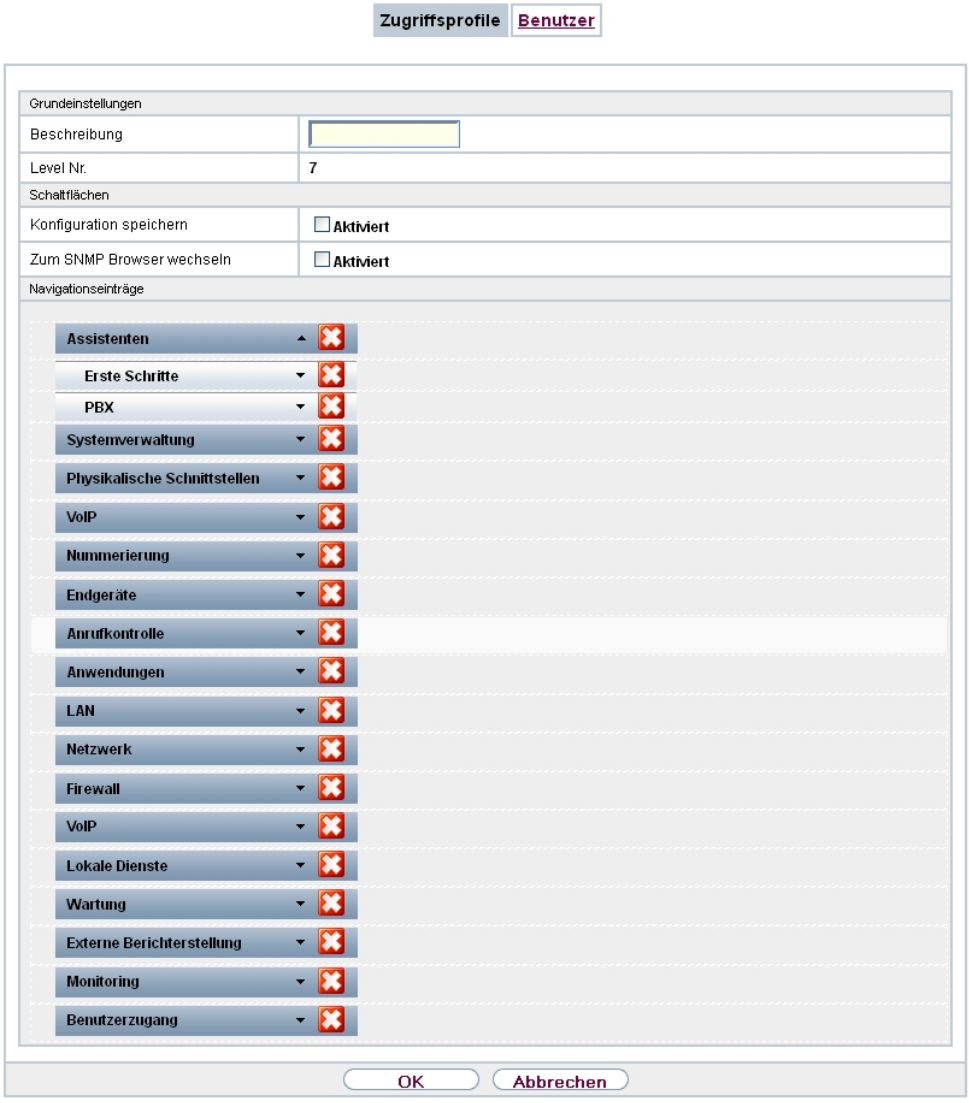


Abb. 36: **Systemverwaltung->Konfigurationszugriff->Zugriffsprofile->Neu**

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

Feld	Beschreibung
	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.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Navigationseinträge

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

7.6.2 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.

Abb. 37: **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**

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

Abb. 38: **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**->

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.

7.6.2.1 Bearbeiten oder Neu

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

Abb. 39: **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**->**Neu**

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 beliebi-

Feld	Beschreibung
	ge Änderungen vornehmen kann. Die Option **Nur lesen** ist in der SNMP-Browser-Ansicht nicht verfügbar. Werden einem Benutzer sich überschneidende Zugriffsprofile zugeordnet, so hat Lesen und Schreiben eine höhere Priorität als **Nur lesen**. Schaltflächen können nicht auf die Einstellung **Nur lesen** gesetzt werden.

7.7 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 Sprachver-

bindungen über Voice over IP ausgestattet.

7.7.1 Zertifikatsliste

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

7.7.1.1 Bearbeiten

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

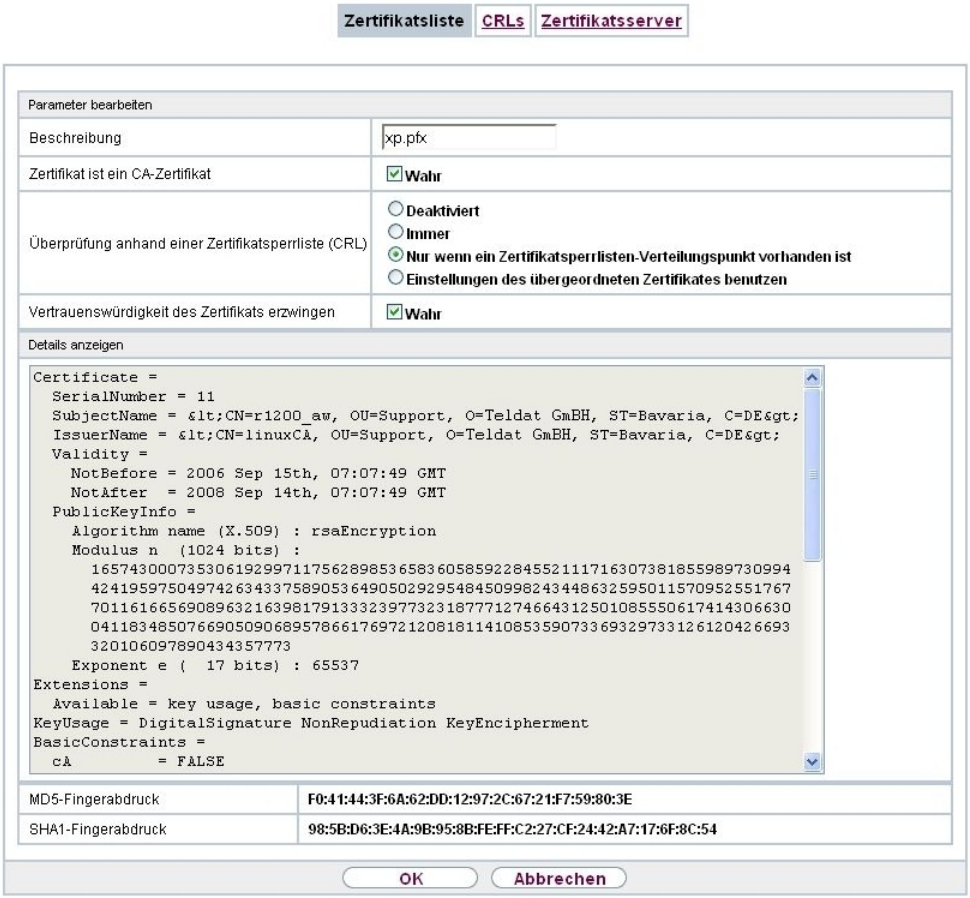


Abb. 40: **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->

Die Zertifikate und Schlüssel an sich können nicht verändert werden, jedoch können - je

nach Typ des gewählten Eintrags - einige externe Attribute verändert werden.

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

Felder im Menü Parameter bearbeiten

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

Feld	Beschreibung
	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.

7.7.1.2 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.

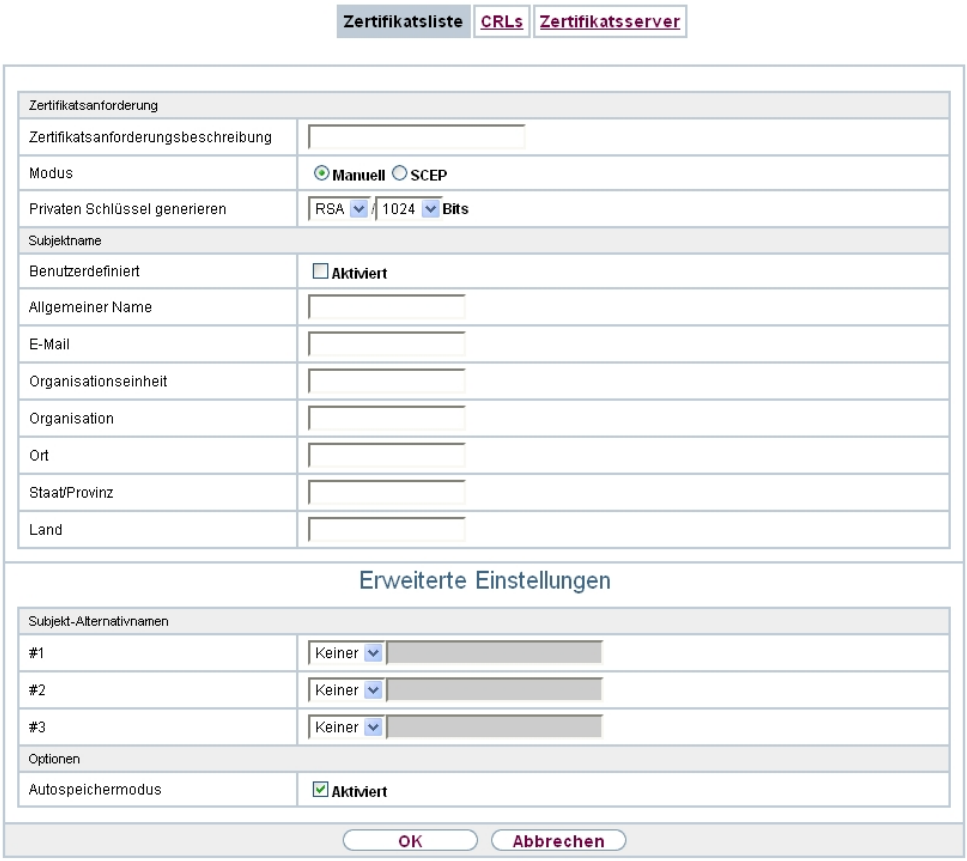


Abb. 41: **Systemverwaltung->Zertifikate->Zertifikatsliste->Zertifikatsanforderung**

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

Feld	Beschreibung
	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.
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.

Feld	Beschreibung
	Es fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü **Zertifikatsanforderung generieren** zurück. Falls das CA-Zertifikat keine CRL-Verteilstelle (Certificate Revocation List, CRL) enthält und auf Ihrem Gerät kein Zertifikatsserver konfiguriert ist, werden Zertifikate von dieser CA nicht auf ihre Gültigkeit überprüft. • <Name eines vorhandenen Zertifikats>: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.
RA-Signierungszertifikat	Nur für **Modus** = *SCEP* Nur für **CA-Zertifikat** nicht = *-- Download --* Wählen Sie ein Zertifikat für die Signierung der SCEP-Kommunikation aus. Der Standardwert ist *-- CA-Zertifikat verwenden --*, d. h. es wird das CA-Zertifikat verwendet.
RA-Verschlüsselungszertifikat	Nur für **Modus** = *SCEP* Nur wenn **RA-Signierungszertifikat** nicht = *-- CA-Zertifikat verwenden --* Wenn Sie ein eigenes Zertifikat zur Signierung der Kommunikation mit der RA verwenden, haben Sie hier die Möglichkeit, ein weiteres zur Verschlüsselung der Kommunikation auszuwählen. Der Standardwert ist *-- RA-Signierungszertifikat verwenden --*, d. h. es wird dasselbe Zertifikat wie zur Signierung verwendet.
Passwort	Nur für **Modus** = *SCEP* Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.

Felder im Menü Subjektname

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

Feld	Beschreibung
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.

7.7.1.3 Importieren

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

Abb. 42: **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->**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`
Passwort	Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort.

Feld	Beschreibung
	Tragen Sie das Passwort hier ein.

7.7.2 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.

7.7.2.1 Importieren

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

Abb. 43: **Systemverwaltung**->**Zertifikate**->**CRLs**->**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.

Feld	Beschreibung
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für die CRL ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät die CRL decodieren kann. Mögliche Werte: • *Auto* (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der CRL-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • *Base64* • *Binär*
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

7.7.3 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.

7.7.3.1 Neu

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

Abb. 44: **Systemverwaltung**->**Zertifikate**->**Zertifikatsserver**->**Neu**

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.

Kapitel 8 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.

8.1 Ethernet-Ports

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

Hinweis

Die Ethernet-Ports ETH1 und ETH2 sind im Auslieferungszustand der Standard-Bridge-Gruppe *br0* zugeordnet, die als DHCP-Client und mit der Fallback-**IP-Adresse** *192.168.0.252* und **Netzmaske** *255.255.255.0* vorkonfiguriert ist.

Die Geräte der **bintec W1003n**-Serie haben nur den Ethernet-Port ETH 1.

8.1.1 Portkonfiguration

Ihr Gerät bietet die Möglichkeit, die zwei Ethernet-Schnittstellen getrennt zu konfigurieren.

Abb. 45: **Physikalische Schnittstellen**->**Ethernet-Ports**->**Portkonfiguration**

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

Felder im Menü Portkonfiguration

Feld	Beschreibung
Port	Zeigt den jeweiligen Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Schnittstelle	Zeigt die logische Schnittstelle an, die dem jeweiligen Ethernet-Port zugeordnet ist.
Konfigurierte Geschwindigkeit/konfigurierter Modus	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vollständige automatische Aushandlung* (Standardwert) • *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: • *100 Mbit/s / Full Duplex* • *100 Mbit/s / Half Duplex* • *10 Mbit/s / Full Duplex* • *10 Mbit/s / Half Duplex* • *Inaktiv*

Kapitel 9 LAN

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

9.1 IP-Konfiguration

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

9.1.1 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.

Hinweis

Beachten Sie bitte:

Hat Ihr Gerät bei der Erstkonfiguration dynamisch von einem in Ihrem Netzwerk betriebenen DHCP-Server eine IP-Adresse erhalten, 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.

9.1.1.1 Bearbeiten oder Neu

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

Abb. 46: **LAN->IP-Konfiguration->Schnittstellen->** **/Neu**

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.

Feld	Beschreibung
	Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
Adressmodus	Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird. Mögliche Werte: • *Statisch* (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in **IP-Adresse / Netzmaske** zugewiesen. • *DHCP*: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
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.
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.
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).

Feld	Beschreibung
	Wenn **Voreingestellte verwenden** aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet. Standardmäßig ist **Voreingestellte verwenden** aktiv.
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*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DHCP-MAC-Adresse	Nur für **Adressmodus** = *DHCP* Ist **Voreingestellte verwenden** aktiviert (Standardeinstellung) wird die Hardware-MAC-Adresse der Ethernet-Schnittstelle verwendet. Bei physikalischen Schnittstellen ist die aktuelle MAC-Adresse standardmäßig eingetragen. Wenn Sie **Voreingestellte verwenden** deaktivieren, geben Sie eine MAC-Adresse für die virtuelle Schnittstelle ein, z. B. *00:e1:f9:06:bf:03*. Manche Provider verwenden hardware-unabhängige MAC-Adressen, um ihren Clients IP-Adressen dynamisch zuzuweisen. Sollte Ihnen Ihr Provider eine MAC-Adresse zugewiesen haben, so tragen Sie diese hier ein.
DHCP-Hostname	Nur für **Adressmodus** = *DHCP* Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.
DHCP Broadcast Flag	Nur für **Adressmodus** = *DHCP* Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-

Feld	Beschreibung
	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.
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.

9.2 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.

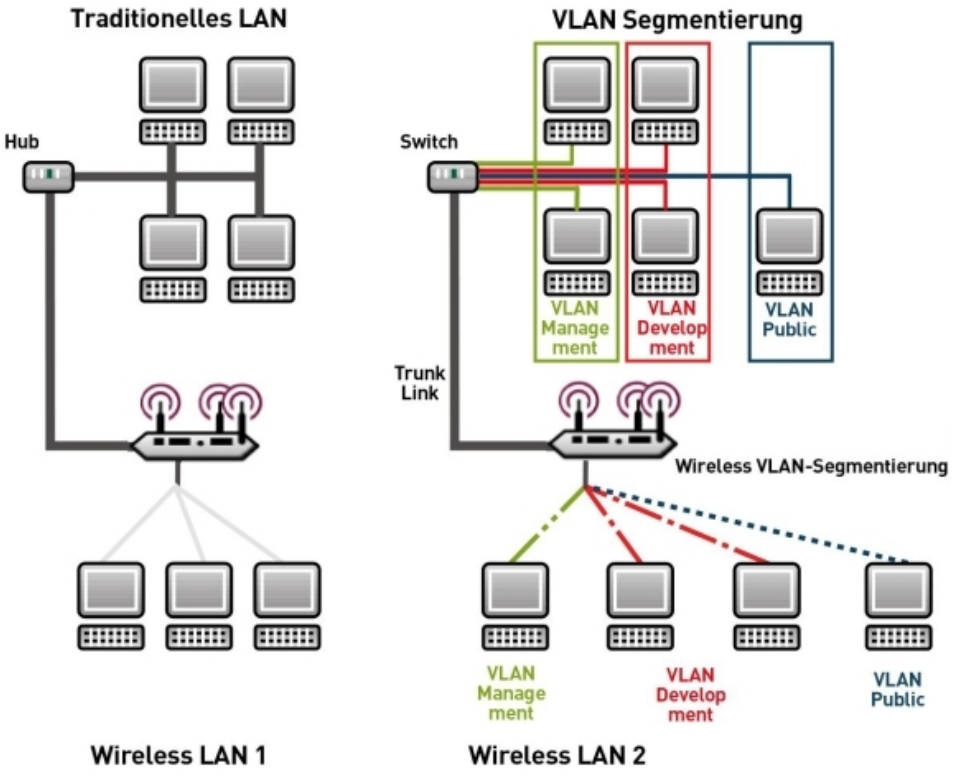


Abb. 47: VLAN-Segmentierung

VLAN für Bridging und VLAN für Routing

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

Achtung

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

9.2.1 VLANs

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

9.2.1.1 Bearbeiten oder Neu

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

Abb. 48: **LAN->VLAN->VLANs->Neu**

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

Felder im Menü VLAN konfigurieren

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

Feld	Beschreibung
	von diesem Port übertragen werden, *Tagged* (also mit VLAN-Information) oder *Untagged* (also ohne VLAN-Information) übertragen werden sollen.

9.2.2 Portkonfiguration

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

Abb. 49: **LAN->VLANs->Portkonfiguration**

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

Felder im Menü Portkonfiguration

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

9.2.3 Verwaltung

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

Abb. 50: **LAN->VLANs->Verwaltung**

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

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

Feld	Beschreibung
VLAN aktivieren	Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe für VLAN. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion deaktiviert.
Verwaltungs-VID	Wählen Sie die VLAN-ID des VLANs aus, in dem Ihr Gerät arbeiten soll.

Kapitel 10 Wireless LAN

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

Netzwerkfunktionen

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

Derzeit gültiger Standard: IEEE 802.11

Bei 802.11-WLANs sind alle Funktionen eines verkabelten Netzwerks möglich. WLAN sendet innerhalb und außerhalb von Gebäuden mit maximal 100 mW.

IEEE 802.11g ist der derzeit am weitesten verbreitete Standard für Funk-LANs und bietet eine maximale Datenübertragungsrate von 54 Mbit/s. Dieses Verfahren arbeitet im Funkfrequenzbereich von 2,4 GHz, der gewährleistet, dass Gebäudeteile möglichst gut und bei nur geringer, gesundheitlich unproblematischer Sendeleistung durchdrungen werden.

Ein zu 802.11g kompatibler Standard ist 802.11b, der im 2,4 GHz-Band (2400 MHz - 2485 MHz) arbeitet und eine maximale Datenübertragungsrate von 11 Mbit/s bietet. 802.11b- und 802.11g-WLAN Systeme sind anmelde- und gebührenfrei.

Mit 802.11a sind im Bereich 5150 GHz bis 5725 MHz Bandbreiten bis 54 Mbit/s nutzbar. Mit dem größeren Frequenzbereich stehen 19 nicht überlappende Frequenzen (in Deutschland) zur Verfügung. Auch dieser Frequenzbereich ist in Deutschland lizenzfrei nutzbar. In Europa werden mit 802.11h nicht nur 30 mW sondern 1000 mW Sendeleistung nutzbar, jedoch nur unter Einsatz von TPC (TX Power Control, Methode zur Regelung der Sendeleistung bei Funksystemen zur Reduktion von Interferenzen) und DFS (Dynamic Frequency Selection). TPC und DFS sollen sicherstellen, dass Satellitenverbindungen und Radargeräte nicht gestört werden.

Der Standard 802.11n (Draft 2.0) verwendet für die Datenübertragung die MIMO-Technik (Multiple Input Multiple Output), was Datentransfer über WLAN über größere Entfernungen oder mit höheren Datenraten ermöglicht. Mit einer Bandbreite von 20 oder 40 MHz werden so 150 bis 300 MBit/s Bruttodatenrate erreicht.

Durch eine Änderung im Telekommunikationsgesetz (TKG) wurde es möglich, das 5,8 GHz-Band (5755 MHz - 5875 MHz) für sogenannte BFWA-Anwendungen (Broadband Fixed Wireless Access) zu nutzen. Dazu ist allerdings eine Anmeldung bei der Bundesnetzagentur nötig. Jedoch ist auch hier der Einsatz von TPC und DFS verbindlich.

10.1 WLAN

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

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

10.1.1 Einstellungen Funkmodul

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

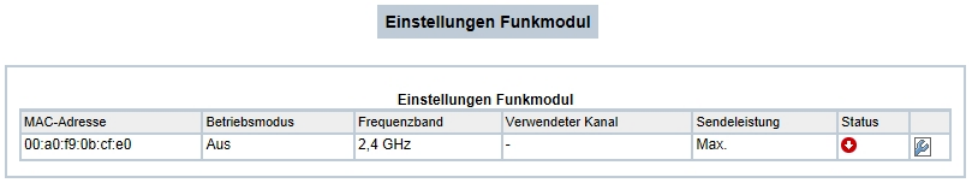


Abb. 51: **Wireless LAN->WLAN->Einstellungen Funkmodul**

10.1.1.1 Einstellungen Funkmodul->

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie das Symbol um die Konfiguration zu bearbeiten.

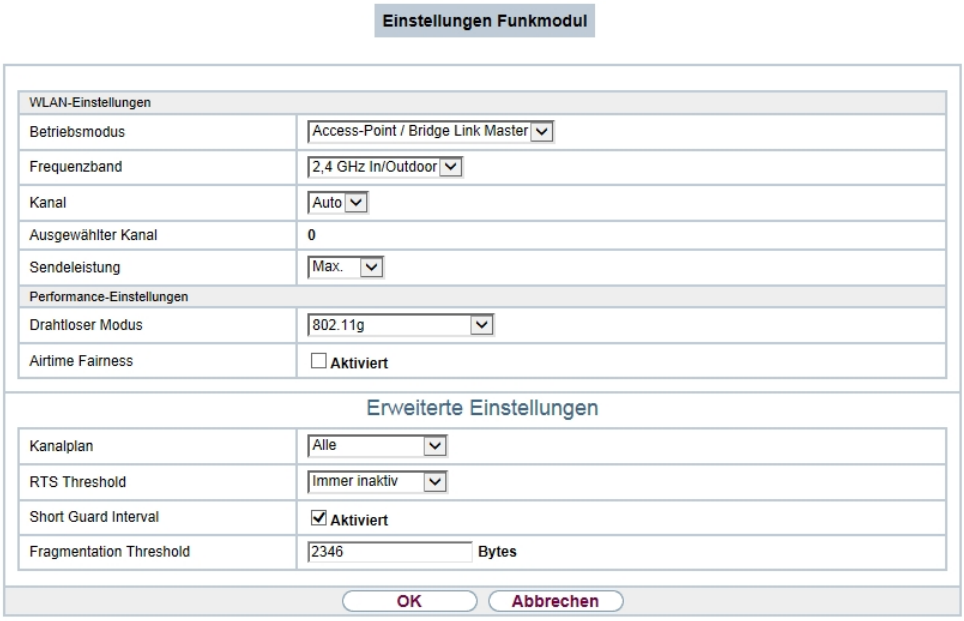


Abb. 52: **Wireless LAN->WLAN->Einstellungen Funkmodul->** *für* **Betriebsmodus** *Access-Point / Bridge Link Master*

Abb. 53: **Wireless LAN WLAN Einstellungen Funkmodul** *für* **Betriebsmodus** *Access Client*

Das Menü **Wireless LAN->WLAN->Einstellungen Funkmodul->** besteht aus folgen-

den Feldern:

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll. Mögliche Werte: • *Aus* (Standardwert): Das Funkmodul ist nicht aktiv. • *Access-Point / Bridge Link Master*: Ihr Gerät dient als Access Point oder als Bridge Link Master in Ihrem Netzwerk. • *Access Client*: Ihr Gerät dient als Access Client in Ihrem Netzwerk. • *Bridge Link Client* : Ihr Gerät dient als Wireless Bridge in Ihrem Netzwerk (nur für die Geräte der **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n**-Serie).
Frequenzband	Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus. Für **Betriebsmodus** = *Access-Point / Bridge Link Master* oder *Bridge Link Client* Mögliche Werte: • *2,4 GHz In/Outdoor* (Standardwert): Ihr Gerät wird mit 2.4 GHz (Mode 802.11b und Mode 802.11g) innerhalb oder außerhalb von Gebäuden betrieben. • *5 GHz Indoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb von Gebäuden betrieben. • *5 GHz Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) außerhalb von Gebäuden betrieben. • *5 GHz In/Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb oder außerhalb von Gebäuden betrieben.
Nutzungsbereich	Nur für **Betriebsmodus** = *Access Client* und **Frequenzband** = *2,4 und 5 GHz* oder *5 GHz* Mögliche Werte: • *Indoor-Outdoor* (Standardwert)

Feld	Beschreibung
	• *Indoor* • *Outdoor*
Kanal	Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate. **Access-Point-Modus / Bridge-Modus:** Durch das Einstellen des Netzwerknamens (SSID) im Access-Point-Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens 4 Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt. Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden Clients diese Kanäle auch unterstützen. Mögliche Werte: • Für **Frequenzband** = *2,4 GHz In/Outdoor* Mögliche Werte sind *1* bis *13* und *Auto* (Standardwert). • Für **Frequenzband** = *5 GHz Indoor* Mögliche Werte sind *36*, *40*, *44*, *48* und *Auto* (Standardwert) • Für **Frequenzband** = *5 GHz In/Outdoor* und *5 GHz Outdoor* Hier ist nur die Option *Auto* möglich. **Access Client Modus:** Im Access Client Modus können Sie kein Kanal auswählen. Der verwendete Kanal wird angezeigt.
Ausgewählter Kanal	Zeigt den verwendeten Kanal an.

Feld	Beschreibung
Zweiter Verwendeter Kanal	Nicht für **Betriebsmodus** = *Access-Point / Bridge Link Master* Zeigt den zweiten verwendeten Kanal an.
Bandbreite	Für **Betriebsmodus** = *Access Client* oder *Access-Point / Bridge Link Master* Nicht für **Frequenzband** = *2,4 GHz In/Outdoor* Wählen Sie aus, wie viele Kanäle verwendet werden sollen. Mögliche Werte: • *20 MHz* (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • *40 MHz*: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontroll-Kanal und der andere als Erweiterungs-Kanal.
Anzahl der Spatial Streams	Nur für **Drahtloser Modus** = *802.11b/g/n*, *802.11g/n* und *802.11n* Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen. Mögliche Werte: • *2*: Zwei Datenströme werden verwendet. • *1*: Ein Datenstrom wird verwendet.
Sendeleistung	Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderabhängig. Mögliche Werte: • *Max.* (Standardwert): Die maximale Antennenleistung wird verwendet. • *5 dBm* • *8 dBm*

Feld	Beschreibung
	• *11 dBm* • *14 dBm* • *16 dBm* • 17 *dBm*

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	Wählen Sie die Wireless-Technologie aus, die der Access Point anwenden soll. Für **Betriebsmodus** = *Access-Point / Bridge Link Master* und **Frequenzband** = *2,4 GHz In/Outdoor* oder für **Betriebsmodus** = *Access Client* und **Frequenzband** = *2,4 GHz* Mögliche Werte: • *802.11g*: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • *802.11b*: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • *802.11 mixed (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. • *802.11 mixed long (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind. • *802.11 mixed short (b/g)*: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach **802.11b** oder **802.11g**. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • *802.11b/g/n*: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • *802.11g/n*: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n.

Feld	Beschreibung
	• *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. Für **Betriebsmodus** = *Access-Point / Bridge Link Master* und **Frequenzband** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* und für **Betriebsmodus** = *Access Client* und **Frequenzband** = *5 GHz* Mögliche Werte: • *802.11a*: Ihr Gerät arbeitet ausschließlich nach 802.11a. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. • *802.11a/n*: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
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.

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

Felder im Menü Erweiterte Einstellungen für Betriebsmodus = Access-Point / Bridge Link Master

Feld	Beschreibung
Kanalplan	Nur für **Betriebsmodus** = *Access-Point / Bridge Link Master* und **Kanal** = *Auto* Wählen Sie den gewünschten Kanalplan aus. Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d. h. dass zwischen den verwendeten Kanälen ein Abstand von

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

Feld	Beschreibung
	Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind *256* bis *2346*. Der Standardwert ist *2346* Bytes.

Wurde für **Betriebsmodus** *Access Client* ausgewählt, stehen unter **Erweiterte Einstellungen** zusätzlich folgende Parameter zur Verfügung:

Abb. 54: **Wireless LAN->WLAN->Einstellungen Funkmodul->->Erweiterte Einstellungen** *für* **Betriebsmodus** *Access Client*

Felder im Menü Erweiterte Einstellungen für Access Client Modus

Feld	Beschreibung
Kanäle scannen	Wählen Sie aus, auf welchen Kanälen der WLAN-Client automatisch nach verfügbaren Drahtlosnetzwerken scannen soll. Mögliche Werte: • *Alle* (Standardwert): Damit wird auf allen Kanälen gescannt. • *Auto*: Der Kanal wird automatisch ausgewählt. • *Benutzerdefiniert*: Damit können die gewünschten Kanäle manuell festgelegt werden.
Benutzerdefinierter Kanalplan	Nur für **Kanäle scannen** = *Benutzerdefiniert* Legen Sie fest, auf welchen Kanälen der WLAN-Client nach verfügbaren Drahtlosnetzwerken scannen soll.

Feld	Beschreibung
Roaming-Profil	Wählen Sie das Roaming-Profil aus. Die zur Verfügung stehende Optionen fassen typische Roaming-Funktionen zusammen. Mögliche Werte: • *Schnelles Roaming*: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung für höhere Datenraten ungeeignet ist. • *Normales Roaming* (Standardwert): Standard-Roaming. • *Langsames Roaming*: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung schwächer wird. • *Kein Roaming*: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, wenn er nicht mit einem Drahtlosnetzwerk verbunden ist. • *Benutzerdefiniertes Roaming*: Legen Sie individuelle Roaming-Parameter fest.
Scan-Schwelle	Zeigt an, ab welchem Wert in dBm im Hintergrund nach verfügbaren Drahtlosnetzwerken gescannt wird. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *-70 dBm*.
Scan-Intervall	Zeigt an, in welchen Abständen in Millisekunden nach verfügbaren Drahtlosnetzwerken gescannt wird. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *5000 ms*.
Min. Zeitraum aktiver Scan	Zeigt die minimale, aktive Scanzeit für eine Frequenz in Millisekunden an. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *10 ms*.
Max. Zeitraum aktiver Scan	Zeigt die maximale, aktive Scanzeit für eine Frequenz in Millisekunden an. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefinier-*

Feld	Beschreibung
	tes Roaming verändert werden. Der Standardwert ist *40 ms*.
Min. Zeitraum passiver Scan	Zeigt die minimale, passive Scanzeit für eine Frequenz in Millisekunden an. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *20 ms*.
Max. Zeitraum passiver Scan	Zeigt die maximale, passive Scanzeit für eine Frequenz in Millisekunden an. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *120 ms*.
Max. Scan Duration	Zeigt die maximale Scandauer für eine Frequenz in Millisekunden an. Der Wert kann nur für **Roaming-Profil** = *Benutzerdefiniertes Roaming* verändert werden. Der Standardwert ist *50000 ms*.

10.1.2 Drahtlosnetzwerke (VSS)

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

Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

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

Einstellen von Netzwerknamen

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

Absicherung von Funknetzwerken

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

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

WEP

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

IEEE 802.11i

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

WPA

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

802.1x (z. B. RADIUS) an.

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

WPA 2

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

Zugangskontrolle

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

Sicherheitsmaßnahmen

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

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

- Beschränken Sie den Zugriff im WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkkarten dieser Clients in die **Erlaubte Adressen**-Liste im Menü **MAC-Filter** ein (siehe *Felder im Menü MAC-Filter* auf Seite 139).

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

10.1.2.1 Bearbeiten oder Neu

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

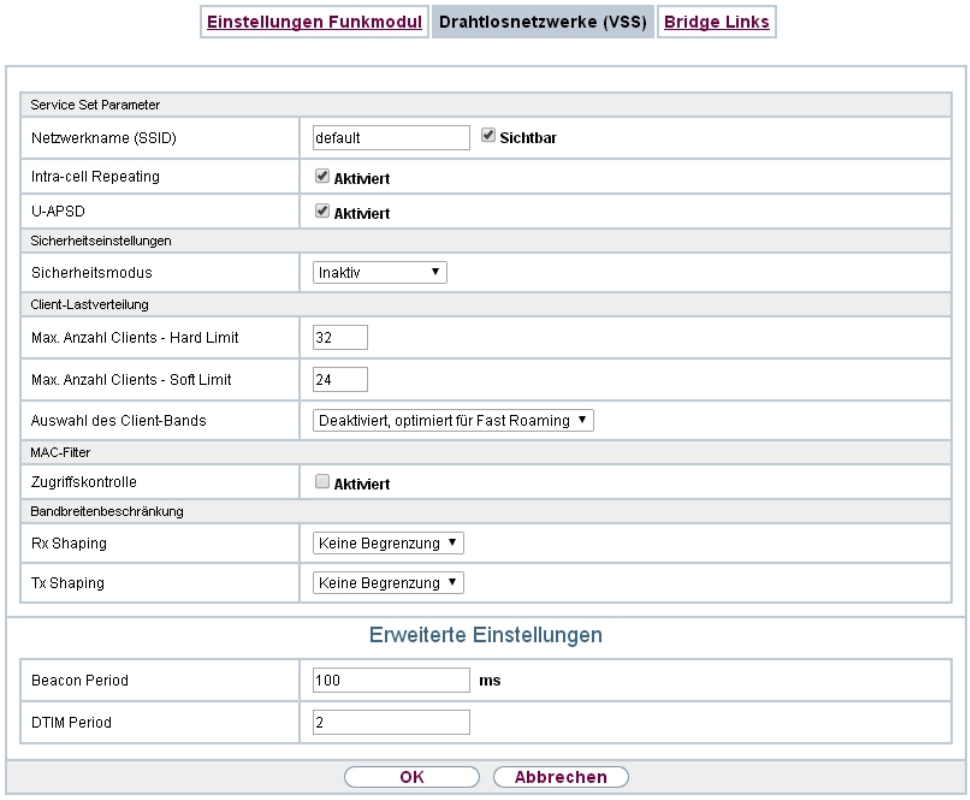


Abb. 55: **Wireless LAN**->**WLAN**->**Drahtlosnetzwerke (VSS)**->->**Neu**

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	Geben Sie den Namen des Wireless Netzwerks (SSID) ein. Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein. Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** übertragen werden soll. Mit Auswahl von *Sichtbar* wird der Netzwerkname sichtbar übertragen. Standardmäßig ist er sichtbar.
Intra-cell Repeating	Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
WMM	Wählen Sie aus, ob für das Drahtlosnetzwerk Sprach- oder Videodaten- Priorisierung mittels **WMM** (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
U-APSD	Wählen Sie aus, ob der Stromsparmodus Unscheduled Automatic Power Save Delivery (U-APSD) aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den **Sicherheitsmodus** (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte:

Feld	Beschreibung
	• *Inaktiv* (Standardwert): Weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11i/TKIP
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 40* oder *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1-4	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für *WEP 40* benötigen Sie eine Zeichenfolge mit 5 Zeichen, für *WEP 104* mit 13 Zeichen, z. B. *hallo* für *WEP 40*, *wep1* für *WEP 104*.
WPA-Modus	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: • *WPA und WPA 2* (Standardwert): **WPA und WPA 2** können angewendet werden. • *WPA*: Nur **WPA** wird angewendet. • *WPA 2*: Nur **WPA 2** wird angewendet.
WPA Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie **WPA** anwenden wollen.

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

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	Diese Funktion wird nicht von allen Geräten unterstützt. Diese Funktion erfordert eine Konfiguration mit zwei Radiomo-

Feld	Beschreibung
	dulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist. Die Option **Auswahl des Client-Bands** ermöglicht es, Clients von dem urspünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht. Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming*(Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • *2,4-GHz-Band bevorzugt*: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • *5-GHz-Band bevorzugt*: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

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

Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
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* ms.
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*.

10.1.3 Client Link

Wenn Sie Ihr Gerät im Access-Client-Modus betreiben (**Wireless LAN**->**WLAN**->**Einstellungen Funkmodul**->->**Betriebsmodus** = `Access Client`), können Sie im Menü **Wireless LAN**->**WLAN**->**Client Link**-> die vorhandenen Client Links bearbeiten.

Der **Client-Modus** kann im Infrastruktur- oder Ad-Hoc-Modus betrieben werden.

In einem Netz im Infrastruktur-Modus kommunizieren alle Clients ausschließlich über Access Points miteinander. Es läuft keine Kommunikation zwischen den einzelnen Clients direkt ab.

Ein Access Client kann im Ad-Hoc-Modus als zentrale Schnittstelle zwischen mehreren Endgeräten verwendet werden. Auf diese Weise können Geräte wie Computer und Drucker kabellos miteinander verbunden werden.

10.1.3.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Abb. 56: **Wireless LAN**->**WLAN**->**Client Link**->

Das Menü **Wireless LAN**->**WLAN**->**Client Link**-> besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Netzwerkname (SSID)	Geben Sie den Namen des Wireless-Netzwerks (SSID) ein. Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: • *Inaktiv* (Standardwert): Weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Keys
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1 - 4	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für *WEP 40* benötigen Sie eine Zeichenfolge mit 5 Zeichen, für *WEP 104* mit 13 Zeichen z. B. *hallo* für *WEP 40*, *wep1* für *WEP 104*.
WPA-Modus	Nur für **Sicherheitsmodus** = *WPA-PSK* Wählen Sie aus, ob Sie WPA oder WPA 2 anwenden wollen. Mögliche Werte: • *WPA* (Standardwert): Nur WPA wird angewendet. • *WPA 2*: Nur WPA2 wird angewendet.
Preshared Key	Nur für **Sicherheitsmodus** = *WPA-PSK* Geben Sie das WPA-Passwort ein. Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.
WPA Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und **WPA-Modus** = *WPA*

Feld	Beschreibung
	Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll. Mögliche Werte: • *TKIP* (Standardwert): Temporal Key Integrity Protocol • *AES*: Advanced Encryption Standard. Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.
WPA2 Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und **WPA-Modus** = *WPA 2* Wählen Sie aus, welche Verschlüsselungsmethode angewendet werden soll. Mögliche Werte: • *AES* (Standardwert): Advanced Encryption Standard. • *TKIP*: Temporal Key Integrity Protocol Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.

10.1.3.2 Client Link Scan

Nachdem die gewünschten Client-Links konfiguriert wurden, wird in der Liste das -Symbol angezeigt.

Über dieses Symbol öffnen Sie das Menü **Scan**.

Abb. 57: **Wireless LAN->WLAN->Client Link->Scan**

Nach erfolgreichem Scannen erscheint in der Scan-Liste eine Auswahl potenzieller Scan-Partner. Klicken Sie in der Spalte **Aktion** auf **Auswählen** um die lokalen Clients mit diesem Client zu verbinden. Wenn die Partner miteinander verbunden sind, erscheint in der Spalte **Verbunden** das -Symbol. In der Spalte **Verbunden** erscheint –Symbol wenn die Verbindung aktiv ist.

Das Menü **Wireless LAN**->**WLAN**->**Client Link**->**Scan** besteht aus den folgenden Feldern:

Felder im Menü Scan

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des von Ihnen konfigurierten Client-Links an.
Aktion	Lösen Sie den Scan durch Klicken von **Scan** aus. Bei sachgerechter Installation der Antennen auf beiden Seiten und freier LOS wird der Client verfügbare Clients finden und in der folgenden Liste anzeigen. Sollte die Partner-Client nicht gefunden werden, überprüfen Sie die Line-of-Sight und die Antenneninstallation. Führen Sie dann erneut **Scan** aus. Der Partner sollte daraufhin gefunden werden.
AP-MAC-Adresse	Zeigt die MAC-Adresse der entfernten Clients an.
Netzwerkname (SSID)	Zeigt den Namen der entfernten Clients an.
Kanal	Zeigt den **Kanal** an, der verwendet worden ist.
Modus	Zeigt den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes an.
Signal	Zeigt die Signalstärke des erkannten Client-Links in dBm an.
Verbunden	Zeigt den Status des Links auf Ihrem Client an.
Aktion	Sie können den Status der Client-Links verändern. In diesem Feld werden die zur Verfügung stehenden Aktionen angezeigt.

10.1.4 Bridge-Links

Nur für die Geräte der **bintec W1003n**, **W2003n**, **W2003n-ext** und **W2004n**-Serie verfügbar.

Mit **Bridge-Links** können Sie mehrere WLAN-Geräte eine dedizierte Verbindung aufbauen

lassen. Dabei wird sich das als Slave betriebene Radiomodul ausschließlich mit dem Master-Radiomodul verbinden und keine weiteren WLAN-Verbindungen aufbauen oder annehmen. Dies dient vor allem der zuverlässigen Verbindung von Netzwerken über eine WLAN-Strecke.

10.1.4.1 Bearbeiten oder Neu

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

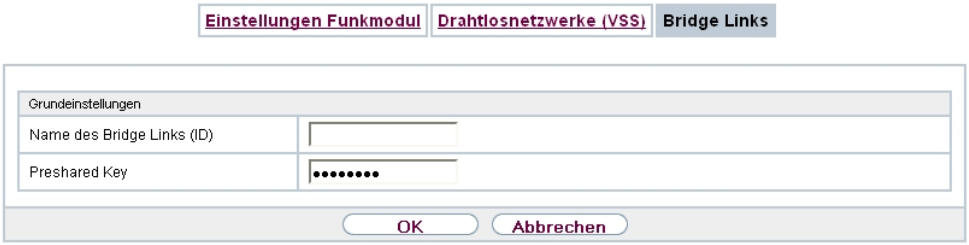


Abb. 58: **Wireless LAN->WLAN->Bridge-Links->->Neu**

Das Menü **Wireless LAN->WLAN->Bridge-Links->->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Name des Bridge Links (ID)	Je nachdem, ob Sie das Funkmodul als Access Point oder als Wireless Bridge Link betreiben, legen Sie hier einen Bridge Link im Master- oder im Slave-Modus an. Befindet sich das Funkmodul im Betriebsmodus **Access-Point / Bridge Link Master**, befindet sich der Bridge Link im Master-Modus. Geben Sie einen Namen für den Bridge Link ein. Dieser Name dient anderen Geräten als ID, unter der sie sich mit diesem Bridge Link verbinden können. Befindet sich das Funkmodul im Betriebsmodus **Bridge Link Client**, befindet sich der Bridge Link im Slave-Modus. Geben Sie hier die ID desjenigen Bridge Links ein, mit dem sich das Gerät verbinden soll.
Preshared Key	Geben Sie das Passwort für diesen Bridge-Link ein. Im Master-Modus ist dies das Passwort, mit dem andere Geräte sich mit diesem Bridge Link verbinden können, im Slave-Modus das

Feld	Beschreibung
	Passwort desjenigen Bridge Links, mit dem eine Verbindung aufgebaut werden soll.

10.2 Verwaltung

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

10.2.1 Grundeinstellungen

Abb. 59: **Wireless LAN**->**Verwaltung**->**Grundeinstellungen**

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

Felder im Menü WLAN Administration

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

Kapitel 11 Wireless LAN Controller

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

In kleineren WLAN-Infrastrukturen mit bis zu sechs APs übernimmt ein AP die Master-Funktion und verwaltet die anderen APs und sich selbst. In größeren WLAN-Netzen übernimmt ein Gateway, z. B. ein **R1202**, die Master-Funktion und verwaltet die APs.

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

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

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

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

11.1 Wizard

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

Bei Aufruf des Wizard erhalten Sie Anweisungen und Erläuterungen auf den einzelnen Assistentenseiten.

Hinweis

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

11.1.1 Grundeinstellungen

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

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

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

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

Wenn Sie z. B. ein 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.

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.

11.1.2 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.

11.1.3 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.

11.1.3.1 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.

Sicherheitsmodus

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

Hinweis: *WPA-Enterprise* bedeutet 802.11x.

WPA-Modus

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

Preshared Key

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

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

Wichtig

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

RADIUS-Server

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

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

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

EAP-Vorabauthentifizierung

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

VLAN

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

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

Hinweis

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

11.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

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

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

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

Standort

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

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

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

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

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

- *Aus*: Das Funkmodul ist nicht aktiv.

Aktives Funkmodulprofil

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

Kanal

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

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

Hinweis

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

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

Sendeleistung

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

Mit **OK** übernehmen Sie die Einstellungen.

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

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

Hinweis

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

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

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

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

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

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

11.2 Controller-Konfiguration

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

11.2.1 Allgemein

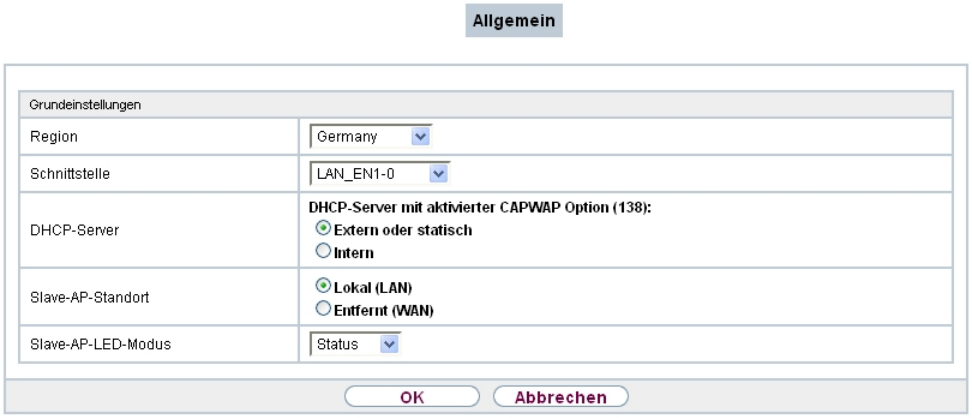


Abb. 60: **Wireless LAN Controller->Controller-Konfiguration->Allgemein**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Wireless LAN Controller betrieben werden soll. Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder. Der Bereich der verwendbaren Kanäle variiert je nach Ländereinstellung. Der Standardwert ist `Germany`.
Schnittstelle	Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.
DHCP-Server	Wählen Sie aus, ob ein externer DHCP-Server die IP-Adressen an die APs vergeben soll bzw. ob Sie selbst feste IP-Adressen vergeben wollen. Alternativ können Sie Ihr Gerät als DHCP-Server verwenden. Bei diesem internen DHCP-Server ist die CAPWAP Option 138 aktiv, um die Kommunikation zwischen Master und Slaves zu ermöglichen.

Feld	Beschreibung
	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. Mögliche Werte: • *Extern oder statisch* (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs. • *Intern*: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	Nur für **DHCP-Server** = *Intern* Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.
Slave-AP-Standort	Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden. Mögliche Werte: • *Lokal (LAN)* (Standardwert) • *Entfernt (WAN)* Die Einstellung *Entfernt (WAN)* ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die

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

11.3 Slave-AP-Konfiguration

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

11.3.1 Slave Access Points

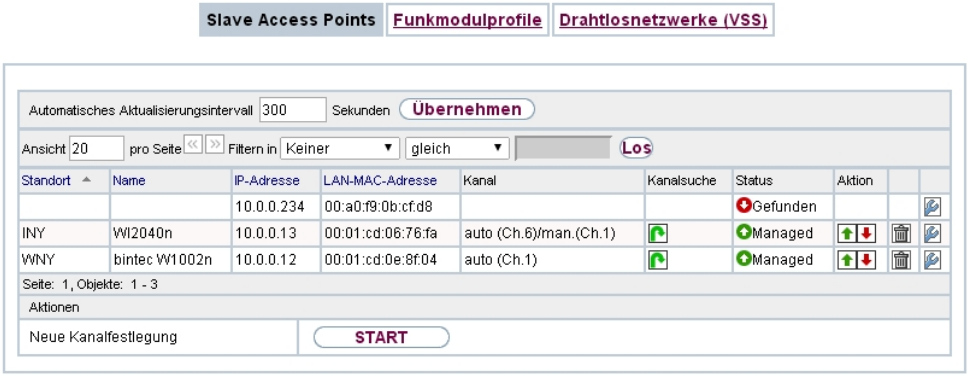


Abb. 61: **Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points**

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

Für jeden Access Point sehen Sie einen Eintrag mit einem Parametersatz (**Standort**, **Na-**

me, **IP-Adresse**, **LAN-MAC-Adresse**, **Kanal**, **Kanalsuche**, **Status**, **Aktion**). Durch Klicken auf die -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wählen Sie aus, ob der gewählte Access Point vom WLAN Controller verwaltet werden soll.

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

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

Mögliche Werte für Status

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

11.3.1.1 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.

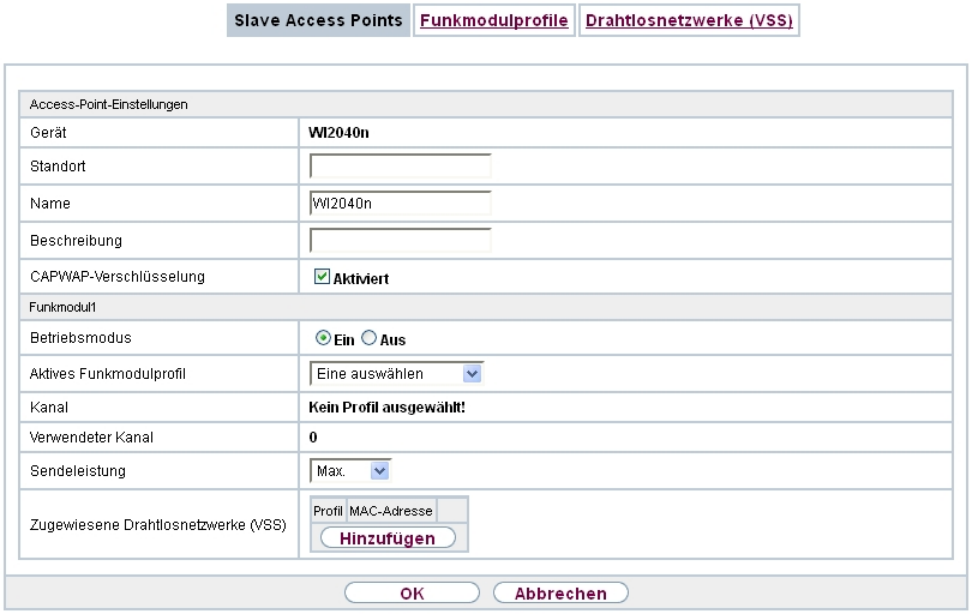


Abb. 62: **Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points->**

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.
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.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Sie können die Verschlüsselung aufheben, um die Kommunikation zu Debug-Zwecken einzusehen.

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

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

Feld	Beschreibung
	stützen. Mögliche Werte (entsprechend dem gewählten Funkmodulprofil): • Für **Aktives Funkmodulprofil** = *2,4 GHz Radio Profile* Mögliche Werte sind *1* bis *13* und *Auto* (Standardwert). • Für **Aktives Funkmodulprofil** = *5 GHz Radio Profile* Mögliche Werte sind *36*, *40*, *44*, *48* und *Auto* (Standardwert)
Verwendeter Kanal	Nur für Managed APs. Zeigt den aktuell benutzten Kanal.
Sendeleistung	Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen. Mögliche Werte: • *Max.* (Standardwert): Die maximale Antennenleistung wird verwendet. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*
Zugewiesene Drahtlosnetzwerke (VSS)	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

11.3.2 Funkmodulprofile

Abb. 63: **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile**

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

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

11.3.2.1 Bearbeiten oder Neu

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

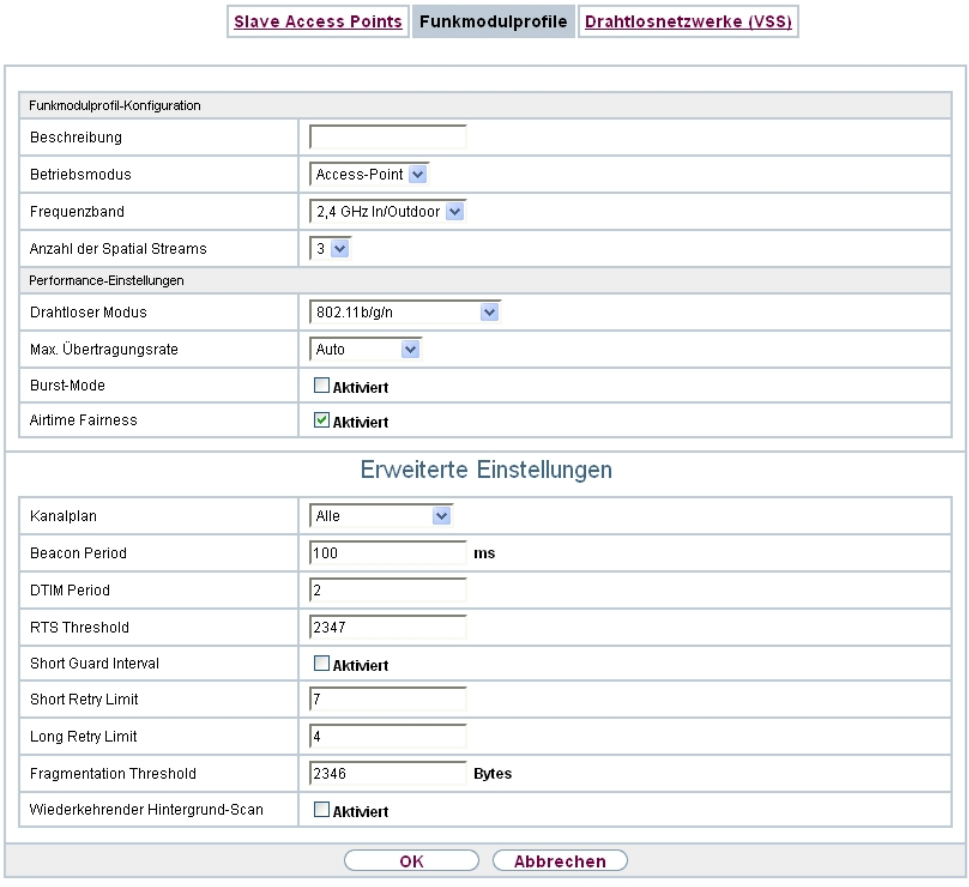


Abb. 64: **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile-> / Neu**

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

Felder im Menü Funkmodulprofil-Konfiguration

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung des Funkmodulprofils ein.
Betriebsmodus	Legen Sie fest, in welchem Modus das Funkmodulpofil betrieben werden soll. Mögliche Werte:

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 (Mode 802.11b, Mode 802.11g und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • *5 GHz Indoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb von Gebäuden betrieben. • *5 GHz Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) außerhalb von Gebäuden betrieben. • *5 GHz In/Outdoor*: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • *5,8 GHz Outdoor*: Nur für so genannte Broadband Fixed Wireless Access (BFWA) Anwendungen. Die Frequenzen im Frequenzbereich von 5 755 MHz bis 5 875 MHz dürfen nur in Verbindung mit gewerblichen Angeboten für öffentliche Netzzugänge genutzt werden und bedürfen einer Anmeldung bei der Bundesnetzagentur.
Bandbreite	Nicht für **Frequenzband** = *2,4 GHz In/Outdoor* Wählen Sie aus, wieviele Kanäle verwendet werden sollen. Mögliche Werte: • *20 MHz* (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • *40 MHz*: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal.
Anzahl der Spatial Streams	Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen. Mögliche Werte: • *3*: Drei Datenströme werden verwendet.

Feld	Beschreibung
	• *2*: Zwei Datenströme werden verwendet. • *1*: Ein Datenstrom wird verwendet.

Felder im Menü Performance-Einstellungen

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

Feld	Beschreibung
	• *802.11a*: Ihr Gerät arbeitet ausschließlich nach 802.11a. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. • *802.11a/n*: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
Max. Übertragungsrate	Wählen Sie die Übertragungsgeschwindigkeit aus. Mögliche Werte: • *Auto* (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • *<Wert>*: Je nach Einstellung für **Frequenzband**, **Bandbreite**, **Anzahl der Spatial Streams** und **Drahtloser Modus** stehen verschiedene feste Werte in MBit/s zur Auswahl.
Burst-Mode	Aktivieren Sie diese Funktion, um die Übertragungsgeschwindigkeit für 802.11g durch Frame Bursting zu erhöhen. Dabei werden mehrere Pakete nacheinander ohne Wartezeiten verschickt. Dies ist besonders effektiv im 11b/g Mischbetrieb. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion nicht aktiv sein.
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.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Kanalplan	Wählen Sie den gewünschten Kanalplan aus. Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d.h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen. Mögliche Werte: • *Alle*: Alle Kanäle können bei der Kanalwahl gewählt werden. • *Auto*: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • *Benutzerdefiniert*: Sie können die gewünschten Kanäle selbst auswählen.
Benutzerdefinierter Kanalplan	Nur für **Kanalplan** = *Benutzerdefiniert* Hier werden die aktuell gewählten Kanäle angezeigt. Mit **Hinzufügen** können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen. Mithilfe von -Symbol können Sie Einträge löschen.
Beacon Period	Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an. Dieser Wert wird in Beacon und Probe Response Frames übermittelt. Mögliche Werte sind *1* bis *65535*. Der Standardwert ist *100*.
DTIM Period	Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.

Feld	Beschreibung
	Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *2*.
RTS Threshold	Sie können hier den Schwellwert in Bytes (1..2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden.
Short Guard Interval	Aktivieren Sie diese Funktion, um den Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
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. 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*.

Feld	Beschreibung
	Der Standardwert ist *2346*.
Wiederkehrender Hintergrund-Scan	Diese Funktion wird nicht von allen Geräten unterstützt. Um in regelmäßigen Abständen automatisch nach benachbarten oder Rogue Access Points im Netzwerk zu suchen, können Sie die Funktion **Wiederkehrender Hintergrund-Scan** aktivieren. Diese Suche erfolgt ohne eine Beeinträchtigung der Funktion als Access Point. Aktivieren oder deaktivieren Sie die Funktion **Wiederkehrender Hintergrund-Scan**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion deaktiviert.

11.3.3 Drahtlosnetzwerke (VSS)

Abb. 65: **Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)**

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

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

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

11.3.3.1 Bearbeiten oder Neu

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

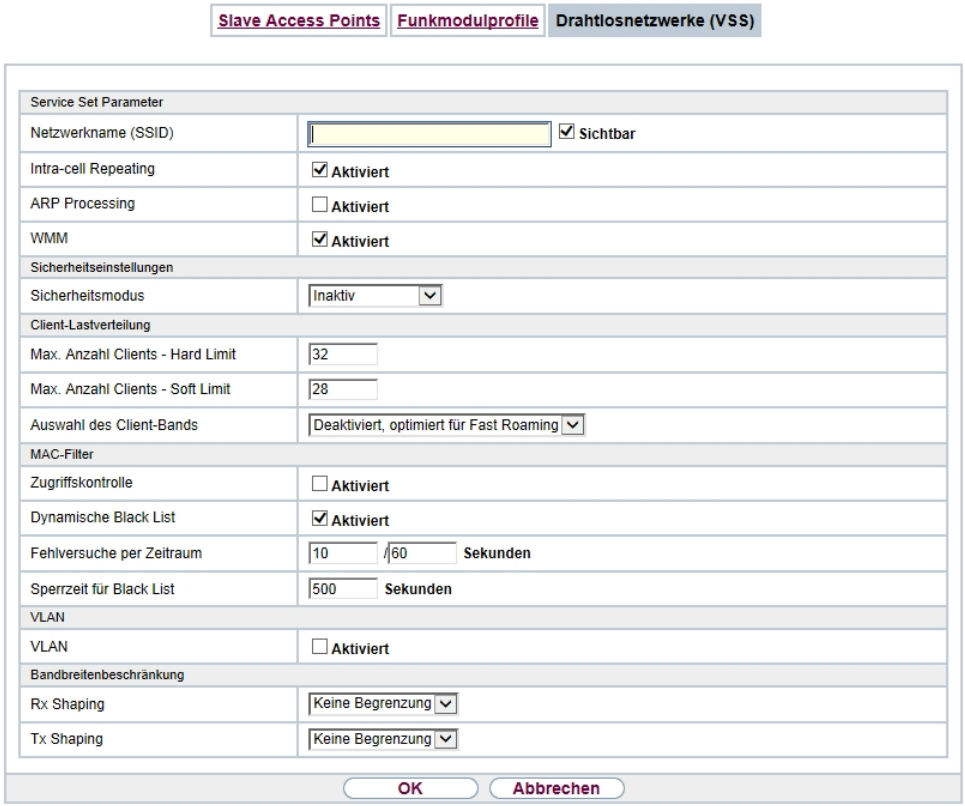


Abb. 66: **Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)->Neu**

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein. Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein. Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** über-

Feld	Beschreibung
	tragen werden soll. Mit Auswahl von *Sichtbar* wird der Netzwerkname sichtbar übertragen. Standardmäßig ist er sichtbar.
Intra-cell Repeating	Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
ARP Processing	Wählen Sie aus, ob die Funktion ARP Processing aktiv sein soll. Dabei wird das ARP-Datenaufkommen im Netzwerk reduziert, indem in ARP-Unicasts umgewandelte ARP-Broadcasts an die intern bekannten IP-Adressen weitergeleitet werden. Unicasts sind zudem schneller, und Clients mit aktivierter Power-Save-Funktion werden nicht angesprochen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Beachten Sie, dass ARP Processing nicht zusammen mit der Funktion MAC-Bridge angewendet werden kann.
WMM	Wählen Sie aus, ob für das Drahtslosnetzwerk Sprach- oder Videodaten- Priorisierung mittels WMM (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Sicherheitseinstellungen

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

Feld	Beschreibung
	Mögliche Werte: • *Inaktiv* (Standardwert): Weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11x
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 40* oder *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1-4	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für *WEP 40* benötigen Sie eine Zeichenfolge mit 5 Zeichen, für *WEP 104* mit 13 Zeichen, z. B. *hallo* für *WEP 40*, *wep104* für *WEP 104*.
WPA-Modus	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: • *WPA und WPA 2* (Standardwert): WPA und WPA 2 können angewendet werden. • *WPA*: Nur WPA wird angewendet. • *WPA 2*: Nur WPA2 wird angewendet.
WPA Cipher	Nur für **Sicherheitsmodus** = *WPA-PSK* und *WPA-Enterprise* und für **WPA-Modus** = *WPA* und *WPA und WPA 2* Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwen-

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

Feld	Beschreibung
	WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen. Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis. Mögliche Werte sind ganze Zahlen von *1* bis *254*. Der Standardwert ist *32*.
Max. Anzahl Clients - Soft Limit	Diese Funktion wird nicht von allen Geräten unterstützt. Um eine vollständie Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehent. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des **Max. Anzahl Clients - Hard Limit** werden Anfragen strikt abgelehnt. Der Wert der **Max. Anzahl Clients - Soft Limit** muss gleich oder kleiner sein als der **Max. Anzahl Clients - Hard Limit**. Der Standardwert ist *28*. Sie können diese Funktion deaktivieren, indem Sie **Max. Anzahl Clients - Soft Limit** und **Max. Anzahl Clients - Hard Limit** auf den gleichen Wert einstellen.

Feld	Beschreibung
Auswahl des Client-Bands	Diese Funktion wird nicht von allen Geräten unterstützt. Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist. Die Option **Auswahl des Client-Bands** ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht. Mögliche Werte: • *Deaktiviert, optimiert für Fast Roaming*(Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • *2,4-GHz-Band bevorzugt*: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • *5-GHz-Band bevorzugt*: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

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

Feld	Beschreibung
	Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden. Ein gesperrten Client wird auf allen vom Wireless LAN Controller verwalteten APs für das betroffene VSS gesperrt, kann sich also auch nicht in einer anderen Funkzelle an diesem VSS anmelden. Soll ein Client permanent gesperrt bleiben, so kann dies im Menü **Wireless LAN Controller**->**Monitoring**->**Rogue Clients** erfolgen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiviert.
Fehlversuche per Zeitraum	Geben Sie hier die Anzahl der Fehlversuche ein, die innerhalb einer bestimmten Zeit von einer MAC-Adresse ausgehen müssen, damit ein Eintrag in der dynamischen Black List angelegt wird. Standardwerte sind *10* Fehlversuche in *60* Sekunden.
Sperrzeit für Black List	Geben Sie die Zeit ein, für die ein Eintrag in der dynamischen Black List gelten soll. Der Standardwert ist *500* Sekunden.

Felder im Menü VLAN

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

Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung. Mögliche Werte sind • *Keine Begrenzung* (Standardwert) • *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*.

11.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

Hinweis

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

11.4.1 WLAN Controller

Abb. 67: **Wireless LAN Controller->Monitoring->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.

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

11.4.2 Slave Access Points

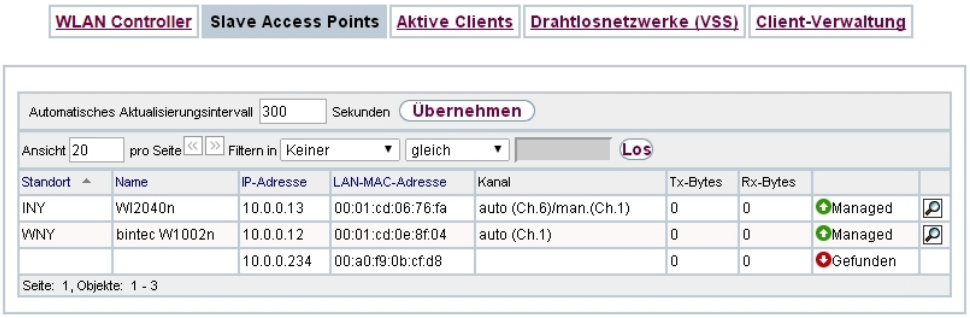


Abb. 68: **Wireless LAN Controller->Monitoring->Slave Access Points**

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

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

11.4.2.1 Übersicht

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

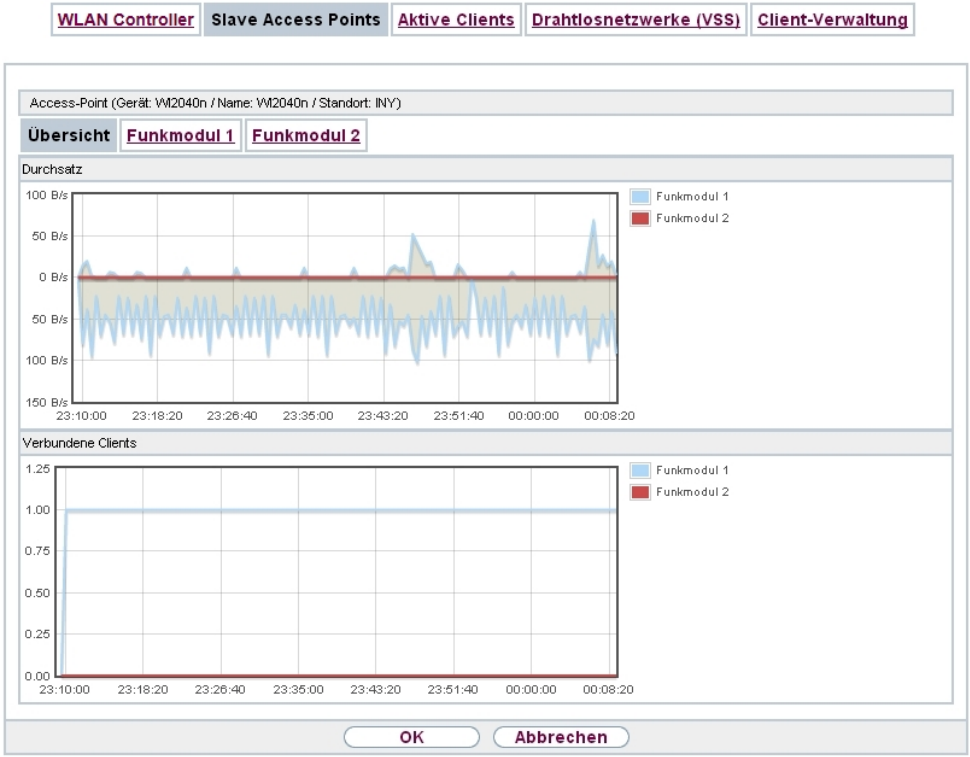


Abb. 69: **Wireless LAN Controller->Monitoring->Slave Access Points->Übersicht**

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.

11.4.2.2 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.

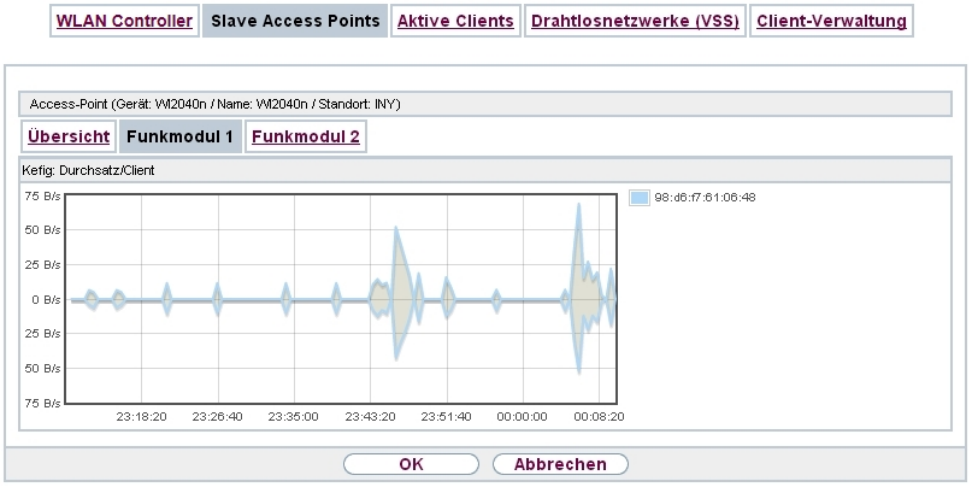


Abb. 70: **Wireless LAN Controller->Monitoring->Slave Access Points->Funkmodul**

Werte in der Liste Funkmodul

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

11.4.3 Aktive Clients

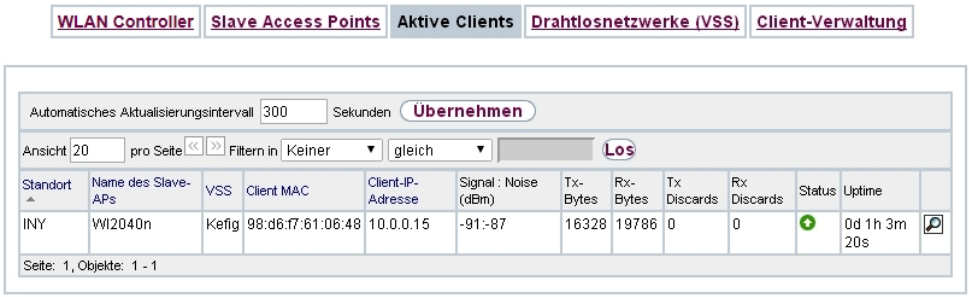


Abb. 71: **Wireless LAN Controller->Monitoring->Aktive Clients**

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

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

Mögliche Werte für Status

Status	Bedeutung
Keiner	Der Client befindet sich in keinem gültigen Zustand.
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.

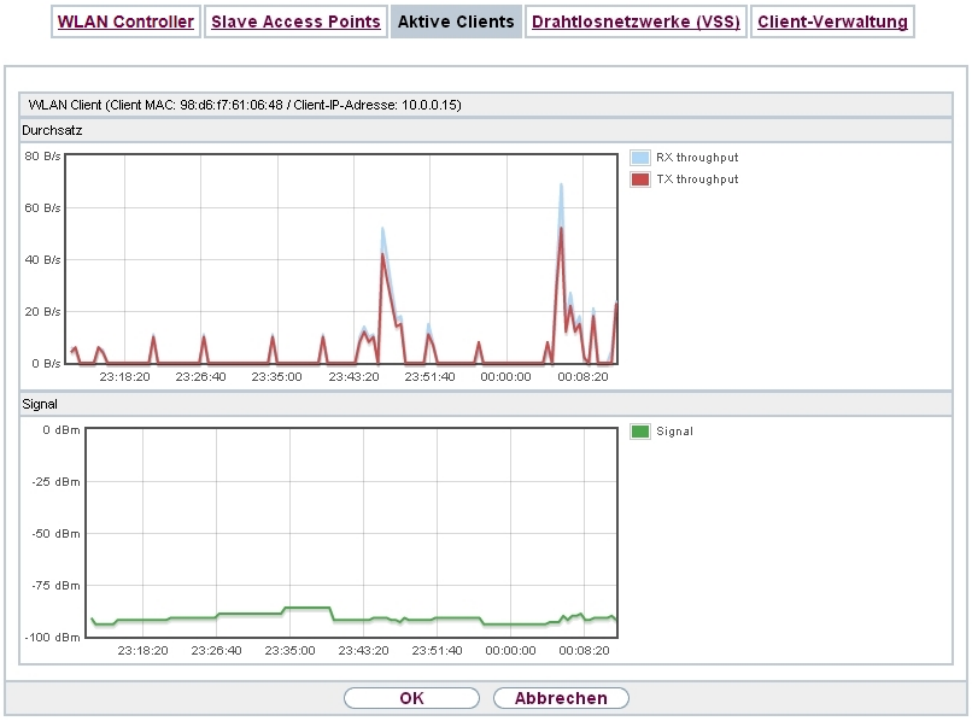


Abb. 72: **Wireless LAN Controller->Monitoring->Aktive Clients->**

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.

Status	Bedeutung
Signal	Zeigt die Signalstärke für den gewählten WLAN Client zeitabhängig an.

11.4.4 Drahtlosnetzwerke (VSS)

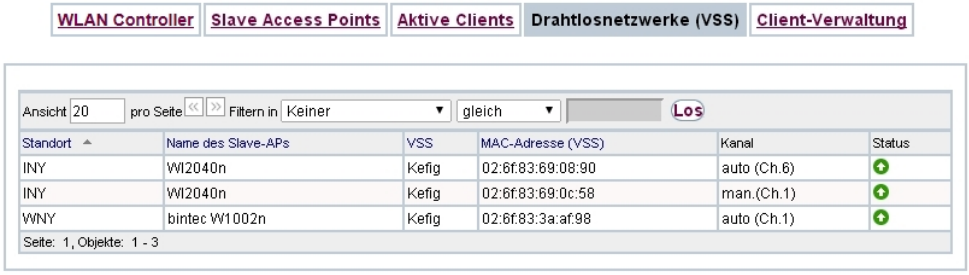


Abb. 73: **Wireless LAN Controller->Monitoring->Drahtlosnetzwerke (VSS)**
Im Menü **Wireless LAN Controller->Monitoring->Drahtlosnetzwerke (VSS)** wird eine Übersicht über die aktuell verwendeten AP angezeigt. Sie sehen, welches Funkmodul welchem Drahtlosnetzwerk zugeordnet ist. Für jedes Funkmodul wird ein Parametersatz angezeigt (**Standort**, **Name des Slave-APs**, **VSS**, **MAC-Adresse (VSS)**, **Kanal**, **Status**).

11.4.5 Client-Verwaltung

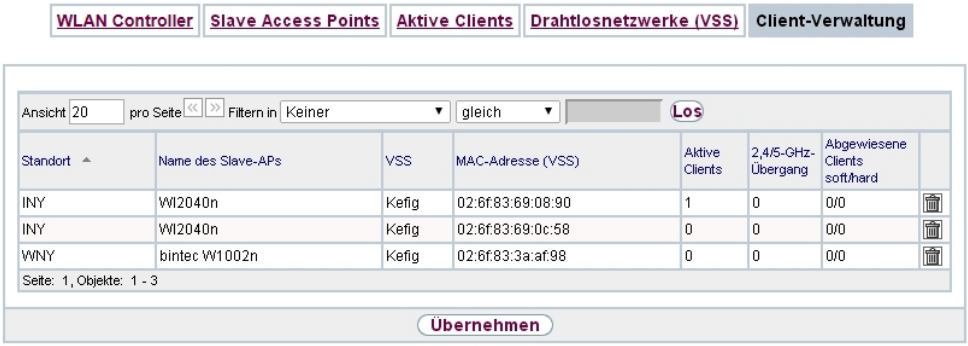


Abb. 74: **Wireless LAN Controller->Monitoring+Client-Verwaltung**

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.

11.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Acces Points und Clients.

11.5.1 Benachbarte APs

Abb. 75: **Wireless LAN Controller**+**Umgebungs-Monitoring**->**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.

11.5.2 Rogue APs

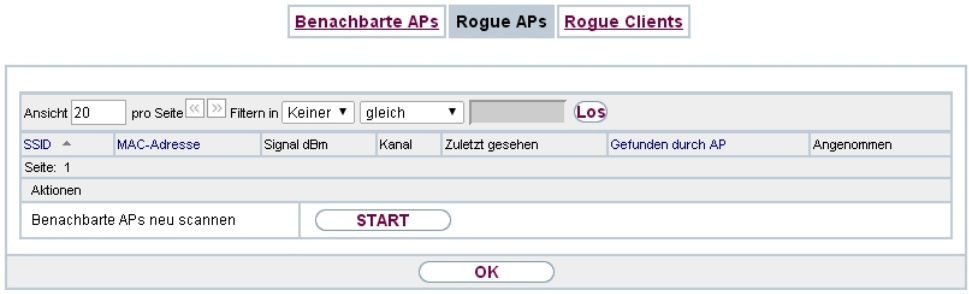


Abb. 76: **Wireless LAN Controller**+**Umgebungs-Monitoring**->**Rogue APs**

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.

11.5.3 Rogue Clients

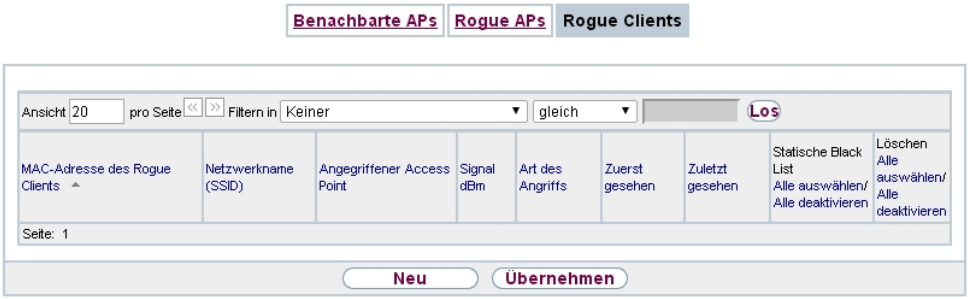


Abb. 77: **Wireless LAN Controller+Umgebungs-Monitoring->Rogue Clients**

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

Mögliche Werte für Rogue Clients

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

11.5.3.1 Neu

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

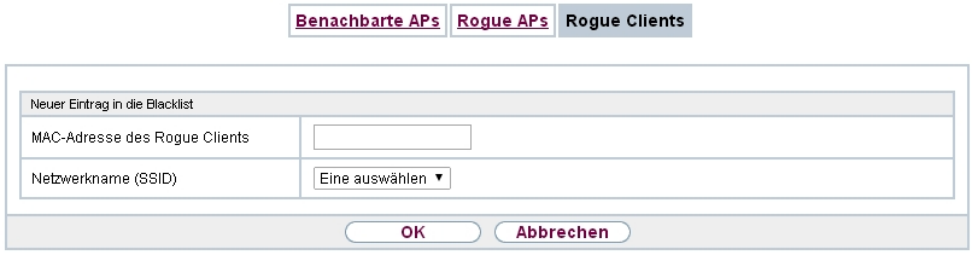


Abb. 78: **Wireless LAN Controller+Umgebungs-Monitoring->Rogue Clients->Neu**

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.

11.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

11.6.1 Firmware-Wartung

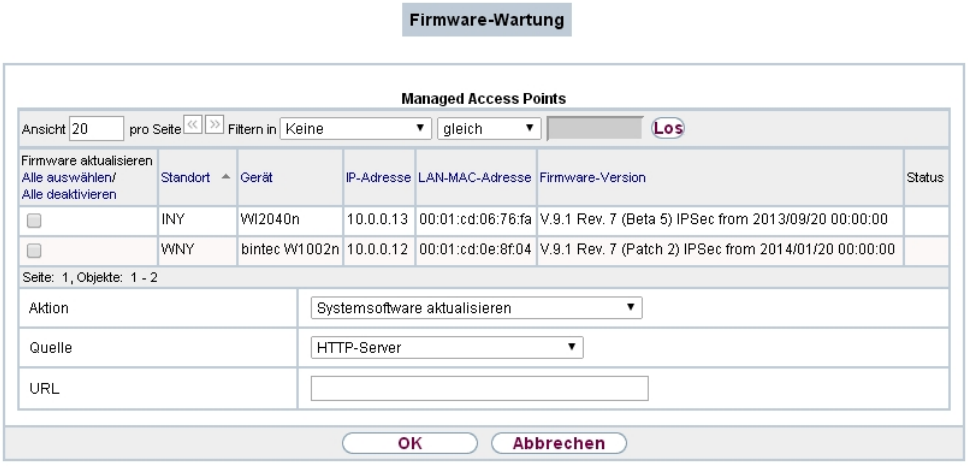


Abb. 79: **Wireless LAN Controller->Wartung->Firmware-Wartung**

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** = *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.

Kapitel 12 Netzwerk

12.1 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.

12.1.1 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,

12.1.1.1 Bearbeiten oder Neu

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

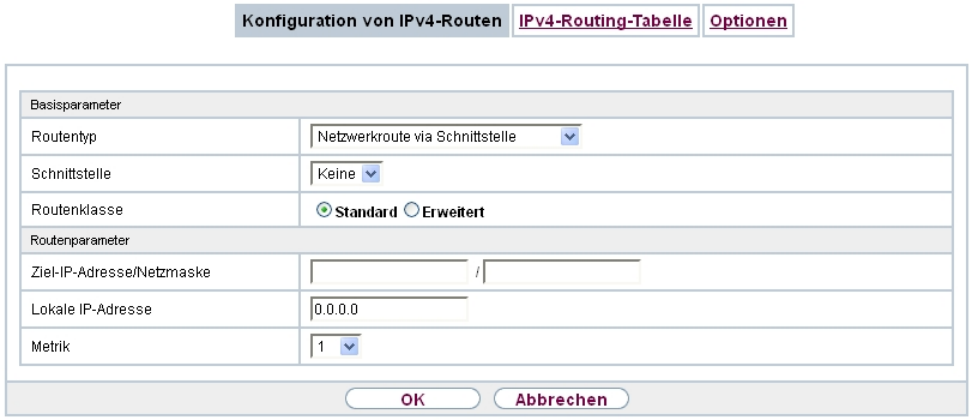


Abb. 80: **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen** ->**Neu** *mit* **Erweiterte Route** = *Standard.*

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

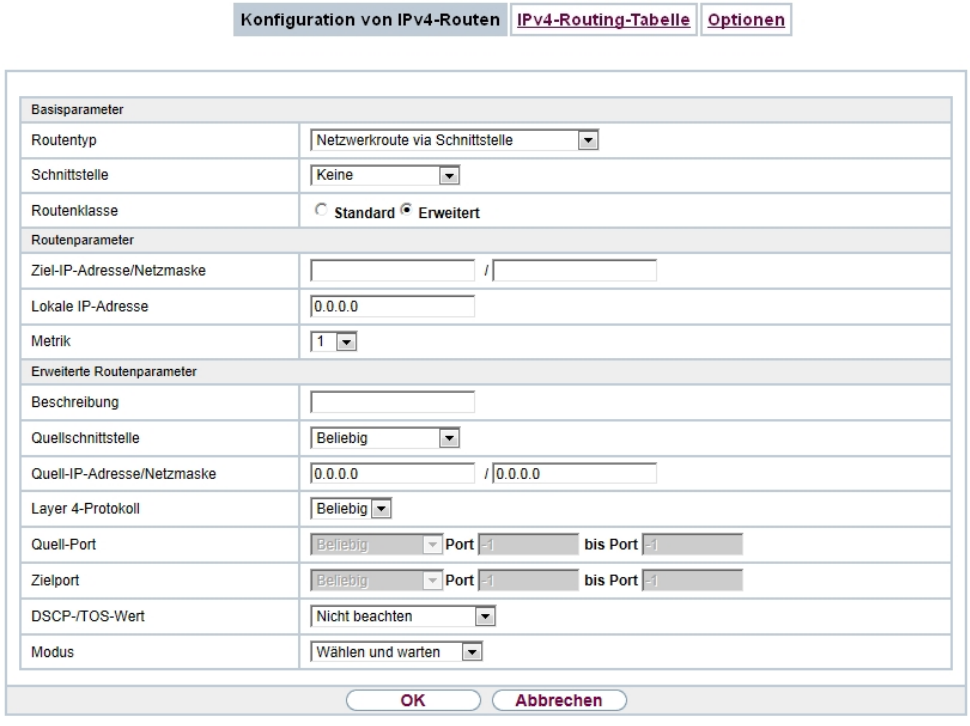


Abb. 81: **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen** ->**Neu** *mit* **Erweitert** = `Aktiviert`

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

Feld 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 Routing-Informationen werden vollständig vom DHCP-Server übernommen. Lediglich erweiterte Parameter können zusätzlich konfiguriert werden. Diese Route bleibt von weiteren für diese

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

Felder im Menü Routenparameter

Feld	Beschreibung
Lokale IP-Adresse	Nur für **Routentyp** = *Standardroute über Schnittstelle*, *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle*

Feld	Beschreibung
	Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Ziel-IP-Adresse/Netzmaske	Nur für **Routentyp** *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein. Bei **Routentyp** = *Netzwerkroute via Schnittstelle* Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.
Gateway-IP-Adresse	Nur für **Routentyp** = *Standardroute über Gateway*, *Host-Route via Gateway* oder *Netzwerkroute via Gateway* 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: *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *L2TP*, *Beliebig*.

Feld	Beschreibung
	Der Standardwert ist *Beliebig*.
Quell-Port	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Quellport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
Zielport	Nur für **Layer 4-Protokoll** = *TCP* oder *UDP* Geben Sie den Zielport an. Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port-Nummern.

Feld	Beschreibung
	• *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
DSCP-/TOS-Wert	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F. Geben Sie für *DSCP-Binärwert*, *DSCP-Dezimalwert*, *DSCP-Hexadezimalwert*, *TOS-Binärwert*, *TOS-Dezimalwert* und *TOS-Hexadezimalwert* den entsprechenden Wert ein.

Feld	Beschreibung
Modus	Wählen Sie aus, wann die in **Routenparameter**->**Schnittstelle** definierte Schnittstelle benutzt werden soll. Mögliche Werte: • *Wählen und warten* (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • *Verbindlich*: Die Route ist immer benutzbar. • *Wählen und fortfahren*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • *Nie einwählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • *Immer wählen*: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" 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.

12.1.2 IPv4-Routing-Tabelle

Im Menü **Netzwerk**->**Routen**->**IPv4-Routing-Tabelle** wird eine Liste aller IPv4-Routen angezeigt. Die Routen müssen nicht alle aktiv sein, können aber durch entsprechenden Datenverkehr jederzeit aktiviert werden.

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,

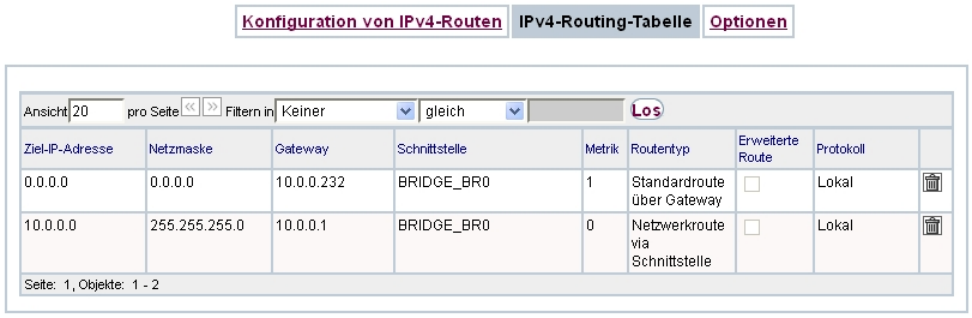


Abb. 82: **Netzwerk->Routen->IPv4-Routing-Tabelle**

Felder im Menü IPv4-Routing-Tabelle

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

12.1.3 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.

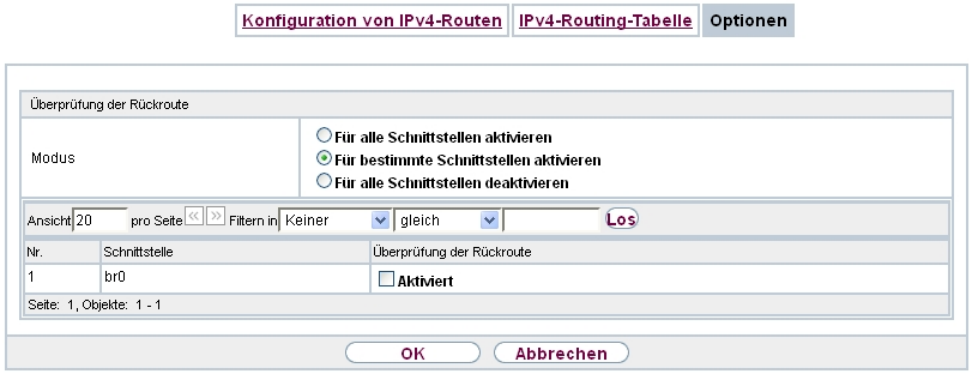


Abb. 83: **Netzwerk->Routen->Optionen**

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`*

Feld	Beschreibung
	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.

12.2 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 201).

12.2.1 NAT-Schnittstellen

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

Abb. 84: **Netzwerk**->**NAT**->**NAT-Schnittstellen**

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.

12.2.2 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.

12.2.2.1 Neu

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

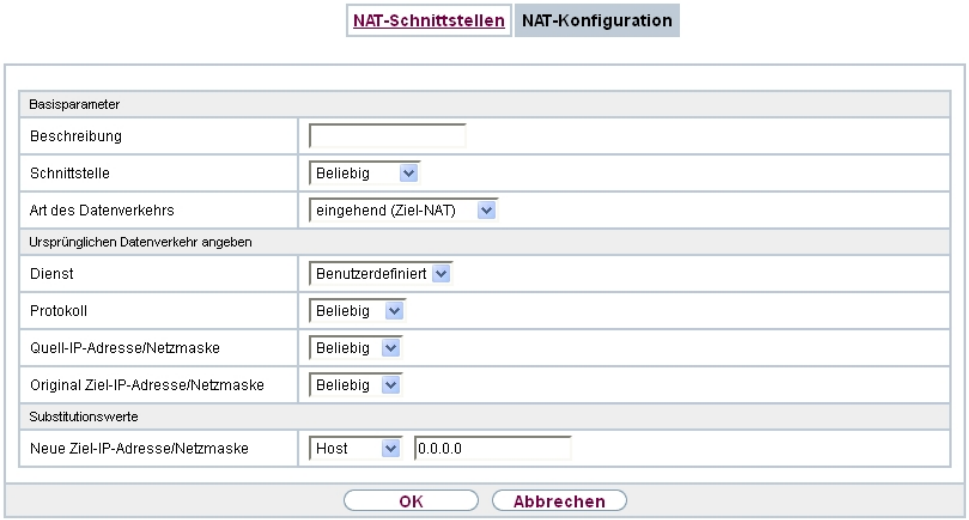


Abb. 85: **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu**

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 Schnittstel-

Feld	Beschreibung
	len aus der Liste aus.
Art des Datenverkehrs	Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll. Mögliche Werte: • *eingehend (Ziel-NAT)* (Standardwert): Der Datenverkehr, der von außen kommt. • *ausgehend (Quell-NAT)*: Der Datenverkehr, der nach außen geht. • *exklusiv (ohne NAT)*: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden. Mögliche Werte: • *full-cone* (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiierende Quelladresse und den initialen Quellport senden. • *restricted-cone* (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. • *port-restricted-cone* (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • *symmetrisch* (Standardwert) Für beliebige Protokolle: In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

Im Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** können Sie konfigurieren, für welchen Datenverkehr NAT verwendet werden soll.

Felder im Menü Ursprünglichen Datenverkehr angeben

Feld	Beschreibung
Dienst	Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. Wählen Sie einen der vorkonfigurierten Dienste aus. Mögliche Werte: • *Benutzerdefiniert* (Standardwert) • *<Dienstname>*
Aktion	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)* Wählen Sie, welche Datenpakete von NAT ausgenommen werden. Mögliche Werte: • *Ausschließen* (Standardwert): Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) übereinstimmen, werden von NAT ausgenommen. • *Nicht ausschließen*: Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) nicht übereinstimmen, werden von NAT ausgenommen.
Protokoll	Nur für bestimmte Dienste. Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. In diesem Fall wird UDP automatich festgelegt. Wählen Sie ein Protokoll aus. Je nach ausgewähltem **Dienst** stehen verschiedene Protokolle zur Verfügung. Mögliche Werte: • *Beliebig* (Standardwert)

Feld	Beschreibung
	• *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *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.

Feld	Beschreibung
Original Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-Port/Bereich	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Originale Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Quell-Port/Bereich	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist. Wenn Sie *Port angeben* wählen, können Sie einen einzelnen Port angeben, mit der Auswahl von *Portbereich angeben* können Sie einen zusammenhängenden Bereich von Ports definieren, der als Filter für den ausgehenden Datenverkehr verwendet wird.
Quell-Port/Bereich	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Quell-Port bzw. den Quell-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *exklusiv (ohne NAT)* bzw. *ausgehend (Quell-NAT)* und **NAT-Methode** = *symmetrisch*

Feld	Beschreibung
	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 ur-

Feld	Beschreibung
	sprüngliche 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* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* 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: • *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.

12.3 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.

12.3.1 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.

12.3.1.1 Neu

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

Abb. 86: **Netzwerk**->**Lastverteilung**->**Lastverteilungsgruppen**->**Neu**

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.

Feld	Beschreibung
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. 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.

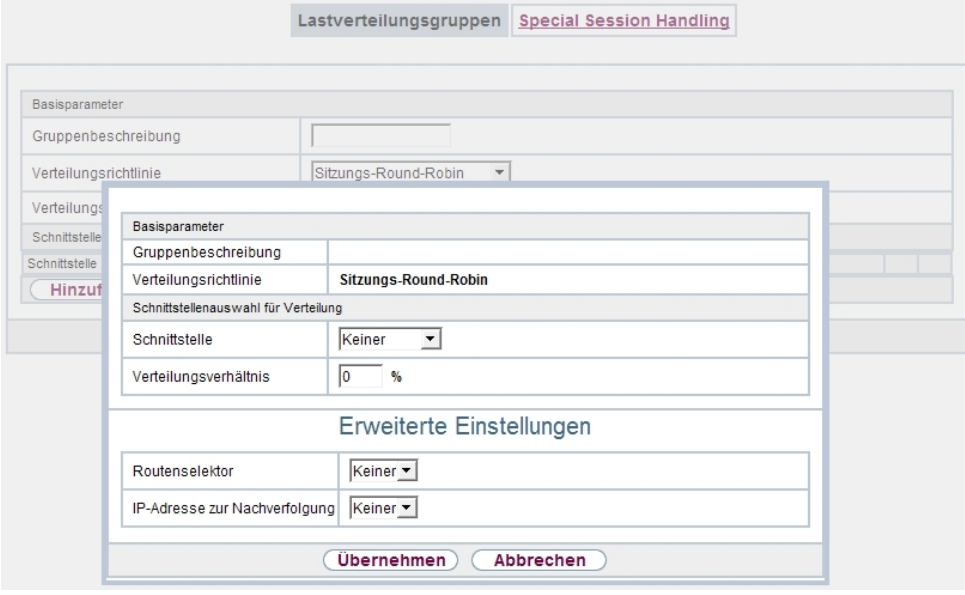


Abb. 87: **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Hinzufügen**

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.

Feld	Beschreibung
	• Für *Lastabhängige Bandbreite* ist die Datenrate maßgeblich.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Routenselektor	Der Parameter **Routenselektor** ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten 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**->**Über-**

Feld	Beschreibung
	wachung->**Hosts**. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion **Überwachung** 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 zum Status des zugewiesenen Host-Überwachungseintrages. Wählen Sie die IP-Adresse der Route, die überwacht werden soll. Sie können unter den IP-Adressen wählen, die Sie im Menü **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu** unter **Überwachte IP-Adresse** eingegeben haben und die mit Hilfe des Feldes **Auszuführende Aktion** überwacht werden (**Aktion** = *Überwachen*) .

12.3.2 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.

12.3.2.1 Bearbeiten oder Neu

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

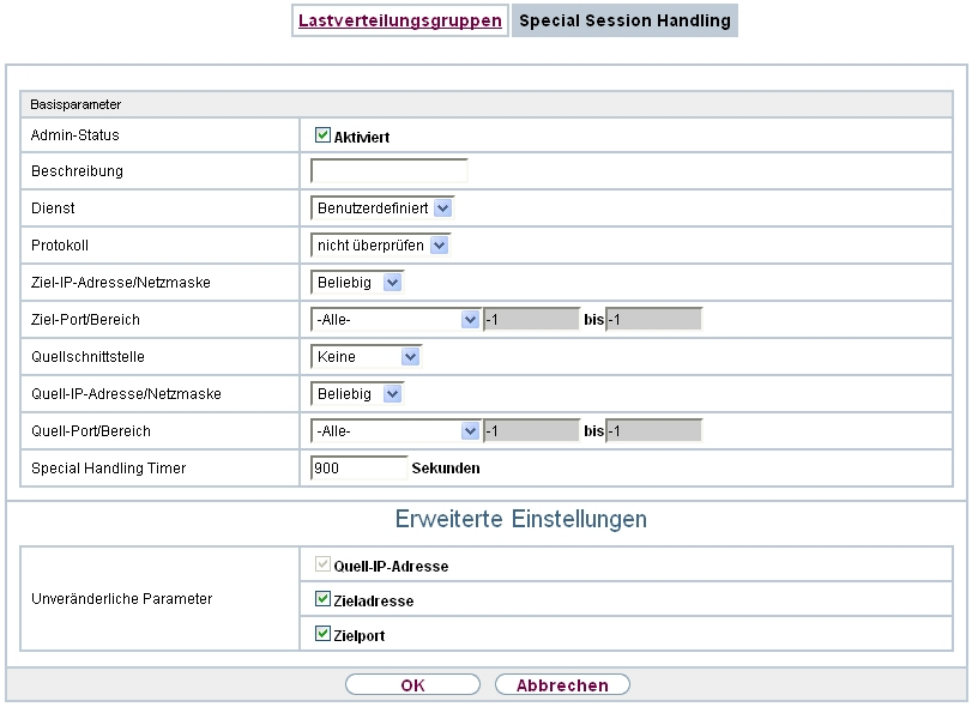


Abb. 88: **Netzwerk->Lastverteilung->Special Session Handling->Neu**

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.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *Benutzerdefiniert*.
Protokoll	Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Ziel-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* (Standardwert) • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Geben Sie, falls gewünscht, eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert.

Feld	Beschreibung
	• *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Ziel-Port-Bereich ein.
Quellschnittstelle	Wählen Sie, falls gewünscht, die Quellschnittstelle Ihres Geräts aus.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* (Standardwert) • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Geben Sie, falls gewünscht, eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Quell-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Quell-Port ein. • *Portbereich angeben*: Geben Sie einen Quell-Port-Bereich ein.
Special Handling Timer	Geben Sie ein, während welcher Zeitspanne die spezifizierten Datenpakete über den festgelegten Weg geroutet werden sollen. Der Standardwert ist *900* Sekunden.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	adresse 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.

12.4 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

12.4.1 QoS-Filter

Im Menü **Netzwerk**->**QoS**->**QoS-Filter** werden IP-Filter konfiguriert.

Die Liste zeigt ebenfalls alle ggf. konfigurierten Einträge aus **Netzwerk**->**Zugriffsregeln**->**Regelketten**.

12.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Filter zu definieren.

Abb. 89: **Netzwerk**->**QoS**->**QoS-Filter**->**Neu**

Das Menü **Netzwerk**->**QoS**->**QoS-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 *Benutzerdefiniert*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.

Feld	Beschreibung
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.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von

Feld	Beschreibung
	Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Ziel-Port-Bereich ein.
DSCP/TOS-Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Wertebereich *0* bis *7*. Der Standardwert ist *Nicht beachten*.

12.4.2 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.

12.4.2.1 Neu

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

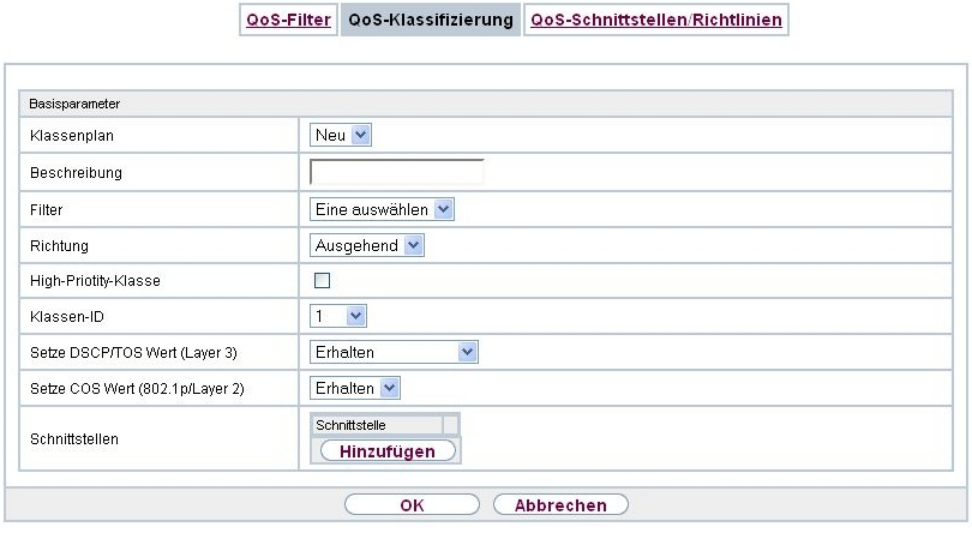


Abb. 90: **Netzwerk**->**QoS**->**QoS-Klassifizierung**->**Neu**

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 angeleg-

Feld	Beschreibung
	ten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	Nur für **Klassenplan** = *Neu* Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll. Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü **Netzwerk**->**QoS**->**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 zu-

Feld	Beschreibung
	weist. **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`.
Setze DSCP/TOS Wert (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)	Hier können Sie die Serviceklasse (Layer-2-Priorität) im VLAN Ethernet Header der IP-Pakete in Abhängigkeit zur definierten Klasse (**Klassen-ID**) setzen/ändern. Mögliche Werte sind ganze Zahlen zwischen `0` und `7`. Der Standardwert ist `Erhalten`.

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

12.4.3 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.

12.4.3.1 Neu

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

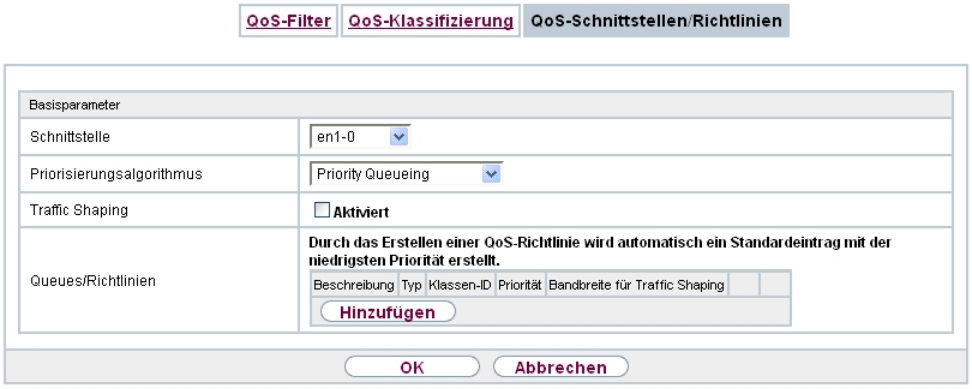


Abb. 91: **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu**

Das Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

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

Feld	Beschreibung
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 Queue eine maximale Datenrate in kBits pro Sekunde in Senderichtung ein. Mögliche Werte sind *0* bis *1000000*. Der Standardwert ist *0*, d. h. es erfolgt keine Begrenzung, die Queue kann die maximale Bandbreite belegen.
Größe des Protokoll-Headers unterhalb Layer 3	Nur für **Traffic Shaping** = aktiviert. Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen. Mögliche Werte: • *Benutzerdefiniert* Wert in Byte. Mögliche Werte sind *0* bis *100*. • *Undefiniert (Protocol Header Offset=0)* (Standardwert) Nur für Ethernet-Schnittstellen auswählbar • *Ethernet* • *Ethernet und VLAN* • *PPP over Ethernet* • *PPPoE und VLAN* Nur für IPSec-Schnittstellen auswählbar: • *IPSec über Ethernet* • *IPSec über Ethernet und VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE und VLAN*

Feld	Beschreibung
Verschlüsselungsmethode	Nur wenn als **Schnittstelle** ein IPSec Peer gewählt ist, **Traffic Shaping** *Aktiviert* ist und die **Größe des Protokoll-Headers unterhalb Layer 3** nicht *Undefiniert (Protocol Header Offset=0)* ist. Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird. Mögliche Werte: • *DES, 3DES, Blowfish, Cast - (Cipher-Blockgröße = 64 Bit)* • *AES128, AES192, AES256, Twofish - (Cipher-Blockgröße = 128 Bit)*
Real Time Jitter Control	Nur für **Traffic Shaping** = aktiviert Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite. Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s). Aktivieren oder deaktivieren Sie Real Time Jitter Control. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Kontrollmodus	Nur für **Real Time Jitter Control** = aktiviert. Wählen Sie den Modus für die Optimierung der Sprachübertragung. Mögliche Werte: • *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream

Feld	Beschreibung
	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.
Queues/Richtlinien	Konfigurieren Sie die gewünschten QoS-Queues. Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und 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

Feld	Beschreibung
	Daten. • *Standard*: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	Nur für **Priorisierungsqueue** = *Klassenbasiert* Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll. Dazu muss vorher im Menü **Netzwerk**->**QoS**->**QoS-Klassifizierung** mindestens eine Klassen-ID vergeben worden sein.
Priorität	Nur für **Priorisierungsqueue** = *Klassenbasiert* Wählen Sie die Priorität der Queue. Mögliche Werte sind *1 (hohe Priorität)* bis *254 (niedrige Priorität)*. Der Standardwert ist *1*.
Gewichtung	Nur für **Priorisierungsalgorithmus** = *Weighted Round Robin* oder *Weighted Fair Queueing* Wählen Sie die Gewichtung der Queue. Mögliche Werte sind *1* bis *254*. Der Standardwert ist *1*.
RTT-Modus (Realtime-Traffic-Modus)	Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen. Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.

Feld	Beschreibung
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung. Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.) Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für **Traffic Shaping** = aktiviert. Geben Sie eine maximale Datenrate in kBit pro Sekunde für die Queue ein. Mögliche Werte sind *0* bis *1000000*. Der Standardwert ist *0*.
Überbuchen zugelassen	Nur für **Traffic Shaping** = aktiviert. Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten. Bei aktiviertem **Überbuchen zugelassen** kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist. Bei deaktiviertem **Überbuchen zugelassen** kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Burst-Größe	Nur für **Traffic Shaping** = aktiviert. Geben Sie die maximale Anzahl an Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist. Mögliche Werte sind *0* bis *64000*. Der Standardwert ist *0*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Dropping-Algorithmus	Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird. Mögliche Werte: • *Tail Drop* (Standardwert): Das neu hinzugekommene Paket wird verworfen. • *Head Drop*: Das älteste Paket in der Queue wird verworfen. • *Random Drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von 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*.

12.5 Zugriffsregeln

Mit Access-Listen werden Zugriffe auf Daten und Funktionen eingegrenzt (welcher Benutzer welche Dienste und Dateien nutzen darf).

Sie definieren Filter für IP-Pakete, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, dass über das Gateway unzulässige Verbindungen aufgebaut werden. Access-Listen definieren die Art des IP-Traffics, den das Gateway annehmen oder ablehnen soll. Die Zugangsentscheidung basiert auf Informationen, die in den IP-Paketen enthalten sind, z. B.:

- Quell- und/oder Ziel IP-Adresse
- Protokoll des Pakets
- Quell- und/oder Ziel-Port (Portbereiche werden unterstützt)

Möchten z. B. Standorte, deren LANs über 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 oder mit ISDN-Login auf Ihr Gateway zu.

12.5.1 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.

Abb. 92: **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter**

12.5.1.1 Bearbeiten oder Neu

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

Abb. 93: **Netzwerk->Zugriffsregeln->Zugriffsfilter->Neu**

Das Menü **Netzwerk->Zugriffsregeln->Zugriffsfilter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *Benutzerdefiniert*.

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Typ	Nur bei **Protokoll** = *ICMP* Mögliche Werte: • *Beliebig* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* Der Standardwert ist *Beliebig*. Siehe RFC 792.
Verbindungsstatus	Nur bei **Protokoll** = *TCP* Sie können ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt. Mögliche Werte: • *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete. • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden.
Ziel-IP-Adresse/Netzmaske	Definieren Sie 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	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.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse und die Netzmaske der Datenpakete 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/TOS-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).

Feld	Beschreibung
	• *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Der Standardwert ist *Nicht beachten*.

12.5.2 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.

Abb. 94: **Netzwerk**->**Zugriffsregeln**->**Regelketten**

12.5.2.1 Bearbeiten oder Neu

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

Abb. 95: **Netzwerk->Zugriffsregeln->Regelketten->Neu**

Das Menü **Netzwerk->Zugriffsregeln->Regelketten->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Regelkette	Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. • *<Name der Regelkette>*: Wählen Sie eine bereits angelegte Regelkette aus und fügen ihr somit eine weitere Regel hinzu.
Beschreibung	Geben Sie die Bezeichnung der Regelkette ein.
Zugriffsfilter	Wählen Sie ein IP-Filter aus. Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll. Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *Zulassen, wenn Filter passt* (Standardwert): Paket annehmen, wenn das Filter passt. • *Zulassen, wenn Filter nicht passt*: Paket anneh-

Feld	Beschreibung
	men, 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.

12.5.3 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.

Abb. 96: **Netzwerk**->**Zugriffsregeln**->**Schnittstellenzuweisung**

12.5.3.1 Bearbeiten oder Neu

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

Abb. 97: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung->Neu**

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.

12.6 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.

12.6.1 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.

12.6.1.1 Neu

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

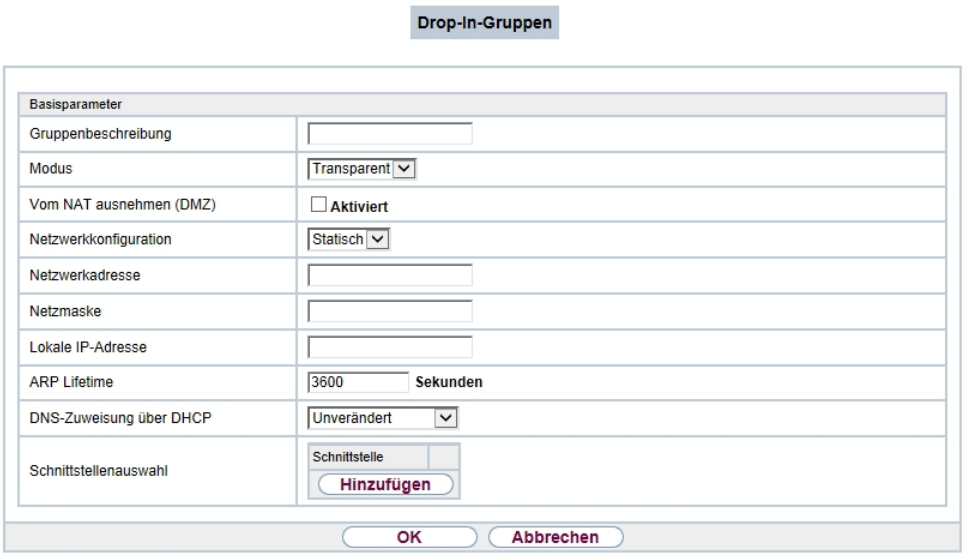


Abb. 98: **Netzwerk**->**Drop-In**->**Drop-In-Gruppen**->**Neu**

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.
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

Feld	Beschreibung
	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.

Kapitel 13 Routing-Protokolle

13.1 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.

13.1.1 RIP-Schnittstellen

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

Abb. 99: **Routing-Protokolle**->**RIP**->**RIP-Schnittstellen**

13.1.1.1 Bearbeiten

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

Abb. 100: **Routing-Protokolle->RIP->RIP-Schnittstellen->**

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

Felder im Menü RIP-Parameter für

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

Feld	Beschreibung
	(Triggered RIP).
Version in Empfangsrichtung	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 (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.

13.1.2 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.

Abb. 101: **Routing-Protokolle**->**RIP**->**RIP-Filter**

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.

13.1.2.1 Neu

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

Abb. 102: **Routing-Protokolle->RIP->RIP-Filter->Neu**

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.

Feld	Beschreibung
	Mögliche Werte sind *-16* bis *16*. Der Standardwert ist *0*.
Metrik-Offset für Inaktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import 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*.

13.1.3 RIP-Optionen

Abb. 103: **Routing-Protokolle->RIP->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 Stan-

Feld	Beschreibung
	dardwert *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 Timer	Wählen Sie aus, ob für die in RFC 2453 beschriebenen Timer 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. 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.

Feld	Beschreibung
	Der Standardwert ist 5 (in Sekunden).

Kapitel 14 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.

14.1 Allgemein

14.1.1 Allgemein

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

Abb. 104: **Multicast**->**Allgemein**->**Allgemein**

Das Menü **Multicast**->**Allgemein**->**Allgemein** 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.

14.2 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.

14.2.1 IGMP

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

14.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um IGMP auf weiteren Schnittstellen zu konfigurieren.

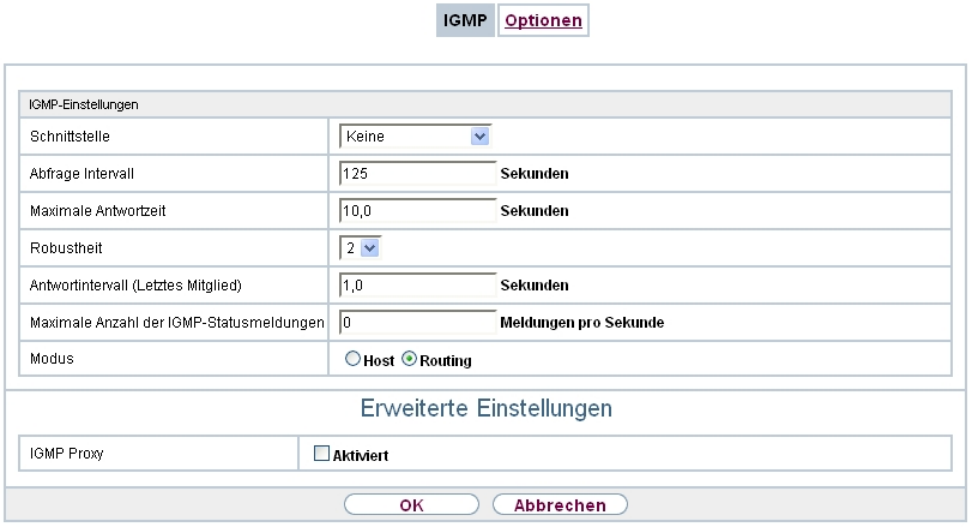


Abb. 105: **Multicast->IGMP->IGMP->Neu**

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). 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*.

Feld	Beschreibung
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.

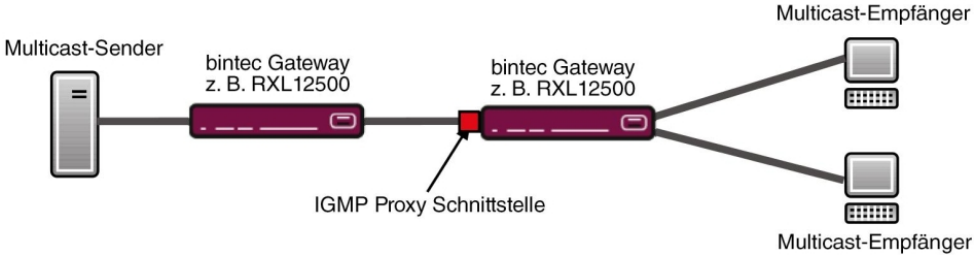


Abb. 106: IGMP Proxy

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IGMP Proxy	Wählen Sie aus, ob Ihr Gerät die IGMP-Meldungen der Hosts im Subnetz über seine definierte **Proxy-Schnittstelle** weiterleiten soll.
Proxy-Schnittstelle	Nur für **IGMP Proxy** = aktiviert Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.

14.2.2 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.

Abb. 107: **Multicast->IGMP->Optionen**

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. 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

Feld	Beschreibung
	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.

14.3 Weiterleiten

14.3.1 Weiterleiten

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

14.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um Weiterleitungsregeln für neue Multicast-Gruppen zu erstellen.

Abb. 108: **Multicast->Weiterleiten->Weiterleiten->Neu**

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.

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

14.4.1 PIM-Schnittstellen

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

Abb. 109: **Multicast**->**PIM**->**PIM-Schnittstellen**

14.4.1.1 Bearbeiten oder Neu

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

Abb. 110: **Multicast->PIM->PIM-Schnittstellen->Neu**

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

Feld	Beschreibung
	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*.

Feld	Beschreibung
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 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.

Feld	Beschreibung
	Wertebereich: *0* bis *65* Sekunden. Der Standardwert ist *3*.

14.4.2 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.

Abb. 111: **Multicast**->**PIM**->**PIM-Rendezvous-Punkte**

14.4.2.1 Bearbeiten oder Neu

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

Abb. 112: **Multicast**->**PIM**->**PIM-Rendezvous-Punkte**->**Neu**

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 pimStaticRPOverrideDynamic 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.

14.4.3 PIM-Optionen

Abb. 113: **Multicast->PIM->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*.

Kapitel 15 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.

15.1 Internet + Einwählen

In diesem Menü können Sie Internetzugänge oder Einwahl-Verbindungen einrichten.

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) und PPP-over-PPTP zur Verfügung.

Hinweis

Beachten Sie die Vorgaben Ihres Providers!

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **Benutzername**n, die **Authentifizierung** und den aktuellen **Status** enthält.

Das Feld **Status** kann folgende Werte annehmen:

Mögliche Werte für Status

Feld	Beschreibung
	verbunden
	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich
	nicht verbunden (z. B. ist aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich)
	administrativ auf inaktiv gesetzt (deaktiviert); Verbindungsaufbau nicht möglich

Authentifizierung

Wenn ein Ruf eingeht, wird je nach Konfiguration eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird. Dazu benötigt Ihr Gerät Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll, anschließend 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.

Default Route

Bei einer Default 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 Default Route ein. Wenn Sie z. B. eine Firmennetzanbindung machen, dann tragen Sie die Route zur Zentrale bzw. zur Filiale nur dann als Default 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 Default Route und zur Firmenzentrale eine Netzwerk-Route ein. Sie können auf Ihrem Gerät mehrere Default-Routen eintragen, nur eine einzige aber kann jeweils wirksam sein. Achten Sie daher auf unterschiedliche Werte für **Metrik**, wenn Sie mehrere Default Routen eintragen.

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.

15.1.1 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.

15.1.1.1 Neu

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

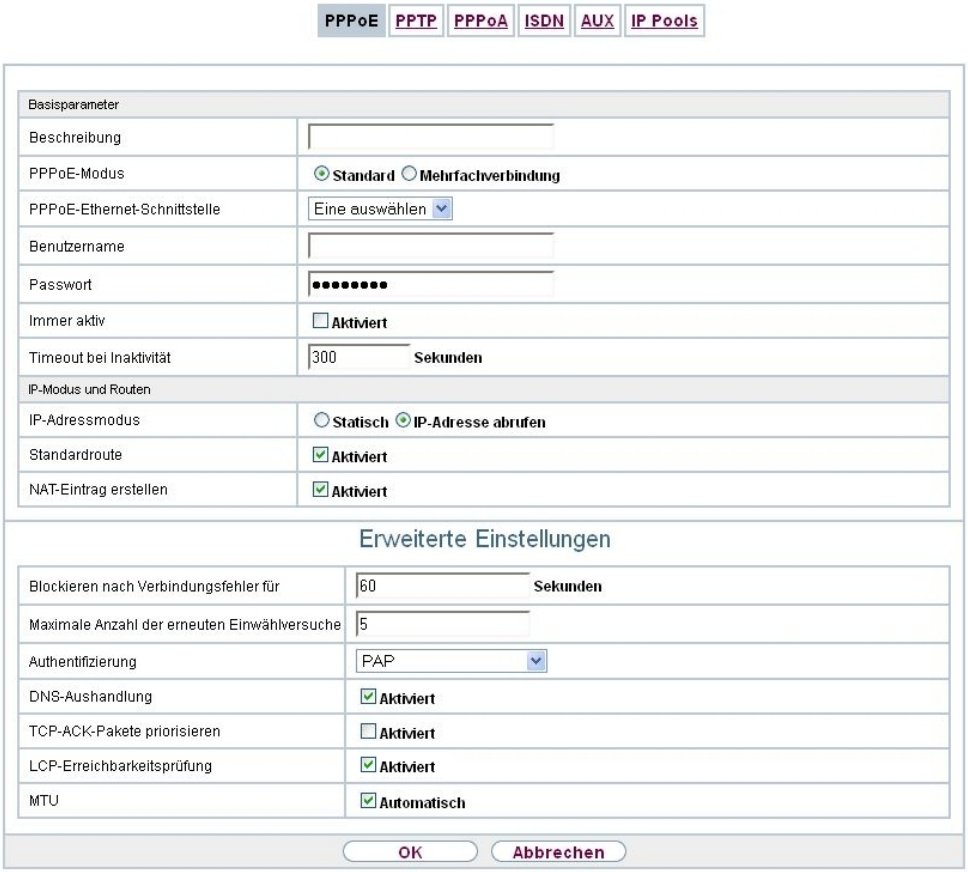


Abb. 114: **WAN->Internet + Einwählen->PPPoE->Neu**

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 stati-

Feld	Beschreibung
	sche 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.
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.
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.

Feld	Beschreibung
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold. Der Standardwert ist *300*. Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

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.

Feld	Beschreibung
	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*.

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.

Feld	Beschreibung
	Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. 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.
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*.

15.1.2 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.

15.1.2.1 Neu

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

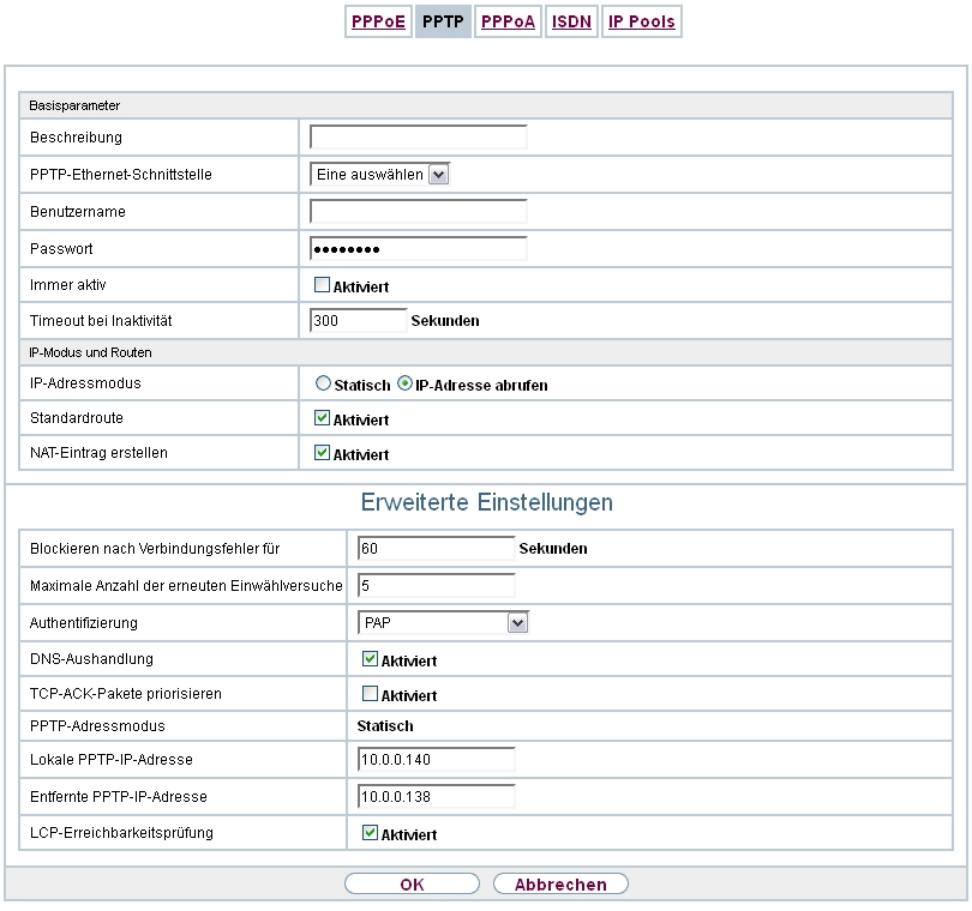


Abb. 115: **WAN->Internet + Einwählen->PPTP->Neu**

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-Ethernet-Schnittstelle	Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden. Bei Verwendung eines externen DSL-Modems, wählen Sie hier

Feld	Beschreibung
	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 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 temporär gültige IP-Adresse vom Provider.

Feld	Beschreibung
	• *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. • *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 un-

Feld	Beschreibung
	ternommen 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 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

Feld	Beschreibung
	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. Standardmäßig ist die Funktion aktiv.

15.1.3 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools angezeigt.

Ihr Gerät kann als dynamischer IP-Adress-Server für PPP-Verbindungen agieren. Dafür stellen Sie einen oder mehrere Pools von IP-Adressen zur Verfügung. Diese IP-Adressen können für die Dauer der Verbindung an einwählende Verbindungspartner vergeben werden.

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der

Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden 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.

15.1.3.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

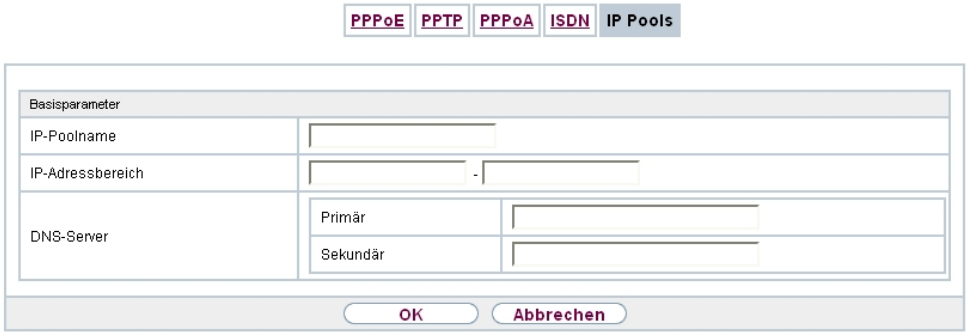


Abb. 116: **WAN->Internet + Einwählen->IP Pools->Neu**

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.

15.2 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.

15.2.1 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.

15.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um für weitere Schnittstellen die Sprachübertragung zu optimieren.

Abb. 117: **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen**->**Neu**

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.

Feld	Beschreibung
	Mögliche Werte: • *Nur kontrollierte RTP-Streams* (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung. • *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. • *Inaktiv*: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • *Immer*: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.
Maximale Upload-Geschwindigkeit	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

Kapitel 16 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.

16.1 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 96) 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 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 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 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 Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.

Hinweis

Der Parameter **Zusätzlicher Filter des 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.

16.1.1 IPSec-Peers

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Im Menü **VPN**->**IPSec**->**IPSec-Peers** wird eine Liste aller konfigurierter IPSec-Peers ange-

zeigt.

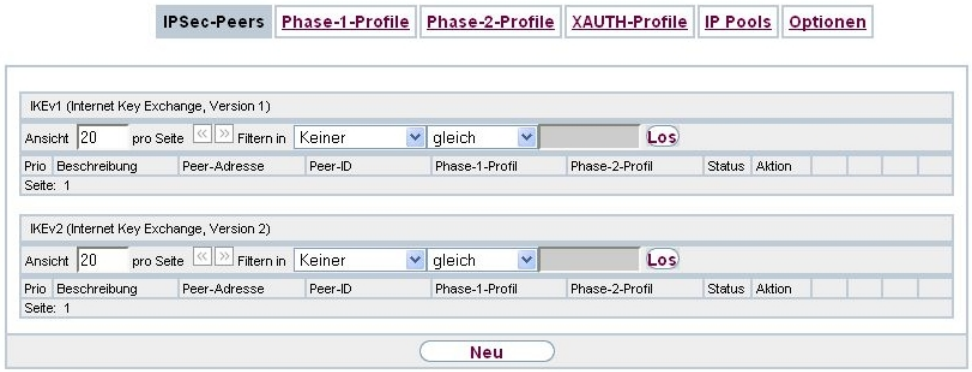


Abb. 118: **VPN->IPSec->IPSec-Peers**

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 458.

16.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPSec-Peers einzurichten.

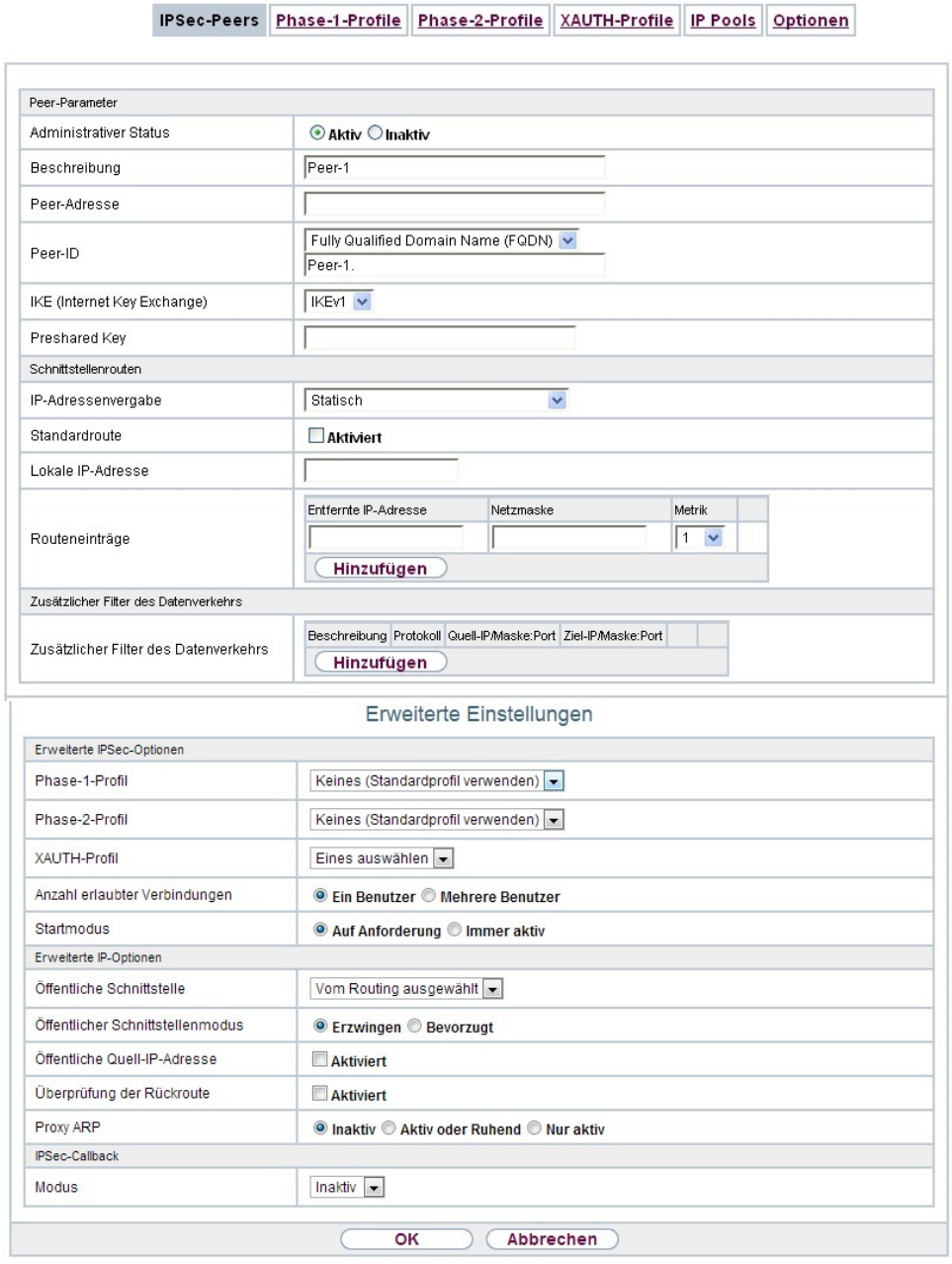


Abb. 119: **VPN->IPSec->IPSec-Peers->Neu**

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	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)	Für Geräte der **WIxxxxn**-Serie nicht verfügbar. Diese Geräte unterstützen nur IKEv1.

Feld	Beschreibung
	Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll. Mögliche Werte: • *IKEv1* (Standardwert): Internet Key Exchange Protocol Version 1 • *IKEv2*: Internet Key Exchange Protocol Version 2
Authentifizierungsmethode	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Wählen Sie die Authentifizierungsmethode aus. Mögliche Werte: • *Preshared Keys* (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Preshared Keys wählen. Diese werden bei der Peerkonfiguration im Menü **IPSec-Peers** konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • *RSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.
Lokaler ID-Typ	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Wählen Sie den Typ der lokalen ID aus. Mögliche ID-Typen: • *Fully Qualified Domain Name (FQDN)* • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)* • *Schlüssel-ID*: Beliebige Zeichenkette
Lokale ID	Nur für **IKE (Internet Key Exchange)** = *IKEv2* Geben Sie die ID Ihres Geräts ein. Für **Authentifizierungsmethode** = *DSA-Signatur* oder *RSA-Signatur* wird die Option **Subjektname aus Zertifikat verwenden** angezeigt. Wenn Sie die Option **Subjektname aus Zertifikat verwenden**

Feld	Beschreibung
	aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet. Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe *Zertifikate* auf Seite 96), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.
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.

Felder im Menü Schnittstellenrouten

Feld	Beschreibung
IP-Adressenvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: • `Statisch` (Standardwert): Geben Sie eine statische IP-Adresse ein. • `Client im IKE-Konfigurationsmodus`: Nur für IKEv1 auswählbar. 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 **IP-Adressenvergabe** = `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.

Feld	Beschreibung
	Dieser Wert muss für beide Seiten des Tunnels identisch sein.
IP-Zuordnungspool	Nur bei **IP-Adressenvergabe** = *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 **IP-Adressenvergabe** = *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 **IP-Adressenvergabe** = *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 **IP-Adressenvergabe** = *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 **IP-Adressenvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* Definieren Sie Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -LANs.

Feld	Beschreibung
	• *Netzmaske*: Netzmaske zu *Entfernte IP-Adresse*. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0 - 15*). der Standardwert ist *1*.

Felder im Menü Zusätzlicher Filter des Datenverkehrs

Feld	Beschreibung
Zusätzlicher Filter des Datenverkehrs	Nur für **IKE (Internet Key Exchange)** = *IKEv1* Legen Sie mithilfe von **Hinzufügen** einen neuen Filter an.

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 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 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 Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.

Hinweis

Der Parameter **Zusätzlicher Filter des 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.

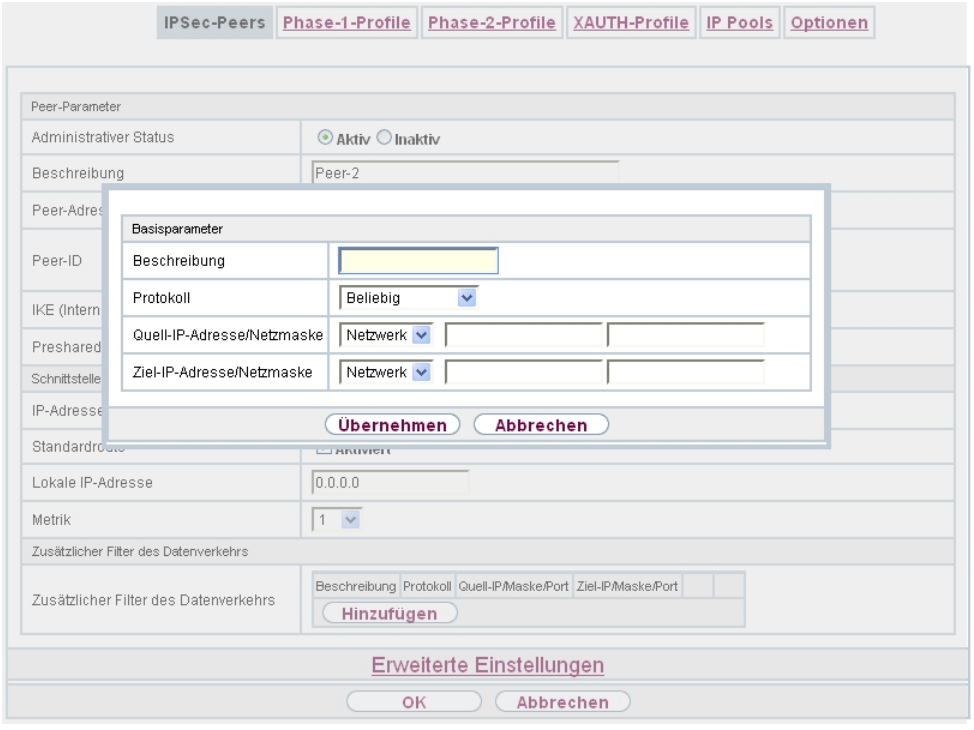


Abb. 120: **VPN->IPSec->IPSec-Peers->Neu->Hinzufügen**

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.

Feld	Beschreibung
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/

Feld	Beschreibung
	MD5 enthält ungeachtet der Proposalauswahl im Menü **VPN**->**IPSec**->**Phase-1-Profile**. • *<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: • *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 Peer

Feld	Beschreibung
	ID verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen. 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.

Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Öffentliche Schnittstelle	Legen Sie diejenige öffentliche (oder WAN-) Schnittstelle fest, über die dieser Peer sich mit seinem VPN-Partner verbinden soll. Wenn Sie *Vom Routing ausgewählt* auswählen, wird die Entscheidung, über welche Schnittstelle der Datenverkehr geleitet wird, gemäß der aktuellen Routingtabelle getroffen. Wenn Sie eine Schnittstelle auswählen, wird unter Beachtung der Einstellung unter **Öffentlicher Schnittstellenmodus** diese Schnittstelle verwendet.
Öffentlicher Schnittstellenmodus	Legen Sie fest, wie strikt die Einstellung unter **Öffentliche Schnittstelle** gehandhabt wird. Mögliche Werte: • *Erzwingen*: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet. • *Bevorzugt*: In Abhängigkeit der Prioritäten der aktuellen Routingtabelle wird die ausgewählte Schnittstelle dann verwendet, wenn keine günstigere Route über eine andere Schnittstelle vorhanden ist.
Öffentliche Quell-IP-Adresse	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 Quell-IP-Adresse**

Feld	Beschreibung
	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 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.
Proxy ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer *aktiv* (aktiv) oder *Ruhend* (ruhend) ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer

Feld	Beschreibung
	(aktiv) ist, wenn also bereits eine Verbindung zum IPSec Peer besteht.

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, müssen Sie eine kostenfreie Zusatzlizenz erwerben.

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.

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 IPSec-Callback* auf Seite 302 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 IPSec-Callback

Feld	Beschreibung
Modus	Wählen Sie den Callback-Modus aus. Mögliche Werte: • *Inaktiv* (Standardwert): IPSec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • *Passiv*: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • *Aktiv*: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • *Beide*: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	Nur für **Modus** = *Passiv* oder *Beide* Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.
Ausgehende Rufnummer	Nur für **Modus** = *Aktiv* oder *Beide* Geben Sie die ISDN-Nummer an, unter der das lokale Gerät

Feld	Beschreibung
	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-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.

Feld	Beschreibung
	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.

16.1.2 Phase-1-Profile

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

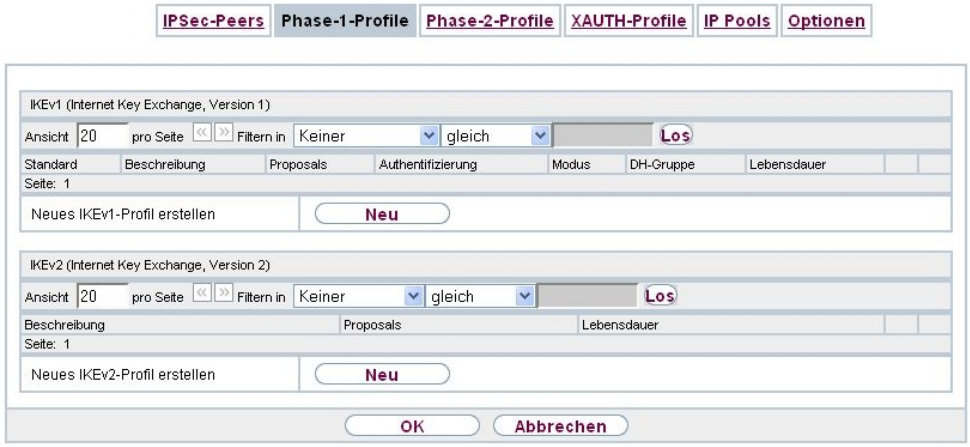


Abb. 121: **VPN**->**IPSec**->**Phase-1-Profile**

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

16.1.2.1 Neu

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

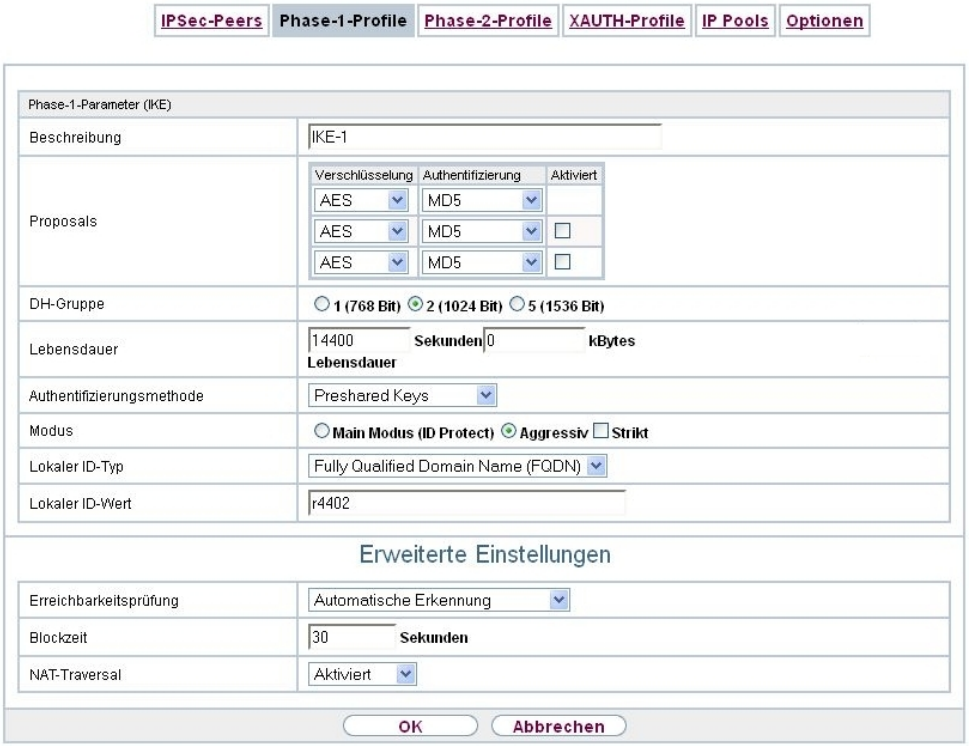


Abb. 122: **VPN**->**IPSec**->**Phase-1-Profile**->**Neu**

Das Menü **VPN**->**IPSec**->**Phase-1-Profile**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Phase-1-Parameter (IKE) / Phase-1-Parameter (IKEv2)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
Proposals	In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Nachrichten-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Nachrichten-Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Mindestens ein Proposal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden. Verschlüsselungsalgorithmen (**Verschlüsselung**): • *3DES* (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit,

Feld	Beschreibung
	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*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter *AES* gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • *AES-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. Hash-Algorithmen (**Authentifizierung**): • *MD5* (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.

Feld	Beschreibung
	• *SHA1*: 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. Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnisstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtpunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.
DH-Gruppe	Nur für **Phase-1-Parameter (IKE)** Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec elmeg-Geräten unterstützt wird, steht für "modular exponentiation". Mögliche Werte: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie die Lebensdauer für Phase-1-Schlüssel fest. Folgende Optionen stehen für die Definition der **Lebensdauer**

Feld	Beschreibung
	zur Verfügung: • Eingabe in **Sekunden**: Geben Sie die Lebensdauer für Phase-1- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist *14400*, das bedeutet, dass die Schlüssel erneuert werden, wenn vier Stunden abgelaufen sind. • Eingabe in **kBytes**: Geben Sie die Lebensdauer für Phase-1-Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist *0*; das bedeutet, dass die Anzahl der gesendeten kBytes keine Rolle spielt.
Authentifizierungsmethode	Nur für **Phase-1-Parameter (IKE)** Wählen Sie die Authentifizierungsmethode aus. Mögliche Werte: • *Preshared Keys* (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Pre Shared Keys wählen. Diese werden bei der Peerkonfiguration im Menü **VPN**->**IPSec**->**IPSec-Peers** konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • *DSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • *RSA-Signatur*: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert. • *RSA-Verschlüsselung*: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	Nur für **Phase-1-Parameter (IKE)** Nur für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.

Feld	Beschreibung
Modus	Nur für **Phase-1-Parameter (IKE)** Wählen Sie den Phase-1-Modus aus. Mögliche Werte: • *Aggressiv* (Standardwert): Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden. Er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals. • *Main Modus (ID Protect)*: Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec-SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (**Strikt**) oder der Peer auch einen anderen Modus vorschlagen kann.
Lokaler ID-Typ	Nur für **Phase-1-Parameter (IKE)** Wählen Sie den Typ der lokalen ID aus. Mögliche Werte: • *Fully Qualified Domain Name (FQDN)* • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)*
Lokaler ID-Wert	Nur für **Phase-1-Parameter (IKE)** Geben Sie die ID Ihres Geräts ein. Für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* wird die Option **Subjektname aus Zertifikat verwenden** angezeigt. Wenn Sie die Option **Subjektname aus Zertifikat verwenden** aktivieren, wird der erste im Zertifikat angegebene Subjekt-

Feld	Beschreibung
	Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet. Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe *Zertifikate* auf Seite 96), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.

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 erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • *Inaktiv*: Ihr Gerät sendet und erwartet keinen Heartbeat.

Feld	Beschreibung
	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. Nur für **Phase-1-Parameter (IKEv2)** Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung. Standardmäßig ist die Funktion aktiv.
Blockzeit	Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche. Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* bedeutet die Übernahme des Wertes im Standardprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird. Der Standardwert ist *30*.
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.

Feld	Beschreibung
	Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gerät zu einem anderen Host bzw. Gerät. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Geräten, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet. Nur für *IKEv1-Profile* Mögliche Werte: • *Aktiviert* (Standardwert): NAT-Traversal ist aktiv. • *Deaktiviert*: NAT-Traversal ist deaktiviert. • *Erzwingen*: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. Nur für *IKEv2-Profile* Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
CA-Zertifikate	Nur für **Phase-1-Parameter (IKE)** Nur für **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur* oder *RSA-Verschlüsselung* Wenn Sie die Option **Folgenden CA-Zertifikaten vertrauen** aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen. Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.

16.1.3 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.

Abb. 123: **VPN**->**IPSec**->**Phase-2-Profile**

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

16.1.3.1 Neu

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

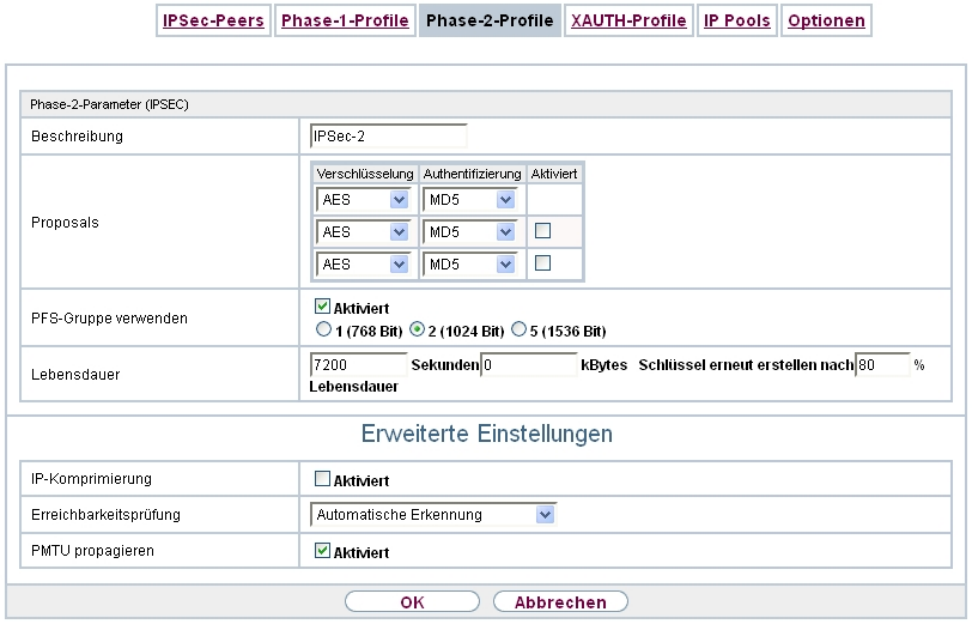


Abb. 124: **VPN**->**IPSec**->**Phase-2-Profile**->**Neu**

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.

Feld	Beschreibung
	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* (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • *-- ALLE --*: Alle Optionen können verwendet werden. • *AES*: 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 an-

Feld	Beschreibung
	gesehen 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* (Standardwert): 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*: 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. Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.
PFS-Gruppe verwenden	Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (*Aktiviert*), sind die Optionen die gleichen, wie bei der Konfiguration von **DH-Gruppe** im Menü **VPN**->**IPSec**->**Phase-1-Profile** . PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind. Das Feld hat folgende Optionen: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)* (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.

Feld	Beschreibung
	• *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen. Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind. Folgende Optionen stehen für die Definition der **Lebensdauer** zur Verfügung: • Eingabe in **Sekunden**: Geben Sie die Lebensdauer für Phase-2- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Der Standardwert ist *7200*. • Eingabe in **kBytes**: Geben Sie die Lebensdauer für Phase-2-Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Der Standardwert ist *0*. **Schlüssel erneut erstellen nach**: Legen Sie fest, bei welchem Prozentsatz des Ablaufes der Lebensdauer die Schlüssel der Phase 2 neu erstellt werden. Die eingegebene Prozentzahl wird sowohl auf die Lebensdauer in Sekunden als auch auf die Lebensdauer in kBytes angewendet. Der Standardwert ist *80* %.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IP-Komprimierung	Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder

Feld	Beschreibung
	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. 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.
PMTU propagieren	Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

16.1.4 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. 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 über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet, jeder Peer eine Filiale repräsentiert und der Angestellte jeweils vor Ort Zugriff auf den Tunnel haben will.

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.

16.1.4.1 Neu

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

Abb. 125: **VPN**->**IPSec**->**XAUTH-Profile**->**Neu**

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.
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.

16.1.5 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 **IP-Adressenvergabe** *Server im IKE-Konfigurationsmodus* eingestellt haben, müssen Sie hier die IP-Pools, aus denen die IP-Adressen vergeben werden, definieren.

16.1.5.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

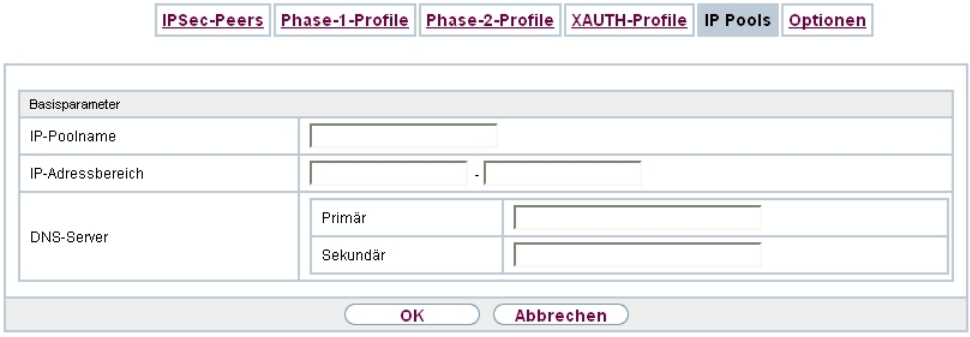


Abb. 126: **VPN->IPSec->IP Pools->Neu**

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.

16.1.6 Optionen

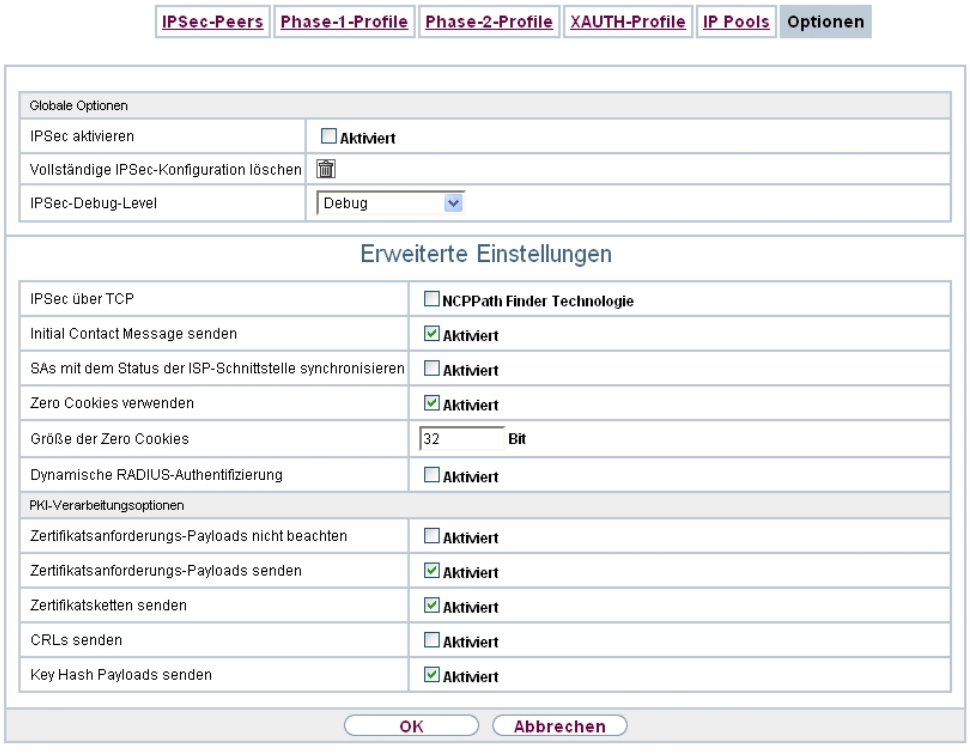


Abb. 127: **VPN->IPSec->Optionen**

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

Feld	Beschreibung
	Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen. Das Löschen der Konfiguration ist nur möglich mit **IPSec aktivieren** = nicht aktiviert.
IPSec-Debug-Level	Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung* • *Benachrichtigung* • *Informationen* • *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,

Feld	Beschreibung
	ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Initial Contact Message senden	Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
SAs mit dem Status der ISP-Schnittstelle synchronisieren	Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von *aktiv* zu *inaktiv*, *ruhend* oder *blockiert* geändert hat. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zero Cookies verwenden	Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen. Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall *Aktiviert*.
Größe der Zero Cookies	Nur für **Zero Cookies verwenden** = aktiviert. Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein. Der Standardwert ist *32*.
Dynamische RADIUS-Authentifizierung	Wählen Sie aus, ob die RADIUS-Authentifizierung über IPSec aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	Wählen Sie aus, ob Zertifikatanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungs-Payloads senden	Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Zertifikatsketten senden	Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen. 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

Feld	Beschreibung
	zu unterdrücken.

16.2 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.

16.2.1 Tunnelprofile

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

16.2.1.1 Neu

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

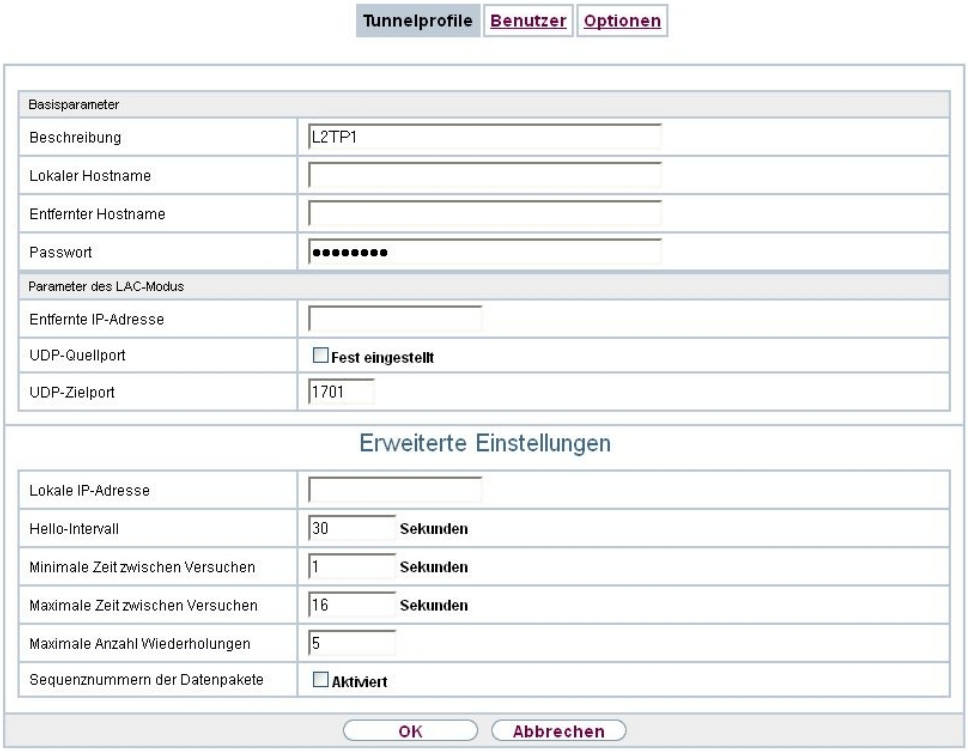


Abb. 128: **VPN->L2TP->Tunnelprofile->Neu**

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).

Feld	Beschreibung
	• *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 alle 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

Feld	Beschreibung
	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. 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

Feld	Beschreibung
	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*.
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.

16.2.2 Benutzer

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

16.2.2.1 Neu

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

Abb. 129: **VPN->L2TP->Benutzer->Neu**

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.

Feld	Beschreibung
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.
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.

Feld	Beschreibung
	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 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. 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. • *Keine*: 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: • *Keine*: 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.
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.
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.

Feld	Beschreibung
	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 *aktiv* (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.

16.2.3 Optionen

Abb. 130: **VPN->L2TP->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.

16.3 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.

16.3.1 PPTP-Tunnel

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

16.3.1.1 Neu

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

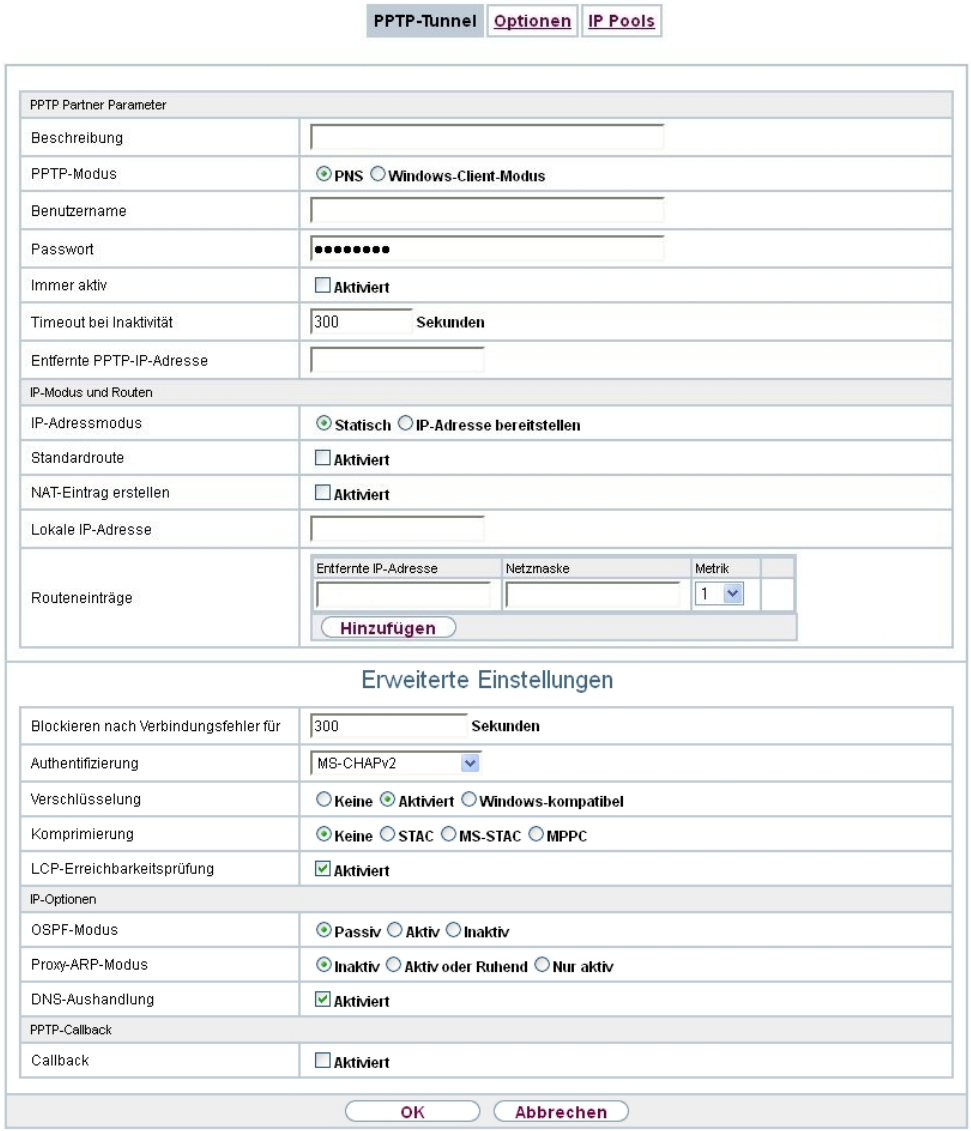


Abb. 131: **VPN**->**PPTP**->**PPTP-Tunnel**->**Neu**

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. 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.
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.

Feld	Beschreibung
	• *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*.
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.

Feld	Beschreibung
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: • *Keine*: 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.
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.

Feld	Beschreibung
	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 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. 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.

16.3.2 Optionen

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

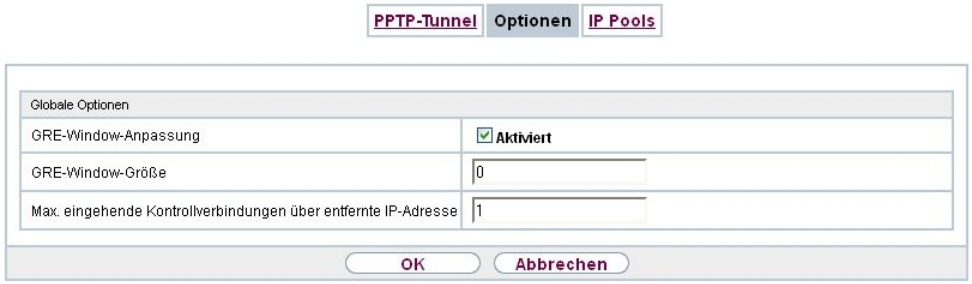


Abb. 132: **VPN->PPTP->Optionen**

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 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	Geben Sie die maximale Anzahl der Kontrollverbindungen ein.

Feld	Beschreibung
entfernte IP-Adresse	

16.3.3 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.

16.3.3.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

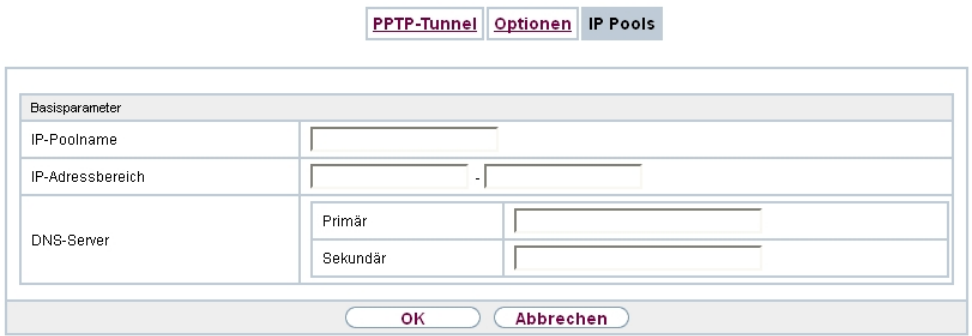


Abb. 133: **VPN->PPTP->IP Pools->Neu**

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 Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

16.4 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.

16.4.1 GRE-Tunnel

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

16.4.1.1 Neu

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

Abb. 134: **VPN->GRE->GRE-Tunnel->Neu**

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.

Feld	Beschreibung
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, 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*.

Kapitel 17 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).

17.1 Richtlinien

17.1.1 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 Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Im Menü **Firewall**->**Richtlinien**->**Filterregeln** wird eine Liste aller konfigurierten Filterregeln angezeigt.

Abb. 135: **Firewall**->**Richtlinien**->**Filterregeln**

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.

17.1.1.1 Neu

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

Abb. 136: **Firewall**->**Richtlinien**->**Filterregeln**->**Neu**

Das Menü **Firewall**->**Richtlinien**->**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 vorkonfi-

Feld	Beschreibung
	guriert, unter anderem: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* Weitere Dienste werden in **Firewall**->**Dienste**->**Diensteliste** angelegt. Außerdem stehen die in **Firewall**->**Dienste**->**Gruppen** konfigurierten Dienstegruppen zur Auswahl.
Aktion	Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll. Möglichen Werte: • *Zugriff* (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • *Verweigern*: Die Pakete werden abgewiesen. • *Zurückweisen*: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.
QoS anwenden	Nur für **Aktion** = *Zugriff* Wählen Sie aus, ob Sie QoS für diese Richtlinie mit der in **Priorität** ausgewählten Priorität aktivieren möchten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Option nicht aktiv. Wenn QoS für diese Richtlinie nicht aktiv ist, beachten Sie, dass auch sendeseitig keine Priorisierung der Daten erfolgen kann. Eine Richtlinie, für die QoS aktiviert wurde, ist auch für die Firewall eingestellt. Beachten Sie daher, dass Datenverkehr, der

Feld	Beschreibung
	nicht ausdrücklich zugelassen wurde, von der Firewall geblockt wird!
Priorität	Nur für **Aktion** = *Zugriff* und **QoS anwenden** = *Aktiviert* Wählen Sie aus, mit welcher Priorität die von der Richtlinie spezifizierten Daten sendeseitig behandelt werden. Mögliche Werte: • *Keine* (Standardwert): Keine Priorität. • *Low Latency*: Low Latency Transmission (LLT), d. h. Behandlung der Daten mit der geringstmöglichen Latenz, z. B. geeignet für VoIP-Daten. • *Hoch* • *Mittel* • *Niedrig*

17.1.2 QoS

Immer mehr Anwendungen benötigen immer größere Bandbreiten. Nicht immer stehen diese zur Verfügung. Quality of Service (QoS) ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt werden und es kann Bandbreite für diese reserviert werden.

Im Menü **Firewall**->**Richtlinien**->**QoS** wird eine Liste aller QoS-Regeln angezeigt.

17.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere QoS-Regeln einzurichten.

Abb. 137: **Firewall**->**Richtlinien**->**QoS**->**Neu**

Das Menü **Firewall**->**Richtlinien**->**QoS**->**Neu** besteht aus folgenden Feldern:

Felder im Menü QoS-Schnittstelle konfigurieren

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der das Bandbreitenmanagement erfolgen soll.
Traffic Shaping	Wählen Sie aus, ob Sie für die gewählte Schnittstelle das Bandbreitenmanagement aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Bandbreite angeben	Nur für **Traffic Shaping** = *Aktiviert* Geben Sie die maximal zur Verfügung stehende Bandbreite in kBit/s für die gewählte Schnittstelle ein.
Filterregeln	Dieses Feld enthält eine Liste aller konfigurierten Firewall-Richtlinien, für die QoS aktiviert wurde (**QoS anwenden** = *Aktiviert*). Für jeden Listeneintrag stehen folgende Optionen zur Verfügung: • **Verwenden**: Wählen Sie aus, ob dieser Eintrag der QoS-Schnittstelle zugeordnet werden soll. Standardmäßig ist diese Option nicht aktiv. • **Bandbreite**: Geben Sie die maximal zur Verfügung stehende Bandbreite in Bit/s für den unter **Dienst** genannten Dienst ein. Standardmäßig ist *0* eingetragen. • **Fest**: Wählen Sie aus, ob eine längerfristige Überschreitung der in **Bandbreite** definierten Bandbreite zulässig ist. Die Aktivierung dieses Feldes schließt eine solche Überschreitung aus. Ist die Option deaktiviert, ist die Überschreitung zulässig und die übersteigende Datenrate wird gemäß der in der entsprechenden Firewall-Richtlinie definierten Priorität behandelt. Standardmäßig ist diese Option nicht aktiv.

17.1.3 Optionen

In diesem Menü können Sie die 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.

Abb. 138: **Firewall->Richtlinien->Optionen**

Das Menü **Firewall->Richtlinien->Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Firewall Status	Aktivieren oder deaktivieren Sie die 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".

Feld	Beschreibung
	• *Annehmen*: Nur Accept-Ereignisse werden angezeigt. • *Keine*: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige Filterung	Hier legen Sie fest, ob nur Pakete gefiltert werden sollen, die an eine andere Schnittstelle gesendet werden als die, welche die Verbindung erzeugt hat. Mit *Aktivieren* werden alle Pakete gefiltert (Standardwert).

Felder im Menü Sitzungstimer

Feld	Beschreibung
UDP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine UDP - Session als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *180*.
TCP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP - Session als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von *30* bis *86400*. Der Standardwert ist *3600*.
PPTP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine PPTP-Session als 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*.

17.2 Schnittstellen

17.2.1 Gruppen

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

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

17.2.1.1 Neu

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

Abb. 139: **Firewall**->**Schnittstellen**->**Gruppen**->**Neu**

Das Menü **Firewall**->**Schnittstellen**->**Gruppen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte **Auswahl**.

17.3 Adressen

17.3.1 Adressliste

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

17.3.1.1 Neu

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

Abb. 140: **Firewall**->**Adressen**->**Adressliste**->**Neu**

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.
Adresstyp	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 **Adresstyp** = *Adresse/Subnetz* Geben Sie die IP-Adresse des Hosts oder eine Netzwerk-Adresse und die zugehörige Netzmaske ein. Der Standardwert ist jeweils *0.0.0.0*.

Feld	Beschreibung
Adressbereich	Nur für **Adresstyp** = *Adressbereich* Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein.

17.3.2 Gruppen

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

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

17.3.2.1 Neu

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

Abb. 141: **Firewall**->**Adressen**->**Gruppen**->**Neu**

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

17.4 Dienste

17.4.1 Diensteliste

Im Menü **Firewall**->**Dienste**->**Diensteliste** wird eine Liste aller zur Verfügung stehender Dienste angezeigt.

17.4.1.1 Neu

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

Abb. 142: **Firewall**->**Dienste**->**Diensteliste**->**Neu**

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*.

Feld	Beschreibung
Quellportbereich	Nur für **Protokoll** = *TCP*, *UDP/TCP* oder *UDP* Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port 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:

Feld	Beschreibung
	• *Beliebig* (Standardwert) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

17.4.2 Gruppen

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

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

17.4.2.1 Neu

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

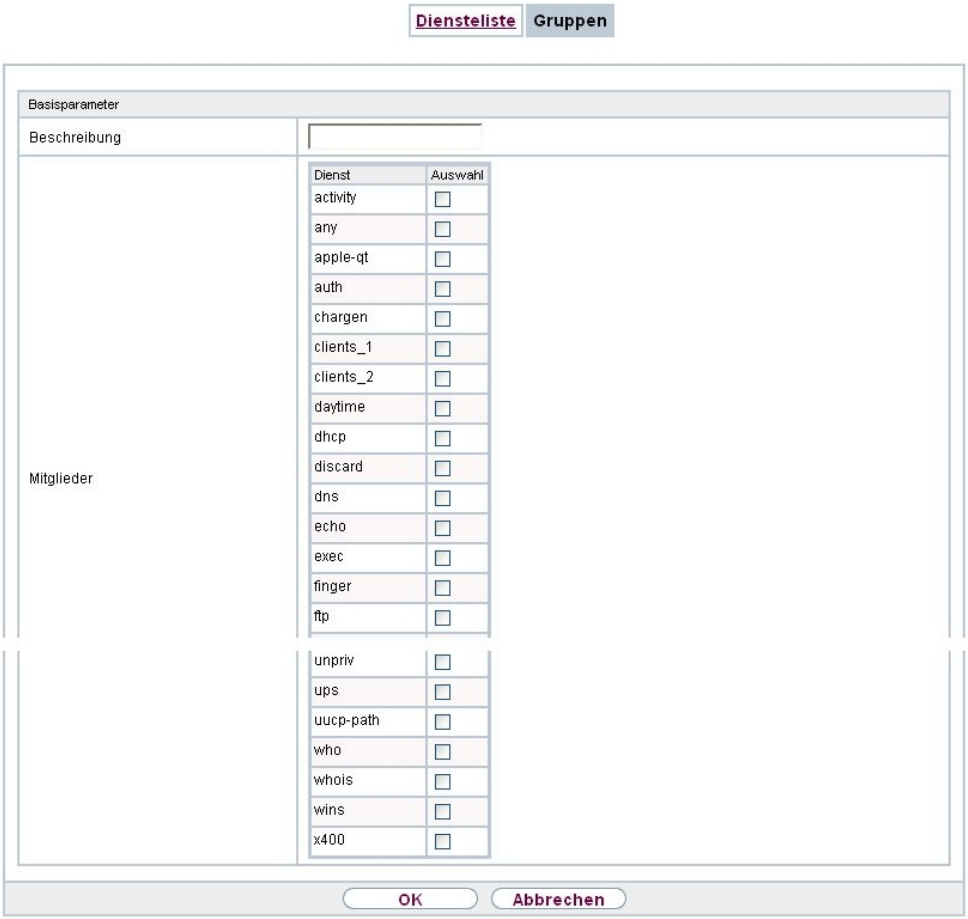


Abb. 143: **Firewall**->**Dienste**->**Gruppen**->**Neu**

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**.

Kapitel 18 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)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Automatische Erkennung und Konfiguration von bintec elmeg-Geräten
- Bereitstellung öffentlicher Internetzugänge (Hotspot).
- Wake on LAN, um Netzwerkgeräte zu aktivieren, die aktuell ausgeschaltet sind.

18.1 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**->**Globale Einstellungen**->**Basisparameter** 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 globalen 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.

18.1.1 Globale Einstellungen

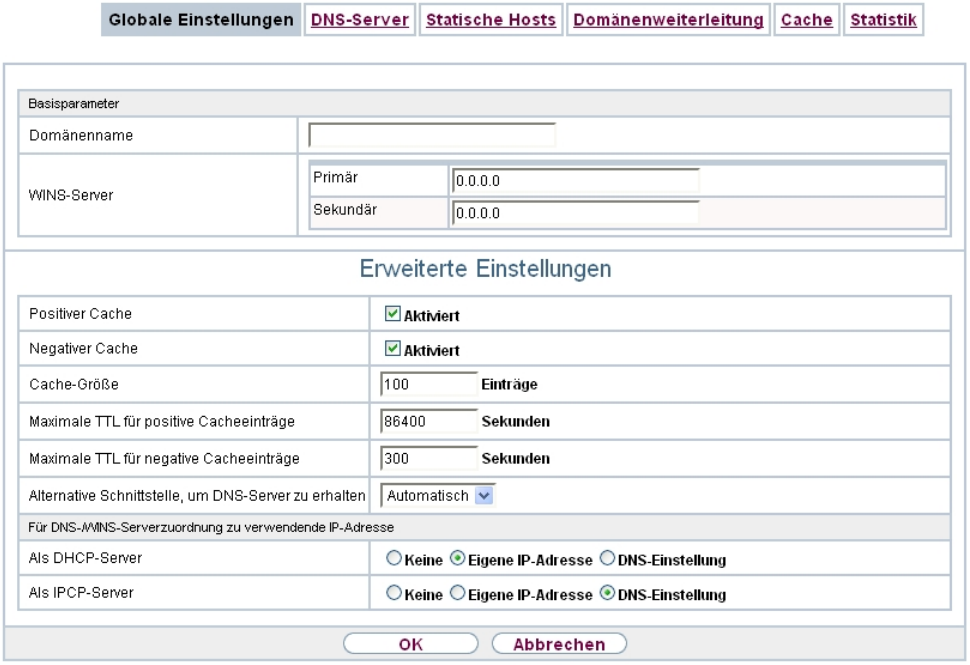


Abb. 144: **Lokale Dienste->DNS->Globale Einstellungen**

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

Feld	Beschreibung
	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 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 Schnittstel-	Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur

Feld	Beschreibung
le, um DNS-Server zu erhalten	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: • *Keine*: Es wird keine Name-Server-Adresse übermittelt. • *Eigene IP-Adresse* (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • *DNS-Einstellung*: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermittelt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird. Mögliche Werte: • *Keine*: 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.

18.1.2 DNS-Server

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

18.1.2.1 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.

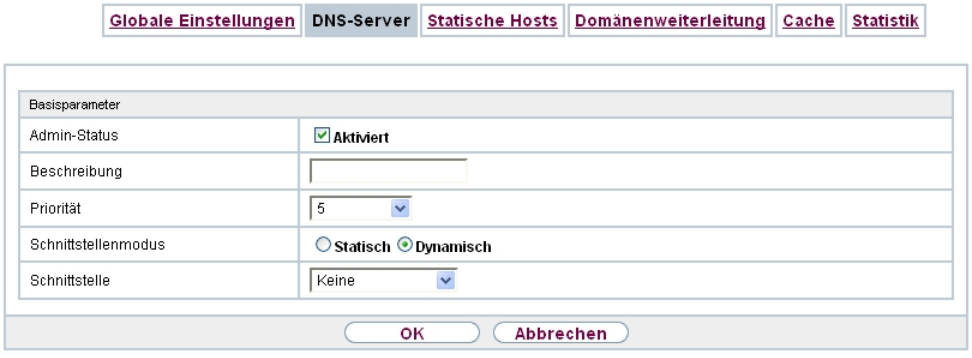


Abb. 145: **Lokale Dienste->DNS->DNS-Server->Neu**

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob der DNS-Server aktiv sein soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	Weisen Sie dem DNS-Server eine Priorität zu. Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) mehrere Paare von DNS-Servern (**Primärer DNS-Server** und **Sekundärer DNS-Server**) zuweisen. Verwendet wird das Paar mit der höchsten

Feld	Beschreibung
	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. Bei **Schnittstellenmodus** = *Dynamisch* Mit der Einstellung *Keine* wird ein globaler DNS-Server angelegt. Bei **Schnittstellenmodus** = *Statisch* Mit der Einstellung *Beliebig* wird ein DNS-Server für alle Schnittstellen konfiguriert.
Primärer DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie die IP-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.
Sekundärer DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie optional die IP-Adresse eines alternativen Name-Servers ein.

18.1.3 Statische Hosts

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

18.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

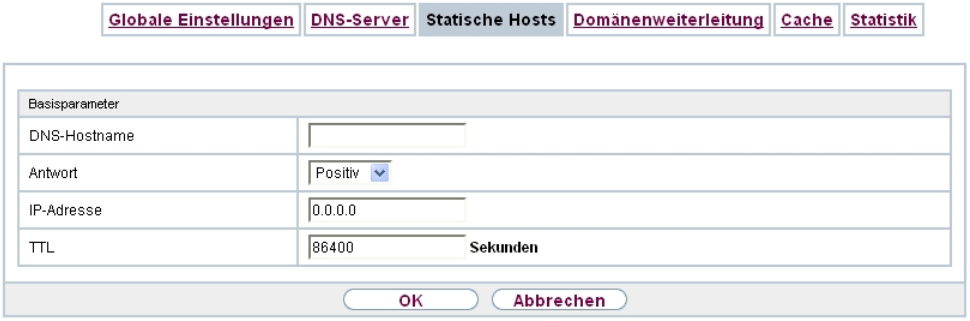


Abb. 146: **Lokale Dienste->DNS->Statische Hosts->Neu**

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Hostname	Geben Sie den Host-Namen ein, dem die in diesem Menü definierte **IP-Adresse** zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt. Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.bintec-elmeg.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **OK** "<**Name**.> " 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.

Feld	Beschreibung
	• *Keine*: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IP-Adresse	Nur bei **Antwort** = *Positiv* Geben Sie die IP-Adresse ein, die nach **DNS-Hostname** zugeordnet wird.
TTL	Geben Sie die Gültigkeitsdauer der Zuordnung von **DNS-Hostname** zu **IP-Adresse** in Sekunden ein (nur relevant bei **Antwort** = *Positiv*), die anfragenden Hosts übermittelt wird. Der Standardwert ist *86400* (= 24 h).

18.1.4 Domänenweiterleitung

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

18.1.4.1 Neu

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

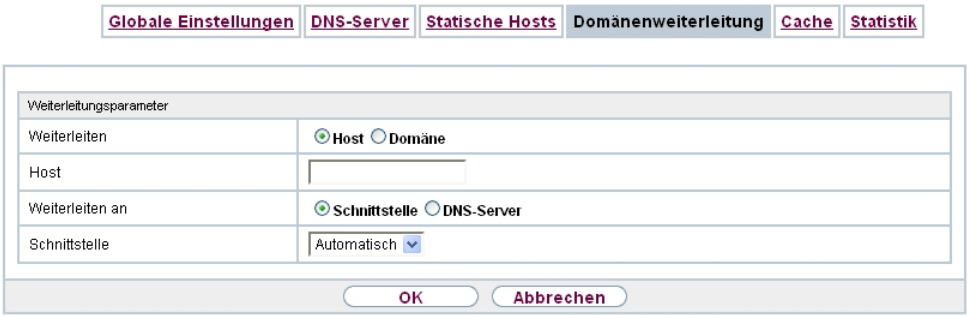


Abb. 147: **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu**

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

Feld	Beschreibung
	Domäne weitergeleitet werden soll. Mögliche Werte: • *Host* (Standardwert) • *Domäne*
Host	Nur für **Weiterleiten** = *Host* 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* Geben Sie den Namen der Domäne ein, für die Anfragen weitergeleitet werden sollen. Der Eintrag kann mit der Wildcard "*" beginnen, z. B. "*.bintec-elmeg.com". Bei Eingabe eines Namens ohne führende Wildcard "*" wird nach Bestätigung mit **OK** automatisch eine führende Wildcard "*" eingefügt.
Weiterleiten an	Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer **Schnittstelle** oder an einen manuell konfigurierten **DNS-Server** weitergeleitet werden sollen. Mögliche Werte: • *Schnittstelle* (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konifgurierten Schnittstelle weitergeleitet. • *DNS-Server*: Anfragen werden an den definierten **DNS-Server** weitergeleitet.
Schnittstelle	Nur für **Weiterleiten an** = *Schnittstelle* Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfra-

Feld	Beschreibung
	gen weitergeleitet werden sollen.
DNS-Server	Nur für **Weiterleiten an** = *DNS-Server* Geben Sie IP-Adresse des primären und sekundären DNS-Servers ein.

18.1.5 Cache

Im Menü **Lokale Dienste**->**DNS**->**Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

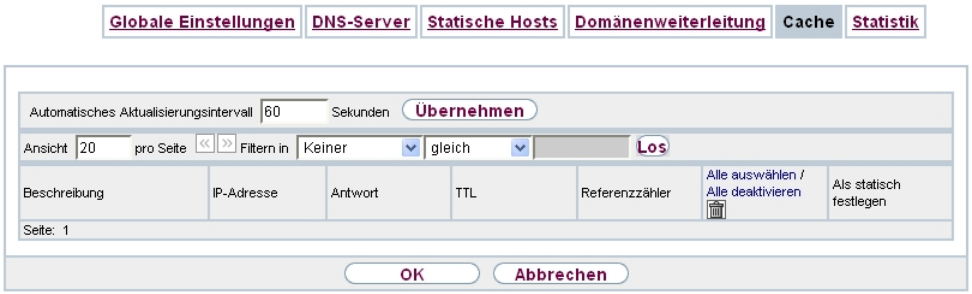


Abb. 148: **Lokale Dienste**->**DNS**->**Cache**

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.

18.1.6 Statistik

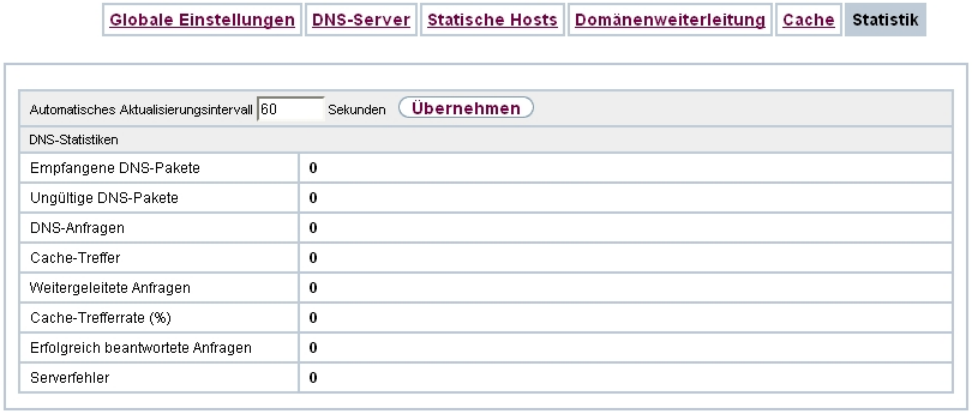


Abb. 149: **Lokale Dienste->DNS->Statistik**

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der **Cache-Treffer** pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

18.2 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.

18.2.1 HTTPS-Server

Im Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Abb. 150: **Lokale Dienste->HTTPS->HTTPS-Server**

Das Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** 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 möch-

Feld	Beschreibung
	ten. • *<Zertifikatsname>*: Wählen Sie ein unter **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** eingetragenes Zertifikat aus.

18.3 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.

18.3.1 DynDNS-Aktualisierung

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

18.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

Abb. 151: **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Weitere DynDNS-Provider können im Menü **Lokale**

Feld	Beschreibung
	DynDNS-Client->**DynDNS-Provider** konfiguriert werden. Der Standardwert ist *DynDNS* .
Aktualisierung aktivieren	Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Mail-Exchanger (MX)	Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.
Wildcard	Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von **Hostname** zur aktuellen IP-Adresse von **Schnittstelle** aktiviert werden soll (Erweiterte Namensauflösung). Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

18.3.2 DynDNS-Provider

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

18.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

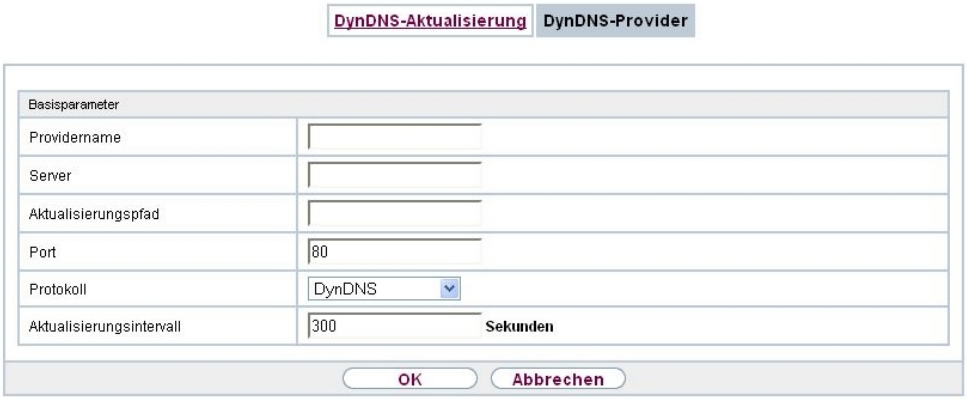


Abb. 152: **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. Der Standardwert ist *80*.
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: • *DynDNS* (Standardwert) • *Static DynDNS*

Feld	Beschreibung
	• *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Aktualisierungsintervall	Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf. Der Standardwert ist *300* Sekunden.

18.4 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.

18.4.1 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 konfigurerte Pools an.

18.4.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

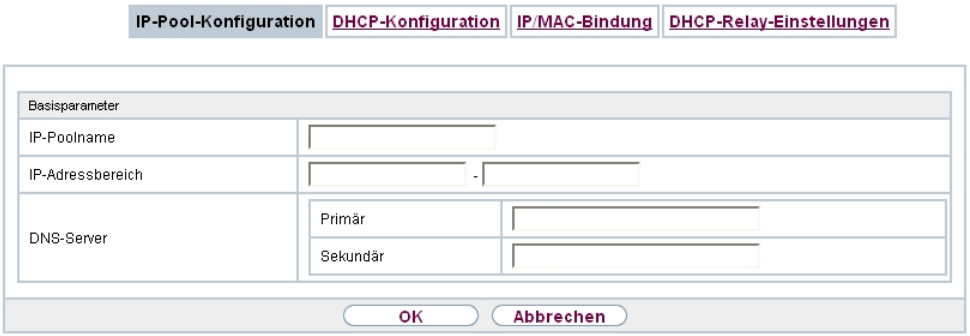


Abb. 153: **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration**->**Neu**

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 Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

18.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** wird eine Liste aller konfigurierter IP-Adresspools 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.

18.4.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP-Adresspools einzurichten. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

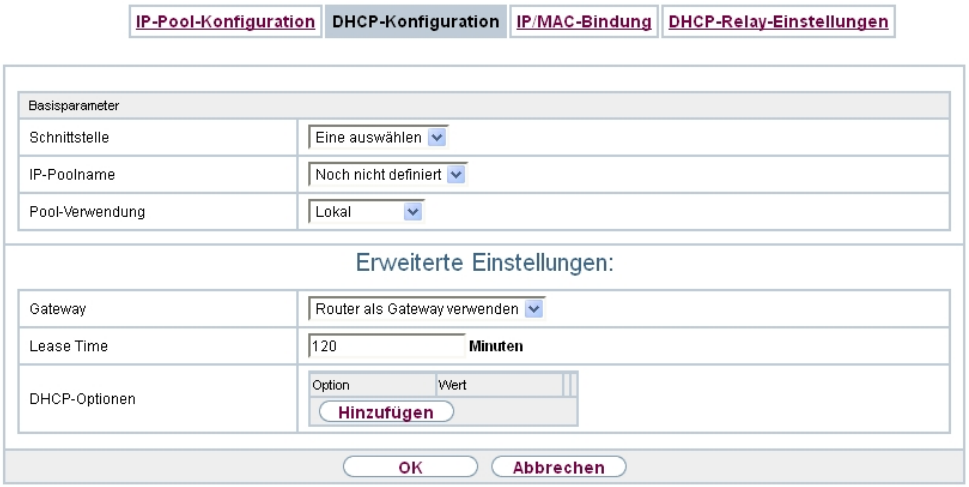


Abb. 154: **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**

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 IP-Pool für DHCP-Anfragen im gleichen Subnetz verwendet werden soll oder für DHCP-Anfragen, die aus einem anderen Subnetz zu Ihrem Gerät weitergeleitet wurden. In diesem Fall ist es möglich, IP-Adressen aus einem anderen Netz zu definieren. Mögliche Werte: • *Lokal* (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz verwendet. • *Lokal/Relais*: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet.

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.

Feld	Beschreibung
Lease Time	Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll. Nachdem **Lease Time** abgelaufen ist, kann die Adresse durch den Server neu vergeben werden. Der Standardwert ist *120*.
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen. Mögliche Werte für **Option**: • *Zeitserver* (Standardwert): Geben Sie die IP-Adresse des Zeitservers ein, die dem Client übermittelt werden soll. • *DNS-Server*: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • *DNS-Domänenname*: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • *WINS/NBNS-Server*: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • *WINS/NBT Node Type*: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • *TFTP-Server*: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • *CAPWAP Controller*: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • *URL (Provisionierungsserver)*: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. Verwenden Sie diese Option, um anfragenden **IP1x0**-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form *http://<IP-Adresse des Provisionierungsservers>/eg_prov* haben. • *Herstellergruppe* (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen übermittlen. Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge

Feld	Beschreibung
	mit der Schaltfläche **Hinzufügen** ein.

Bearbeiten

Im Menü **Lokale Dienste** -> **DHCP-Server** ->**DHCP-Konfiguration**->**Erweiterte Einstellungen** können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option** = *Herstellergruppe* gewählt ist.

Wählen Sie das Symbol  , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

Felder im Menü Basisparameter

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	Nur für **Hersteller auswählen** = *Siemens* Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll. Für die Einstellung **Hersteller auswählen** = *Siemens* wird der Standardwert *sdlp* angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.
Herstellerbeschreibung	Nur für **Hersteller auswählen** = *Sonstige* Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Benutzerdefinierte DHCP-Optionen	Nur für **Hersteller auswählen** = *Sonstige* Fügen Sie mit **Hinzufügen** weitere Einträge hinzu. Sie können DHCP-Optionen hinzufügen.

18.4.3 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** ein gültiger IP-Pool zugewiesen ist.

18.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

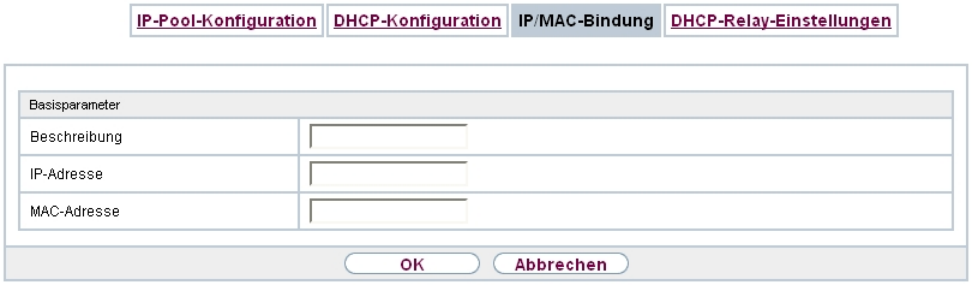


Abb. 155: **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung**->**Neu**

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.

Feld	Beschreibung
	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.

18.4.4 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.

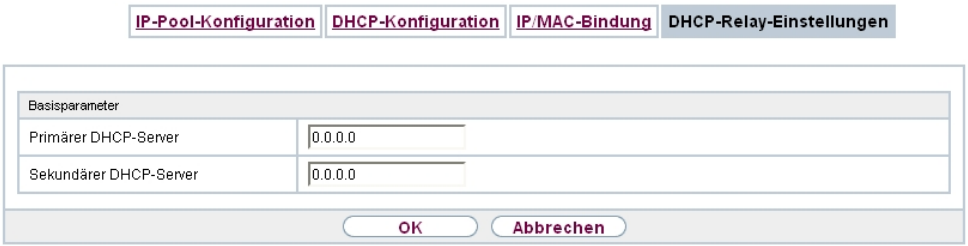


Abb. 156: **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen**

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`.

18.5 Scheduling

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

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

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

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

Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der 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.

18.5.1 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.

18.5.1.1 Neu

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

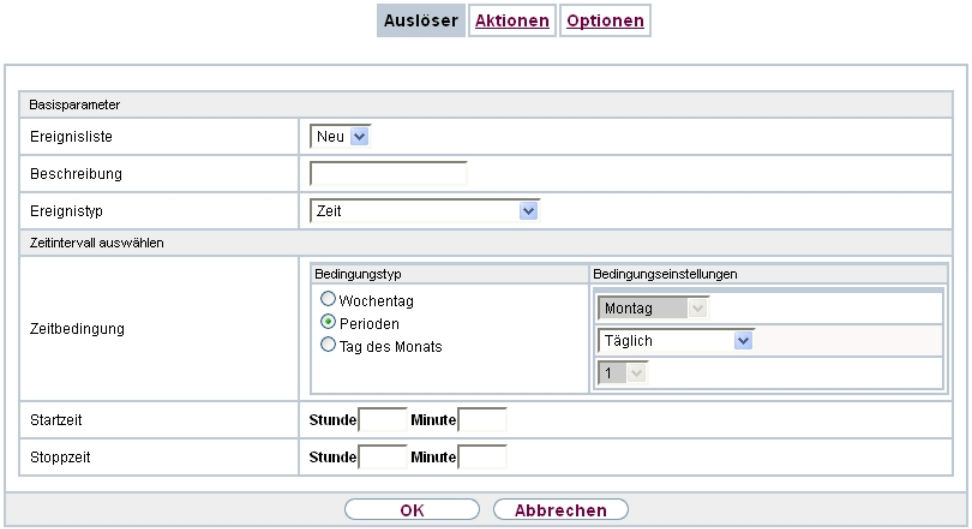


Abb. 157: **Lokale Dienste->Scheduling->Auslöser->Neu**

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 Ereingnisse werden in derseben Reihenfolge abgearbeitet wie sie in der Liste angelegt sind.
Beschreibung	Nur für **Ereignisliste** = *Neu* Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.

Feld	Beschreibung
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. • *Status der GEO-Zone* :Die in **Aktionen** konfigurierten 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.

Feld	Beschreibung
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 **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.

Feld	Beschreibung
	• *Inaktiv*: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen. Mögliche Werte: • *RX* (Standardwert): Der eingehende Datenverkehr wird überwacht. • *TX*: Der ausgehende Datenverkehr wird überwacht.
Bedingung des Schnittstellenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie aus, ob der Wert für Datenverkehr *Größer* (Standardwert) oder *Kleiner* dem in *Übertragener Datenverkehr* angegebenen Wert sein muss, um die Aktion auszulösen.
Übertragener Datenverkehr	Nur für **Ereignistyp** *Schnittstellenverkehr* Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in **kBytes** ein. Der Standardwert ist *0*.
Ziel-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden 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.

Feld	Beschreibung
Status	Nur für **Ereignistyp** *Ping-Test* Wählen Sie aus, ob **Ziel-IP-Adresse** *Erreichbar* (Standardwert) oder *Nicht erreichbar* sein muss, um die Aktion auszulösen.
Intervall	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll. Der Standardwert ist *60* Sekunden.
Versuche	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis **Ziel-IP-Adresse** als *Nicht erreichbar* gilt. 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.

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 Wochentag aus. • *Perioden* (Standardwert): Wählen Sie in **Bedingungseinstellungen** einen bestimmten Turnus aus.

Feld	Beschreibung
	• *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.

18.5.2 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.

18.5.2.1 Neu

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

Abb. 158: **Lokale Dienste->Scheduling->Aktionen->Neu**

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.

Feld	Beschreibung
	• *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. • *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/	Nur bei **Befehlstyp** = *MIB/SNMP*

Feld	Beschreibung
SNMP-Variable	Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das **System** aus und dann die **MIB-Tabelle**. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.
Befehlsmodus	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie aus, auf welche Weise der MIB-Eintrag manipuliert werden soll. Zur Verfügung stehen: • *Vorhandenen Eintrag ändern* (Standardwert): Ein bestehender Eintrag soll verändert werden. • *Neuen MIB-Eintrag erstellen*: Ein neuer Eintrag soll angelegt 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*

Feld	Beschreibung
	Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll. Ist der Auslöser aktiv (**Status des Auslösers** *Aktiv*), wird die MIB-Variable mit dem in **Aktiver Wert** eingetragenen Wert beschrieben. Ist der Auslöser inaktiv, **Status des Auslösers** *Inaktiv*), wird die MIB-Variable mit dem in **Inaktiver Wert** eingetragenen Wert beschrieben. Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (**Status des Auslösers** *Beide*), wird sie mit einem aktiven Auslöser mit dem in **Aktiver Wert** eingetragenen Wert und mit einem inaktiven Auslöser mit dem in **Inaktiver Wert** eingetragenen Wert beschrieben. Legen Sie weitere Einträge mit **Hinzufügen** an.
Schnittstelle	Nur bei **Befehlstyp** = *Schnittstellenstatus* Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.
Schnittstellenstatus festlegen	Nur bei **Befehlstyp** = *Schnittstellenstatus* Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll. Mögliche Werte: • *Aktiv* (Standardwert) • *Inaktiv* • *Zurücksetzen*
Lokale WLAN-SSID	Nur bei **Befehlstyp** = *WLAN-Status* Wählen Sie das gewünschte Drahtlosnetzwerk aus, dessen Status verändert werden soll.
Status festlegen	Nur bei **Befehlstyp** = *WLAN-Status* oder *WLC: VSS-Status* Wählen Sie den Status aus, den das Drahtlosnetzwerk erhalten soll.

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

Feld	Beschreibung
Aktion	Bei **Befehlstyp** = *Konfigurationsmanagement* Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll. Mögliche Werte: • *Konfiguration importieren* (Standardwert) • *Konfiguration exportieren* • *Konfiguration umbenennen* • *Konfiguration löschen* • *Konfiguration kopieren* Bei **Befehlstyp** = *Zertifikatverwaltung* Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten. 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.

Feld	Beschreibung
	Das CSV-Format kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Standardmäßig ist die Funktion aktiv.
Dateiname auf Server	Nur bei **Befehlstyp** = *Konfigurationsmanagement* Für **Aktion** = *Konfiguration importieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server, von dem sie geholt werden soll, gespeichert ist. Für **Aktion** = *Konfiguration exportieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.
Lokaler Dateiname	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren*, *Konfiguration umbenennen* oder *Konfiguration kopieren* Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.
Dateiname in Flash	Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration exportieren* Wählen Sie die Datei aus, die exportiert werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration umbenennen* Wählen Sie die Datei aus, die umbenannt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration löschen* Wählen Sie die Datei aus, die gelöscht werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration kopieren* Wählen Sie die Datei aus, die kopiert werden soll.

Feld	Beschreibung
Konfiguration enthält Zertifikate/Schlüssel	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen. Standardmäßig ist die Funktion nicht aktiv.
Konfiguration verschlüsseln	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob die Daten der gewählten **Aktion** verschlüsselt werden sollen. Standardmäßig ist die Funktion nicht aktiv.
Nach Ausführung neu starten	Nur bei **Befehlstyp** = *Konfigurationsmanagement* Wählen Sie aus, ob Ihr Gerät nach der gewünschten **Aktion** neu gestartet werden soll. Standardmäßig ist die Funktion nicht aktiv.
Versionsprüfung	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* Wählen Sie aus, ob beim Import einer Konfigurationsdatei überprüft werden soll, ob auf dem Server eine aktuellere Version der schon geladenen Konfiguration vorhanden ist. Wenn nicht, wird der Datei-Import abgebrochen. Standardmäßig ist die Funktion nicht aktiv.
Ziel-IP-Adresse	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.
Quell-IP-Adresse	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Automatisch* (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • *Spezifisch*: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Intervall	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll. Der Standardwert ist *1* Sekunde.
Versuche	Nur bei **Befehlstyp** = *Ping-Test* Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis **Ziel-IP-Adresse** als unerreichbar gilt. 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.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Ähnliches Zertifikat überschreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie ein auf Ihrem Gerät schon vorhandenes Zertifikat mit dem neuen überschreiben wollen. Standardmäßig ist die Funktion nicht aktiv.
Zertifikat in Konfiguration schreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungsbeschreibung	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.
SCEP-Server-URL	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie die URL des SCEP-Servers ein, z. B. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Subjektname	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie einen Subjektnamen mit Attributen ein. Beispiel: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA-Name	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP*

Feld	Beschreibung
	Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows*. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Passwort	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.
Schlüsselgröße	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind *1024* (Standardwert), *2048* und *4096*.
Autospeichermodus	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert. Standardmäßig ist die Funktion aktiv.
CRL verwenden	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Werte: • *Auto* (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatsperrlisten-Verteilungspunkt (CDP, CRL Distri-

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

Feld	Beschreibung
)	

18.5.3 Optionen

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

Abb. 159: **Lokale Dienste**->**Scheduling**->**Optionen**

Das Menü **Lokale Dienste**->**Scheduling**->**Optionen** 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).

18.6 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.

18.6.1 Hosts

Im Menü **Lokale Dienste**->**Überwachung**->**Hosts** wird eine Liste aller überwachten Hosts angezeigt.

18.6.1.1 Bearbeiten oder Neu

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

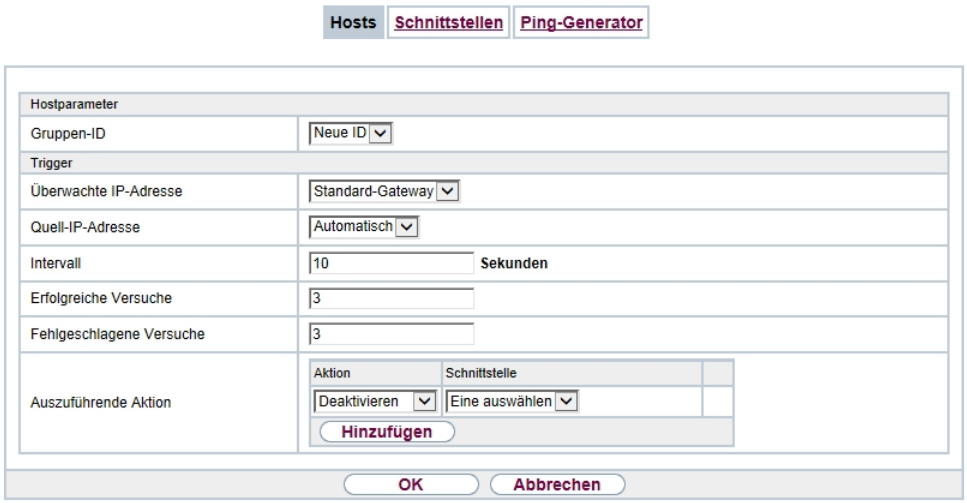


Abb. 160: **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu**

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.

Feld	Beschreibung
	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. Die in **Schnittstelle** konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.

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.
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, da-

Feld	Beschreibung
	mit 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	Wählen Sie aus, welche **Aktion** ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine **Schnittstelle**, auf die sich die **Aktion** bezieht. Auswählbar sind alle physikalischen und virtuellen 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. Mit **Aktion** = *Überwachen* können Sie die IP-Adresse überwachen, die unter **Überwachte IP-Adresse** angegeben ist. Diese Information kann für andere Funktionen, wie die **IP-Adresse zur Nachverfolgung**, genutzt werden.

18.6.2 Schnittstellen

Im Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

18.6.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Abb. 161: **Lokale Dienste->Überwachung->Schnittstellen->Neu**

Das Menü **Lokale Dienste->Überwachung->Schnittstellen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von **Überwachte Schnittstelle** aus, der eine bestimmte **Schnittstellenaktion** auslösen soll. Mögliche Werte: • *Schnittstelle wird aktiviert.* (Standardwert) • *Schnittstelle wird deaktiviert.*
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in **Trigger** definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in **Schnittstelle** ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: • *Aktivieren* (Standardwert): Aktivierung der Schnittstelle(n)

Feld	Beschreibung
	• *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*.

18.6.3 Ping-Generator

Im Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

18.6.3.1 Bearbeiten oder Neu

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

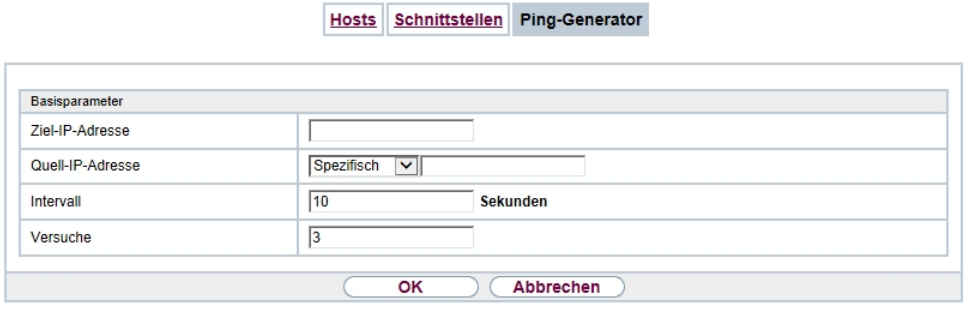


Abb. 162: **Lokale Dienste**->**Überwachung**->**Ping-Generator**->**Neu**

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.

Feld	Beschreibung
	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.
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, bis die **Ziel-IP-Adresse** als *Nicht erreichbar* gilt. Der Standardwert ist *3*.

18.7 Hotspot-Gateway

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.

18.7.1 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 konfigurierter Hotspot Netzwerke angezeigt.

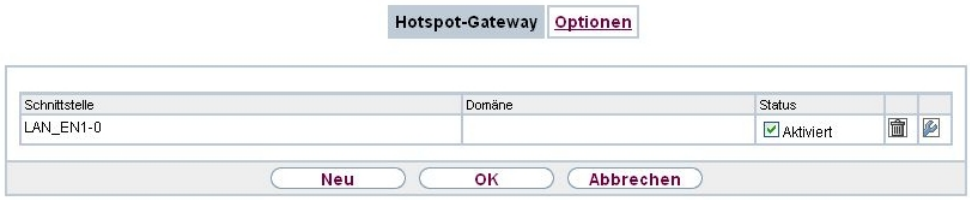


Abb. 163: **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktieren.

18.7.1.1 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.

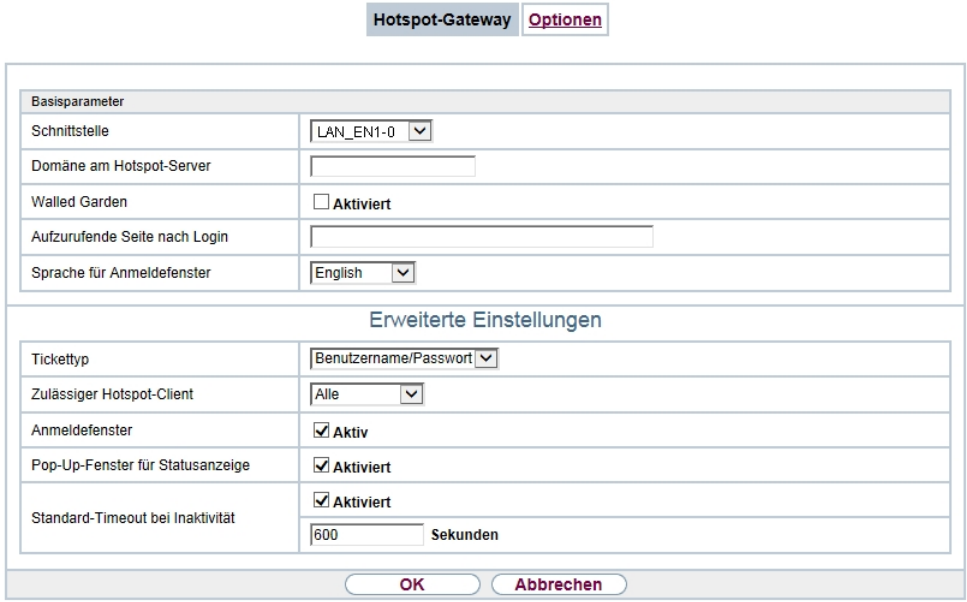


Abb. 164: **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**->

Das Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**-> 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 der Access Point angeschlossen ist.

Feld	Beschreibung
	 **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 erreichbar sein.

Feld	Beschreibung
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 anmelden dürfen.

Feld	Beschreibung
	Mögliche Werte: • *Alle*: Alle Clients werden zugelassen. • *DHCP-Client*: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
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.

18.7.2 Optionen

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

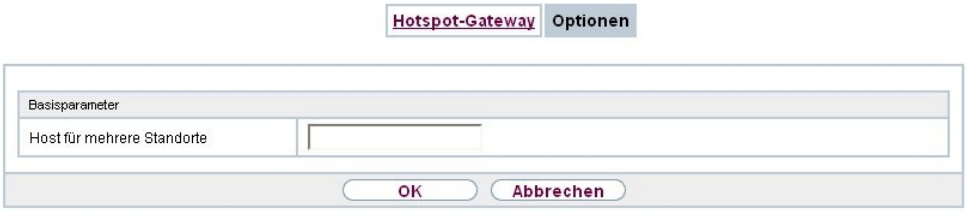


Abb. 165: **Lokale Dienste->Hotspot-Gateway->Optionen**

Das Menü **Lokale Dienste->Hotspot-Gateway->Optionen** 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.

18.8 Wake-On-LAN

Mit der Funktion **Wake-On-LAN** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

18.8.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

18.8.1.1 Bearbeiten oder Neu

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

Abb. 166: **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter->Neu**

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* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Der Standardwert ist *Beliebig*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.

Feld	Beschreibung
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.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von

Feld	Beschreibung
	Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Ziel-Port-Bereich ein.
DSCP/TOS-Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS). Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Wertebereich *0* bis *7*. Der Standardwert ist *Nicht beachten*.

18.8.2 WOL-Regeln

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** wird eine Liste aller konfigurierten WOL-Regeln angezeigt.

18.8.2.1 Bearbeiten oder Neu

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

Abb. 167: **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln**->**Neu**

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.

Feld	Beschreibung
Beschreibung	Nur für **Wake-On-LAN-Regelkette** = *Neu* Geben Sie die Bezeichnung der Regelkette ein.
Wake-on-LAN-Filter	Wählen Sie ein WOL-Filter aus. Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll. Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** konfiguriert sein.
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *WOL aufrufen, wenn Filter zutrifft*: WOL ausführen, wenn der Filter zutrifft. • *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*

Feld	Beschreibung
	Geben Sie die MAC-Adresse desjenigen Netzwerkgerätes ein, das mittels WOL aktiviert werden soll.
Passwort	Nur für **Aktion** = *WOL aufrufen, wenn Filter zutrifft* und *Aufrufen, wenn Filter nicht zutrifft* Wenn das Netzwerkgerät, das aktiveirt werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.

18.8.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

18.8.3.1 Bearbeiten oder Neu

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

Abb. 168: **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung**->**Neu**

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 Regel-

Feld	Beschreibung
	kette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.

Kapitel 19 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.

19.1 Diagnose

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

19.1.1 Ping-Test

Abb. 169: **Wartung**->**Diagnose**->**Ping-Test**

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an. Durch Eingabe der IP-Adresse, die getestet werden soll, in **Ping-Befehl testweise an Adresse senden** und Klicken auf die **Los**-Schaltfläche wird der Ping-Test gestartet.

19.1.2 DNS-Test

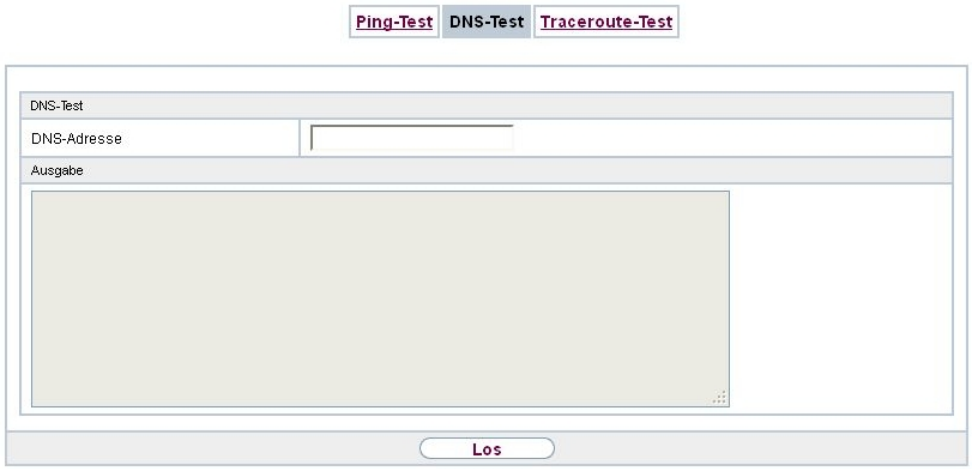


Abb. 170: **Wartung**->**Diagnose**->**DNS-Test**

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.

19.1.3 Traceroute-Test

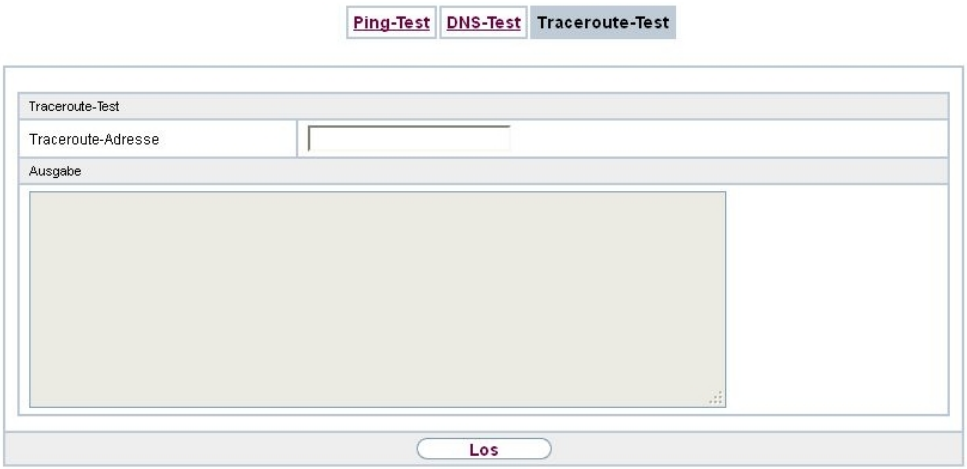


Abb. 171: **Wartung**->**Diagnose**->**Traceroute-Test**

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese errreichbar ist. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an. Durch Eingabe der Adresse, die getestet werden soll, in **Traceroute-Adresse** und Klicken auf die **Los**-Schaltfläche wird der Traceroute-Test gestartet.

19.2 Software &Konfiguration

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

19.2.1 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.

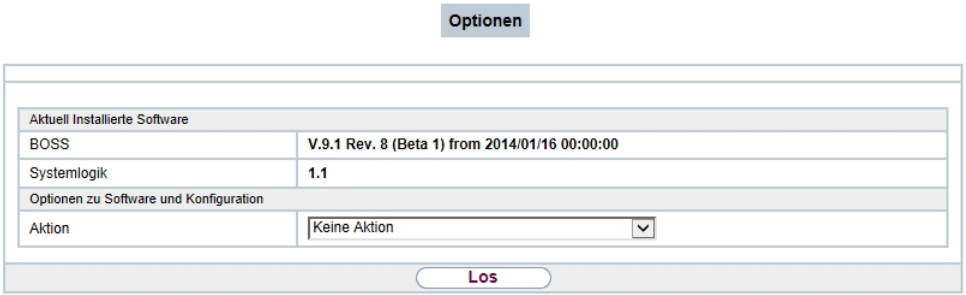


Abb. 172: **Wartung->Software &Konfiguration->Optionen**

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.
ADSL-Logik	Zeigt die aktuelle Version der ADSL-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. • *Sicherung wiederherstellen*: Nur, wenn unter **Konfiguration speichern** mit der Einstellung *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern* die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • *Software/Firmware löschen*: Die Datei im Feld **Datei auswählen** wird gelöscht. • *Sprache importieren*: Sie können weitere Sprachversionen des **GUI** auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von *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 ADSL-Logik und des BOOTmonitors initiieren. • *Voice Mail Wave-Dateien importieren* (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist.): Wählen Sie in **Dateiname** die Datei *vms_wavfiles.zip* aus, die Sie importieren wollen. • *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

Feld	Beschreibung
	Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	Für **Aktion** = *Konfiguration exportieren* Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.
Zertifikate und Schlüssel einschließen	Für **Aktion** = *Konfiguration exportieren* Wählen Sie aus, ob die gewählte **Aktion** auch für Zertifikate und Schlüssel gelten soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Verschlüsselung der Konfiguration	Nur für **Aktion** = *Konfiguration exportieren*, *Konfiguration importieren*, *Konfiguration mit Statusinformationen exportieren* Wählen Sie aus, ob die Daten der gewählten **Aktion** verschlüsselt werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiviert ist, können Sie in das Textfeld das **Passwort** eingeben.
Dateiname	Nur für **Aktion** = *Konfiguration importieren*, *Sprache importieren*, *Systemsoftware aktualisieren* Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.
Name der Quelldatei	Nur für **Aktion** = *Konfiguration kopieren* Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für **Aktion** = *Konfiguration kopieren* Geben Sie den Namen der Kopie ein.

Feld	Beschreibung
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.

19.3 Neustart

19.3.1 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.

Abb. 173: **Wartung->Neustart->Systemneustart**

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

Kapitel 20 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. Außerdem können Sie Ihr Gerät für die Überwachung mit dem Activity Monitor vorbereiten.

20.1 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 *Informationen* 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*).

20.1.1 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.

20.1.1.1 Neu

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

Abb. 174: **Externe Berichterstellung**->**Systemprotokoll**->**Syslog-Server**->**Neu**

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)

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

Feld	Beschreibung
	Mögliche Werte: • *System &Accounting* (Standardwert) • *System* • *Accounting*

20.2 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.

20.2.1 Schnittstellen

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

Abb. 175: **Externe Berichterstellung->IP-Accounting->Schnittstellen**

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.

20.2.2 Optionen

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

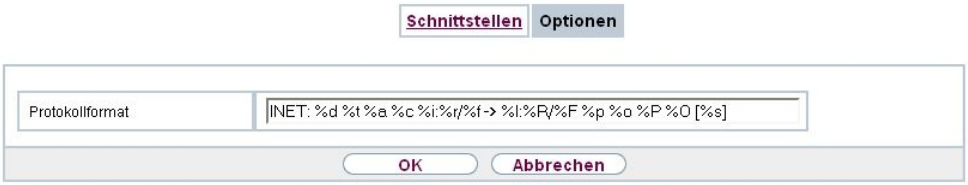


Abb. 176: **Externe Berichterstellung->IP-Accounting->Optionen**

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

Mögliche Format-Tags:

Format-Tags für IP-Accounting Meldungen

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

Feld	Beschreibung
%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]

20.3 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.

20.3.1 Benachrichtigungsempfänger

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

20.3.1.1 Neu

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

Abb. 177: **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungs-empfänger->Neu**

Das Menü **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungs-**

empfänger->**Neu** besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungs-dienst	Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen. Mögliche Werte: • E-Mail • SMS
Empfänger	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkompri-mierung	Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse. Aktivieren oder deaktivieren Sie das Feld. Standardmäßig ist die Funktion aktiv.
Betreff	Sie können einen Betreff eingeben.
Ereignis	Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar. Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll. Mögliche Werte: • *Systemmeldung enthält Zeichenfolge* (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • *Neuer Neighbor-AP gefunden*: Ein neuer benachbarter AP wurde gefunden. • *Neuer Rogue-AP gefunden*: Ein neuer Rough AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • *Neuer Slave-AP (WTP) gefunden*: Eine neuer unkonfigurierter AP hat sich beim WLAN Controller gemeldet. • *Verwalteter AP offline*: Ein managed AP ist nicht mehr

Feld	Beschreibung
	erreichbar.
Enthaltene Zeichenfolge	Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms. Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "*") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
Schweregrad	Wählen Sie den Schweregrad aus, auf dem der im Feld **Enthaltene Zeichenfolge** konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird. Mögliche Werte: *Notfall* (Standardwert), *Alarm*, *Kritisch*, *Fehler*, *Warnung*, *Benachrichtigung*, *Informationen*, *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*.

20.3.2 Benachrichtigungseinstellungen

Abb. 178: **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungseinstellungen**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Maximale 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.

Feld	Beschreibung
	Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Authentifizierung	Authentifizierung, die der SMTP-Server erwartet. Mögliche Werte: • *Keine* (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.
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

Feld	Beschreibung
	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*.

20.4 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

20.4.1 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.

Abb. 179: **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen**

Das Menü **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen** 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-Trap-Community	Nur wenn **SNMP Trap Broadcasting** aktiviert ist. 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*.

20.4.2 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.

20.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Abb. 180: **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu**

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.

20.5 Activity Monitor

Im diesem Menü finden Sie die Einstellungen, die nötig sind, um Ihr Gerät mit dem Windows-Tool **Activity Monitor** (Bestandteil von **BRICKware** for Windows) überwachen zu können.

Zweck

Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten ihres Geräts überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen sind leicht mit einem einzigen Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen Ihres Geräts ist damit

möglich.

Funktionsweise

Ein Status-Daemon sammelt Informationen über Ihr Gerät und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse der ersten LAN-Schnittstelle (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Bis zu 100 physikalische und virtuelle Schnittstellen können überwacht werden, soweit die Paketgröße von 4096 Bytes nicht überschritten wird. Der **Activity Monitor** auf Ihrem PC empfängt die Pakete und kann die enthaltenen Informationen je nach Konfiguration auf verschiedene Arten darstellen.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- das/die zu überwachende(n) Gerät(e) entsprechend konfigurieren
- die Windows-Anwendung auf Ihrem PC starten und konfigurieren (**BRICKware** for Windows, können Sie vom Download-Bereich auf *www.bintec-elmeg.com* auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen).

20.5.1 Optionen

Abb. 181: **Externe Berichterstellung->Activity Monitor->Optionen**

Das Menü **Externe Berichterstellung->Activity Monitor->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstellen	Wählen Sie die Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Keine* (Standardwert): Deaktiviert das Senden von Informationen an den **Activity Monitor**. • *Physikalisch*: Nur Informationen über physikalische Schnittstellen werden gesendet. • *Physikalisch/WAN/VPN*: Informationen über physikalische und virtuelle Schnittstellen werden gesendet.
Informationen senden an	Wählen Sie aus, an wen Ihr Gerät die UDP Pakete schicken soll. Mögliche Werte: • *Alle IP-Adressen (Broadcast)* (Standardwert): Mit dem Standardwert *255.255.255.255* wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet. • *Einzelner Host*: Die UDP-Pakete werden an die im nebenstehenden Eingabefeld eingetragene IP-Adresse geschickt.
Aktualisierungsintervall	Geben Sie das Aktualisierungsintervall (in Sekunden) ein. Mögliche Werte sind *0* bis *60*. Der Standardwert ist *5*.
UDP-Zielport	Geben Sie die Port-Nummer für die Windows-Anwendung **Activity Monitor** ein. Der Standardwert ist *2107* (registriert durch IANA - Internet Assigned Numbers Authority).
Passwort	Geben Sie das Passwort für den **Activity Monitor** ein.

Kapitel 21 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.

21.1 Internes Protokoll

21.1.1 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.

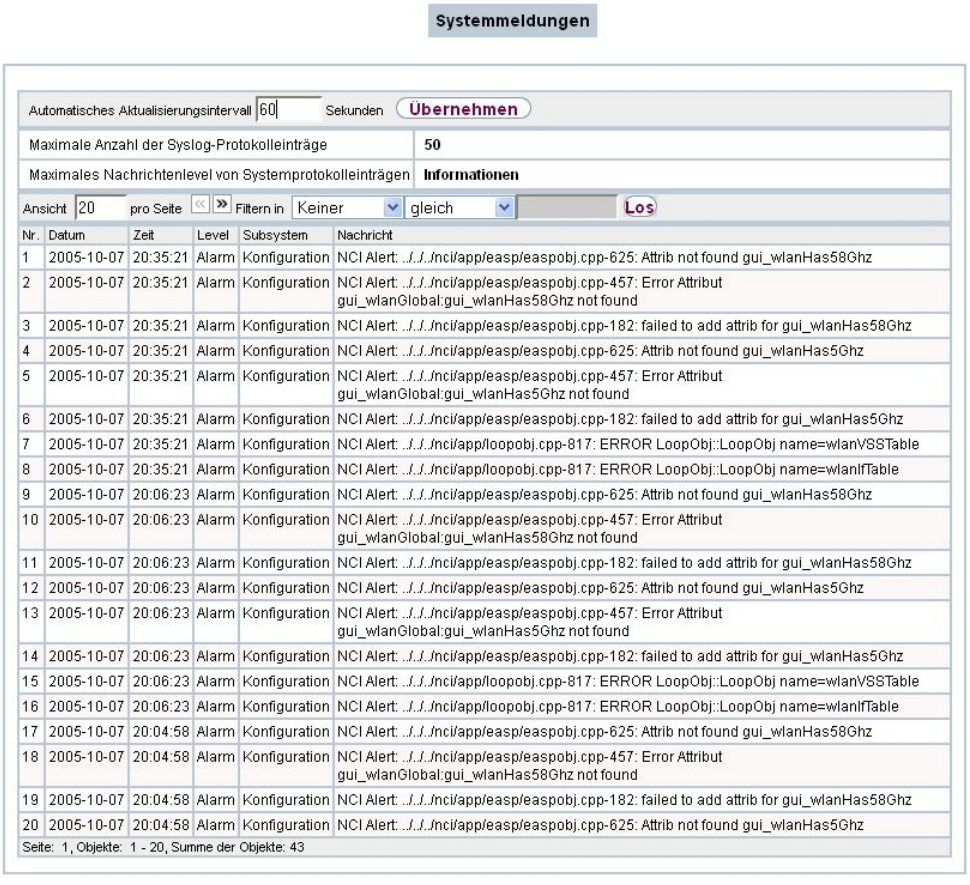


Abb. 182: **Monitoring->Internes Protokoll->Systemmeldungen**

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.

21.2 IPSec

21.2.1 IPSec-Tunnel

Im Menü **Monitoring**->**IPSec**->**IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.

Abb. 183: **Monitoring**->**IPSec**->**IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

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

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

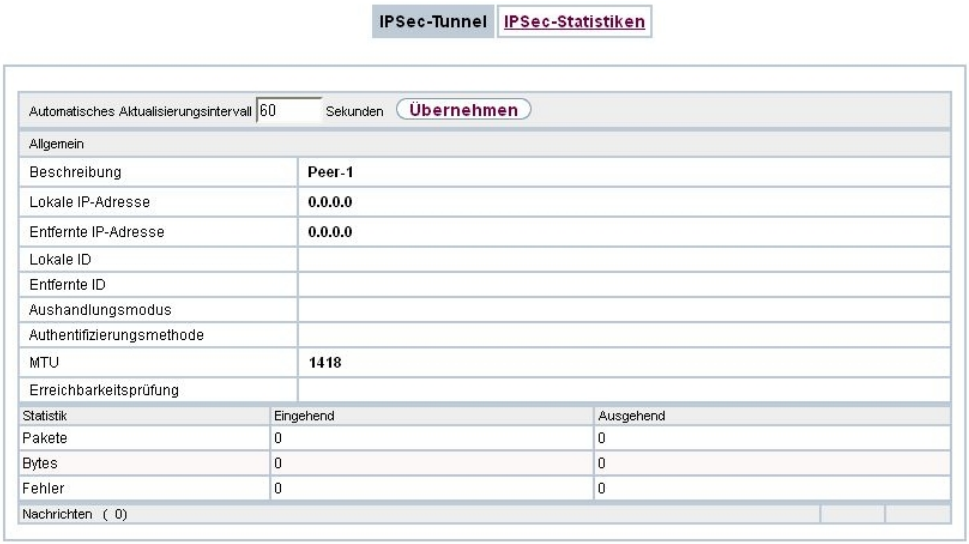


Abb. 184: **Monitoring->IPSec->IPSec-Tunnel->**

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.

Feld	Beschreibung
IKE (Phase-1) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

21.2.2 IPSec-Statistiken

Im Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

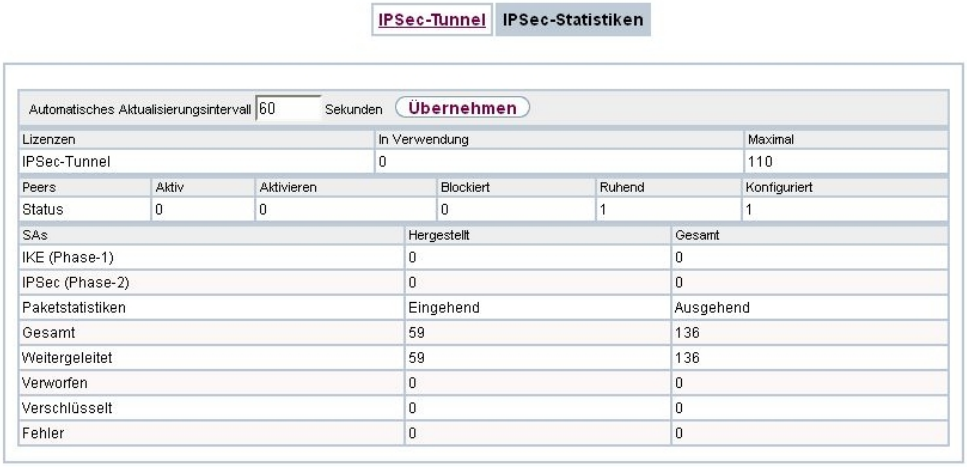


Abb. 185: **Monitoring**->**IPSec**->**IPSec-Statistiken**

Das Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** 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

Feld	Beschreibung
	(**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.

21.3 Schnittstellen

21.3.1 Statistik

Im Menü **Monitoring**->**Schnittstellen**->**Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

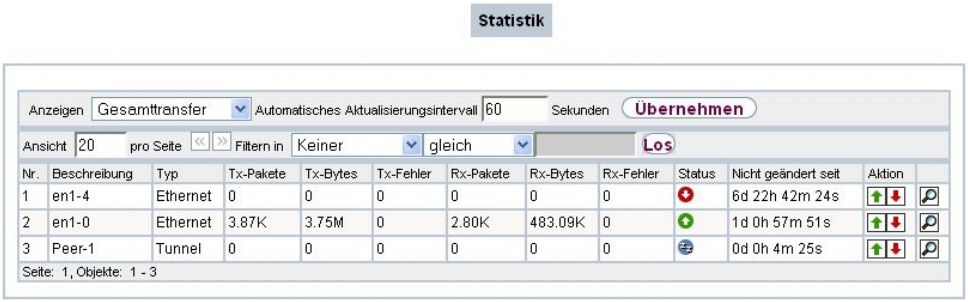


Abb. 186: **Monitoring**->**Schnittstellen**->**Statistik**

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

Werte in der Liste Statistik

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
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

Feld	Beschreibung
	zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

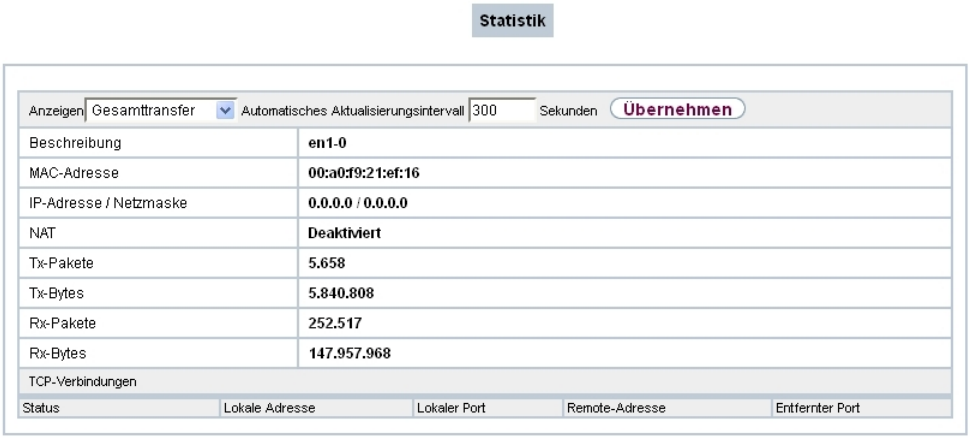


Abb. 187: **Monitoring->Schnittstellen->Statistik->**

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt den Schnittstellentyp 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.

Feld	Beschreibung
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.

21.4 WLAN

21.4.1 WLANx

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

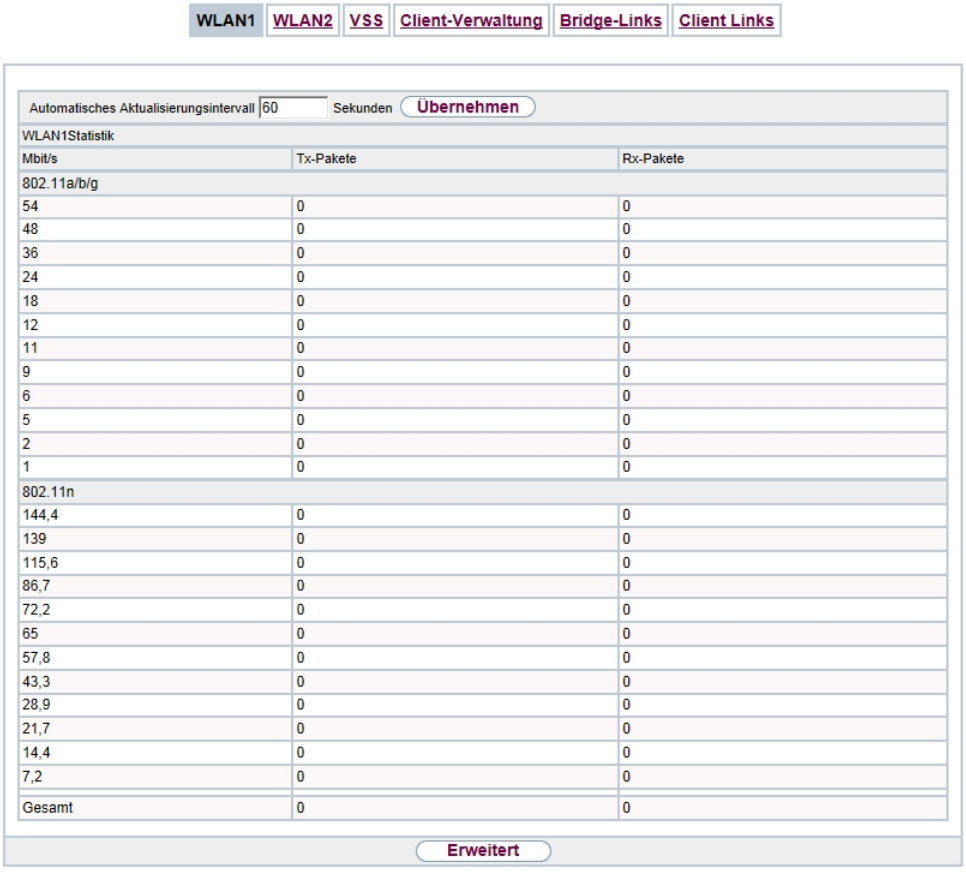


Abb. 188: **Monitoring**->**WLAN**->**WLAN**

Werte in der Liste WLAN

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

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

Abb. 189: **Monitoring->WLAN->WLAN->Erweitert**

Werte in der Liste Erweitert

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

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Unicast MSDUs erfolgreich übertragen	Zeigt die Anzahl der erfolgreich an Unicast-Adressen versandten MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wurde ein Acknowledgement empfangen.
Erfolgreich übertragene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich an Multicast-Adressen (inklusive der Broadcast MAC-Adresse) versandten MSDUs an.
Übertragene MPDUs	Zeigt die Anzahl der erfolgreich empfangenen MPDUs an.

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

21.4.2 VSS

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

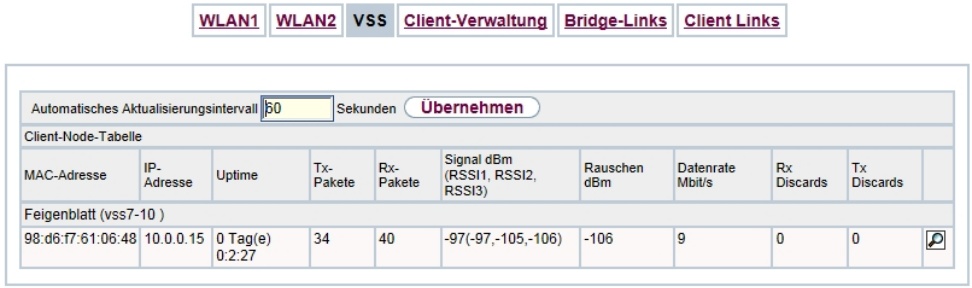


Abb. 190: **Monitoring**->**WLAN**->**VSS**

Werte in der Liste VSS

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

VSS - Details für Verbundene Clients

Im Menü **Monitoring**->**WLAN**->**VSS**->**<Verbundener Client>**-> werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

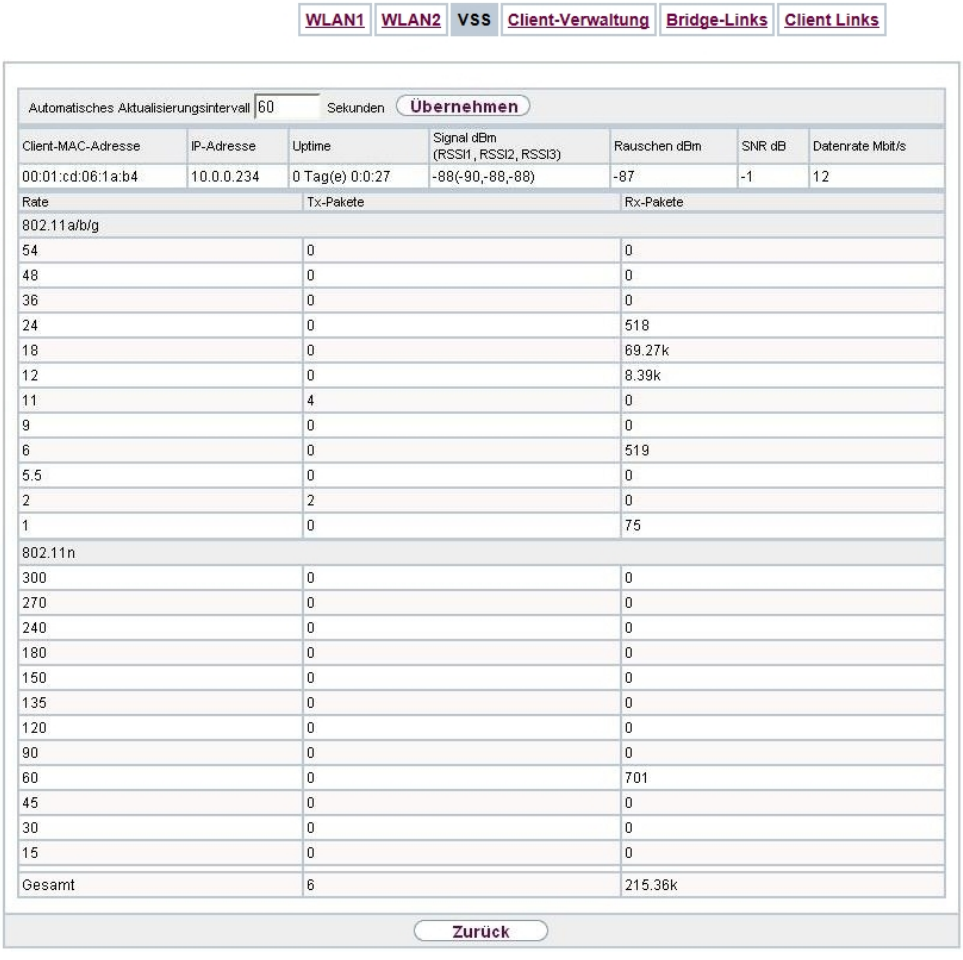


Abb. 191: **Monitoring->WLAN->VSS-><Verbundener Client>->**

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen

Feld	Beschreibung
	Indikator für die Qualität der Verbindung im Funk dar. Werte: • > 25 dB exzellent • 15 – 25 dB gut • 2 – 15 dB grenzwertig • 0 – 2 dB schlecht.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Tx-Pakete	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.
Rx-Pakete	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.

21.4.3 Client-Verwaltung

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

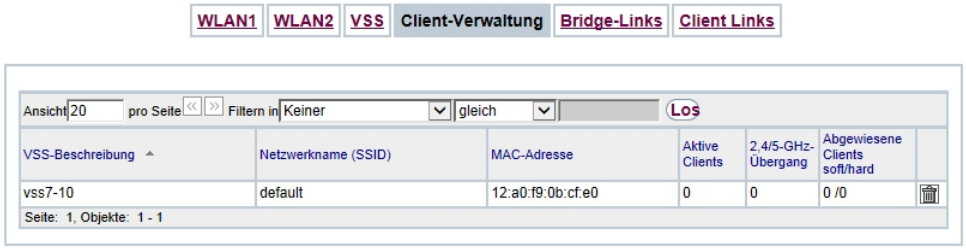


Abb. 192: **Monitoring->WLAN+Client-Verwaltung**

Werte in der Liste Client-Verwaltung

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

21.4.4 Bridge-Links

Im Menü **Monitoring**->**WLAN**->**Bridge-Links** werden die aktuellen Werte und Aktivitäten der Bridge-Links angezeigt.

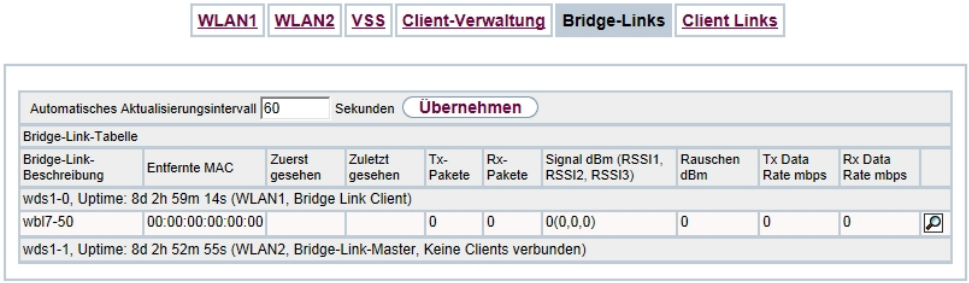


Abb. 193: **Monitoring**->**WLAN**->**Bridge-Links**

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

Feld	Beschreibung
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Tx**Datenrate Mbit/s**	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Rx **Datenrate Mbit/s**	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Bridge-Link aktiv ist.

Bridge-Link Details

Über das  -Symbol öffnen Sie eine Übersicht über weitere Details zu den Bridge-Links.

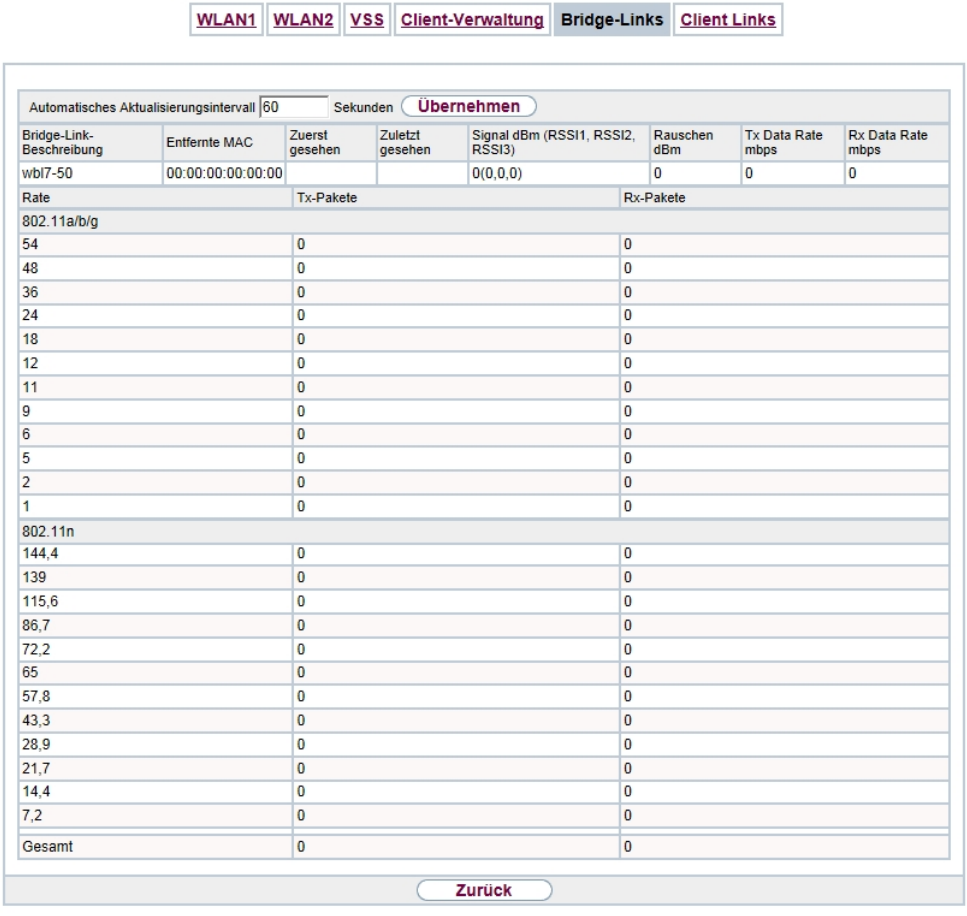


Abb. 194: **Monitoring->WLAN->Bridge-Links->**

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.

Feld	Beschreibung
Tx **Datenrate Mbit/s**	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Rx **Datenrate Mbit/s**	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für **Tx-Pakete** und **Rx-Pakete** einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

21.4.5 Client Links

Im Menü **Monitoring**->**WLAN**->**Client Links** werden die aktuellen Werte und Aktivitäten der Client Links angezeigt.

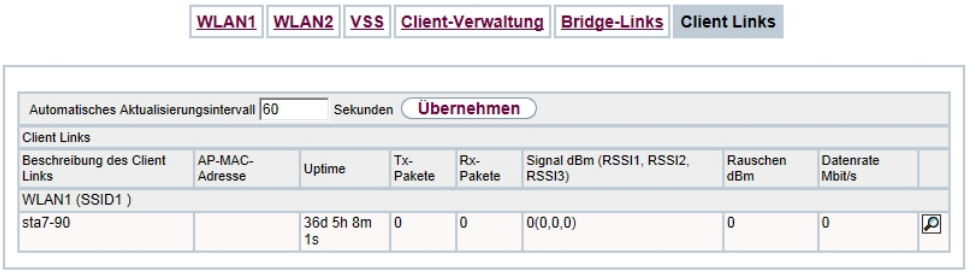


Abb. 195: **Monitoring**->**WLAN**->**Client Links**

Werte in der Liste Client Links

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des Client Links an.
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.

Client Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Client Links.

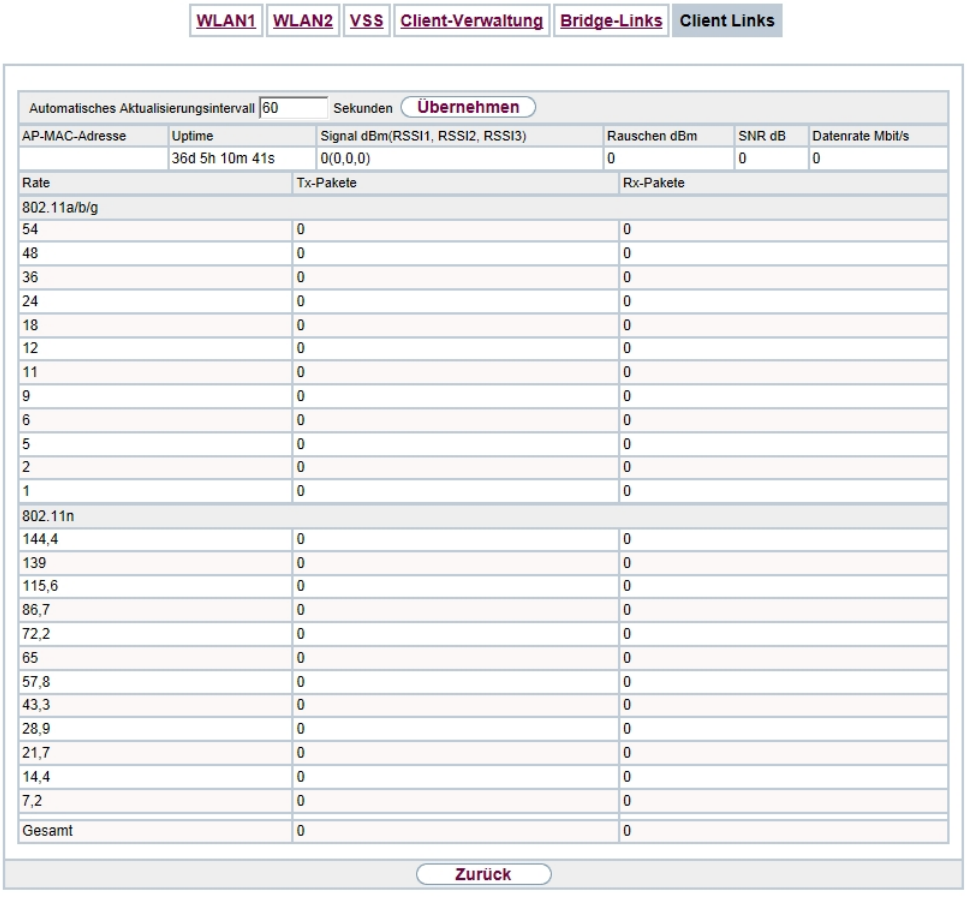


Abb. 196: **Monitoring->WLAN->Client Links->**

Werte in der Liste Client Links

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.

Feld	Beschreibung
SNR dB	Zeigt die Qualität des Signals in dB an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für **Tx-Pakete** und **Rx-Pakete** einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

21.5 Bridges

21.5.1 br<x>

Im Menü **Monitoring**->**Bridges**-> **br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

Abb. 197: **Monitoring**->**Bridges**

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.

21.6 Hotspot-Gateway

21.6.1 Hotspot-Gateway

Im Menü **Monitoring**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

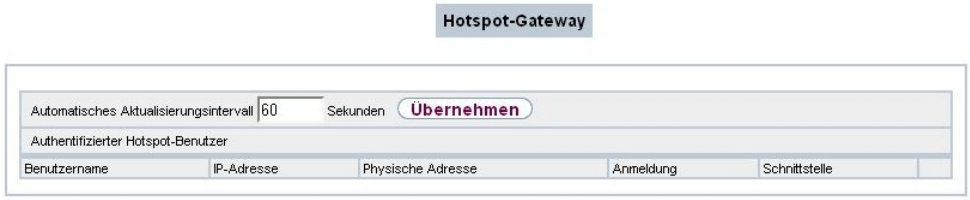


Abb. 198: **Monitoring->Hotspot-Gateway->Hotspot-Gateway**

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.

21.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

21.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

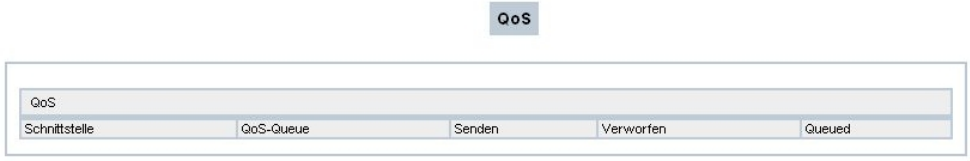


Abb. 199: **Monitoring->QoS->QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.

Feld	Beschreibung
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.

21.8 PIM

21.8.1 Allgemeine Statusangaben

Im Menü **Monitoring**->**PIM**->**Allgemeine Statusangaben** wird der Status aller konfigurierten PIM Komponenten angezeigt.

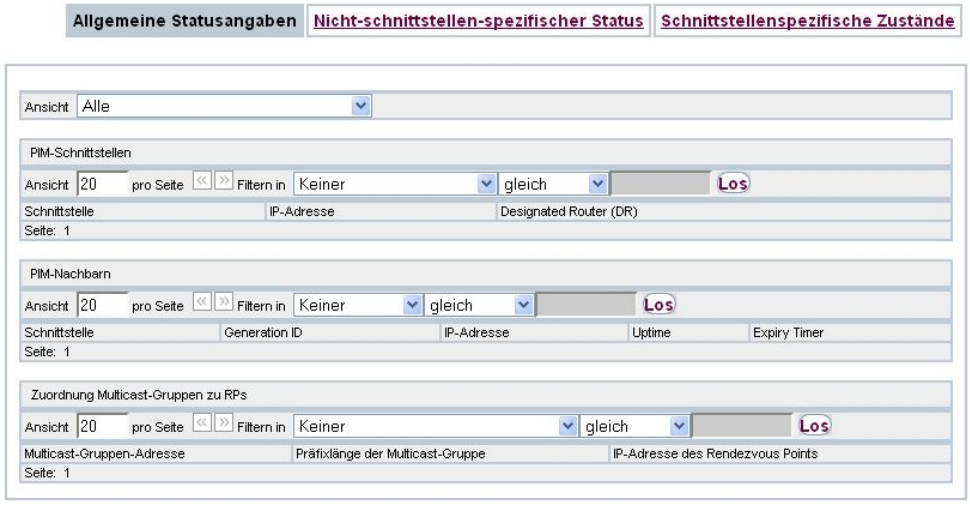


Abb. 200: **Monitoring**->**PIM**->**Allgemeine Statusangaben**

Werte in der Liste Allgemeine Statusangaben

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus.

Feld	Beschreibung
	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.
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.

21.8.2 Nicht-schnittstellen-spezifischer Status

Das Menü **Monitoring**->**PIM**->**Nicht-schnittstellen-spezifischer Status** enthält Status-Angaben für alle PIM-Schnittstellen.

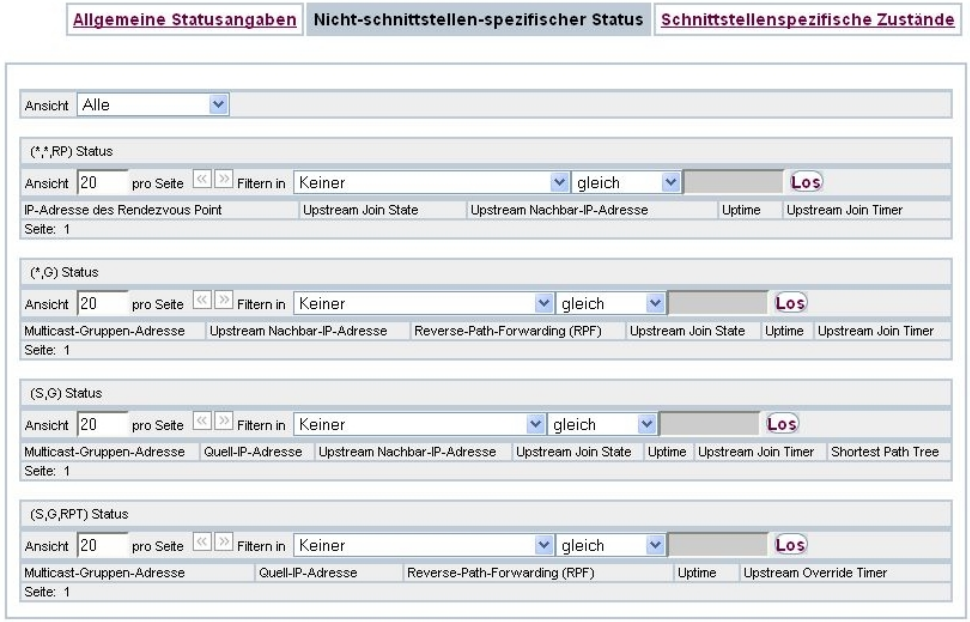


Abb. 201: **Monitoring->PIM->Nicht-schnittstellen-spezifischer Status**

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-IP-Adresse	Zeigt die primäre IP-Adresse des Upstream Neighbors, oder unknown(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.

Feld	Beschreibung
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 oder kein PIM Neighbor ist. InetAddressType wird im Objekt pimSGAddressType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF'(S,G) genannt.

Feld	Beschreibung
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.

21.8.3 Schnittstellenspezifische Zustände

Das Menü **Monitoring**->**PIM**->**Schnittstellenspezifische Zustände** enthält schnittstellenspezifische Status-Angaben.

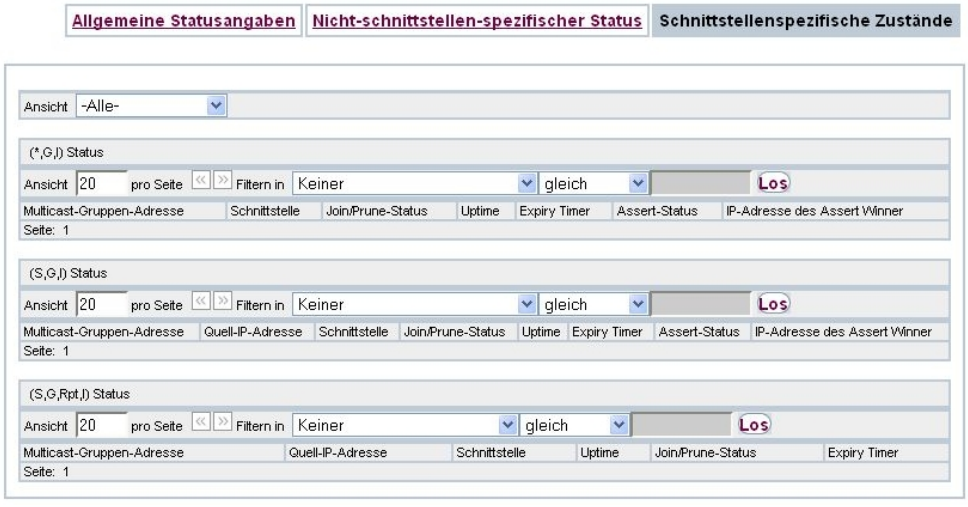


Abb. 202: **Monitoring->PIM->Schnittstellenspezifische Zustände**

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.

Feld	Beschreibung
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. 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 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.

Glossar

2G Siehe GSM.

3DES Siehe DES.

3G Siehe UMTS.

4G Siehe LTE.

802.11 Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)

Access Client Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.

Access Point Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).

Accounting Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.

Activity Monitor Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.

Ad-Hoc-Netzwerk In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.

ADSL Asymmetric Digital Subscriber Line. Siehe DSL.

AES Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.

Aggressive Mode Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.

AH Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.

Anlagenanschluss Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, …) Siehe auch Mehrgeräteanschluss.

Anlagenanschluss-Rufnummer Siehe Anlagenanschluss.

Annex A Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.

Annex B Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.

Annex J Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbündelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.

Annex L Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.

Annex M Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.

ANSI T1.413 ANSI T1.413 ist eine ADSL-Variante.

ARP Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.

ATM Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.

Authentifikation Überprüfung der Identität des Nutzers (Authentisierung).

Autorisierung Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.

AUX AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.

B-Kanal Siehe Basisanschluss und Primärmultiplexanschluss.

Backbone Area Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.

Basisanschluss Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.

Beacon Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.

Bit Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.

Black / White List Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnum-

	mer 01234987 kann trotzdem in der White List freigegeben werden.)
Blowfish	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
BootP	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Siehe Basisanschluss.
Bridge	Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.
Broadcast	Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8
BRRP	BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.
CA	Certificate Authority. Siehe Zertifikat.
Cache	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
Called Party's Number	Rufnummer des angerufenen Teilnehmers.
Calling Party's Number	RufnNummer des Anrufers.
CAPI	Das Common ISDN Application Programming Interface (CAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch TAPI.

CAPWAP Das Control And Provisioning of Wireless Access Points Protocol (CAPWAP) dient zur Überwachung von Wireless Access Points (Slaves) durch einen WLAN-Controller (Master). Es verwendet die UDP-Ports 5246 zur Kontrolle und 5247 zur Datenübertragung.

CAST CAST ist ein Verschlüsselungsverfahren (siehe Cipher). CAST verwendet eine fixe Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 40 und 128 Bit gewählt werden. Alternative Bezeichnungen sind CAST-128 oder CAST5.

CHAP Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.

Cipher Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.

Client Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.

CoS Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugeteilte Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, … In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen eingerichtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).

CRC Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.

CRL Siehe Zertifikat.

D-Kanal Siehe Basisanschluss und Primärmultiplexanschluss.

Daemon Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.

Datagramm Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.

Datenkompression Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.

Dead Peer Detection In IPSec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.

Default Gateway An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.

Default Route Siehe Standardroute.

Deffie-Hellman Diffie-Hellman ist ein Public-Key-Algorithmus zur Aushandlung und Etablierung von Schlüsseln. Da Daten weder verschlüsselt noch signiert werden, ist das Verfahren nur sicher, falls sich die Verbindungspartner über andere Mechanismen, wie RSA oder DSA, authentifizieren.

Denial-Of-Service Attack Bei einem Denial-of-Service-Angriff (DoS) wird eine Netzwerkkomponente mit Anfragen überflutet, sodass diese völlig überlastet wird. Das System oder ein bestimmter Dienst ist in Folge dessen nicht mehr funktionsfähig.

DES Data Encryption Standard (DES) ist ein Verschlüsselungsverfahren (siehe Cipher). DES verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge beträgt 56 Bit. Triple-DES oder 3DES basiert auf der dreimaligen Anwendung von DES (drei verschiedene unabhängige Schlüssel).

DFÜ DFÜ steht für Datenfernübertragung.

DHCP Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Zuweisung von IP-Adressen. Ein DHCP-Server vergibt an jeden Client im Netzwerk eine IP-Adresse aus einem definierten Adress-Pool. Die Clients müssen dazu entsprechend konfiguriert sein.

DIME Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.

DNS Mithilfe des Domain Name System (DNS) wird der Domänenname

(z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).

Domäne Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).

Downstream Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.

DSA Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung als RSA.

DSCP Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.

DSL-Modem Siehe Modem.

DSS1 Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.

DTIM Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.

Durchwahl (VoIP) Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, …)

Durchwahlausnahme Siehe Anlagenanschluss und Durchwahl (VoIP).

Durchwahlbereich Siehe Rufnummernblock bei Anlagenanschluss und Durchwahl (VoIP).

Durchwahlnummer Siehe Anlagenanschluss und Durchwahl (VoIP).

Dynamische IP-Adresse Im Gegensatz zu einer statischen IP-Adresse wird die dynamische IP-Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.

DynDNS Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.

Einzelrufnummer (VoIP) Beim Einzelrufnummer-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von VoIP-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Durchwahl (VoIP).

Encapsulation Enkapsulierung (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.

Encryption Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.

ESP Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.

Ethernet Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.

Euro-ISDN In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.

Eurofile-Transfer EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.

Filter Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Treffen diese Kriterien für ein Datenpaket zu, kann das Datenpaket einer bestimmten Aktion (weiterleiten, ablehnen, …) unterworfen werden. Dadurch entsteht eine Filterregel.

Filterregel Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.

Firmware Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts

bereitgestellt.

Fragmentierung Falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit (MTU) der Netzwerkschnittstelle ist, muss das Datenpaket durch IP-Fragmentierung auf mehrere physikalische Datenblöcke aufgeteilt werden. Der umgekehrte Prozess wird Reassembly genannt.

Frame Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells

Frame Relay Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.

FTP Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.

Full-Duplex Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.

G.991.1 Datenübertragungsempfehlung für HDSL.

G.991.2 Datenübertragungsempfehlung für SHDSL.

G.992.1 Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)

G.992.2 Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)

G.992.3 Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.

G.992.4 Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)

G.992.5 Datenübertragungsempfehlung für xDSL2+. Es existieren drei Vari-

anten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.

G.993.1 Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)

G.993.2 Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)

G.DMT Siehe F.992.1.

G.Lite Siehe F.992.2.

G.SHDSL Siehe G.991.2.

Gateway Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.

GPRS General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.

GRE Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.

GSM Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.

Half-Duplex Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.

Hash Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der

Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).

HDSL High Data Rate Digital Subscriber Line. Siehe DSL.

Heartbeat Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.

Hop Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.

Host Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.

Host-Name Domänenname eines Host. Siehe DNS.

Hostroute Eine Hostroute bezeichnet die Route zu einem einzelnen Host.

Hotspot Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.

HSDPA High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.

HTTP Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.

HTTPS Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.

Hyperchannel Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.

ICMP Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.

IGMP Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.

IKE Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.

Infrastruktur-Netzwerk In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.

IP Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).

IP-Adresse IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.

IPCP Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPV6CP) bereitgestellt.

IPSec IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der Authentification-Header (AH) verwendet die Protokollnummer 51, das Encapsulating-Security-Payload (ESP) die Nummer 50.

IPv6 Siehe IP.

ISDN Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.

ISDN-Adresse Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.

ISDN-Login Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.

ISDN-Nummer Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.

ISDN-Router Siehe Router.

ISP Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.

ITU Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.

Kanal Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.

Kanalbündelung Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.

Keepalive Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.

Keepalive Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.

Konfiguration Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gesichert, von extern geladen oder gelöscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

L2TP Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten zu Aufrechterhaltung der Erreichbarkeit der Tunnelendpunkte abgesichert übertragen werden.

LAC Siehe L2TP.

LAN Ein Local Area Network (LAN) bezeichnet ein räumlich eng begrenztes Netzwerk und umspannt meist ein Gebäude oder einen Firmensitz.

Lastverteilung Bei der Lastverteilung werden Daten über unterschiedliche Schnittstellen gesendet, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. Im Unterschied zu Multilink funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.

Layer Ein Layer bezeichnet eine Schicht im OSI-Modell.

LCP Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die Enkapsulierung automatisch auszuhandeln, Grenzen für variierende Paketgrößen zu verarbeiten, den Verbindungspartner zu authentifizieren, einen defekten Link zu bestimmen, Verbindungsfehler zu erkennen und die Verbindung zu beenden.

LDAP Das Lightweight Directory Access Protocol (LDAP) regelt die Kommunikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.

Lease Time Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.

Leased Line Siehe Standleitung.

LLC Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.

LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrgeräteanschluss	Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.
Metrik	Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).
MIB	Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.

MLP Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.

Modem Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.

MPDU Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.

MPPC Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.

MPPE Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.

MS-CHAP Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).

MSDU Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.

MSN Siehe Mehrfachrufnummer.

MSS Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.

MSS Clamping Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.

MTU Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.

Multicast Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::/8-Adressen und ICMPv6.

Multilink Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, …) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.

NAPT Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.

NAT Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.

NBNS NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.

Netzabschluss Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.

Netzmaske Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.

Netzwerkadresse Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24

Netzwerkroute Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.

NT Siehe Netzabschluss.

NTP Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.

OAM OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.

OSI-Modell Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen

	physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.
OSPF	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
PAP	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
PAT	Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.
Peer	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
Phase-1/2	Siehe IKE.
PIM	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.
PKCS	Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.
PKI	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
PMTU	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
Point-to-Multipoint	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).

Point-to-Point Siehe Anlagenanschluss und Durchwahl (VoIP).

Pool Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.

POP3 Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.

Port Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, …) ein ankommendes Datenpaket weitergeleitet wird.

PPP Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.

PPPoA Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.

PPPoE Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.

PPTP Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.

Präfix Siehe Netzwerkadresse.

Präfixdelegation In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.

Präfixlänge Siehe Netzmaske.

Preshared Key Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.

PRI Siehe Primärmultiplexanschluss.

Primärmultiplexanschluss Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.

Proposal Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.

Protokoll Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP

Proxy Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.

PVID Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.

Q-SIG Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.

QoS Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.

Queue In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.

RADIUS Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzername und Kennwort. Siehe auch TACACS+.

RE-ADSL2 Siehe G.992.5.

Real Time Jitter Control Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.

Regelkette In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.

Registrar Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.

Repeater Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.

Reset Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.

RFC Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.

Rijndael Siehe AES.

RIP Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.

RipeMD 160 RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.

RJ45 RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.

Roaming Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.

Router Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.

Router Advertisement Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router Advertisments Präfixe verteilt, die Autokonfiguration organisiert und der Standardrouter festgelegt.

Routing Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.

RSA Mithilfe des RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über die Signatur können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. RSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch DSA. RSA ist langsamer in der Schlüsselerzeugung aber schneller in der Schlüsselverarbeitung als DSA.

RTP Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.

RTS Threshold Sobald die Anzahl der Frames im Datenpaket über der RTS-Schwelle (RTS Threshold) liegt, wird vor dem Senden eines Datenpakets eine Verbindungsüberprüfung (RTS/CTS-Handshake) durchgeführt.

RTSP Das Real-Time Streaming Protocol (RTSP) steuert die Übertragung von Audio- und Videodaten (Streams) über IP-basierte Netzwerke. Während das Real-Time Transport Protocol (RTP) zur Übertragung der Nutzdaten dient, besteht die Funktion von RTSP hauptsächlich in der Steuerung der Datenströme.

S2M-Anschluss Siehe Primärmultiplexanschluss.

SA Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.

SAD Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über

jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer eingehende Verbindung wird die SAD angesprochen, um festzulegen, wie das Paket verarbeitet wird.

SCEP Das Simple Certificate Enrollment Protocol (SCEP) dient zur Verwaltung digitaler Zertifikate.

Scheduling Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.

Serielle Schnittstelle Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).

Server Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.

SFP Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.

SHA1 Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.

SHDSL Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.

Shell Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder grafische Benutzerschnittstelle) zwischen Computer und Benutzer.

Shorthold Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.

SIF Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.

SIP Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.

SIP-Provider Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.

SNMP Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.

Spatial Streams Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrate.

SPD Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die Security-Policy-Datenbank führt die Formen des Datenverkehrs auf, die gesichert werden sollen. Dazu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.

SRTP Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).

SSH Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.

SSID Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).

SSL Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer

Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.

STAC Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).

Standardroute Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.

Standardrouter Siehe Default Gateway.

Standleitung Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.

Statische IP-Adresse Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.

STUN-Server Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.

Subadressierung Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.

Subnetz Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).

Switch Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerksegmente miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells berieben werden. Das dem

Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.

SWYX SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.

Syslog Das Syslog-Protokoll wird zur Übermittlung von Status-Meldungen in einem IP-Netzwerk verwendet. Verschiedene Netzwerkkomponenten können somit von einem zentralen System aus überwacht werden. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP-Port 514 gesendet.

T.38 T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.

TACACS+ Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.

TAPI Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.

TCP Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.

TCP-ACK-Paket Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.

TE Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein

	ISDN-Endgerät dar. Siehe auch NT.
Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
TLS	Siehe SSL.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpakete bis zum abgefragten Ziel-Host vermittelt werden.
Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128,192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.

UDP Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.

ULA Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.

UMTS Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.

Unicast Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertagen.

UPnP Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.

Upstream Das Gateway leitet die Daten des eigenen Netzwerks weiter.

URL Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htp (Web-Seite im Internet)

V.110 V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.

VDSL Very High Speed Digital Subscriber Line. Siehe DSL.

VID Siehe VLAN.

VLAN Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definieren Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.

VoIP Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Ab-

	bau der Telefonverbindung erfolgt dabei über Signalisierungsprotokolle, wie z. B. SIP.
VPN	Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IPSec, PPTP, L2TP und GRE.
VSS	Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.
Wählverbindung	Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.
Walled Garden	Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.
WAN	Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausgedehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.
WDS	Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.
Web-Server	Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.
WEP	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
WINS	Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
WMM	Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.

WPA Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.

WPA - Enterprise WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.

WPA - PSK WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.

WPA 2 Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.

X.25 X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.

X.31 Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.

X.500 Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.

X.509 Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine Public-Key-Infrastruktur (PKI).

X.75 X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.

XAuth Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.

Zeitschlitz Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.

Zertifikat Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentli-

chen Schlüssel her. Zertifikate mit öffentlichem Schlüsseln werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.

Index

B

C

D

E

P

Q

R

S

T

U

V

W

X

Z