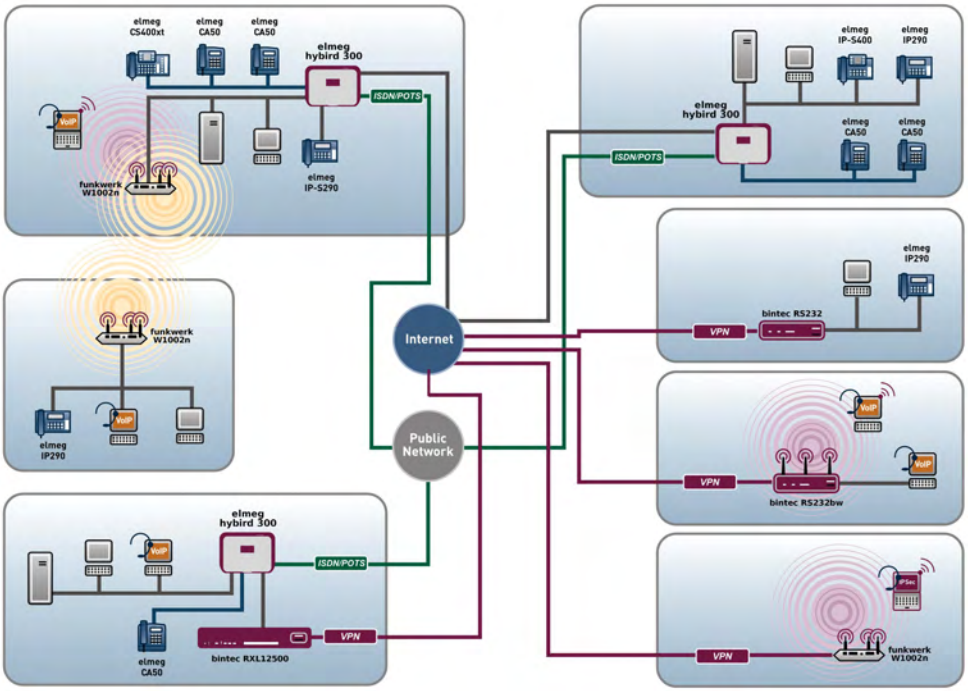


Benutzerhandbuch bintec R200-Serie

Referenz

Rechtlicher Hinweis

Ziel und Zweck
Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von funkwerk-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.funkwerk-ec.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. Funkwerk Enterprise Communications 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 funkwerk-Gateways finden Sie unter *www.funkwerk-ec.com* .

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

Marken
funkwerk und das funkwerk-Logo, bintec und das bintec-Logo, artem und das artem-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

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

Richtlinien und Normen

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

Wie Sie Funkwerk Enterprise Communications GmbH erreichen
Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25
Funkwerk Enterprise Communications 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.funkwerk-ec.com*

Inhaltsverzeichnis

Kapitel 1 Einleitung

Die leistungsstarken Gateways **bintec R230a**, **bintec R230b**, **bintec R230aw**, **bintec R232a**, **bintec R232b** und **bintec R232bw** ermöglichen Ihnen die kostengünstige Verbindung kleiner Netzwerke sowie die Anbindung Ihres Einzelarbeitsplatzes oder kleinen Unternehmens an das Internet und an andere Partnernetze (z. B. eine Firmenzentrale).

Sicherheitshinweise

Was Sie im Umgang mit Ihrem **bintec** Gateway beachten müssen, erfahren Sie in den Sicherheitshinweisen, die im Lieferumfang Ihres Gerätes enthalten sind.

Installation

Wie Sie Ihr Gerät anschließen, erfahren Sie in *Aufstellen und Anschließen* auf Seite 6. Dieses Kapitel sagt Ihnen auch, welche Vorbereitungen zur Konfiguration nötig sind.

Konfiguration

Wie Sie Ihr Gerät das Laufen lehren, erfahren Sie im Kapitel *Grundkonfiguration* auf Seite 10. Dort zeigen wir Ihnen, wie Sie Ihr Gerät innerhalb weniger Minuten von einem Windows-PC aus mit einem Konfigurationsassistenten in Betrieb nehmen und wie Sie weitere nützliche Hilfsprogramme installieren. Am Ende dieses Kapitels sind Sie in der Lage, im Internet zu surfen, E-Mails zu verschicken und zu empfangen und eine Verbindung mit einem Partnernetz herzustellen, um beispielsweise auf Daten einer Firmenzentrale zuzugreifen.

Passwort

Wenn Sie bereits **bintec**-Geräte konfiguriert haben und gleich beginnen möchten, fehlen Ihnen nur noch der werkseitig eingestellte Benutzername und das Passwort.

Benutzername: `admin`

Passwort: `funkwerk`

Hinweis

Denken Sie daran, das Passwort sofort zu ändern, wenn Sie sich das erste Mal auf Ihrem Gerät einloggen.

Alle **bintec**-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 15 beschrieben.

Workshops

Anwendungsbezogene Schritt-für-Schritt-Anleitungen zu den wichtigsten Konfigurationsaufgaben finden Sie im separaten Handbuch **FEC Anwendungs-Workshops**, das unter *www.funkwerk-ec.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. 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**-Geräte mit einer System-Software ab Software-Version 7.10.1.

Das Handbuch, die Sie vor sich haben, enthält folgende Kapitel:

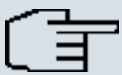
Benutzerhandbuch - Referenz

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 Netzwerk** **Routing-Protokolle** **Multicast** **WAN**	In diesen Kapiteln werden alle Konfigurationsoptionen des **Funkwerk Configuration Interface** 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
VPN **Firewall** **VoIP** **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 (Courier),`
 	
`z. B. ping 192.168.1.254`
	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.funkwerk-ec.com*	Kennzeichnet Hyperlinks.

Kapitel 3 Inbetriebnahme

Achtung

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

3.1 Aufstellen und Anschließen

Hinweis

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

Achtung

Die Verwendung eines falschen Netzadapters kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich den mitgelieferten Netzadapter! Falls Sie ausländische Adapter/Netzteile benötigen, wenden Sie sich bitte an unseren funkwerk Service.

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

Hinweis

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

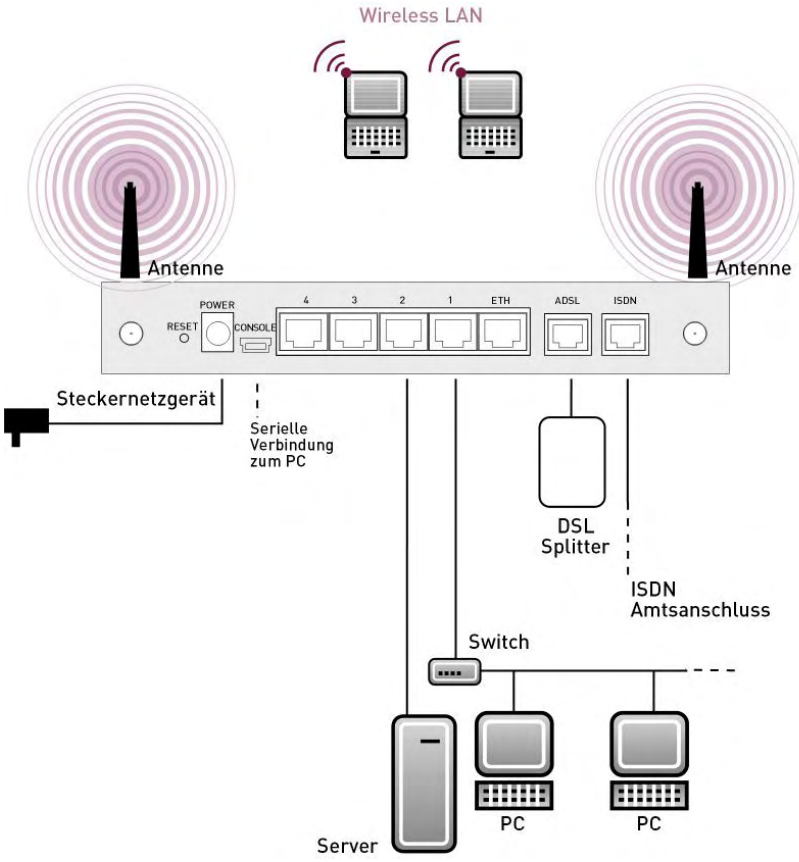


Abb. 2: Anschlussmöglichkeiten am Beispiel **bintec R232bw**

Gehen Sie beim Aufstellen und Anschließen in der folgenden Reihenfolge vor (siehe Anschlusspläne für die einzelnen Geräte im Kapitel *Technische Daten* auf Seite 22):

(1) Antennen: Schrauben Sie die beiden mitgelieferten externen Standardantennen auf die dafür vorgesehenen RSMA-Anschlüsse (nur **bintec R230aw** und **bintec R232bw**).

(2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

(3) LAN: Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den ersten Switch-Port (**1**) Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

(4) ADSL: Verbinden Sie die ADSL-Schnittstelle (**ADSL**) Ihres Geräts über das mitgelieferte DSL-Kabel mit dem DSL-Ausgang des Splitters.

(5) Netzanschluss: Schließen Sie das Gerät mit dem mitgelieferten Netzadapter an eine Steckdose an.

Optionale Anschlüsse

- ISDN: Schließen Sie die ISDN-Schnittstelle (**ISDN**) des Geräts mit dem mitgelieferten ISDN-Kabel an Ihre ISDN-Dose an (nur **bintec R232a**, **bintec R232b** und **bintec R232bw**).
- DMZ: Verbinden Sie die WAN-Schnittstelle (**ETH**) Ihres Geräts über ein weiteres Ethernet-Kabel mit dem Ethernet-Anschluss Ihrer DMZ (nur **bintec R232a**, **bintec R232b** und **bintec R232bw**).
- Weitere LANs/WANs: Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports (**2**, **3** oder **4**) Ihres Geräts mittels weiterer Ethernet-Kabeln an.
- Serielle Verbindung: Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs (**COM1** oder **COM2**) mit der seriellen Schnittstelle des Geräts (**Console**). Verwenden Sie dazu das mitgelieferte serielle Kabel. Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

Das Gerät ist nun für die Konfiguration mit dem **Schnellinstallations-Assistenten** vorbereitet.

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 Support Information

Wenn Sie zu Ihrem neuen Produkt Fragen haben oder zusätzliche Informationen wünschen, erreichen Sie das Support Center von Funkwerk Enterprise Communications GmbH montags bis freitags von 8:00 bis 17 Uhr. Folgende Kontaktmöglichkeiten stehen Ihnen zur Verfügung:

Email	hotline@funkwerk-ec.com
Internationale Supportkoordination	Telefon: +49 911 9673 1550 Fax: +49 911 9673 1599
Endkunden-Hotline	0900 1 38 65 93 (1,10 €/min aus dem deutschen Festnetz)

Ausführliche Informationen zu unseren Support Leistungen erhalten Sie unter *www.funkwerk-ec.com* .

Kapitel 4 Grundkonfiguration

Die Konfiguration Ihres Geräts wird mit dem **Funkwerk Configuration Interface** durchgeführt.

Für den Einsatz als Gateway sind einige grundlegende Konfigurationsschritte nötig. In diesem Kapitel erfahren Sie, wie Sie die Konfiguration vorbereiten, welche Daten Sie vorher sammeln müssen, wie Sie die Konfiguration eines üblichen ADSL-Anschlusses durchführen, ein WLAN einrichten, ggf. Anpassungen der PC-Konfigurationen im Netzwerk machen und nach Abschluss der Konfiguration die Verbindung testen. Tiefergehende Netzwerkkenntnisse sind dabei nicht erforderlich. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

4.1 Voreinstellungen

4.1.1 IP-Konfiguration

Ihr Gerät wird mit einer vordefinierten IP-Konfiguration ausgeliefert:

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

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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

Hinweis

Alle **bintec**-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!

Darüber hinaus ist das Gerät werksseitig als DHCP-Server eingerichtet, es übermittelt also PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie Ihren PC für den automatischen Bezug einer IP-Konfiguration einrichten, ist in *PC einrichten* auf Seite 14 beschrieben.

Hinweis

Sollten Sie in Ihrem LAN bereits einen DHCP-Server betreiben, empfiehlt sich die Konfiguration des Geräts an einem Einzel-PC, der nicht in Ihr LAN integriert ist.

Folgende Einstellungen werden an einen unkonfigurierten PC übertragen:

- eine zur Konfiguration des Geräts passende IP-Adresse (es werden IP-Adressen aus dem Bereich 192.168.0.10 bis 192.168.0.49 vergeben)
- die entsprechende Netzmaske (255.255.255.0)
- die IP-Adresse des Geräts als Standardgateway und als Standard-DNS-Server.

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 **Funkwerk Configuration Interface** im Menü **Wartung**->**Software &Konfiguration** vornehmen.

Eine Bescheibung des Update-Vorgangs finden Sie in *Softwareaktualisierung* auf Seite 18.

4.2 System-Voraussetzungen

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

- Betriebssystem Microsoft Windows ab Windows 2000
- Internet Explorer 6 oder 7, Mozilla Firefox ab Version 1.2
- Installierte Netzwerkkarte (Ethernet)
- DVD-Laufwerk
- Installiertes TCP/IP-Protokoll
- Hohe Farbanzeige (mehr als 256 Farben) für die korrekte Darstellung der Grafiken.

4.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration und den Internet-Anschluss bereitlegen sowie ggf. die nötigen Daten für die Anbindung der gewünschten WLAN-Clients sammeln.

- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.

Darüber hinaus können Sie ...

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

4.3.1 Daten sammeln

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

Darüber hinaus können Sie allen PCs vom Gerät eine gültige IP-Konfiguration zuweisen lassen, so dass zeitaufwändiges Konfigurieren Ihres LANs entfällt. Gegebenenfalls können Sie die Beispielwerte übernehmen.

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

- Grundkonfiguration (obligatorisch sofern sich Ihr Gerät im Auslieferungszustand befindet)
- Internetzugang (optional)
- Wireless LAN (optional, nur für **bintec R230aw** und **bintec R232bw**).

In den folgenden Tabellen 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:

Basisinformationen

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

Internetzugang über ADSL

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

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

Daten für den Internetzugang über ADSL

Zugangsdaten	Beispielwert	Ihre Werte
Provider-Name	*GoInternet*	
Protokoll	*PPP over Ethernet (PPPoE)*	
Enkapsulierung	*bridged-no-fcs*	
VPI (Virtual Path Identifier)	*1*	
VCI (Virtual Circuit Identifier)	*32*	
Ihr Benutzername	*MyName*	
Passwort	*TopSecret*	

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

Zusätzliche Informationen für T-Online

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

Hinweis

Geben Sie bei der Konfiguration eines T-Online-Internetzugangs in das Feld **Benutzername** nacheinander und ohne Leerzeichen folgende Nummern ein: Anschlusskennung (12-stellig) + T-Online Nummer (meist 12-stellig) + Mitbenutzernummer (für den Hauptnutzer immer 0001). Sollte Ihre T-Online Nummer weniger als 12 Stellen enthalten, muss zwischen der T-Online Nummer und der Mitbenutzernummer das Zeichen "#" stehen. Wenn Sie T-DSL nutzen, müssen Sie dieser Zahlenfolge noch die Endung "@t-online.de" hinzufügen. Ihr Benutzername könnte dann so aussehen: 000123456789061123456 78#0001@t-online.de

Wireless LAN (nur bintec R230aw und bintec R232bw)

Sie können Ihr Gerät als Access-Point betreiben und somit mittels WLAN (Wireless LAN) einzelne Arbeitsstationen (z. B. Laptops, PCs mit Wireless-Karte oder Wireless-Adapter) per Funk in Ihr lokales Netzwerk einbinden und miteinander kommunizieren lassen. Die Tabelle “Daten für die Wireless LAN Konfiguration” zeigt die Angaben, die dazu benötigt werden.

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.

Beachten Sie dazu Folgendes:

- Folgen Sie den Sicherheitshinweisen bei der Konfiguration Ihres WLANs.
- Bitte lesen Sie auch **Sicherheit im Funk-LAN** herausgegeben vom Bundesministerium für Sicherheit in der Informationstechnik, siehe *http://www.bsi.de* .

Daten für die Wireless LAN Konfiguration

Zugangsdaten	Beispielwert	Ihre Werte
Preshared Key für WPA2-PSK	ohne Vorgabe	
Aufstellungsort Ihres Systems	*Germany*	
Kanal, der für WLAN verwendet werden soll	*11*	
Netzwerkname (SSID) für Ihr WLAN	ohne Vorgabe	
Sichtbarkeit der SSID im Funknetz	*nicht sichtbar*	
Sicherheitseinstellung	*WPA2-PSK*	

4.3.2 PC einrichten

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

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

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

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

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

Wenn Sie nun alle Fenster mit **OK** schließen, wird Ihrem PC eine passende IP-Konfiguration vom Gerät übermittelt und dieser erfüllt nun alle Voraussetzungen zur Konfiguration Ihres Geräts. Ebenso kann der Rechner über das Gerät auf das Internet zugreifen, sobald ein Internetzugang eingerichtet ist.

Hinweis

Zur Konfiguration können Sie nun das **Funkwerk Configuration Interface** aufrufen, indem Sie in einem unterstützen Browser (Internet Explorer 6 oder 7, Mozilla Firefox ab Version 1.2) die IP-Adresse Ihres Gerätes eingeben (192.168.0.254) und sich mit den voreingestellten Anmeldedaten (**User**: *admin*, **Password**: *funkwerk*) anmelden.

4.3.3 Systempasswort ändern

Alle **bintec**-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.

4.4 Internetverbindung einrichten

Sie können mit Ihrem Gerät unterschiedliche Arten von Internetverbindungen aufbauen, die Konfiguration der beiden häufigsten werden im Folgenden beschrieben, bei der Konfiguration weiterer Verbindungsarten hilft Ihnen der Internet-Assistent des **Funkwerk Configuration Interface**.

4.4.1 Internetverbindung über das interne ADSL-Modem

Alle Geräte verfügen über ein integriertes ADSL2+-Modem zum Aufbau einer schnellen Internetverbindung. Zur einfachen Konfiguration eines ADSL-Internetzugangs verfügt das **Funkwerk Configuration Interface** über einen Assistenten, mit dem Sie die Verbindung unkompliziert und schnell einrichten können. Eine Auswahl an vorkonfigurierten Zugängen der wichtigsten Anbieter (T-Home, Arcor) vereinfacht die Konfiguration noch einmal.

(1) Gehen Sie im **Funkwerk Configuration Interface** in das Menü **Assistenten**->**Internetzugang**.

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

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

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

4.4.2 Andere Internetverbindungen

Neben einem ADSL-Anschluss über das interne ADSL2+-Modem können Sie Ihr Gerät noch über weitere Verbindungsarten mit dem Internet verbinden, so etwa über ein externes Modem (z. B. ein Kabelmodem) oder ein externes Gateway. Bei dieser Art von Konfigurationen unterstützt Sie der entsprechende Assistent des **Funkwerk Configuration Interface**. Sie finden den Internet-Assistenten neben weiteren Assistenten zur vereinfachten Konfiguration unterschiedlicher Anwendungen an oberster Stelle des Menübaums unter **Assistenten**.

4.4.3 Konfiguration prüfen

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

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

(1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. *192.168.0.254*). Es erscheint ein Fenster mit dem Hinweis `"Antwort von..."`.

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

Hinweis

Durch eine Fehlkonfiguration der Geräte im LAN kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob das Gerät Verbindungen nur zu gewollten Zeiten aufbaut! Beobachten Sie die Leuchtanzeigen Ihres Geräts (Leuchtanzeige ISDN, ADSL und die der Ethernet-Schnittstellen, an denen Sie WANs angeschlossen haben).

4.5 Wireless LAN einrichten

Gehen Sie folgendermaßen vor, um ihr Gerät (nur bintec **bintec R230aw**, und **bintec R232bw**) als Access Point zu nutzen:

(1) Gehen Sie im **Funkwerk Configuration Interface** 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 konfigurieren, 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.

4.6 Softwareaktualisierung

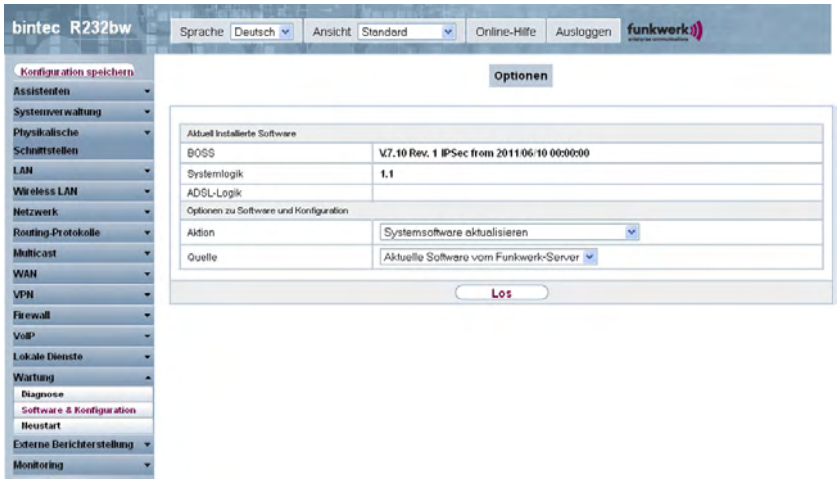
Die Funktionsvielfalt von **bintec**-Geräten wird permanent erweitert. Diese Erweiterungen stellt Ihnen Funkwerk Enterprise Communications GmbH stets kostenlos zur Verfügung. Die Überprüfung auf neue Software-Versionen und die Aktualisierung können einfach über das **Funkwerk Configuration Interface** 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 Funkwerk-Server*

(3) Bestätigen Sie mit **Los**.



Das Gerät verbindet sich nun mit dem Download-Server der Funkwerk Enterprise Communications 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 Reset

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

Dabei werden fast alle bestehenden Konfigurationsdaten ignoriert, nur die aktuellen Benutzer-Passwörter bleiben erhalten. Auf dem Gerät gespeicherte Konfigurationen werden nicht gelöscht und können nach dem Neustart des Geräts ggf. wieder geladen werden.

Gehen Sie folgendermaßen vor:

(1) Trennen Sie Ihr Gerät vom Strom.

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

(3) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.

(4) Achten Sie auf die LEDs:
- Zunächst leuchten die LEDs *Power* und *Status* auf.
- Dann blinken die Ethernet-LEDs (*1* bis *4*) für die Ports, die an das Ethernet angeschlossen sind.
- Das Gerät durchläuft die Boot-Sequenz.
- Lassen Sie nach fünfmaligem Blinken der *Status* -LED die **Reset**-Taste los.

Sollen beim Zurücksetzen des Geräts auch sämtliche Benutzerpasswörter in den Auslieferungszustand zurückgesetzt und gespeicherte Konfigurationen gelöscht werden, gehen Sie wie folgt vor:

- Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Starten Sie Ihr Gerät neu und verfolgen Sie die Boot-Sequenz. Starten Sie den BOOTmonitor und wählen Sie die Option **(4) Konfiguration löschen** und folgen Sie den Anweisungen.

oder

- Führen Sie die oben beschriebene Reset-Prozedur mit der **Reset**-Taste aus. Stellen Sie anschließend eine serielle Verbindung oder eine Telnet-Verbindung (Telnet: Verwenden Sie die IP-Adresse des Auslieferungszustands) zu Ihrem Gerät her. Geben Sie auf der Kommandozeile beim Anmeldeprompt *erase bootconfig* als **Login** ein. Lassen Sie das Passwort leer und drücken Sie die Eingabetaste. Das Gerät durchläuft erneut die Boot-Sequenz.

Hinweis

Wenn Sie über das **Funkwerk Configuration Interface** (Menü **Wartung**->**Software &Konfiguration**) 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.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab *Grundkonfiguration* auf Seite 10 beschrieben.

Kapitel 6 Technische Daten

In diesem Kapitel sind alle Hardware-Eigenschaften der Geräte **bintec R230a**, **bintec R230b**, **bintec R230aw**, **bintec R232a**, **bintec R232b** und **bintec R232bw** zusammengefasst.

6.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	**Software**	**Dokumentation**
bintec R230a	Ethernet-Kabel DSL-Kabel Serielles Anschlusskabel Steckernetzteil	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD) Release Notes, falls erforderlich Sicherheitshinweise
bintec R230b	Ethernet-Kabel DSL-Kabel Serielles Anschlusskabel Steckernetzteil	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD) Release Notes, falls erforderlich Sicherheitshinweise
bintec R230aw	Ethernet-Kabel DSL-Kabel Serielles Anschlusskabel Steckernetzteil 2 Standardantennen	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD) Release Notes, falls erforderlich Sicherheitshinweise
bintec R232a	Ethernet-Kabel DSL-Kabel ISDN-Kabel	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD)

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
	Serielles Anschlusskabel Steckernetzteil		Release Notes, falls erforderlich Sicherheitshinweise
bintec R232b	Ethernet-Kabel DSL-Kabel ISDN-Kabel Serielles Anschlusskabel Steckernetzteil	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD) Release Notes, falls erforderlich Sicherheitshinweise
bintec R232bw	Ethernet-Kabel DSL-Kabel ISDN-Kabel Serielles Anschlusskabel Steckernetzteil 2 Standardantennen	Companion DVD	Kurzanleitung (gedruckt) Benutzerhandbuch (auf DVD) Release Notes, falls erforderlich Sicherheitshinweise

6.2 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 bintec R230a, bintec R230b, bintec R230aw

Produktname	bintec R230a	bintec R230b	bintec R230aw
Maße und Gewicht:			
Gerätemaße ohne Kabel (B x H x T)	158 mm x 25,7 mm x 123,1 mm	158 mm x 25,7 mm x 123,1 mm	158 mm x 25,7 mm x 123,1 mm
Gewicht	ca. 550 g	ca. 550 g	ca. 550 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1,2 kg	ca. 1,2 kg	ca. 1,2 kg

Produktname	bintec R230a	bintec R230b	bintec R230aw
Speicher	32 MB SDRAM, 8 MB Flash-ROM	32 MB SDRAM, 8 MB Flash-ROM	32 MB SDRAM, 8 MB Flash-ROM
LEDs	11 (1x Power, 4x2 Ethernet, 1x Status, 1x ADSL)	11 (1x Power, 4x2 Ethernet, 1x Status, 1x ADSL)	12 (1x Power, 4x2 Ethernet, 1x WLAN, 1x Status, 1x ADSL)
Leistungsaufnahme Gerät	4,7 Watt	4,7 Watt	4,7 Watt
Spannungsversorgung	12 V DC 500 mA EU PSU	12 V DC 500 mA EU PSU	12 V DC 800 mA EU PSU
Umweltanforderungen:			
Lagertemperatur	-20° bis +70 °C	-20° bis +70 °C	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C	0° bis 40 °C	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:			
ADSL-Schnittstelle	Internes ADSL-Modem für Annex A	Internes ADSL-Modem für Annex B	Internes ADSL-Modem für Annex A
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX
WLAN-Schnittstelle (Antennen)	-		802.11b und 802.11g mit Antenna Diversity

Produktname	bintec R230a	bintec R230b	bintec R230aw
			Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s
Vorhandene Buchsen:			
Serielle Schnittstelle V.24	5-polige MiniUSB-Buchse	5-polige MiniUSB-Buchse	5-polige MiniUSB-Buchse
Ethernet-Schnittstelle	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ADSL-Schnittstelle	RJ11-Buchse	RJ11-Buchse	RJ11-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET TM Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	Dime Manager (auf DVD)	Dime Manager (auf DVD)	Dime Manager (auf DVD)
Mitgelieferte gedruckte Dokumentation	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD
Online-Dokumentation	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz

Allgemeine Produktmerkmale bintec R232a, bintec R232b, bintec R232bw

Produktname	bintec R232a	bintec R232b	bintec R232bw
Maße und Gewicht:			
Gerätemaße ohne Kabel (B x H x T)	189,2 mm x 27 mm x 123,1 mm	189,2 mm x 27 mm x 123,1 mm	189,2 mm x 27 mm x 123,1 mm
Gewicht	ca. 550 g	ca. 550 g	ca. 550 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1,2 kg	ca. 1,2 kg	ca. 1,2 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM	32 MB SDRAM, 8 MB Flash-ROM	32 MB SDRAM, 8 MB Flash-ROM
LEDs	13 (1x Power, 4x2 Ethernet, 1x ETH, 1x Status, 1x ADSL, 1x ISDN)	13 (1x Power, 4x2 Ethernet, 1x ETH, 1x Status, 1x ADSL, 1x ISDN)	14 (1x Power, 4x2 Ethernet, 1x ETH, 1x WLAN, 1x Status, 1x ADSL, 1x ISDN)
Leistungsaufnahme Gerät	4,7 Watt	4,7 Watt	4,7 Watt
Spannungsversorgung	12 V DC 800 mA EU PSU	12 V DC 800 mA EU PSU	12 V DC 800 mA EU PSU
Umweltanforderungen:			
Lagertemperatur	-20° bis +70 °C	-20° bis +70 °C	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C	0° bis 40 °C	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:			
ADSL-Schnittstelle	Internes ADSL-Modem für Annex A	Internes ADSL-Modem für Annex B	Internes ADSL-Modem für Annex B
Serielle Schnittstelle	Fest eingebaut, unter-	Fest eingebaut, unter-	Fest eingebaut, unter-

Produktname	bintec R232a	bintec R232b	bintec R232bw
V.24	stützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	stützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud	stützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX
ISDN-WAN S0	Fest eingebaut	Fest eingebaut	Fest eingebaut
ETH	Zusätzlicher Ethernet Switch-Port	Zusätzlicher Ethernet Switch-Port	Zusätzlicher Ethernet Switch-Port
WLAN-Schnittstelle (Antennen)	-		802.11b und 802.11g mit Antenna Diversity Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s
Vorhandene Buchsen:			
Serielle Schnittstelle V.24	5-polige MiniUSB-Buchse	5-polige MiniUSB-Buchse	5-polige MiniUSB-Buchse
Ethernet-Schnittstelle	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ADSL-Schnittstelle	RJ11-Buchse	RJ11-Buchse	RJ11-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET TM Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec

Produktname	bintec R232a	bintec R232b	bintec R232bw
Mitgelieferte Software	Dime Manager (auf DVD)	Dime Manager (auf DVD)	Dime Manager (auf DVD)
Mitgelieferte gedruckte Dokumentation	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD	Kurzanleitung und Sicherheitshinweise Benutzerhandbuch funkwerk Dime Manager auf DVD
Online-Dokumentation	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz

6.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die LEDs von **bintec R230a** / **bintec R230b** sind folgendermaßen angeordnet:

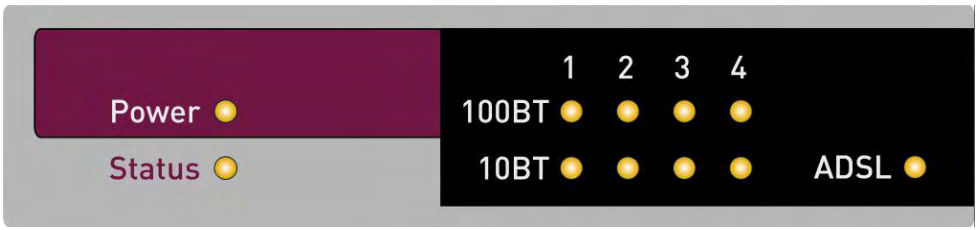


Abb. 3: LEDs von **bintec R230a** / **bintec R230b**

Im Betriebsmodus zeigen die LEDs von **bintec R230a** / **bintec R230b** folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	an	Das Gerät wird gestartet.
	blinkend	Das Gerät ist aktiv.

LED	Status	Information
1 bis 4	an	Das Gerät ist an das Ethernet angeschlossen (100 Mbit/s bzw. 10 Mbit/s).
	blinkend	Datenverkehr über die Ethernet-Schnittstelle (100 Mbit/s bzw. 10 Mbit/s).
ADSL	an	ADSL-Verbindung ist aktiv.

Die LEDs von **bintec R230aw** sind folgendermaßen angeordnet:

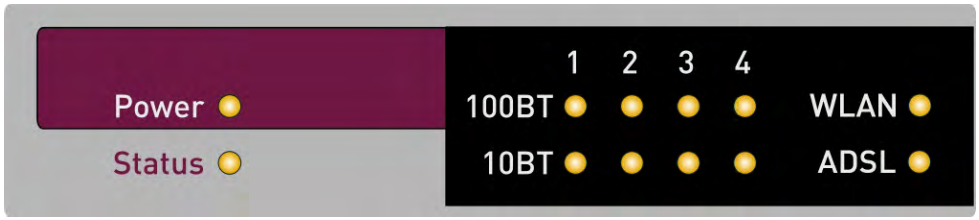


Abb. 4: LEDs von **bintec R230aw**

Im Betriebsmodus zeigen die LEDs von **bintec R230aw** folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	an	Das Gerät wird gestartet.
	blinkend	Das Gerät ist aktiv.
1 bis 4	an	Das Gerät ist an das Ethernet angeschlossen (100 Mbit/s bzw. 10 Mbit/s).
	blinkend	Datenverkehr über die Ethernet-Schnittstelle (100 Mbit/s bzw. 10 Mbit/s).
WLAN	an	Das WLAN-Modul ist aktiv.
	blinkend	Datenverkehr über die WLAN-Schnittstelle.
ADSL	an	ADSL-Verbindung ist aktiv.

Die LEDs von **bintec R232a** / **bintec R232b** sind folgendermaßen angeordnet:

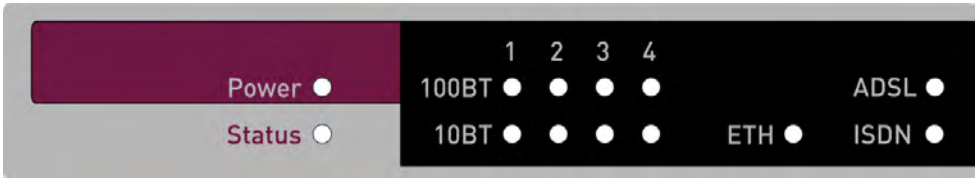


Abb. 5: LEDs von **bintec R232a** / **bintec R232b**

Im Betriebsmodus zeigen die LEDs von **bintec R232a** / **bintec R232b** folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	an	Das Gerät wird gestartet.
	blinkend	Das Gerät ist aktiv.
1 bis 4	an	Das Gerät ist an das Ethernet angeschlossen (100 Mbit/s bzw. 10 Mbit/s).
	blinkend	Datenverkehr über die Ethernet-Schnittstelle (100 Mbit/s bzw. 10 Mbit/s).
ETH	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ADSL	an	ADSL-Verbindung ist aktiv.
ISDN	an	Ein B-Kanal wird benutzt.
	blinkend	Beide B-Kanäle werden benutzt.

Die LEDs von **bintec R232bw** sind folgendermaßen angeordnet:

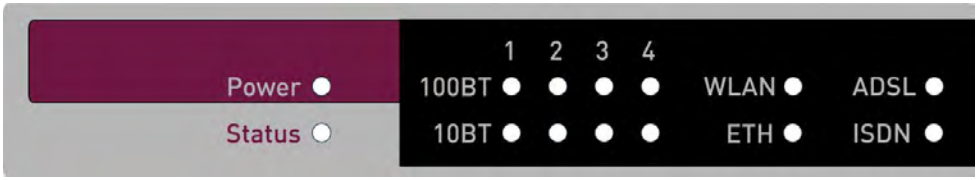


Abb. 6: LEDs von **bintec R232bw**

Im Betriebsmodus zeigen die LEDs von **bintec R232bw** folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	an	Das Gerät wird gestartet.
	blinkend	Das Gerät ist aktiv.
1 bis 4	an	Das Gerät ist an das Ethernet angeschlossen (100 Mbit/s bzw. 10 Mbit/s).
	blinkend	Datenverkehr über die Ethernet-Schnittstelle (100 Mbit/s bzw. 10 Mbit/s).
WLAN	an	Das WLAN-Modul ist aktiv.
	blinkend	Datenverkehr über die WLAN-Schnittstelle.
ETH	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ADSL	an	ADSL-Verbindung ist aktiv.
ISDN	an	Ein B-Kanal wird benutzt.
	blinkend	Beide B-Kanäle werden benutzt.

6.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts.

bintec R230a und **bintec R230b** verfügen über einen 4-Port Ethernet Switch, eine ADSL-Schnittstelle sowie über eine serielle Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

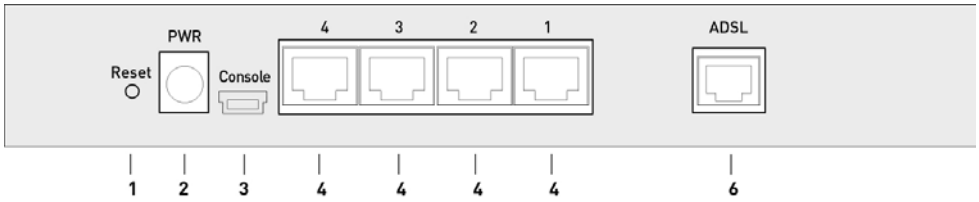


Abb. 7: **bintec R230a** / **bintec R230b** *Rückseite*

bintec R230a / bintec R230b Rückseite

1	Reset	Reset-Taste
2	PWR	Buchse für Steckernetzteil
3	Console	Serielle Schnittstelle
4	4/3/2/1	10/100 Base-T Ethernet-Schnittstelle
6	ADSL	ADSL-Schnittstelle

bintec R230aw verfügt über einen 4-Port Ethernet Switch, eine ADSL-Schnittstelle sowie über eine serielle Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

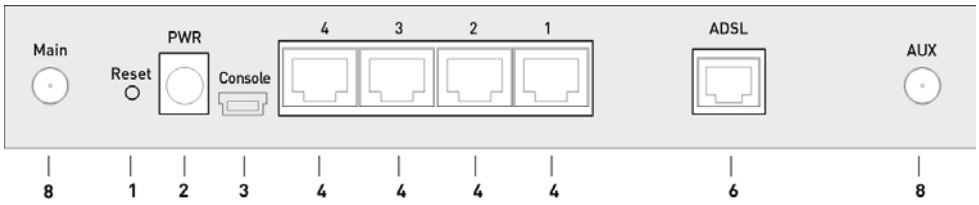


Abb. 8: **bintec R230aw** *Rückseite*

bintec R230aw Rückseite

1	Reset	Reset-Taste

2	PWR	Buchse für Steckernetzteil
3	Console	Serielle Schnittstelle
4	4/3/2/1	10/100 Base-T Ethernet-Schnittstelle
6	ADSL	ADSL-Schnittstelle
8	Main/AUX	RSMA-Anschluss

bintec R232a und **bintec R232b** verfügen über einen 4-Port Ethernet Switch, eine ADSL-Schnittstelle sowie über eine serielle Schnittstelle. **bintec R232a** und **bintec R232b** verfügen weiterhin über einen separaten ETH/DMZ-Port und eine ISDN-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

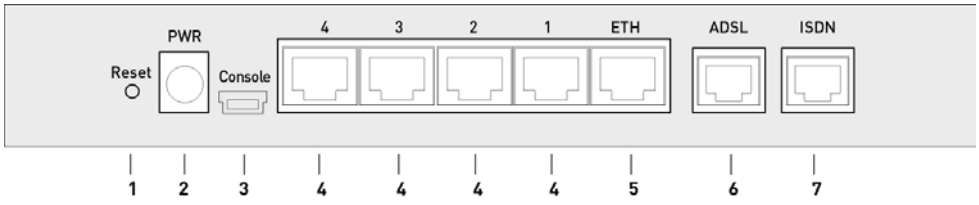


Abb. 9: **bintec R232a** / **bintec R232b** *Rückseite*

bintec R232a / bintec R232b Rückseite

1	Reset	Reset-Taste
2	PWR	Buchse für Steckernetzteil
3	Console	Serielle Schnittstelle
4	4/3/2/1	10/100 Base-T Ethernet-Schnittstelle
5	ETH	Ethernet-Schnittstelle
6	ADSL	ADSL-Schnittstelle
7	ISDN	ISDN-Schnittstelle

bintec R232bw verfügt über einen 4-Port Ethernet Switch, eine ADSL-Schnittstelle sowie über eine serielle Schnittstelle. **bintec R232bw** verfügt weiterhin über einen separaten ETH/DMZ-Port und eine ISDN-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

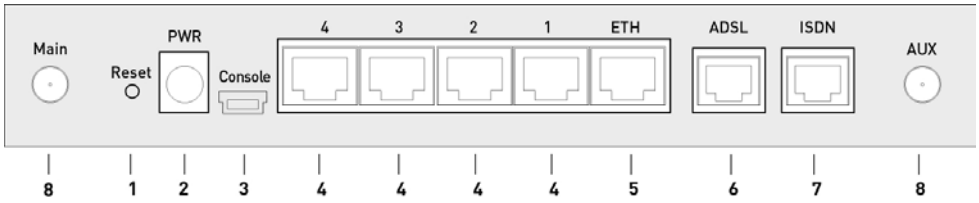


Abb. 10: **bintec R232bw** *Rückseite*

bintec R232bw Rückseite

1	Reset	Reset-Taste
2	PWR	Buchse für Steckernetzteil
3	Console	Serielle Schnittstelle
4	4/3/2/1	10/100 Base-T Ethernet-Schnittstelle
5	ETH	Ethernet-Schnittstelle
6	ADSL	ADSL-Schnittstelle
7	ISDN	ISDN-Schnittstelle
8	Main/AUX	RSMA-Anschluss

6.5 Pin-Belegungen

6.5.1 Serielle Schnittstelle

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

Die Schnittstelle ist als 5-polige MiniUSB-Buchse ausgeführt.

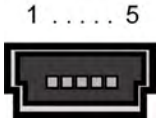


Abb. 11: 5-polige MiniUSB-Buchse

Die Pin-Belegung ist wie folgt:

Pin-Belegung der MiniUSB-Buchse

Pin	Funktion
1	Nicht genutzt
2	TxD

Pin	Funktion
3	RxD
4	Nicht genutzt
5	GND

6.5.2 Ethernet-Schnittstelle

Die Geräte verfügen über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch. Dieser dient zur Anbindung einzelner PCs oder weiterer Switches.

Der Anschluss erfolgt über eine RJ45-Buchse. **bintec R232a**, **bintec R232b** und **bintec R232bw** verfügen weiterhin über eine fünfte Ethernet-Schnittstelle.

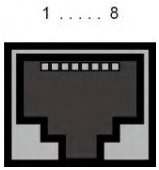


Abb. 12: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für LAN-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

6.5.3 ADSL-Schnittstelle

Die ADSL-Schnittstelle wird mittels eines RJ11-Steckers angebunden. Das mitgelieferte Kabel verbindet den RJ11-Stecker, der für das Gerät benötigt wird, mit einem RJ11-Stecker, der für die meisten ADSL-Splitter benötigt wird.

Nur die inneren beiden Pins werden für die ADSL-Verbindung verwendet:

Abb. 13: ADSL-Schnittstelle (RJ11)

Die Pin-Zuordnung für die ADSL-Schnittstelle (RJ11-Buchse) ist wie folgt:

RJ11-Buchse für ADSL-Anschluss

Pin	Funktion
1	Nicht genutzt
2	a
3	b
4	Nicht genutzt

6.5.4 ISDN-S0-Schnittstelle

bintec R232a, **bintec R232b** und **bintec R232bw** verfügen über eine zusätzliche ISDN-S0-Schnittstelle, die z. B. für Backup-Funktionen genutzt werden kann.

Der Anschluss erfolgt über eine RJ45-Buchse.

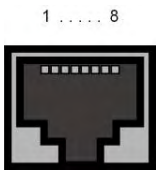


Abb. 14: ISDN-S0 -BRI-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die ISDN-S0-BRI-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für ISDN-Anschluss

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

6.6 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 7 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

7.1 Zugangsmöglichkeiten

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

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

- Über Ihr LAN
- Über die serielle Schnittstelle
- Über eine ISDN-Verbindung (nur **bintec R232a**, **bintec R232b** und **bintec R232bw**)

7.1.1 Zugang über LAN

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

Achtung

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

7.1.1.1 HTTP/HTTPS

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

- *http://192.168.0.254*

  oder

- *https://192.168.0.254*

7.1.1.2 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 46.

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 46.

7.1.1.3 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 45).

(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 **Funkwerk Configuration Interface** auf und melden Sie sich an Ihrem Gerät an (siehe *Das Funkwerk Configuration Interface aufrufen* auf Seite 49).

(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 45 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 45 fort.

Hinweis

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

7.1.2 Zugang über die serielle Schnittstelle

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

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

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

Windows

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

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

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

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

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

Überprüfen

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

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

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

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

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

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

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

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

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

Unix

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

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

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

7.1.3 Zugang über ISDN

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

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

Hinweis

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

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

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

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

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

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

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

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

Fahren Sie fort mit *Anmelden zur Konfiguration* auf Seite 46.

7.2 Anmelden

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

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

7.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

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

Um Konfigurationsänderungen vorzunehmen und zu speichern, müssen Sie sich mit dem Benutzernamen `admin` einloggen. Auch die Zugangsdaten (Benutzernamen und Passwörter) können geändert werden, wenn sich der Benutzer mit dem Benutzernamen `admin` eingloggt. Aus Sicherheitsgründen sind Passwörter 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**-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!

7.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 39 beschrieben.

Funkwerk Configuration 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 **Funkwerk Configuration Interface**.

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. `funkwerk`, und bestätigen Sie mit der **Eingabetaste**.

Ihr Gerät meldet sich mit dem Eingabeprompt, z. B. `r232bw:>`. 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**.

7.3 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:

- **Funkwerk Configuration Interface**
- Assistent
- SNMP-Shell-Kommandos

Hinweis

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

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

Verbindungs- und Konfigurationsarten

Verbindungsart	Mögliche Konfigurationsarten
LAN	Assistent, **Funkwerk Configuration Interface**, Shell-Kommandos
Serielle Verbindung	Shell-Kommandos

Im Folgenden wird die Konfiguration anhand des **Funkwerk Configuration Interface** beschrieben.

Hinweis

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

7.3.1 Funkwerk Configuration Interface

Das **Funkwerk Configuration Interface** 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 **Funkwerk Configuration Interface** 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 *ww.funkwerk-ec.com* heruntergeladen und auf dem Gerät installiert werden. Gehen Sie hierzu vor wie in *Optionen* auf Seite 438 beschrieben.

Die Einstellungsänderungen, die Sie mit dem **Funkwerk Configuration Interface** 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 **Funkwerk Configuration Interface** können Sie ebenfalls die wichtigsten Funktionsparameter Ihres Geräts überwachen.

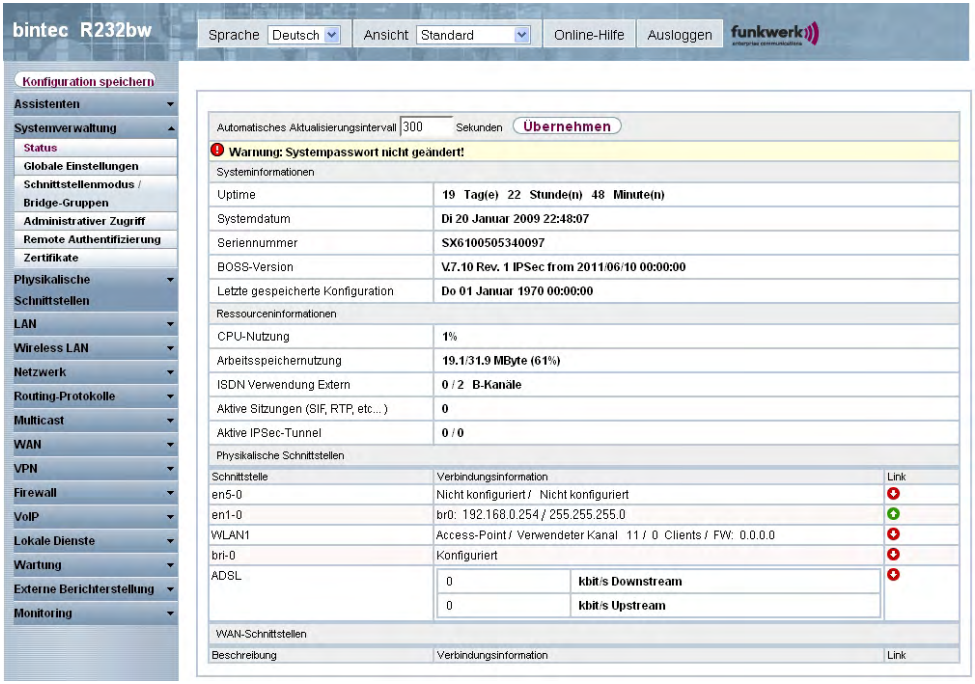


Abb. 16: **Funkwerk Configuration Interface** *Startseite*

7.3.1.1 Das Funkwerk Configuration Interface aufrufen

(1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe *Aufstellen und Anschließen* auf Seite 6).

(2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe *PC einrichten* auf Seite 14).

(3) Öffnen Sie einen Webbrowser.

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

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

Sie befinden sich nun im Statusmenü des **Funkwerk Configuration Interface** Ihres Geräts (siehe *Status* auf Seite 68).

7.3.1.2 Bedienelemente

Funkwerk Configuration Interface Fenster

Das **Funkwerk Configuration Interface** Fenster ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

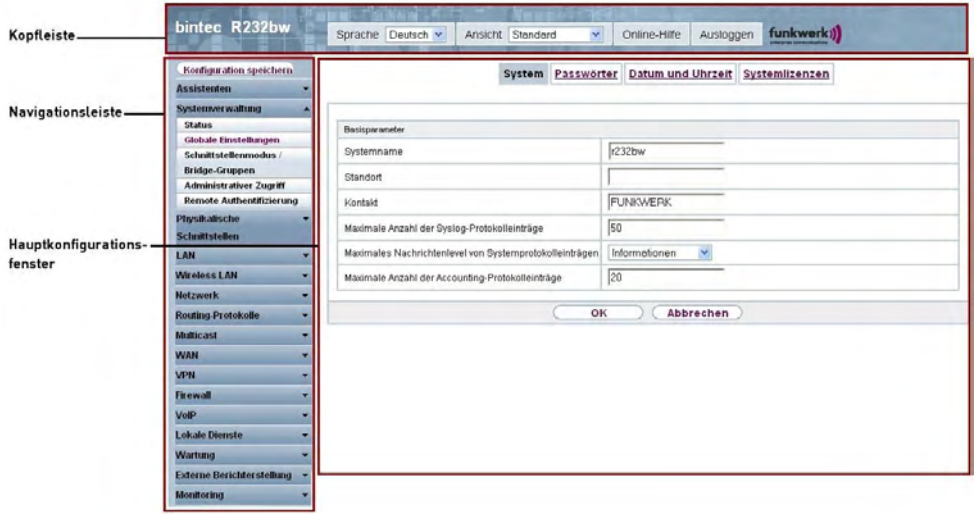


Abb. 17: Bereiche des **Funkwerk Configuration Interface**

Kopfleiste

Abb. 18: **Funkwerk Configuration Interface** *Kopfleiste*

Funkwerk Configuration Interface Kopfleiste

Menü	Funktion
Sprache Deutsch	**Sprachauswahl**: Wählen Sie in dem Dropdown-Menü die gewünschte Sprache aus, in der das **Funkwerk Configuration Interface** 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.
	Online-Hilfe: Klicken Sie auf diese Schaltfläche, wenn Sie zu

Menü	Funktion
Online-Hilfe	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. 19: Konfiguration speichern Schaltfläche

Abb. 20: 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 FCI 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 **Funkwerk Configuration Interface** aufrufen, erscheint nach der Anmeldung zunächst die Statusseite Ihres Geräts. Auf dieser werden die wichtigsten Daten Ihres Gerätes auf einen Blick sichtbar.

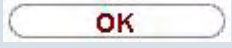
Hauptkonfigurationsfenster

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 **Funkwerk Configuration Interface** ausführen können, werden mit Hilfe folgender Schaltflächen ausgelöst:

Funkwerk Configuration Interface 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.

Schaltfläche	Funktion
Neu	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.
Hinzufügen	Fügt einen Eintrag zu einer internen Liste hinzu.

Funkwerk Configuration Interface Schaltflächen für spezielle Funktionen

Schaltfläche	Funktion
Finden	Im Menü **Access-Point-Suche** starten Sie mit dieser Schaltfläche die automatische Erkennung aller im Netzwerk vorhandener und per Ethernet verbundener Access-Points.
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.
Verb. beenden	Im Menü **Monitoring**->**ISDN/Modem**->**Aktuelle Anrufe** werden durch Drücken dieser Schaltfläche die in der Spalte  ausgewählten aktiven Rufe beendet.

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

Funkwerk Configuration Interface 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 ei-

Symbol	Funktion
	ner Verbindung.
	Kennzeichnet den Status "Aktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Inaktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Blockiert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet 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:

Funkwerk Configuration Interface 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.

Menü	Funktion
Konfigurationselemente	Einige Listen enthalten Konfigurationselemente. So können Sie direkt in der Liste die Konfiguration des entsprechenden Listeneintrags ändern.

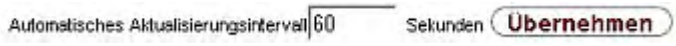


Abb. 21: Konfiguration des Aktualisierungsintervalls

Abb. 22: Liste filtern

Struktur der Funkwerk Configuration Interface Konfigurationsmenüs

Die Menüs des **Funkwerk Configuration Interface** enthalten folgende Grundstrukturen:

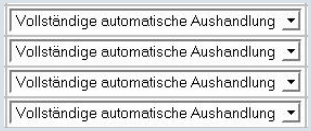
Funkwerk Configuration Interface Menüstruktur

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:

Funkwerk Configuration Interface Konfigurationselemente

Menü	Funktion
Eingabefelder	z. B. leeres Textfeld

Menü	Funktion
	 Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.
Radiobuttons	z. B.  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 **Funkwerk Configuration Interface** verändern, kann dies Inkonsistenzen oder Fehlfunktionen verursachen. Daher wird empfohlen, die Konfiguration mit dem Setup Tool fortzuführen.

7.3.1.3 Funkwerk Configuration Interface 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.funkwerk-ec.com*.

Das **Funkwerk Configuration Interface** enthält folgende Menüs:

Assistenten

Menü	Funktion
Erste Schritte	In diesem Menü nehmen Sie die grundlegenden Einstellungen vor, die nötig sind um Ihr Gateway in Ihr Lokales Netzwerk (LAN) zu integrieren.
Internetzugang	Der Assistent führt Sie durch die einzelnen Konfigurationsschritte, um Ihr Lokales Netzwerk (LAN) an das Internet anzuschlie-

Menü	Funktion
	ßen.
VPN	In diesem Menü werden Sie durch alle Einstellungen geführt, die notwendig sind um Ihre LAN-LAN Verbindung als Virtual Private Network (VPN) einzurichten.
Wireless LAN	Bei Wireless LAN handelt es sich um den Aufbau eines Netzwerkes mittels Funktechnik.
VoIP PBX im LAN	Der Assistent wird für bestimmte Telefonanlagen im LAN wie z. B. **Hybird** benötigt, um die SIP-Kompatibilität zu gewährleisten. Dazu erfolgt die Kommunikation nach außen über eine einzige IP-Adresse, NAT wird als full-cone NAT realisiert.

Systemverwaltung

Menü	Funktion
Status	In diesem Menü werden allgemeine Informationen über Ihr Gerät auf einen Blick angezeigt. Hierzu gehören u. a. Seriennummer, Softwareversion, aktuelle Speicher- und Prozessornutzung, Status der physikalischen Schnittstellen und die letzten zehn Systemmeldungen.
Globale Einstellungen	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen Ihres Geräts ein, wie z. B. Systemname, -datum, -uhrzeit und Passwörter. Sie können weiterhin Lizenzen verwalten, die für die Verwendung bestimmter Funktionen notwendig sind.
Schnittstellenmodus / Bridge-Gruppen	In diesem Menü definieren Sie, in welchem Modus die Schnittstellen Ihres Geräts betrieben werden sollen (Routing oder Bridging) und können ggf. Bridge-Gruppen definieren.
Administrativer Zugriff	In diesem Menü konfigurieren Sie die Zugangsmöglichkeiten zu den einzelnen Schnittstellen.
Remote Authentifizierung	In diesem Menü konfigurieren Sie die Authentifizierung über einen RADIUS-Server oder einen TACACS+-Server.
Zertifikate	In diesem Menü können Sie Schlüssel generieren, importieren und zertifizieren lassen.

Physikalische Schnittstellen

Menü	Funktion
Ethernet-Ports	In diesem Menü konfigurieren Sie die Ethernet-Schnittstellen Ihres Geräts. Hier wählen Sie z. B. die Geschwindigkeit und die Art der Schnittstelle aus.
ISDN-Ports	Nur für **R232a** , **R232b** und **R232bw**. In diesem Menü konfigurieren Sie die ISDN- Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluss Ihr Gerät angeschlossen ist.
ADSL-Modem	In diesem Menü nehmen Sie grundlegende Einstellungen Ihrer ADSL-Verbindung vor.

LAN

Menü	Funktion
IP-Konfiguration	In diesem Menü nehmen Sie die IP-Konfiguration der LAN-Schnittstellen Ihres Geräts vor.
VLAN	In diesem Menü konfigurieren Sie die VLANs.

Wireless LAN

Menü	Funktion
WLAN	In diesem Menü konfigurieren Sie Ihr Funkmodul als Access Point oder als Bridge.
Verwaltung	In diesem Menü nehmen Sie grundlegende WLAN-Einstellungen vor.

Netzwerk

Menü	Funktion
Routen	In diesem Menü tragen Sie weitere Routen ein.
NAT	In diesem Menü konfigurieren Sie die NAT-Firewall (NAT, Network Address Translation).
Lastverteilung	In diesem Menü konfigurieren Sie applikationsgesteuertes Bandbreitenmanagement.

Menü	Funktion
QoS	In diesem Menü konfigurieren Sie alle Einstellungen zu "Quality of Service".
Zugriffsregeln	In diesem Menü werden Zugriffe auf Daten und Funktionen eingegrenzt.

Routing-Protokolle

Menü	Funktion
RIP	In diesem Menü konfigurieren Sie die dynamische Aktualisierung der Routing-Tabelle mittels RIP.

Multicast

Menü	Funktion
Allgemein	In diesem Menü aktivieren oder deaktivieren Sie das Multicast Routing.
IGMP	In diesem Menü konfigurieren Sie die Schnittstellen, auf denen IGMP aktiv sein soll.
Weiterleiten	In diesem Menü legen Sie fest, welche Multicast-Gruppen zwischen den Schnittstellen Ihres Geräts immer weitergeleitet werden.

WAN

Menü	Funktion
Internet + Einwählen	In diesem Menü definieren Sie Internetverbindungen für die verschiedenen Verbindungsprotokolle oder Einwahlverbindungen.
ATM	In diesem Menü nehmen Sie die Konfiguration der ATM-Profile vor, die für alle ADSL-Verbindungen benötigt werden, sowie das Verbindungsmonitoring (OAM) und ATM QoS.
Real Time Jitter Control	In diesem Menü können Sie die Übertragung von Sprachdaten-Paketen bei geringer Bandbreite optimieren.

VPN

Menü	Funktion
IPSec	In diesem Menü konfigurieren Sie VPN-Verbindungen über IPSec.

Menü	Funktion
L2TP	In diesem Menü konfigurieren Sie die Verwendung von L2TP (Layer 2 Tunneling Protocol).
PPTP	In diesem Menü konfigurieren Sie einen verschlüsselten PPTP-Tunnel.
GRE	In diesem Menü wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.

Firewall

Menü	Funktion
Richtlinien	In diesem Menü konfigurieren Sie die Filterregeln der Firewall.
Schnittstellen	In diesem Menü können Sie die zu filternden Schnittstellen in Gruppen zusammenfassen.
Adressen	In diesem Menü können Sie zu filternde Adress-Aliase anlegen.
Dienste	In diesem Menü können Sie zu filternde Service-Aliase anlegen.

VoIP

Menü	Funktion
SIP	In diesem Menü konfigurieren Sie einen Netzübergang zwischen unterschiedlichen Telekommunikationsnetzen.
RTSP	In diesem Menü konfigurieren Sie die Verwendung des RealTime Streaming Protokolls.

Lokale Dienste

Menü	Funktion
DNS	In diesem Menü konfigurieren Sie die Namensauflösung.
HTTPS	In diesem Menü konfigurieren sie Port und Zertifikat für eine Konfigurationssitzung über HTTPS.
DynDNS-Client	In diesem Menü konfigurieren Sie die dynamische Namensauflösung.
DHCP-Server	In diesem Menü konfigurieren Sie Ihr Gerät als DHCP-Server.

Menü	Funktion
Web-Filter	In diesem Menü konfigurieren Sie die Verwendung des URL-basierten Proventia Web Filters der Fa. ISS (*www.iss.net*).
CAPI-Server	In diesem Menü konfigurieren Sie Ihr Gerät als CAPI-Server.
Scheduling	In diesem Menü konfigurieren Sie zeitabhängige Standardaktionen Ihres Geräts.
Überwachung	In diesem Menü konfigurieren Sie die Überwachung von Schnittstellen oder von Hosts im Netzwerk.
ISDN-Diebstahlsicherung	In diesem Menü können Sie die Funktion ISDN-Diebstahlsicherung schnittstellenabhängig konfigurieren.
Funkwerk Discovery	In diesem Menü können Sie Management-Funktionen für **bintec** Access Points konfigurieren.
UPnP	In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.
Hotspot-Gateway	In diesem Menü konfigurieren Sie das bintec Hotspot Gateway.
BRRP	In diesem Menü können Sie eine redundante Netzwerkumgebung konfigurieren.

Wartung

Menü	Funktion
Diagnose	In diesem Menü können Sie die Erreichbarkeit von Hosts, DNS Servern oder Routen testen.
Software &Konfiguration	In diesem Menü verwalten Sie den Softwarestand, die Konfigurationsdateien und die Sprachversionen Ihres Geräts.
Neustart	In diesem Menü können Sie den Neustart des Geräts initiieren.

Externe Berichterstellung

Menü	Funktion
Systemprotokoll	In diesem Menü konfigurieren Sie den Host, zu dem die intern auf dem Gerät protokollierten Daten zur Speicherung und Weiterverarbeitung weitergeleitet werden sollen.
IP-Accounting	In diesem Menü legen Sie fest, für welche Schnittstellen Ac-

Menü	Funktion
	counting-Meldungen generiert werden sollen.
E-Mail-Benachrichtigung	In diesem Menü werden dem Administrator je nach Konfiguration Emails gesendet, sobald relevante Syslog Meldungen auftreten.
SNMP	In diesem Menü konfigurieren Sie, ob das Gerät auf externe SNMP-Zugriffe lauschen und SNMP Traps senden soll.
Activity Monitor	In diesem Menü konfigurieren Sie die Überwachung Ihres Geräts mit dem Windows-Tool Activity Monitor.

Monitoring

Menü	Funktion
Internes Protokoll	In diesem Menü werden die Systemmeldungen angezeigt.
IPSec	In diesem Menü werden die aktuell aktiven IPSec-Verbindungen und Verbindungsstatistiken angezeigt.
ISDN/Modem	In diesem Menü werden die ISDN-Verbindungen angezeigt.
Schnittstellen	In diesem Menü werden Verbindungsstatistiken und der Status aller Schnittstellen angezeigt.
WLAN	In diesem Menü können Sie die WLAN-Verbindungsstatistiken einsehen.
Bridges	In diesem Menü können Sie die aktuellen Werte der konfigurierten Bridges einsehen.
Hotspot-Gateway	In diesem Menü wird eine Liste aller bintec Hotspot Benutzer angezeigt.
QoS	In diesem Menü werden Statistiken für alle Schnittstellen angezeigt, für die QoS konfiguriert wurde.

SNMP-Browser

Wenn Sie in der Kopfleiste unter **Ansicht** die Option `SNMP-Browser` auswählen, erhalten Sie eine HTML-Ansicht aller systeminternen MIB-Tabellen und können die gespeicherten Werte verändern. Diese Ansicht ist nur für die professionelle Konfiguration und das erweiterte Monitoring vorgesehen.

SNMP (Simple Network Management Protocol) ist ein Protokoll, das den Zugriff für die

Konfiguration Ihres Geräts ermöglicht. Alle Konfigurationsparameter werden in der sog. MIB (Management Information Base) in Form von MIB-Tabellen und MIB-Variablen gespeichert. Diese können Sie über den SNMP-Browser direkt lesen und verändern.

Achtung

Diese Konfigurationsmethode setzt vertiefte Systemkenntnisse über Funkwerk-Geräte voraus!

7.3.2 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.

7.4 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. Seriennummer, MAC-Adresse und Software-Versionen.

Der BOOTmonitor wird wie folgt gestartet.

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.

```
Press <sp> for boot monitor or any other key to boot system


R232aw Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by Funkwerk Enterprise Communications GmbH

(1) Boot System
(2) Software Update via TFTP
(3) Software Update via XMODEM
(4) Delete Configuration
(5) Default Bootmonitor Parameters
(6) Show System Information

Your Choice> _
```

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 8 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 9 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.

9.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

- System-Status
- Aktivitäten Ihres Geräts: Ressourcenauslastung, aktive Sessions und Tunnel
- Status und die Grundkonfiguration der LAN-, WAN-, ISDN-, WLAN- und ADSL-Schnittstellen
- die letzten zehn Systemmeldungen

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!

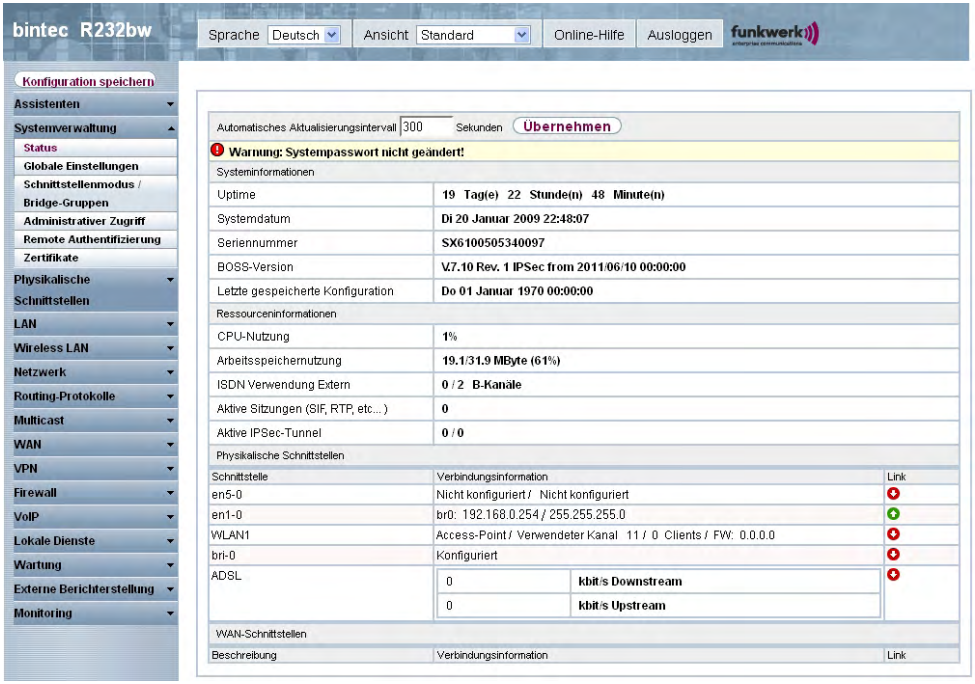


Abb. 24: **Systemverwaltung->Status**

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.

Feld	Wert
ISDN Verwendung Extern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl an zur Verfügung stehenden B-Kanäle für ausgehende Verbindungen.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF, TDRC und IP-Lastverteilung Sessions an.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Weitere Felder im Menü StatusPhysikalische 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 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 • Anzahl der WDS-Links • Softwareversion der Funkkarte

Felder im Menü StatusWAN-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.

9.2 Globale Einstellungen

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

9.2.1 System

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

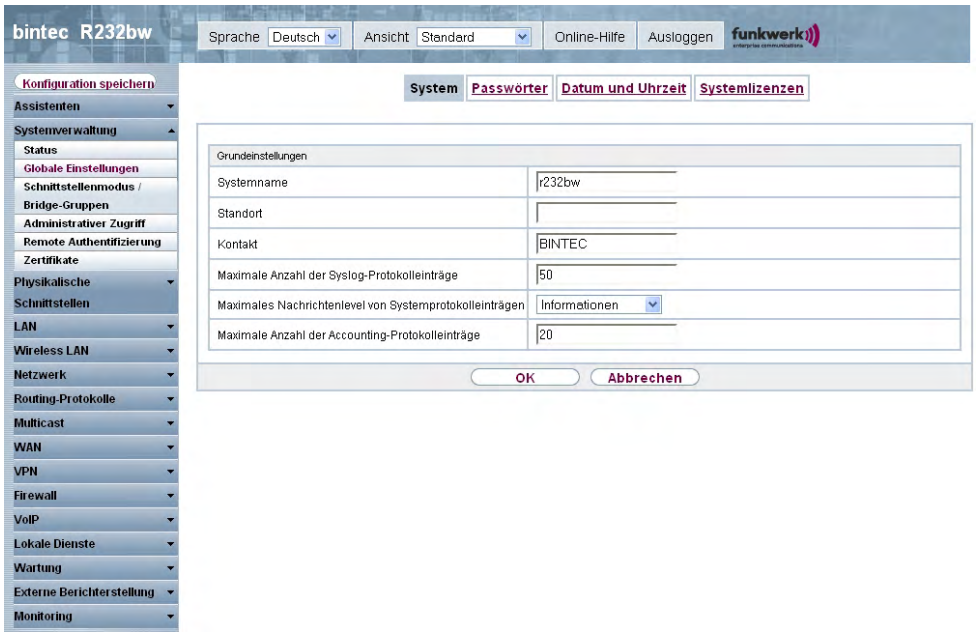


Abb. 25: **Systemverwaltung**->**Globale Einstellungen**->**System**

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

Felder im Menü SystemGrundeinstellungen

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird auch als PPP-Host-Name benutzt. Möglich ist eine Zeichenkette mit bis zu 255 Zeichen. Als Standardwert ist der Gerätetyp voreingestellt.
Standort	Geben Sie an, wo sich Ihr Gerät befindet.
Kontakt	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Möglich ist eine Zeichenkette mit bis zu 255 Zeichen. Standardwert ist *FUNKWERK*.
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*. 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,

Feld	Wert
	Alarm, Kritisch, Fehler und Warnung aufgezeichnet. • *Benachrichtigung*: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet. • *Informationen* (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet. • *Debug*: Es werden alle Meldungen aufgezeichnet.
Maximale Anzahl der Accounting-Protokolleinträge	Geben Sie die maximale Anzahl an Einträgen an, die zur Gebührenerfassung auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind *0* bis *1000*. Standardwert ist *20*.

9.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

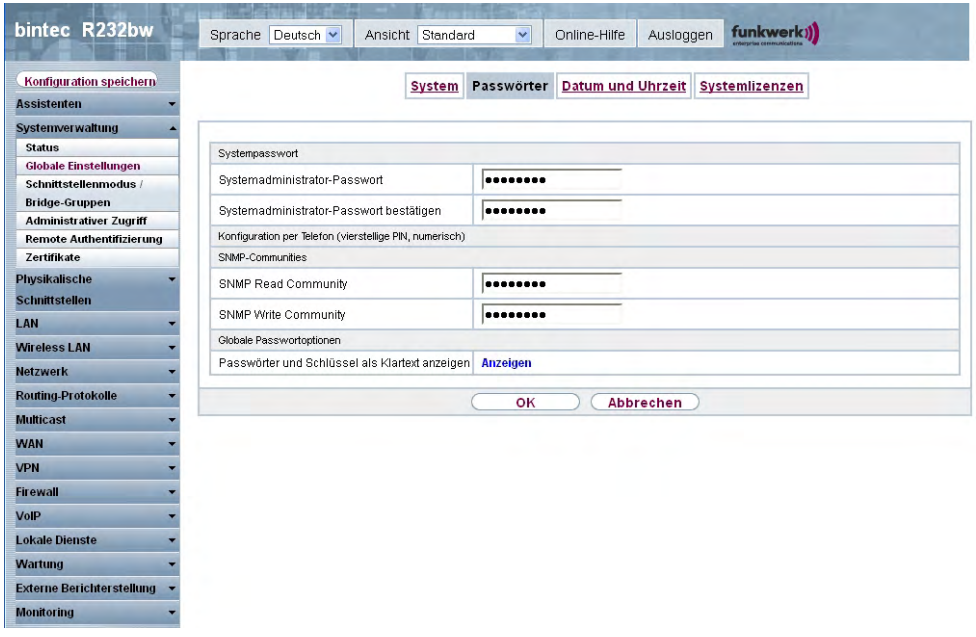


Abb. 26: **Systemverwaltung->Globale Einstellungen->Passwörter**

Hinweis

Alle **bintec**-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 PasswörterSystempasswort

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

Felder im Menü PasswörterSNMP-Communities

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

Feld im Menü PasswörterGlobale Passwortoptionen

Feld	Wert
Passwörter und Schlüssel als Klartext anzeigen	Wählen Sie aus, ob die Passwörter im Klartext angezeigt werden sollen. Mit *`Anzeigen`* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv. Wenn Sie die Funktion aktivieren, werden alle Passwörter und

Feld	Wert
	Schlüssel in allen Menüs als Klartext angezeigt und können in Klartext bearbeitet werden. Eine Ausnahme bilden die WLAN- und IPSec-Schlüssel. Diese können nur im Klartext eingegeben werden. Bei Drücken von **OK** oder erneutem Aufruf des Menüs werden sie als Sternchen angezeigt.

9.2.3 Datum und Uhrzeit

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

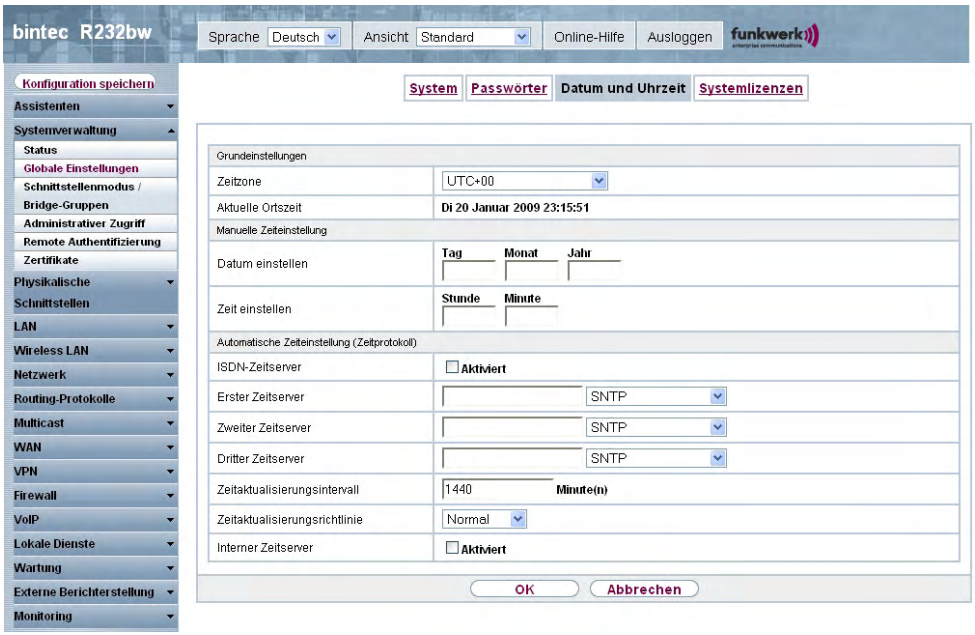


Abb. 27: **Systemverwaltung->Globale Einstellungen->Datum und Uhrzeit**

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

ISDN/Manuell

Die Systemzeit kann über ISDN aktualisiert, d.h. beim ersten ausgehenden Ruf werden Datum und Uhrzeit aus dem ISDN entnommen, oder 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 Datum und UhrzeitGrundeinstellungen

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 Datum und UhrzeitManuelle 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. Format: • **Stunde**: hh • **Minute**: mm

Felder im Menü Datum und UhrzeitAutomatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	Legen Sie fest, ob die Zeitinformation, die an einer eingehenden ISDN-Verbindung empfangen wird, zur Aktualisierung der Systemzeit benutzt wird. Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeits-Server 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 mit 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 mit UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37.

Feld	Beschreibung
	• *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst mit 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 mit 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 mit UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst mit 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 mit 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 mit UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst mit TCP-Port 37. • *Deaktiviert*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.

Feld	Beschreibung
	Der Standardwert ist *1440*.
Zeitaktualisierungs-richtlinie	Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen. Mögliche Werte: • *Normal*(Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • *Aggressiv*: Zehn Minuten lang wird versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • *Endlos*: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. Bei der Verwendung von Zertifikaten für die Verschlüsseluing 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.

9.2.4 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.funkwerk-ec.com* abrufen können.

Lizenzdaten eintragen

Die Lizenzdaten der Zusatzlizenzen erhalten Sie über die Online-Lizenzierungs-Seiten im Support-Bereich auf *www.funkwerk-ec.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).

9.2.4.1 Bearbeiten oder Neu

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

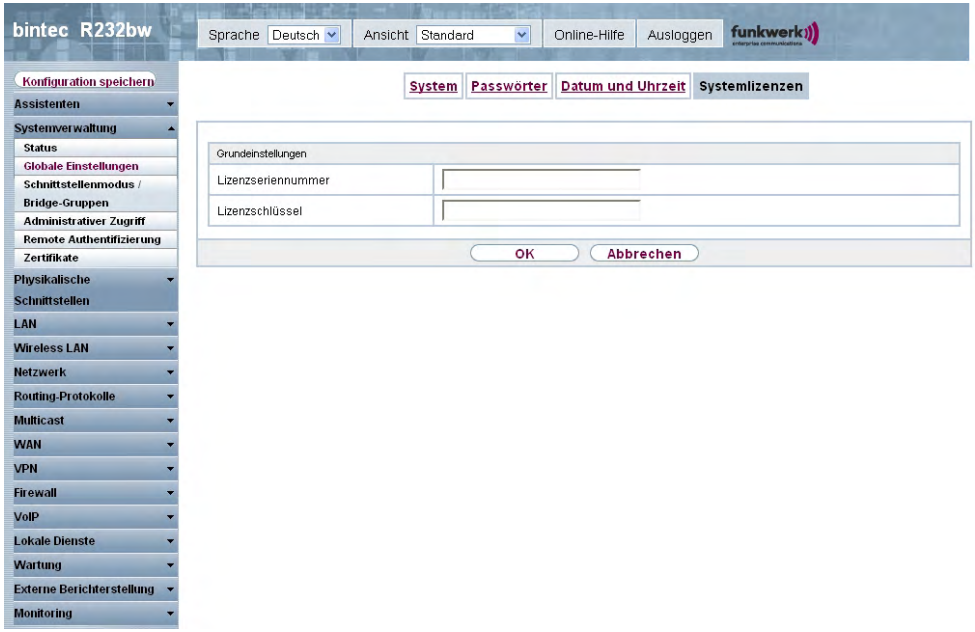


Abb. 28: **Systemverwaltung->Globale Einstellungen->Systemlizenzen->Neu**

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 SystemlizenzenGrundeinstellungen

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 Funktionalität 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) Drücken 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.

9.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

Mit Bridging werden gleichartiger Netze verbunden. Im Gegensatz zum Routing 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 der Schicht 3 (Netzwerkschicht) des OSI-Modells verbunden und Informationen von einem Netz in das andere weitergeleitet (routen).

Konventionen für die Port-/Schnittstellennamen

Die Namen der Funk-Ports in der Benutzeroberfläche Ihres Geräts setzen sich 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, dabei steht en für Ethernet

(b) Nummer des Ports

Beispiel: *ETH1*

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

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Ethernet-Ports

(c) Nummer der Schnittstelle

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

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

(a) Abkürzung für den Schnittstellentyp

(b) Nummer der Bridge-Gruppe

Beispiel: *br0* (erste Bridge-Gruppe)

Der Name der Drahtlosnetzwerke setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Funkmoduls

(c) Nummer der Schnittstelle

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

Der Name der virtuellen Schnittstellen, die an einen Ethernet-Port gebunden sind, 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)

9.3.1 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.

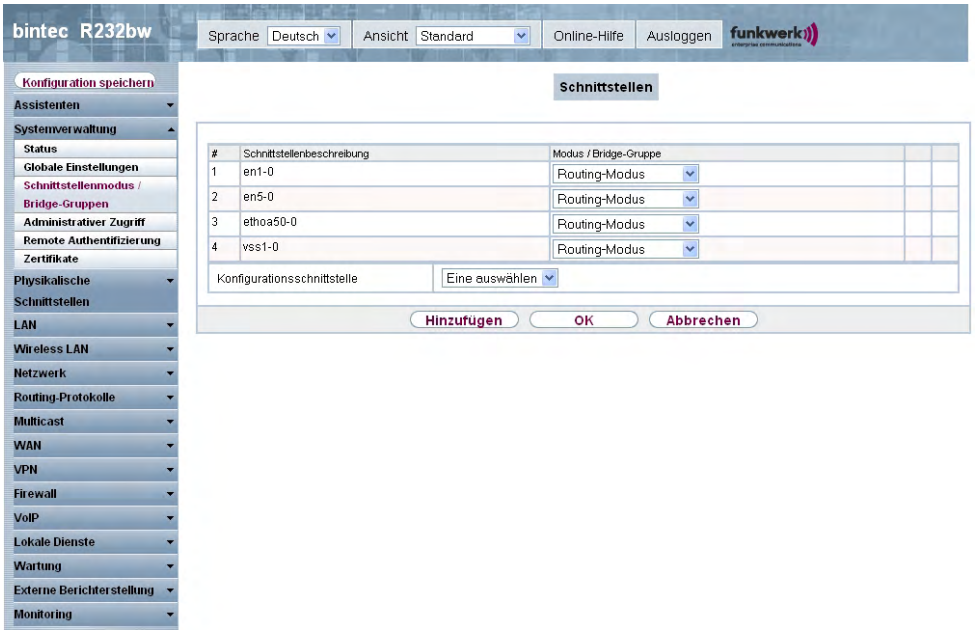


Abb. 29: **Systemverwaltung->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen**

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschreibung	Zeigt den Namen der Schnittstelle an.
Modus / Bridge-Grup-	Wählen Sie aus, ob Sie die Schnittstelle im `Routing-Modus` betreiben möchten oder ordnen die Schnittstelle einer beste-

Feld	Beschreibung
pe	henden (*br0*, *br1* usw.) oder neuen Bridge-Gruppe (*Neue Bridge-Gruppe*) zu. Bei Auswahl von *Neue Bridge-Gruppe* wird nach Klicken 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.

9.4 Administrativer Zugriff

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

9.4.1 Zugriff

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

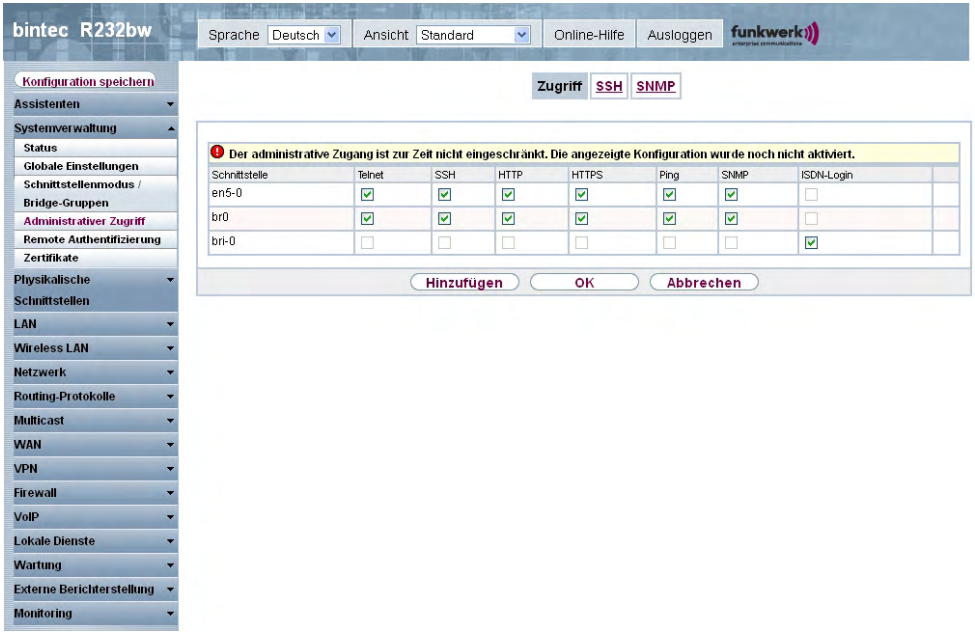


Abb. 30: **Systemverwaltung**+**Administrativer Zugriff**->**Zugriff**

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

9.4.1.1 Hinzufügen

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

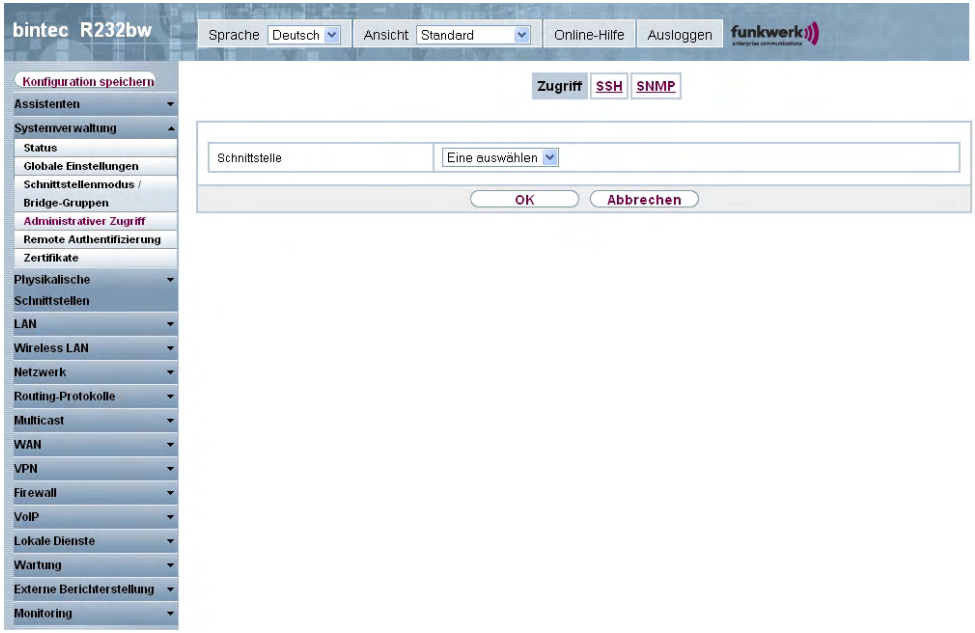


Abb. 31: **Systemverwaltung**+**Administrativer Zugriff**->**Zugriff**->**Hinzufügen**

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.

9.4.2 SSH

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

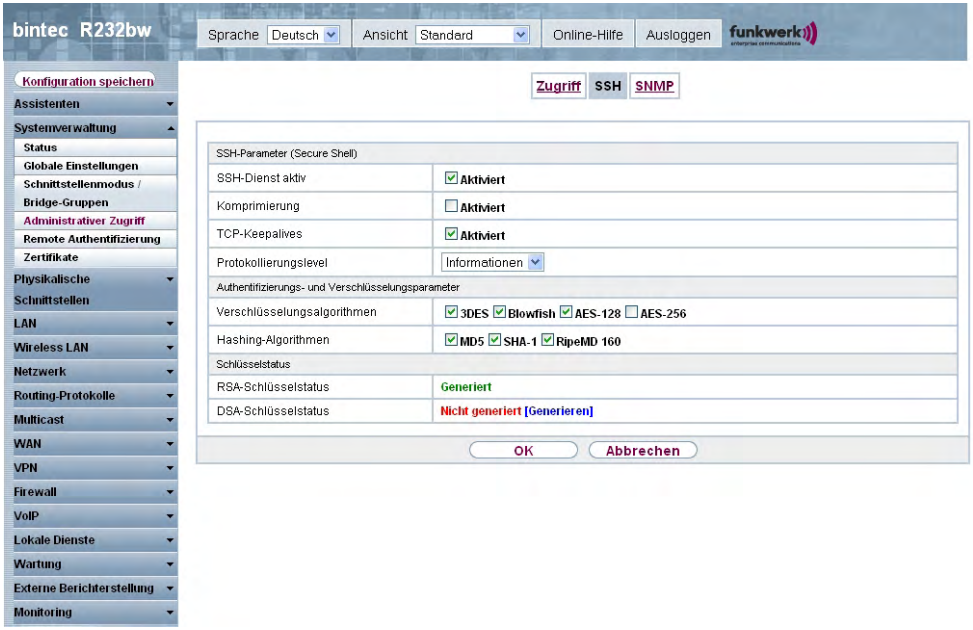


Abb. 32: **Systemverwaltung->Administrativer Zugriff->SSH**

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.funkwerk-ec.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 SSHSSH-Parameter (Secure Shell)

Feld	Wert
SSH-Dienst aktiv	Wählen Sie aus, ob der SSH-Daemon aktiviert werden soll.

Feld	Wert
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
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: • *Informationen* (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.

Felder im Menü SSHAuthentifizierungs- 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*

Feld	Wert
	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 SSHSchlüsselstatus

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.
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*

Feld	Wert
	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.

9.4.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

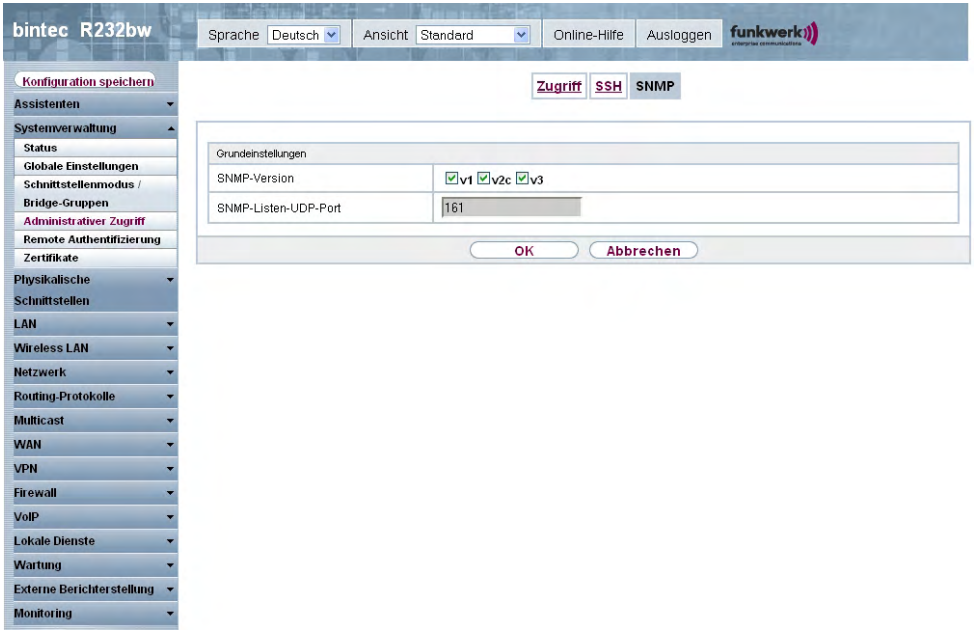


Abb. 33: **Systemverwaltung->Administrativer Zugriff->SNMP**

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

Felder im Menü SNMPGrundeinstellungen

Feld	Wert
SNMP-Version	Wählen Sie aus, mit welcher SNMP-Version Ihr Gerät auf externe SNMP-Zugriffe lauschen 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.

Tipp

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

9.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

9.5.1 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-Verbindungparameter 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.

9.5.1.1 Bearbeiten oder Neu

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

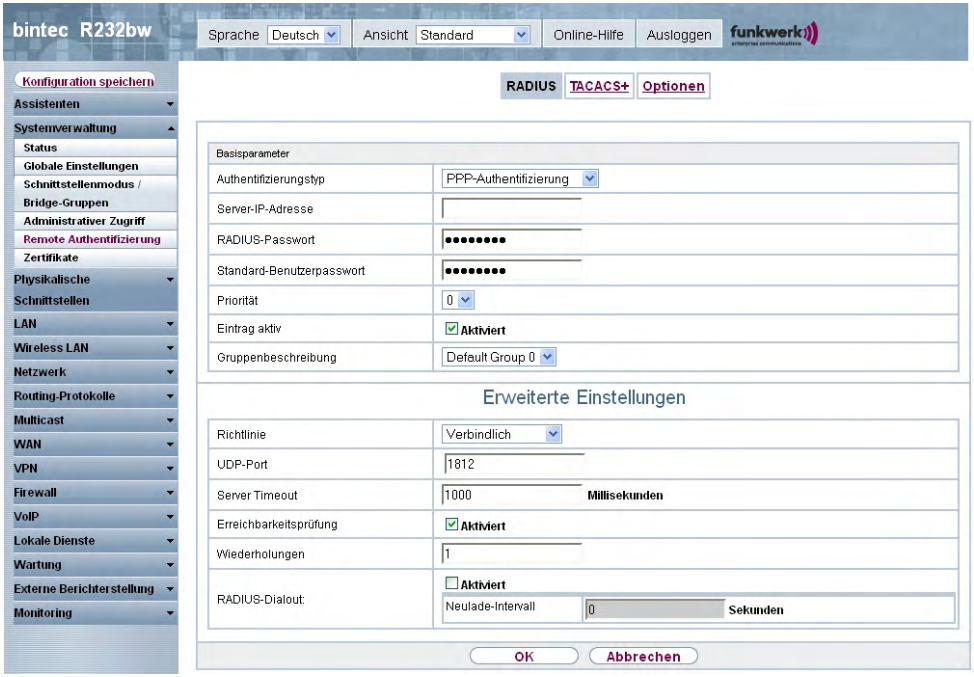


Abb. 34: **Systemverwaltung->Remote Authentifizierung->RADIUS->Neu**

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

Felder im Menü RADIUSBasisparameter

Feld	Wert
Authentifizierungstyp	Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll. Mögliche Werte: • *PPP-Authentifizierung*(Standardwert; nur für PPP-Verbindungen): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. • *Accounting*(nur für PPP-Verbindungen): Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet. • *Login-Authentifizierung*: Der RADIUS-Server wird verwendet, um den Zugang zur SNMP Shell Ihres Geräts zu kontrollieren. • *IPSec-Authentifizierung*: Der RADIUS-Server wird ver-

Feld	Wert
	wendet, 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 bintec 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 nächst niedrigeren Priorität verwendet usw. Mögliche Werte von *0* (höchste Priorität) bis *7* (niedrigste Priorität). Standardwert ist *0* . Siehe auch **Richtlinie** in den **Erweiterte Einstellungen**.

Feld	Wert
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. • *Default Group 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.
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 Gebührenerfas-

Feld	Wert
	sung (1646 in älterne RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist. 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*. 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 Erreichbarkeit wird **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. Mögliche Werte sind ganze Zahlen zwischen *0* und *10*. Standardwert ist *1*. Um zu verhindern, dass **Status** auf *inaktiv* gesetzt wird, setzen Sie diesen Wert auf *0*.
RADIUS-Dialout	Nur für **Authentifizierungstyp** = *Authentifizierung* und

Feld	Wert
	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. • *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. Standardmäßig ist das *Standard-Benutzerpasswort* leer.

9.5.2 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**-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.

9.5.2.1 Bearbeiten oder Neu

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

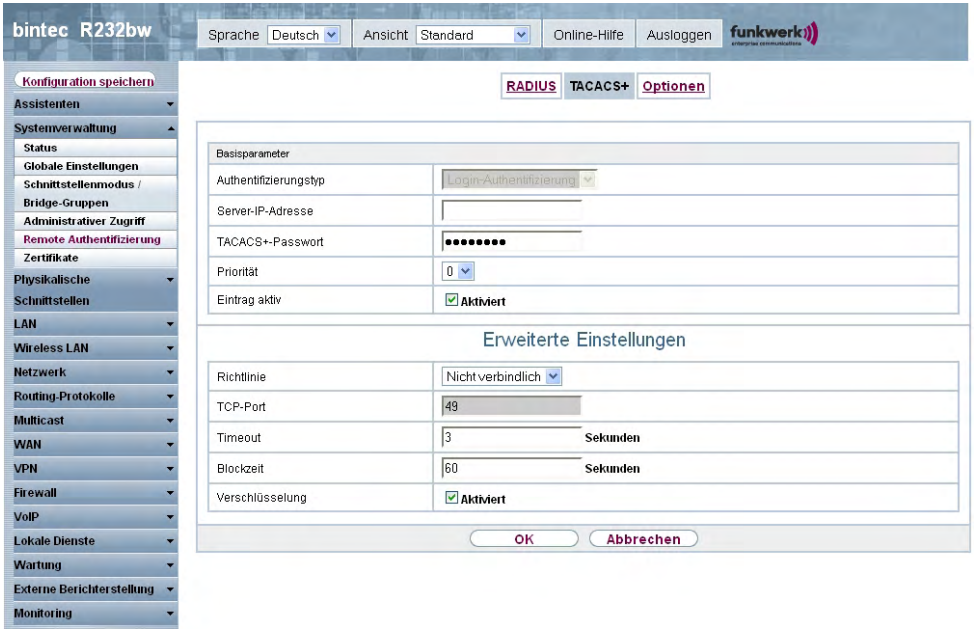


Abb. 35: **Systemverwaltung->Remote Authentifizierung->TACACS+ ->Neu**

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

Felder im Menü TACACS+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 gibt 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 kommt. • *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 benutzte Standard-TCP-Port (*49*) an. Der Wert kann nicht verändert werden.

Feld	Beschreibung
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 bleiben soll. Nach Ende der Blockierungsdauer 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.

9.5.3 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.

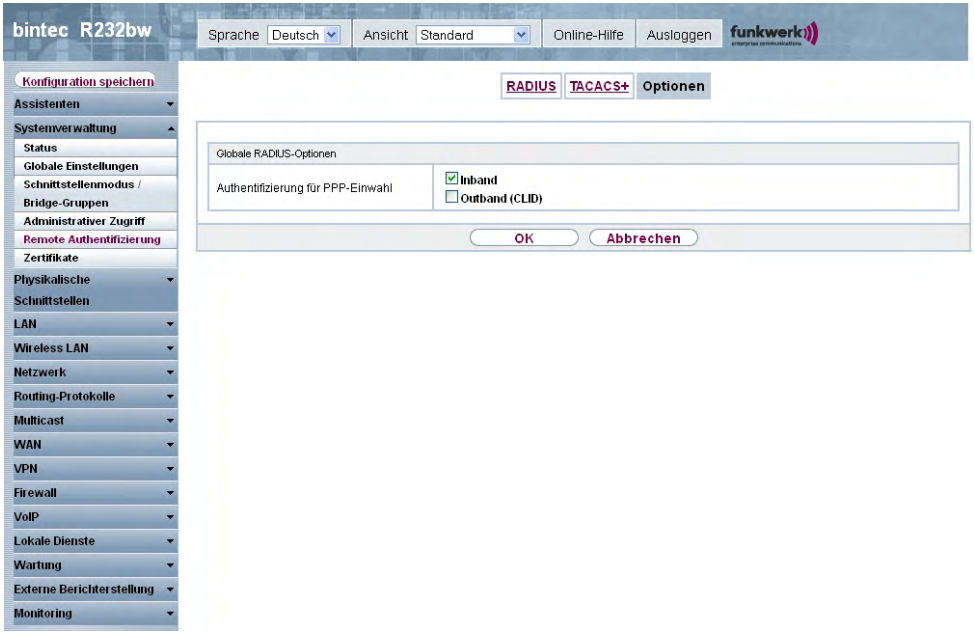


Abb. 36: **Systemverwaltung**->**Remote Authentifizierung**->**Optionen**

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

Felder im Menü OptionenGlobale 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* akiviert.

9.6 Zertifikate

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

Für die Verschlüsselung benötigt der Sender den öffentlichen Schlüssel des Empfängers. Der Empfänger entschlüsselt die Daten mit seinem privaten Schlüssel. Um sicherzustellen, dass der öffentlich 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 Zerifikate nicht nur eine einzige Ausgabestelle gibt, wie z. B. das Passamt für einen Ausweis, sondern Zertifikate von vielen verschiedenen Stellen und in unterschiedlicher Qualität ausgegeben werden, kommt der Vertrauenswürdigkeit der Ausgabestelle eine zentrale Bedeutung zu. Die Qualität eines Zertifikats regelt das deutsche Signaturgesetz bzw. die entsprechende EU-Richtlinie.

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

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

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

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

9.6.1 Zertifikatsliste

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

9.6.1.1 Bearbeiten

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

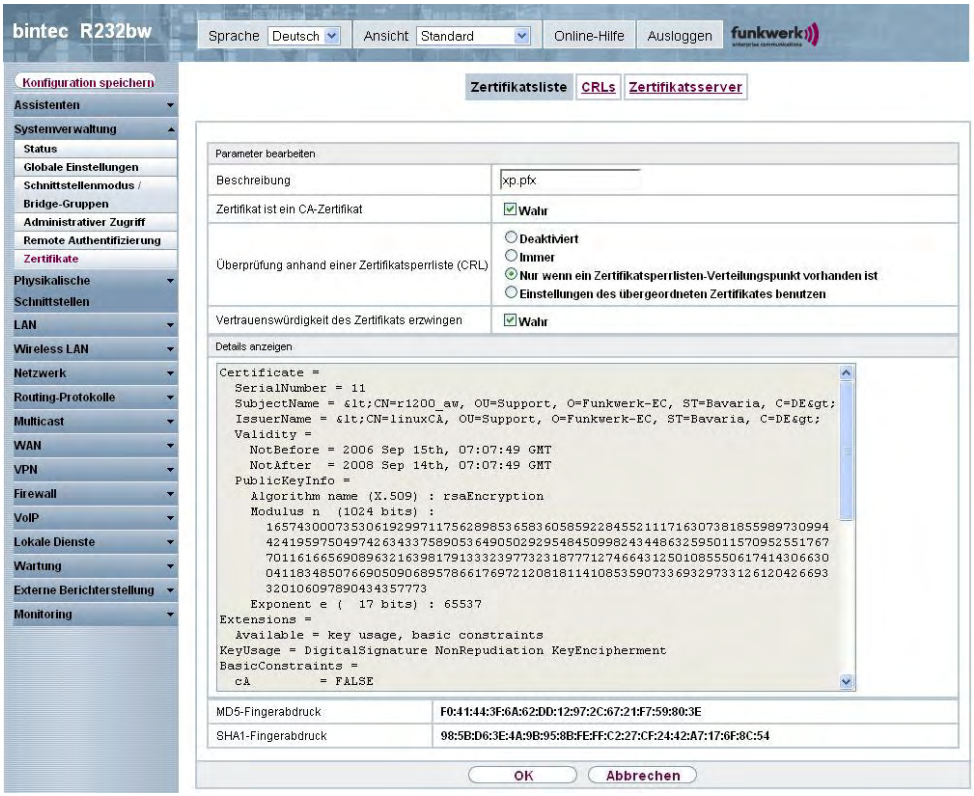


Abb. 37: **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->

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

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.

Feld	Beschreibung
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. 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.

9.6.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

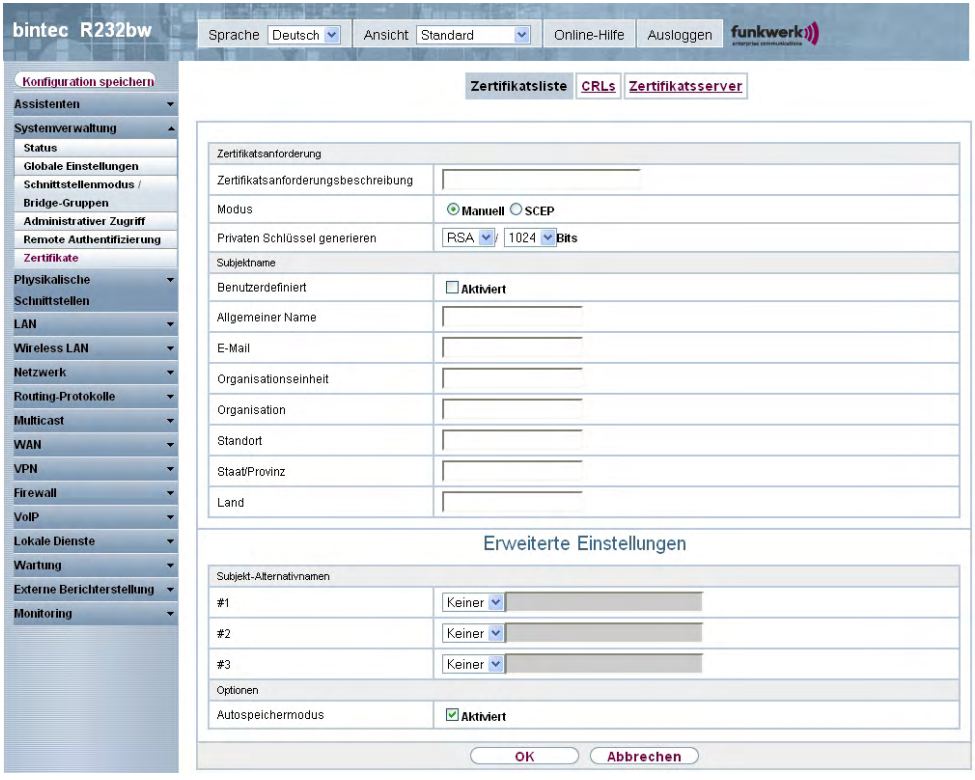


Abb. 38: **Systemverwaltung->Zertifikate->Zertifikatsliste->Zertifikatsanforderung**

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

Felder im Menü ZertifikatslisteZertifikatsanforderung

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

Feld	Beschreibung
	den. • *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.funkwerk.de:8080/scep/scep.dll Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
CA-Zertifikat	Nur für **Modus** = *SCEP* Wählen Sie das CA-Zertifikat aus. • *-- Download --*: Geben Sie in **CA-Name** den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows*. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator. Falls keine CA-Zertifikate zur Verfügung stehen, wird Ihr Gerät zuerst das CA-Zertifikat der betroffenen CA herunterladen. Es fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü **Zertifikatsanforderung generieren** zurück.

Feld	Beschreibung
	Falls das CA-Zertifikat keine CRL-Verteilstelle (Certificate Revocation List, CRL) enthält und auf Ihrem Gerät kein Zertifikatserver 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. 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. 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 ZertifikatslisteSubjektname

Feld	Beschreibung
Benutzerdefiniert	Wählen Sie aus, ob Sie die Namenskomponenten des Subjektnamens einzeln laut Vorgabe durch die CA oder einen speziel-

Feld	Beschreibung
	len 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**, **Standort**, **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.
Standort	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie den Standort laut CA ein.
Staat/Provinz	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie den Staat/das Bundesland laut CA ein.
Land	Nur für **Benutzerdefiniert** = deaktiviert.

Feld	Beschreibung
	Geben Sie das Land laut CA ein.

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

Felder im Menü Erweiterte EinstellungenSubjekt-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 Erweiterte EinstellungenOptionen

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.

9.6.1.3 Importieren

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

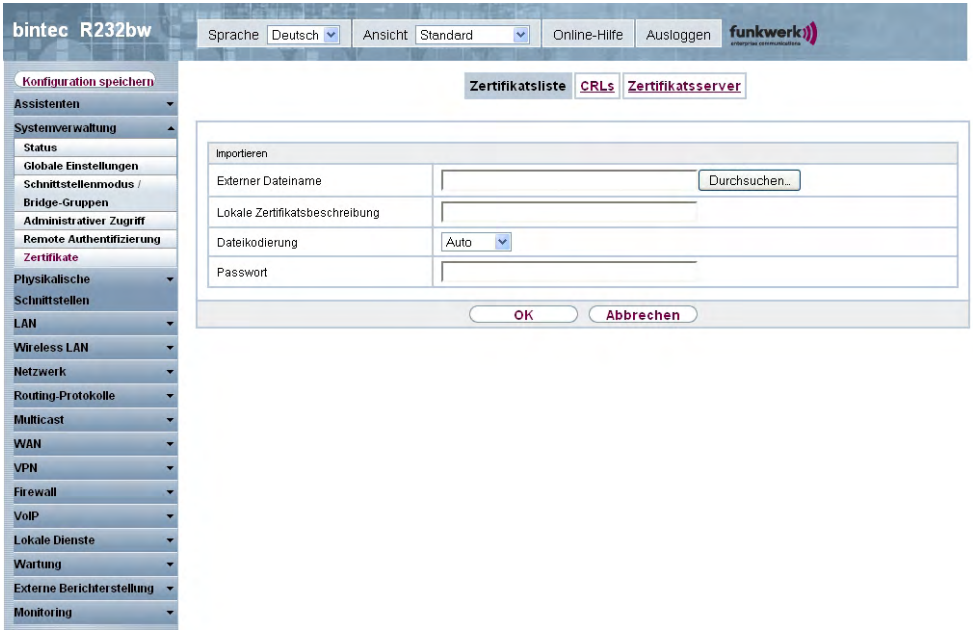


Abb. 39: **Systemverwaltung->Zertifikate->Zertifikatsliste->Importieren**

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

Felder im Menü ZertifikatslisteImportieren

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 Codierung, so dass Ihr Gerät das Zertifikat decodieren 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*

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

9.6.2 CRLs

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

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

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

9.6.2.1 Importieren

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

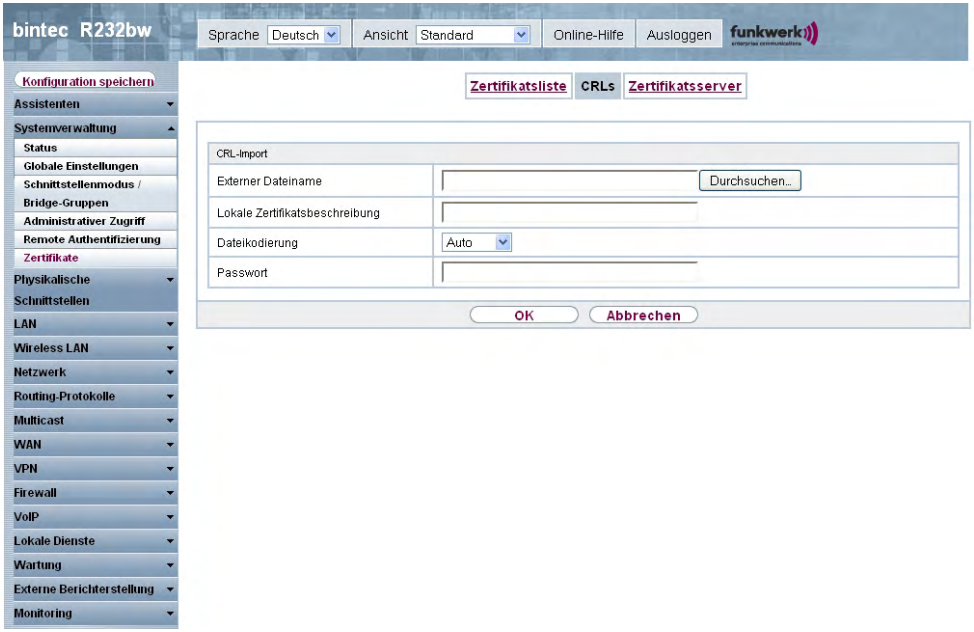


Abb. 40: **Systemverwaltung->Zertifikate->CRLs->Importieren**

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

Felder im Menü CRLsCRL-Import

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

Feld	Beschreibung
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

9.6.3 Zertifikatsserver

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

Ein Zertifikatserver hält Zertifikatsperrlisten (CRL) bereit, die zur Prüfung von Zertifikaten entweder per LDAP oder HTTP vom Gerät abgefragt werden.

9.6.3.1 Neu

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

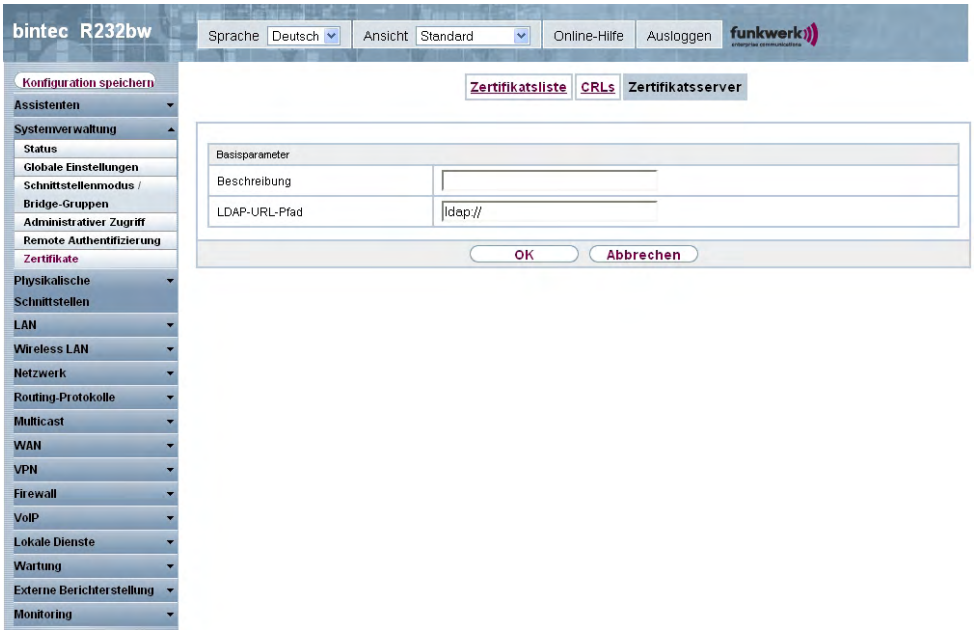


Abb. 41: **Systemverwaltung**->**Zertifikate**->**Zertifikatsserver**->**Neu**

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

Felder im Menü ZertifikatsserverBasisparameter

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

Kapitel 10 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.

10.1 Ethernet-Ports

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

Die Ethernet-Ports **1** bis **4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.0.254* und **Netzmaske** *255.255.255.0*vorkonfiguriert.

Der Port **ETH** ist der logischen Ethernet-Schnittstelle *en5-0* zugewiesen und nicht vorkonfiguriert.

Hinweis

Um die Erreichbarkeit Ihres Geräts zu gewährleisten, achten Sie beim Aufteilen der Ports darauf, dass die Ethernet-Schnittstelle *en1-0* mit der vorkonfigurierten IP-Adresse und Netzmaske einem Port zugewiesen wird, der per Ethernet erreichbar ist. Führen Sie im Zweifelsfall die Konfiguration per serieller Verbindung über die **Console**-Schnittstelle durch.

1 - 4

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

ETH

Port **ETH5** ist fest die logische Ethernet-Schnittstelle *en5-0* zugewiesen. Die Konfigurationsoptionen sind identisch mit denen der Ports **1** - **4**.

VLANs für Routing-Schnittstellen

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

10.1.1 Portkonfiguration

Portseparation

Ihr Gerät bietet die Möglichkeit, die Switch Ports **1** - **4** als eine Schnittstelle zu betreiben oder diese logisch voneinander zu trennen und als eigenständige Ethernet-Schnittstellen zu konfigurieren.

Bei der Konfiguration sollten Sie Folgendes beachten: Die Aufteilung der Switch Ports auf mehrere Ethernet-Schnittstellen trennt diese nur logisch voneinander. Die verfügbare Gesamtbandbreite von max. 100 Mbit/s Full Duplex für alle entstandenen Schnittstellen bleibt unverändert. Wenn Sie also z. B. alle Switch Ports voneinander trennen, verfügt jede der entstehenden Schnittstellen nur über einen Teil der vollen Bandbreite. Wenn Sie mehrere Switch Ports zu einer Schnittstelle zusammenfassen, so stehen für alle Ports gemeinsam die volle Bandbreite von max. 100 Mbit/s Full Duplex zur Verfügung.

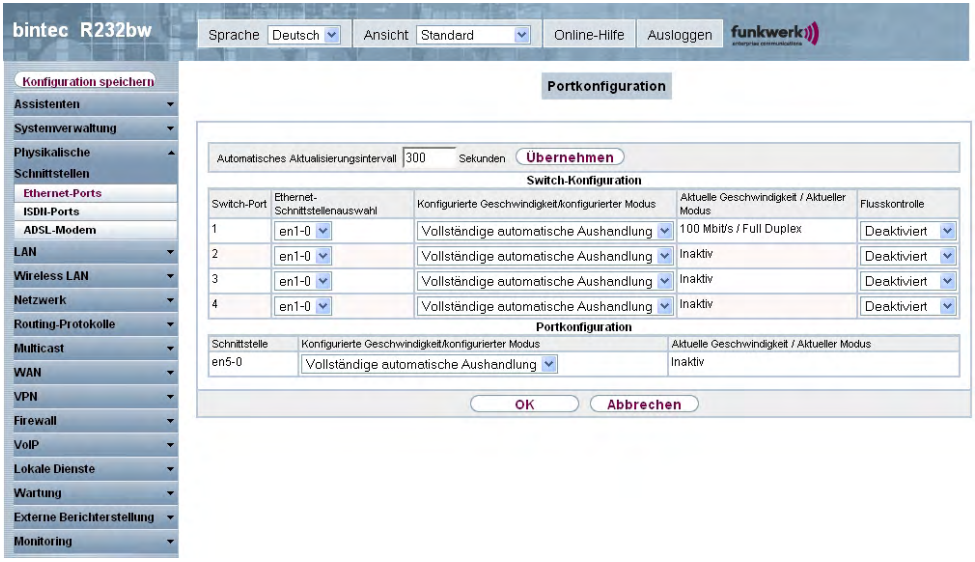


Abb. 42: **Physikalische Schnittstellen->Ethernet-Ports->Portkonfiguration**

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

Felder im Menü PortkonfigurationSwitch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Ethernet-Schnittstellenauswahl	Ordnen Sie dem jeweiligen Switch-Port eine Ethernet-Schnittstelle zu. Zur Auswahl stehen vier Schnittstellen, *en1-0* bis *en1-3*. In der Grundeinstellung ist allen Switch Ports die Schnittstelle *en1-0* zugeordnet.
Konfigurierte Geschwindigkeit/konfigurierter Modus	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll. Mögliche Werte: • *Vollständige automatische Aushandlung* (Standardwert) • *Auto 1000 Mbit/s only*

Feld	Beschreibung
	• *Auto 100 Mbit/s only* • *Auto 10 Mbit/s only* • *Auto 100 Mbit/s / Full Duplex* • *Auto 100 Mbit/s / Half Duplex* • *Auto 10 Mbit/s / Full Duplex* • *Auto 10 Mbit/s / Half Duplex* • *Fest 1000 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Half Duplex* • *Fest 10 Mbit/s / Full Duplex* • *Fest 10 Mbit/s / Half Duplex* • *Keiner* : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an. Mögliche Werte: • *1000 Mbit/s / Full Duplex* • *100 Mbit/s / Full Duplex* • *100 Mbit/s / Half Duplex* • *10 Mbit/s / Full Duplex* • *10 Mbit/s / Half Duplex* • *Inaktiv*

Felder im Menü PortkonfigurationPortkonfiguration

Feld	Beschreibung
Schnittstelle	Zeigt den Schnittstellennamen des separaten Ethernet-Ports ETH an.
Konfigurierte Geschwindigkeit/konfigurierter Modus	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll. Mögliche Werte sind: • *Vollständige automatische Aushandlung* (Standardwert)

Feld	Beschreibung
	• *Auto 100 Mbit/s only* • *Auto 10 Mbit/s only* • *Auto 100 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 100 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Half Duplex* • *Fest 10 Mbit/s / Full Duplex* • *Fest 10 Mbit/s / Half Duplex* • *Deaktiviert* : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an. Mögliche Werte: • *1000 Mbit/s / Full Duplex* • *100 Mbit/s / Full Duplex* • *100 Mbit/s / Half Duplex* • *10 Mbit/s / Full Duplex* • *10 Mbit/s / Half Duplex* • *Inaktiv*

10.2 ISDN-Ports

In diesem Menü konfigurieren Sie die ISDN-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluss Ihr Gerät angeschlossen ist.

Die ISDN-BRI-Schnittstelle Ihres Geräts können Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen. Um die ISDN-BRI-Schnittstelle zu konfigurieren, müssen Sie zwei Schritte durchführen:

- Einstellungen Ihres ISDN-Anschlusses eintragen: Hier tragen Sie die wichtigsten Parameter Ihres ISDN-Anschlusses ein.

- MSN-Konfiguration: Hier teilen Sie Ihrem Gerät mit, wie auf eingehende Rufe aus dem WAN reagiert werden soll.

10.2.1 ISDN-Konfiguration

Hinweis

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

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

10.2.1.1 Bearbeiten mit

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

Abb. 43: **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN-Konfiguration**->

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

Felder im Menü ISDN-KonfigurationBasisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Automatische Konfiguration beim Start	Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Ergebnis der automatischen Konfiguration	Zeigt den Status der ISDN-Autokonfiguration an. Die automatische D-Kanal-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter **Port-Verwendung** manuell ausgewählt ist. Das Feld kann nicht editiert werden. Angezeigt wird das Ergebnis der automatischen Konfiguration für die **Port-Verwendung** und den **ISDN-Konfigurationstyp**. Mögliche Werte: • Alle möglichen Werte für die **Port-Verwendung** und den **ISDN-Konfigurationstyp**. • *Wird ausgeführt*: Erkennung läuft noch.
Port-Verwendung	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist. Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll. Mögliche Werte: • *Nicht verwendet*: Der ISDN-Anschluss wird nicht genutzt. • *Dialup (Euro-ISDN)* • *Standleitung* • *Q-SIG*
ISDN-Konfigurationstyp	Nur wenn **Automatische Konfiguration beim Start** deaktiviert ist und für **Port-Verwendung** = *Dialup (Euro-ISDN)* oder *Q-SIG* Wählen Sie die ISDN-Anschlussart aus.

Feld	Beschreibung
	Mögliche Werte: • *Punkt-zu-Mehrpunkt* (Standardwert): Mehrgeräteanschluss. • *Punkt-zu-Punkt*: Anlagenanschluss.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	Packet Switch stellen Sie ein, wenn Sie den X.31-TEI für das X.25-Gerät nutzen möchten.

10.2.2 MSN-Konfiguration

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

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

Das Gerät unterstützt die Dienste:

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

Wenn ein Ruf eingeht, überprüft Ihr Gerät zunächst anhand der Einträge in diesem Menü die Art des Anrufs (Daten- oder Sprachruf) und die Called Party Number, wobei nur der Teil

der Called Party Number das Gerät erreicht, der von der Ortsvermittlung bzw., falls vorhanden, von der TK-Anlage weitergeleitet wird. Anschließend wird der Ruf dem passenden Dienst zugewiesen.

Hinweis

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

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

10.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um die MSNs zu bearbeiten.

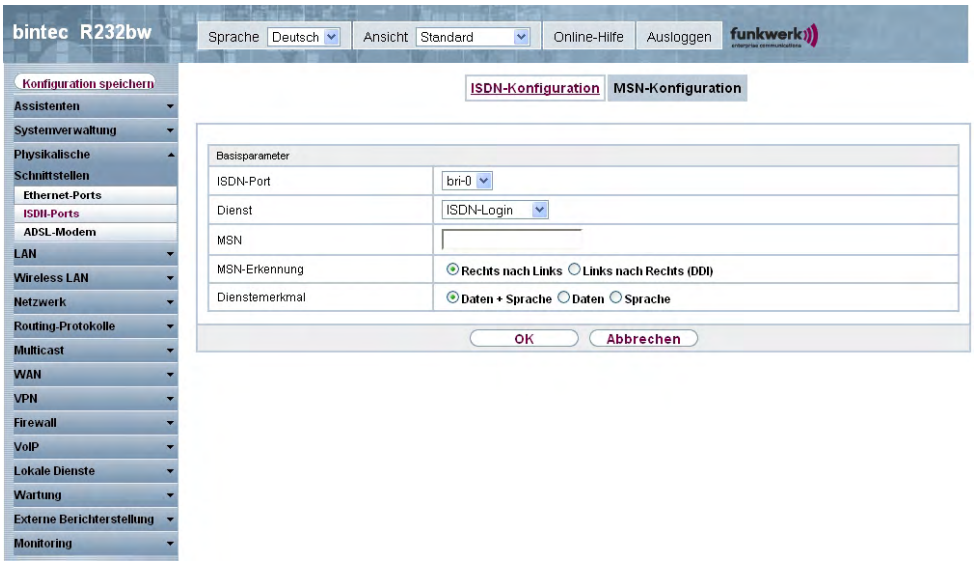


Abb. 44: **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu**

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

Felder im Menü MSN-KonfigurationBasisparameter

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

Feld	Beschreibung
	aus. Mögliche Werte: • *Daten + Sprache* (Standardwert): Sowohl Daten- als auch Sprachruf. • *Daten*: Datenruf • *Sprache*: Sprachruf (Modem, Sprache, analoges Fax)

10.3 ADSL-Modem

Das ADSL Modem von **bintec R232x** und **bintec R232xw** ist für die Standards ANNEX A oder ANNEX B (siehe Kapitel **Technische Daten**) geeignet und somit in vielen Ländern universell einsetzbar. Es eignet sich besonders für den High-Speed Internet Zugang und den Remote-Access Einsatz in kleinen bis mittleren Unternehmen oder Remote-Offices.

10.3.1 ADSL-Konfiguration

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

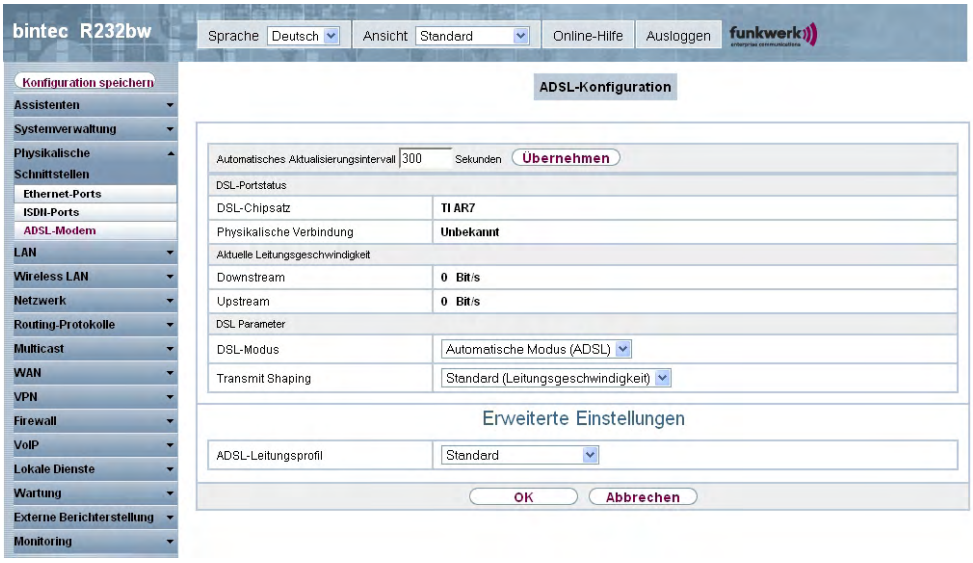


Abb. 45: **Physikalische Schnittstellen->ADSL-Modem->ADSL-Konfiguration**

Das Menü **Physikalische Schnittstellen->ADSL-Modem->ADSL-Konfiguration** besteht

aus folgenden Feldern:

Felder im Menü ADSL-KonfigurationDSL-Portstatus

Feld	Beschreibung
DSL-Chipsatz	Zeigt die Kennung des eingebauten Chipsatzes an.
Physikalische Verbindung	Zeigt den aktuellen ADSL-Betriebsmodus an. Der Wert kann nicht verändert werden. Mögliche Werte: • *Unbekannt*: Der ADSL Link ist nicht aktiv. • *ANSI T1.413*: ANSI T1.413 • *ADSL1*: ADSL classic, G.DMT, ITU G.992.1 • *G.lite G992.2*: Splitterless ADSL, ITU G.992.2 • *ADSL2*: G.DMT.Bis, ITU G.992.3 • *ADSL2 DELT*: ADSL2 Double Ended Line Test • *ADSL2 Plus*: ADSL2 Plus, ITU G.992.5 • *ADSL2 Plus DELT*: ADSL2 Plus Double Ended Line Test • *READSL2*: Reach Extended ADSL2 • *READSL2 DELT*: Reach Extended ADSL2 Double Ended Line Test. • *ADSL2 ITU-T G.992.3 Annex M* • *ADSL2+ ITU-T G.992.5 Annex M*

Felder im Menü ADSL-KonfigurationAktuelle Leitungsgeschwindigkeit

Feld	Beschreibung
Downstream	Zeigt die Datenrate in Empfangsrichtung (Richtung von CO/DSLAM zu CPE/Router) in Bits pro Sekunde an. Der Wert kann nicht verändert werden.
Upstream	Zeigt die Datenrate in Senderichtung (Richtung CPE/Router zu CO/DSLAM) in Bits pro Sekunde an. Der Wert kann nicht verändert werden.

Felder im Menü ADSL-KonfigurationDSL Parameter

Feld	Beschreibung
DSL-Modus	Wählen Sie den ADSL-Synchronisierungstyp aus.

Feld	Beschreibung
	Mögliche Werte: • *Automatische Modus (ADSL)* (Standardwert): Der ADSL-Modus wird dem der Gegenstelle automatisch angepasst. • *ADSL1*: ADSL1 / G.DMT wird angewendet. • *ADSL2*: ADSL2 / G.992.3 wird angewendet. • *ADSL2 Plus*: ADSL2 Plus / G.992.5 wird angewendet. • *Inaktiv*: Die ADSL-Schnittstelle ist nicht aktiv.
Transmit Shaping	Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig. Mögliche Werte: • *Standard (Leitungsgeschwindigkeit)*: Die Datenrate in Senderichtung wird nicht reduziert. • *128.000 Bit/s*, *192.000 Bit/s*, *256.000 Bit/s*, *512.000 Bit/s*, *768.000 Bit/s*, *1.024.000 Bit/s*, *1.536.000 Bit/s* und *2.048.000 Bit/s*: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 Bit/s bis 2.048.000 Bit/s in festgesetzten Schritten. • *Benutzerdefiniert*: Die Datenrate wird reduziert auf den in **Maximale Upstream-Bandbreite** eingegebenen Wert. Standardwert ist *Standard (Leitungsgeschwindigkeit)*.
Maximale Upstream-Bandbreite	Nur für **Transmit Shaping** = *Benutzerdefiniert* Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.

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

Felder im Menü ADSL-KonfigurationErweiterte Einstellungen

Feld	Beschreibung
ADSL-Leitungsprofil	Wählen Sie das für Ihren Provider benötigte ADSL-Leitungsprofil aus. Mögliche Werte: • *Standard* (Standardwert): Ist kein besonderes ADSL-

Feld	Beschreibung
	Leitungsprofil nötig, belassen Sie diese Einstellung. • *<Provider>*: Wählen Sie einen der voreingestellten Provider aus der Liste.

Kapitel 11 LAN

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

11.1 IP-Konfiguration

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

11.1.1 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.

Standardmäßig sind alle vorhandenen Schnittstellen Ihres Geräts im Routing-Modus. Die Schnittstelle **en1-0** ist mit der IP-Adresse *192.168.0.254* mit Netzmaske *255.255.255.0* vorbelegt.

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.

11.1.1.1 Bearbeiten oder Neu

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

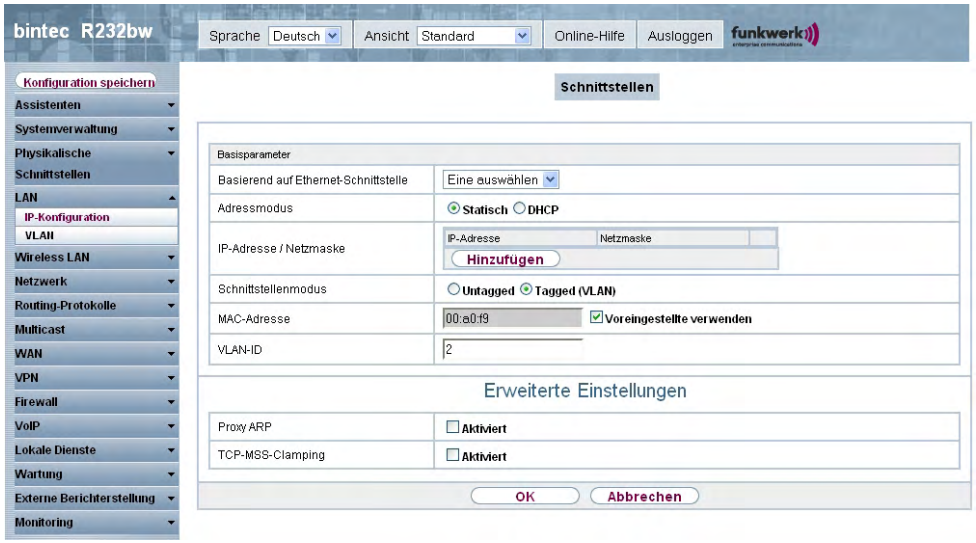


Abb. 46: **LAN->IP-Konfiguration->Schnittstellen->** **/Neu**

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

Felder im Menü SchnittstellenBasisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird. Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
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-

Feld	Beschreibung
	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. 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	Nur bei virtuellen Schnittstellen und nur für **Schnittstellenmodus** = *Untagged* 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. Das ist allerdings nicht notwendig. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden).
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-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 an-

Feld	Beschreibung
	wenden 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.

11.2 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 wie eine VLAN-aware Switch mit der Erweiterung, Clients in VLAN-Gruppen zusammenzufassen. Generell ist die VLAN-Segmentierung mit allen Schnittstellen konfigurierbar.

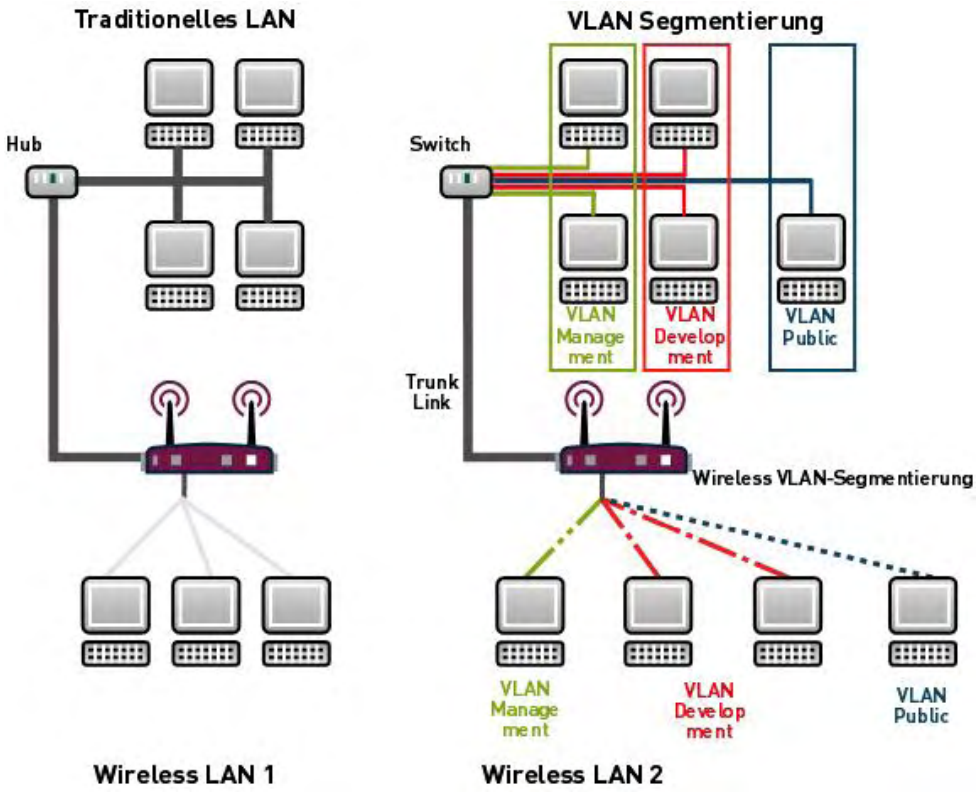


Abb. 47: VLAN-Segmentierung

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. Dieses definieren Sie über die Parameter **Schnittstellenmodus** = `Tagged (VLAN)` und das Feld **VLAN-ID** im Menü **LAN**->**IP-Konfiguration**->**Schnittstellen**->**Neu**.

11.2.1 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* vorhanden, dem alle Schnittstellen zugeordnet sind.

11.2.1.1 Bearbeiten oder Neu

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

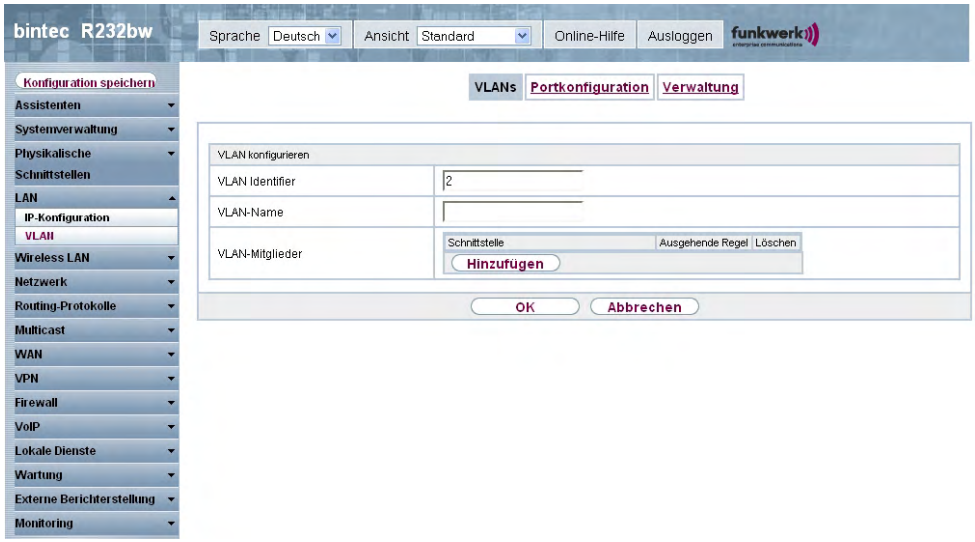


Abb. 48: **LAN->VLAN->VLANs->** **/Neu**

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

Felder im Menü VLANsVLAN 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* bis *4094*
VLAN-Name	Geben Sie einen eindeutigen Namen für das VLAN ein. Möglich ist eine Zeichenkette mit bis zu 32 Zeichen.

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

11.2.2 Portkonfiguration

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

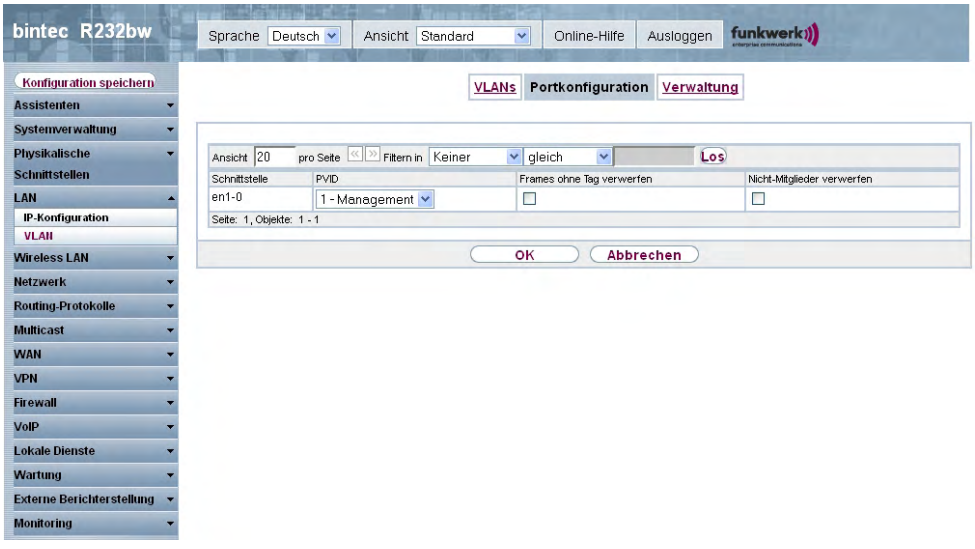


Abb. 49: **LAN->VLANs->Portkonfiguration**

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

Feld	Beschreibung
	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.

11.2.3 Verwaltung

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

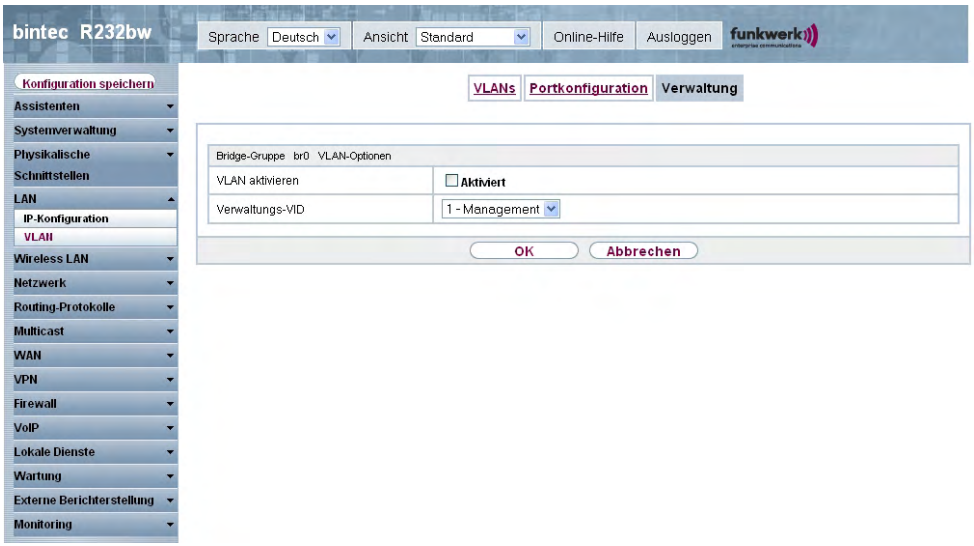


Abb. 50: **LAN->VLANs->Verwaltung**

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

Felder im Menü VLANVerwaltung

Feld	Beschreibung
VLAN aktivieren	Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe

Feld	Beschreibung
	für VLAN. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion deaktiviert.
Verwaltungs-VID	Wählen Sie die VLAN ID des VLANs an, in dem Ihr Gerät arbeiten soll.

Kapitel 12 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, 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.

12.1 WLAN

Im Menü **Wireless LAN**->**WLAN** können Sie das WLAN-Modul Ihres Geräts konfigurieren.

12.1.1 Einstellungen Funkmodul

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

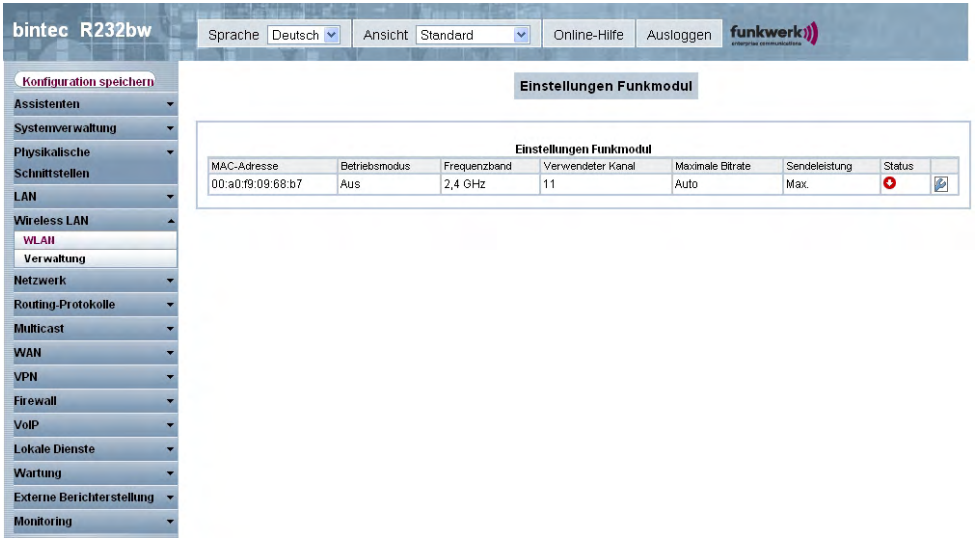


Abb. 51: **Wireless LAN->WLAN->Einstellungen Funkmodul**

12.1.1.1 Einstellungen Funkmodul-> 

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie die Schaltfläche  , um die Konfiguration zu bearbeiten.

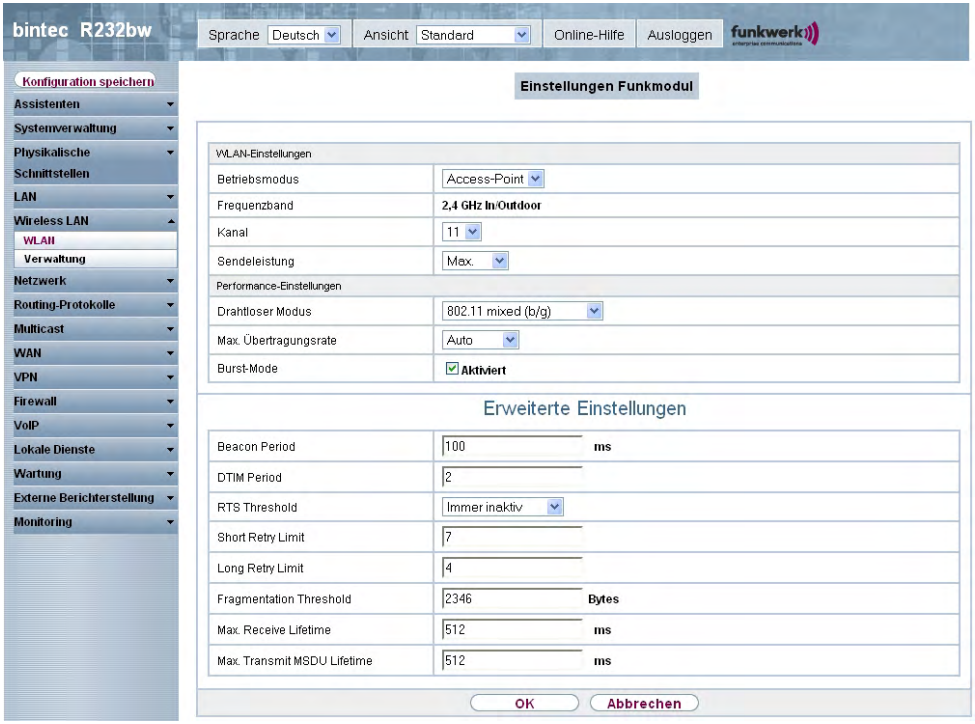


Abb. 52: **Wireless LAN->WLAN->Einstellungen Funkmodul->**

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

Felder im Menü Einstellungen FunkmodulWLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	Legen Sie fest, ob Ihr Gerät als `Access-Point` betrieben werden soll oder das Funkmodul deaktiviert werden soll (`Aus`, Standardwert).
Frequenzband	Zeigt das Frequenzband und den Einsatzbereich des Access-Points an. Mögliche Werte: • `2,4 GHz Indoor-Outdoor` (Standardwert): Der Access-Point wird innerhalb oder außerhalb von Gebäuden betrieben.
Kanal	Wählen Sie den Kanal aus, der verwendet werden soll.

Feld	Beschreibung
	Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate. Mögliche Werte sind *1* bis *13*. Der Standardwert ist *11*. 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.
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. • *7 dBm* • *9 dBm* • *12 dBm* • *15 dBm*

Felder im Menü Einstellungen FunkmodulPerformance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll.

Feld	Beschreibung
	Mögliche Werte: • *802.11g*: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • *802.11b*: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • *802.11 mixed (b/g)* (Standardwert) / *802.11 mixed short (b/g)*: Ihr Gerät passt sich der Technologie der Clients an. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • *802.11 mixed long (b/g)*: Ihr Gerät passt sich der Technologie der Clients an. 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.
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 aktiviert. Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion deaktiviert werden.

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

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*. Standardwert ist *100* msec.
DTIM Period	Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an. Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *2*.
RTS Threshold	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 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*.

Feld	Beschreibung
Long Retry Limit	Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, der länger ist als der in **RTS Threshold** definierten Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *4*.
Fragmentation Threshold	Geben Sie maximale Grösse an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Wert in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind *256* bis *2346*. Der Standardwert ist *2346* Bytes.
Max. Receive Lifetime	Geben Sie die Zeit nach dem initialen Empfangen des ersten Fragments eines Datenpakets ein, nach deren Ablauf keine weiteren Versuche unternommen werden. Das Datenpaket wird verworfen. Mögliche Werte sind *1* bis *4294967295*. Der Standardwert ist *512* msec.
Max. Transmit MSDU Lifetime	Geben Sie die Zeit nach dem initialen Senden des ersten Fragments eines Datenpakets ein, nach deren Ablauf keine weiteren Sendeversuche unternommen werden. Das Datenpaket wird verworfen. Mögliche Werte sind *1* bis *4294967295*. Der Standardwert ist *512* msec.

12.1.2 Drahtlosnetzwerke (VSS)

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

Hinweis

Das voreingestellte Drahtlosnetzwerk Funkwerk-EC 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 von 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.

WPA2

Die Erweiterung von WPA ist WPA2. In WPA2 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 (**ACL-Modus** 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 auf dem 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)** = *Funkwerk-ec*, 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* oder beidem, und tragen Sie den entsprechenden Schlüssel im Access-Point unter **WEP-Schlüssel** 1 - 4 oder **Preshared Key** und in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmäßig geändert werden. Wechseln Sie dazu **Übertragungsschlüssel**. Wählen Sie den längeren 104 Bit WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevanten Informationen sollte **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 auf das 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 156).

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

12.1.2.1 Bearbeiten oder Neu

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

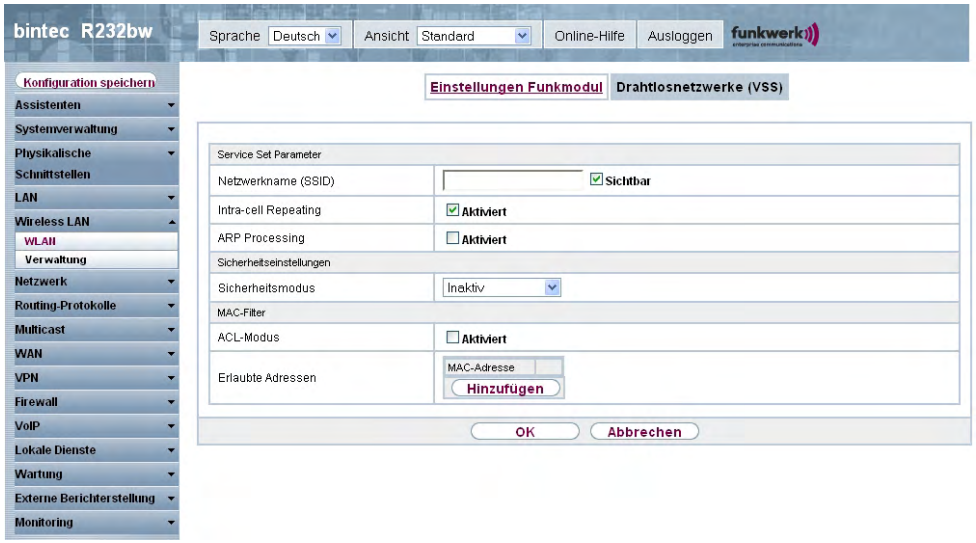


Abb. 53: **Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->** **->Neu**

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

Felder im Menü Drahtlosnetzwerke (VSS)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.

Feld	Beschreibung
	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 umgewandelt 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 in Zusammenhang mit der Funktion MAC-Bridge angewendet werden kann.

Felder im Menü Drahtlosnetzwerke (VSS)Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: • *Inaktiv* (Standardwert): weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11i/TKIP
Übertragungsschlüssel	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** 1 - 4 konfigurierten Schlüssel als Standardschlüssel aus. Standardwert ist *Schlüssel 1*.
WEP-Schlüssel 1-4	Nur für **Sicherheitsmodus** = *WEP 40* , *WEP 104* Geben Sie den WEP-Schlüssel ein.

Feld	Beschreibung
	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*, *funkwerk-wep1* für *WEP 104*.
WPA-Modus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: • *Inaktiv* (Standardwert): weder Verschlüsselung noch Authentifizierung • *WEP 40*: WEP 40 Bit • *WEP 104*: WEP 104 Bit • *WPA-PSK*: WPA Preshared Key • *WPA-Enterprise*: 802.11i/TKIP
WPA Cipher	Nur für **Sicherheitsmodus** = *WEP 40*, *WEP 104* Wählen Sie einen der in **WEP-Schlüssel** 1 - 4 konfigurierten Schlüssel als Standardschlüssel aus. Standardwert ist *Schlüssel 1*.
WPA2 Cipher	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*, *funkwerk-wep1* für *WEP 104*.
Preshared Key	Nur für **Sicherheitsmodus** = *WPA-PSK* Geben Sie das WPA-Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein. Beachte: Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!

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

Felder im Menü MAC-Filter

Feld	Beschreibung
ACL-Modus	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	Legen Sie Einträge mit **Hinzufügen** an und geben Sie die MAC-Adressen der Clients (**MAC-Adresse**) ein, die zugelassen werden sollen.

12.2 Verwaltung

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

12.2.1 Grundeinstellungen

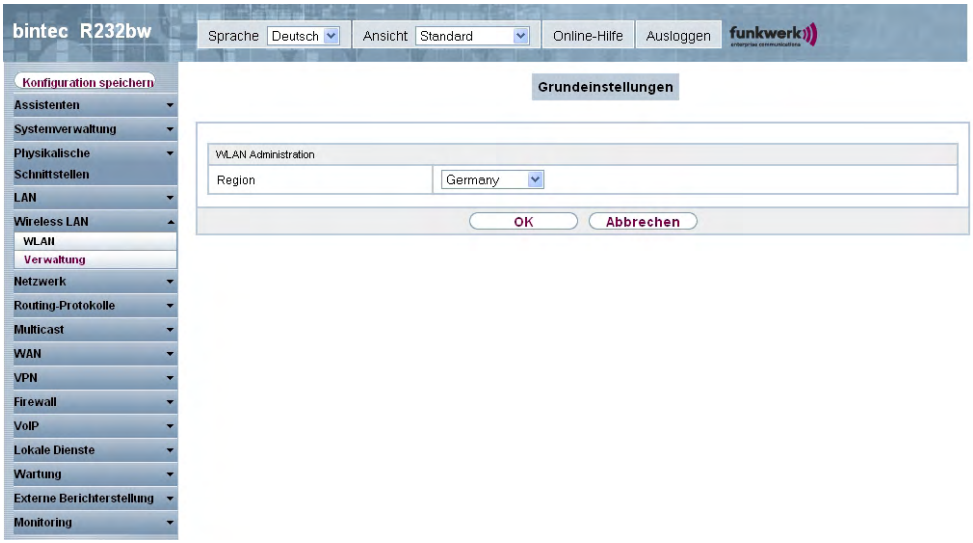


Abb. 54: **Wireless LAN->Verwaltung->Grundeinstellungen**

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

Feld im Menü GrundeinstellungenWLAN Administration

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

Kapitel 13 Netzwerk

13.1 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 machen, 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 **Metrik**, wenn Sie mehrere Standard-Routen eintragen.

13.1.1 IP-Routen

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

13.1.1.1 Bearbeiten oder Neu

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

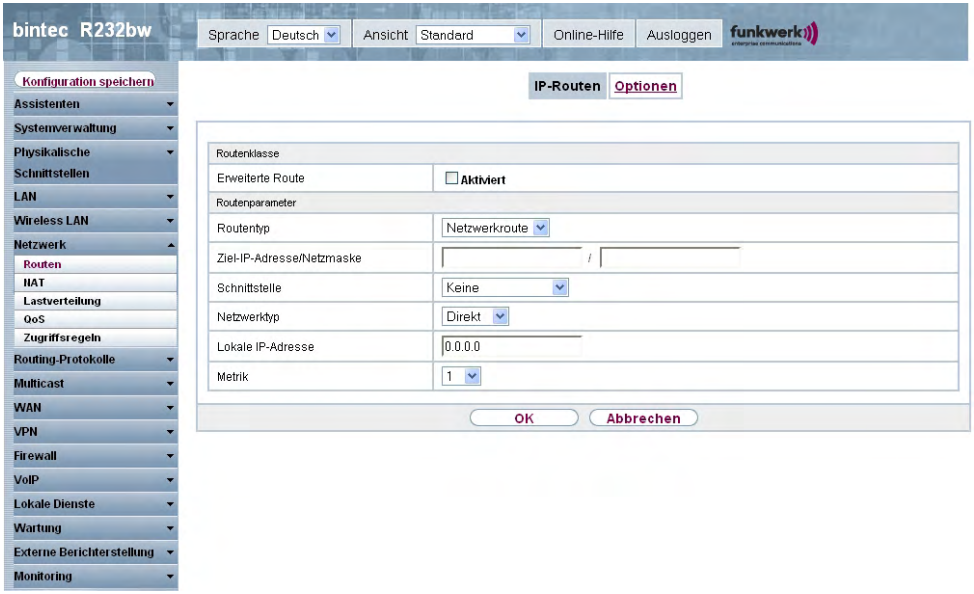


Abb. 55: **Netzwerk**->**Routen**->**IP-Routen**->**Neu** *mit* **Erweiterte Route** *= nicht aktiviert.*

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

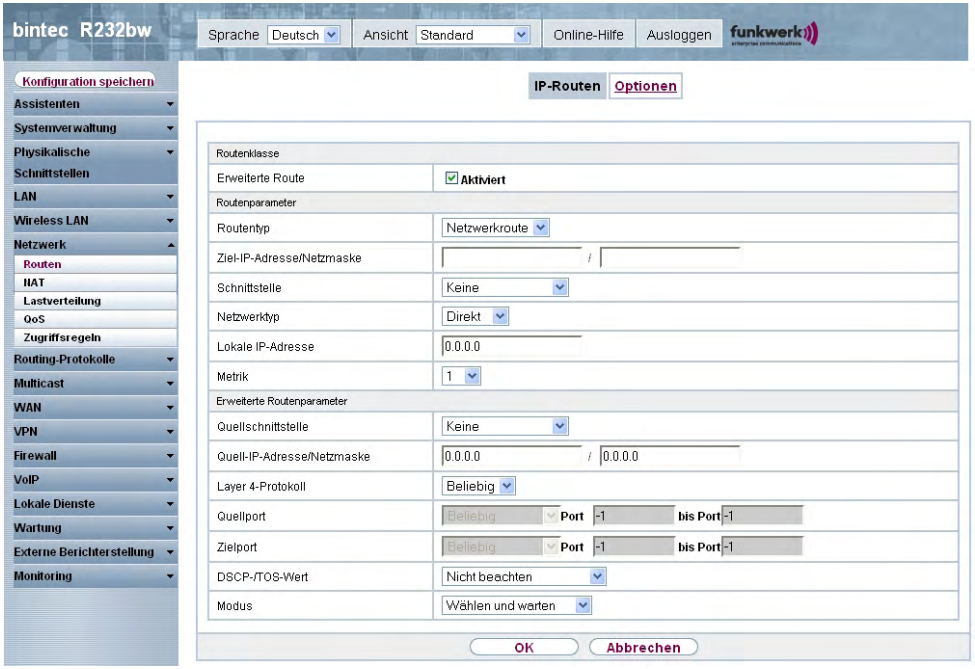


Abb. 56: **Netzwerk**->**Routen**->**IP-Routen**->**Neu** *mit* **Erweiterte Route** = `Aktiviert`

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

Feld im Menü IP-RoutenRoutenklasse

Feld	Beschreibung
Erweiterte Route	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. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü IP-RoutenRoutenparameter

Feld	Beschreibung
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte:

Feld	Beschreibung
	• *Netzwerkroute* (Standardwert): Route zu einem Netzwerk. • *Standardroute* : Wird benutzt, wenn keine andere passende Route verfügbar ist. • *Hostroute* : Route zu einem einzelnen Host.
Ziel-	Nur für **Routentyp** *Hostroute* oder *Netzwerkroute* Geben Sie die IP-Adresse des Ziel-Hosts ein. Bei **Routentyp** = *Netzwerkroute* Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske.

Feld	Beschreibung
Ziel-IP-Adresse/Netzmaske	
Schnittstelle	Wählen Sie ggf. die Schnittstelle aus, welche für diese Route verwendet werden soll.

Netzwerktyp	Nicht für **Routentyp** = *Standardroute*
	Wählen Sie zusätzlich den Netzwerktyp aus.
	Mögliche Werte:
	• *Direkt*(Standardwert):
	  • im LAN: Sie definieren eine weitere IP-Adresse für die Schnittstelle.
	  • im WAN: Sie definieren eine Route ohne Transitnetzwerk.
	• *Indirekt*:
	  • im LAN: Sie definieren eine Gateway-Route.
	  • im WAN: Sie definieren eine Route mit Transitnetzwerk.

Lokale IP-Adresse	Nur für **Netzwerktyp** = *Direkt* Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Gateway	Nur für **Netzwerktyp** = *Indirekt* Geben Sie die IP-Adresse des Hosts 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* . Standardwert ist *1* .

Felder im Menü IP-RoutenErweiterte Routenparameter

Feld	Beschreibung
Quellschnittstelle	Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen.

Feld	Beschreibung
	Standardwert ist *Keine*.
Neue 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*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *L2TP*, *Beliebig*. Standardwert ist *Beliebig*.
Quellport	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.

Feld	Beschreibung
	Wählen Sie zunächst den Portnummernbereich aus. Mögliche Werte: • *Beliebig* (Standardwert): Die Route gilt für alle Port-Nummern. • *Einzeln*: Ermöglicht Eingabe einer Port-Nummer. • *Bereich*: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • *Privilegiert*: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • *Server*: Eingabe von Server Port-Nummern: 5000 ... 32767. • *Clients 1*: Eingabe von Client Port-Nummern: 1024 ... 4999. • *Clients 2*: Eingabe von Client Port-Nummern: 32768 ... 65535. • *Nicht privilegiert*: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in **Port** (einzelner bzw. Anfangsport) und ggf. in **bis Port** (Endport) die entsprechenden Werte ein.
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). • *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. Geben Sie für *DSCP-Binärwert*, *DSCP-Dezimalwert*, *TOS-*

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

13.1.2 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.

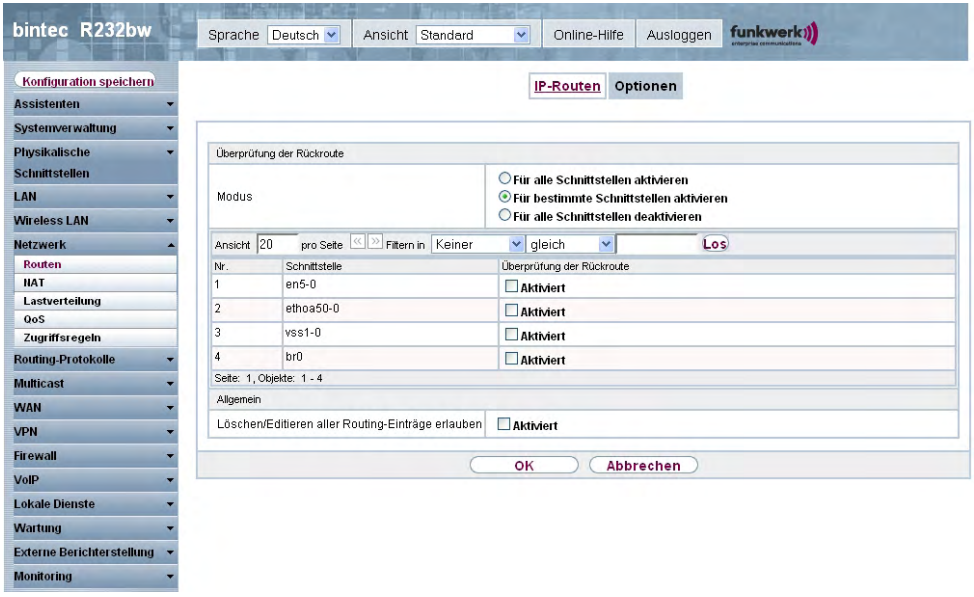


Abb. 57: **Netzwerk->Routen->Optionen**

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

Felder im Menü OptionenÜberprüfung der Rückroute

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

Feld	Beschreibung
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.

Felder im Menü OptionenAllgemein

Feld	Beschreibung
Löschen/Editieren aller Routing-Einträge erlauben	Legen Sie fest,ob alle auf Ihrem Gerät eingetragenen Routen im Menü **Netzwerk**->**Routen**->**IP-Routen** editierbar und löschbar sein sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion für alle Schnittstellen deaktiviert.

13.2 NAT

13.2.1 NAT-Schnittstellen

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 169).

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

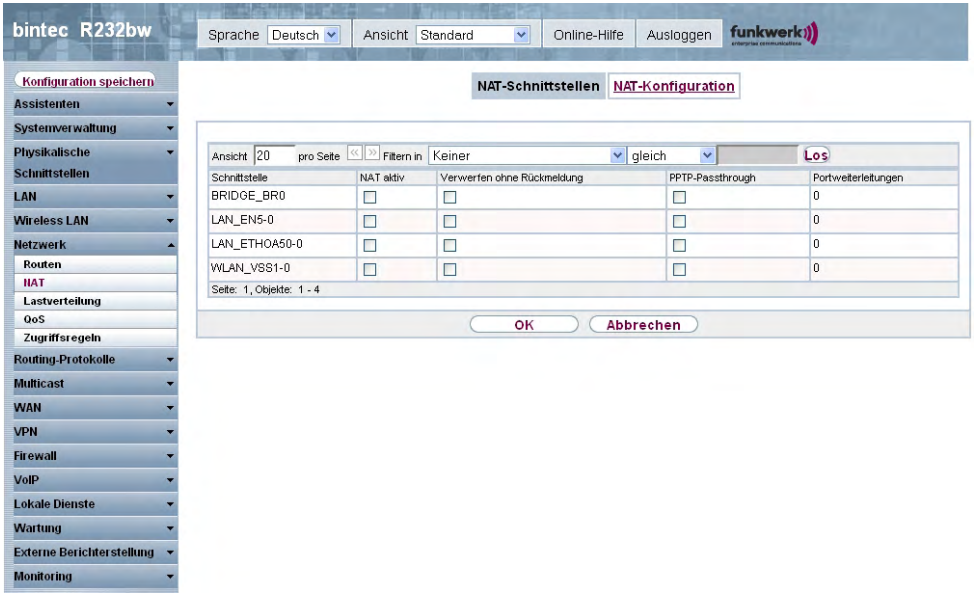


Abb. 58: **Netzwerk->NAT->NAT-Schnittstellen**

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

Außerdem wird in *Portweiterleitungen* angezeigt, wieviele 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.
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.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv. Wenn**PPTP-Passthrough** aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.
Port	Zeigt die Anzahl der in **Netzwerk**->**NAT**->**NAT-Konfiguration** konfigurierten Portweiterleitungsregeln an.

13.2.2 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.

13.2.2.1 Neu

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

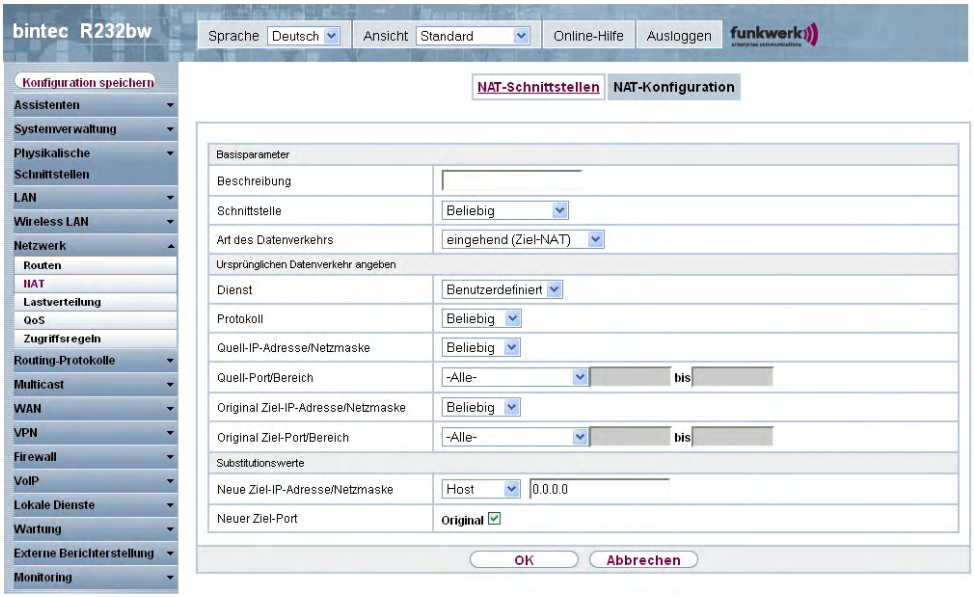


Abb. 59: **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu**

Das Menü **Netzwerk**->**NAT**->**NAT-Konfiguration** ->**Neu** besteht aus folgenden Feldern:

Feld im Menü NAT-KonfigurationBasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll. Mögliche Werte: • *Beliebig* (Standardwert): NAT wird für alle Schnittstellen konfiguriert. • *<Schnittstellenname>* : Wählen Sie eine der Schnittstellen aus der Liste aus.
Art des Datenverkehrs	Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll. Mögliche Werte: • *eingehend (Ziel-NAT)* (Standardwert): Der Datenverkehr, der von außen kommt. • *ausgehend (Quell-NAT)*: Der Datenverkehr, der nach außen geht. • *exklusiv (ohne NAT)*: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*. Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden. Mögliche Werte: • *full-cone*(nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiierende Quelladresse und den initialen Quellport senden. • *restricted-cone* (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen.

Feld	Beschreibung
	• *port-restricted-cone*(nur UDP): Wie restricted- cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • *symmetrisch* (Standardwert) beliebiges Protokoll: 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 NAT-KonfigurationUrsprünglichen 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>*
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 automatisch festgelegt. Wählen Sie ein Protokoll aus. Je nach ausgewähltem **Dienst** stehen verschiedene Protokolle zur Verfügung. Mögliche Werte: • *Beliebig* (Standardwert) • *AH* • *Chaos* • *EGP* • *ESP*

Feld	Beschreibung
	• *GGP* • *GRE* • *HMP* • *ICMP* • *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	Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Quellport	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch* und **Dienst** = *Benutzerdefiniert*. Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Quell-Port/Bereich	Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*. Geben Sie den Quellport bzw. den Quellportbereich der ursprünglichen Datenpakete ein. Die Standardeinstel-

Feld	Beschreibung
	lung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.
Original Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-Port/Bereich	Nur für **Dienst** = *Benutzerdefiniert*. 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 NAT-KonfigurationSubstitutionswerte

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)*. 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)*. Geben Sie diejenige Quell-IP-Adresse mit zugehöriger Netzmaske ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll.
Neuer Quell-Port	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*. Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-

Feld	Beschreibung
	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 q-Port eingeben. Standardmäßig ist *Original* aktiv.

13.3 Lastverteilung

13.3.1 Lastverteilungsgruppen

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 nach folgenden Prinzipien:

- 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 Lupensymbol neben einem Listeneitrag gelanegen Sie zu einer Übersicht über diese Gruppe betreffende Grundparamater.

Hinweis

Beachten Sie, dass die Schnittstellen, die zu einer Lastverteilungsgruppe zusammengefasst werden, Routen mit gleicher Metrik haben müssen. Gehen Sie ggf. in das Menü **Netzwerk**->**Routen** und überprüfen Sie dort die Einträge.

13.3.1.1 Neu

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

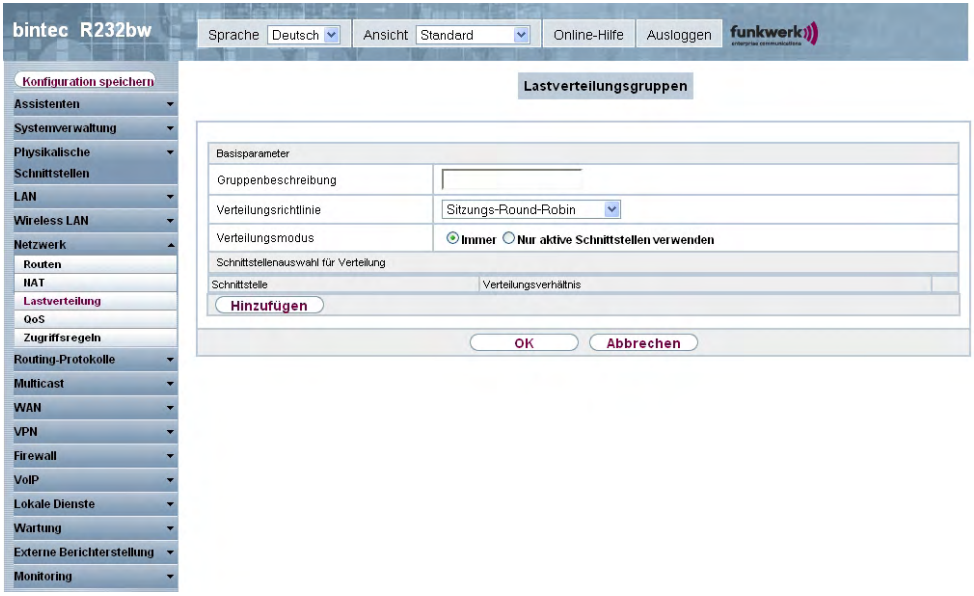


Abb. 60: **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**

Das Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü LastverteilungsgruppenBasisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
Verteilungsrichtlinie	Wählen Sie aus, auf welche Art der Datenverkehr auf die für die Gruppe konfigurierten Schnittstellen verteilt werden soll. Mögliche Werte: • `Sitzungs-Round-Robin`(Standardwert): Eine neu hinzukommende Session wird je nach prozentualer Belegung der Schnittstellen mit Sessions einer der Gruppen-Schnittstellen zugewiesen. Die Anzahl der Sessions ist maßgeblich. • `Lastabhängige Bandbreite`: Eine neu hinzukommende Session wird je nach Anteil der Schnittstellen an der Gesamtdatenrate einer der Gruppen-Schnittstellen zugewiesen. Maßgeblich ist die aktuelle Datenrate, wobei der Datenverkehr sowohl in Sende- als auch in Empfangsrichtung berücksichtigt wird.

Feld	Beschreibung
Berücksichtigen	Nur für **Verteilungsrichtlinie** = *Lastabhängige Bandbreite* Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll. Optionen: • *Download*: Nur die Datenrate in Empfangsrichtung wird berücksichtigt. • *Upload*: Nur die Datenrate in Senderichtung wird berücksichtigt. Standardmäßig sind die Optionen *Download* und *Upload* deaktiviert.
Verteilungsmodus	Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden. Mögliche Werte: • *Immer*(Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen. • *Nur aktive Schnittstellen verwenden*: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.

Im Bereich **Schnittstelle** fügen Sie Schnittstellen hinzu, die dem aktuellen Gruppenkontext entsprechen und konfigurieren diese. Sie können auch Schnittstellen löschen.

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

Felder im Menü LastverteilungsgruppenSchnittstellenauswahl 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 verwendeter **Verteilungsverhältnis**:

Feld	Beschreibung
	• für *Sitzungs-Round-Robin* wird die Anzahl verteilten Sessions zugrunde gelegt. • für *Lastabhängige Bandbreite* ist die Datenrate maßgeblich.

13.4 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.

13.4.1 QoS-Filter

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

13.4.1.1 Neu

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

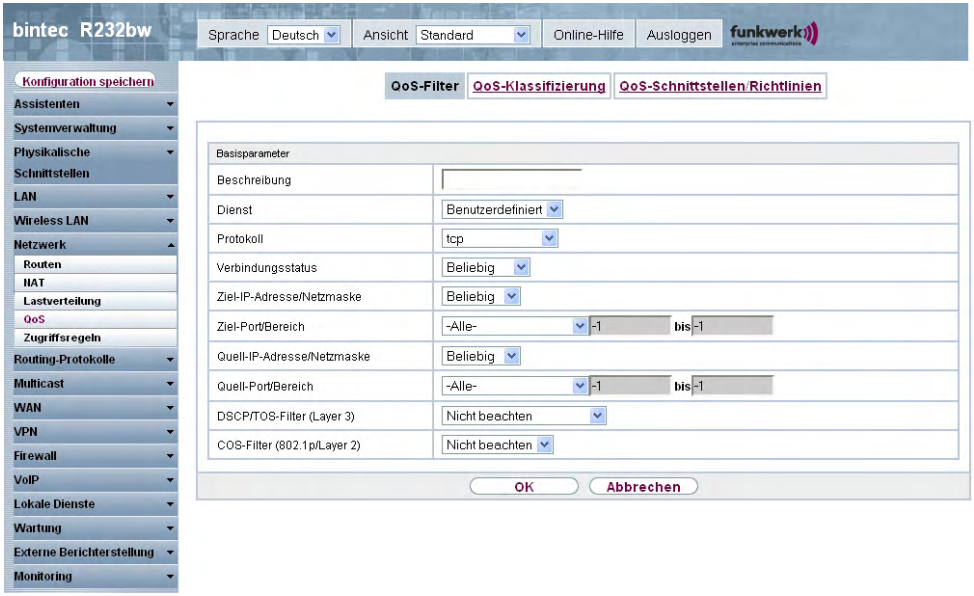


Abb. 61: **Netzwerk->QoS->QoS-Filter->Neu**

Das Menü **Netzwerk->QoS->QoS-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü QoS-FilterBasisparameter

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* Standardwert ist *Benutzerdefiniert*.

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option *nicht überprüfen* (Standardwert) passt auf jedes Protokoll.
Typ	Nur für **Protokoll** = *icmp* Wählen Sie einen Typ aus. Mögliche Werte: *Beliebig*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Siehe RFC 792. 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 Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Zielport ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.

Feld	Beschreibung
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 Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Zielport ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Zielport ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
DSCP/TOS-Filter (Layer 3)	Wählen Sie, wie die Priorität der IP-Pakete signalisiert ist. Mögliche Werte: • *Nicht beachten* (Standardwert): Es wird keine Signalisierung der Priorität verwendet. • *DSCP-Binärwert*: Differentiated Services Code Point wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *TOS-Binärwert*: Type of Service wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 8 Bit). • *TOS-Dezimalwert*: Type of Service wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format) . Weitergehende Informationen zu DSCP und TOS finden Sie in den RFCs 3260 und 1349.
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*.

Feld	Beschreibung
	Der Standardwert ist *0*.

13.4.2 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.

13.4.2.1 Neu

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

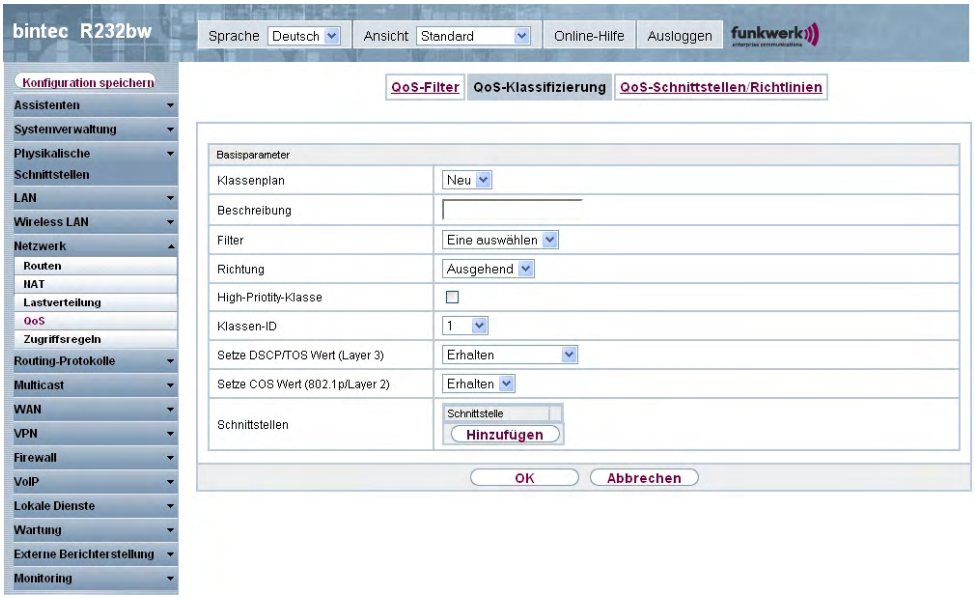


Abb. 62: **Netzwerk**->**QoS**->**QoS-Klassifizierung**->**Neu**

Das Menü **Netzwerk**->**QoS**->**QoS-Klassifizierung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü QoS-KlassifizierungBasisparameter

Feld	Beschreibung
Klassenplan	Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen.

Feld	Beschreibung
	Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. • *<Name des Klassenplans>*: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können. 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.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Klassen-ID	Nur für **High-Priority-Klasse** nicht aktiv. Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist. Hinweis: Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.) Mögliche Werte sind ganze Zahlen zwischen *1* und *254*.
Setze DSCP/TOS Wert (Layer 3)	Hier können Sie den DSCP/TOS Wert der IP Datenpakete in Abhängigkeit zur definierten Klasse ("Klassen-ID") setzen/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 Signalierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem 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.
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*. Standardwert ist *Erhalten*.
Schnittstellen	Nur für **Klassenplan** = *Neu*. Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen

Feld	Beschreibung
	Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.

13.4.3 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.

13.4.3.1 Neu

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

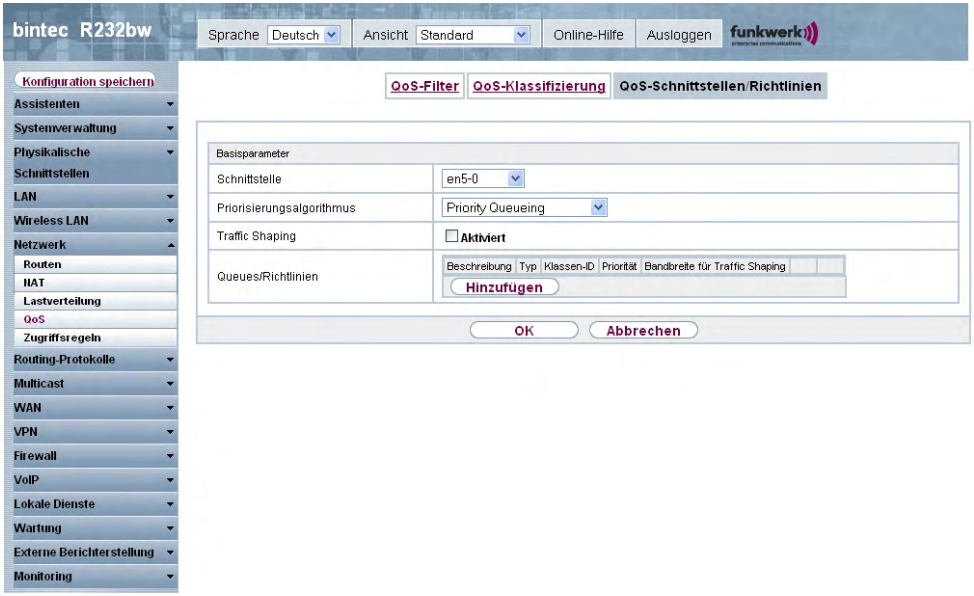


Abb. 63: **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu**

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

Felder im Menü QoS-Schnittstellen/RichtlinienBasisparameter

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

Feld	Beschreibung
	den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. • *Deaktiviert* (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für **Traffic Shaping** aktiviert. Geben Sie für die 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	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*

Feld	Beschreibung
	• *IPSec über Ethernet und VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE und VLAN*
Real Time Jitter Control	Nur für **Traffic Shaping** aktiviert Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite. Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s). Aktivieren oder deaktivieren Sie Real Time Jitter Control. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Kontrollmodus	Nur für **Real Time Jitter Control** aktiviert. Wählen Sie den Modus für die Optimierung der Sprachübertragung. Mögliche Werte: • *Alle RTP-Streams*: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. • *Inaktiv*: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • *Nur kontrollierte RTP-Streams*: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW. • *Immer*: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.

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

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.
Priorisierungs-Queue	Wählen Sie den Typ für die Priorisierung der Queue aus. Mögliche Werte: • *Klassenbasiert* (Standardwert): Queue für "normal"-klassifizierte Daten. • *Hohe Priorität*: Queue für "high-priority"- klassifizierte Daten. • *Standard*: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	Nur für **Priorisierungs-Queue** = *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 **Priorisierungs-Queue** = *Klassenbasiert*. Wählen Sie die Piorität der Queue. Mögliche Werte sind *1* bis

Feld	Beschreibung
	254. Der Standardwert ist *1*.
Gewichtung	Nur für **Priorisierungsalgorithmus** = *Weighted Round Robin* oder *Weighted Fair Queueing* Wählen Sie die Gewichtung der Queue. Mögliche Werte sind *1* bis *254*. Der Standardwert ist *1*.
RTT-Modus (Realtime-Traffic-Modus)	Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen. Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung. Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.) Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upload-Geschwindigkeit	Nur für **Traffic Shaping** aktiviert. Geben Sie eine maximale Datenrate in kBit pro Sekunde für die Queue ein. Mögliche Werte sind *0* bis *1000000*.

Feld	Beschreibung
	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 Bandbreitenbegrnzung 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 von 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.

Feld	Beschreibung
Vermeidung von Datenstau (RED)	Wählen Sie das Verfahren, nach dem Pakete zwischen **Min. Queue-Größe** und **Max. Queue-Größe** vorbeugend verworfen werden, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Mögliche Werte: • *Keiner* (Standardwert): Es werden keine Pakete verworfen. • *weighted-random*: Abhängig vom Füllungsgrad der Queue werden Pakete verworfen. Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden können.
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*.

13.5 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** 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.

13.5.1 Zugriffsfilter

In diesem Menü werden die Access Filter konfiguriert. Jedes Filter beschreibt einen bestimmten Teil von 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.

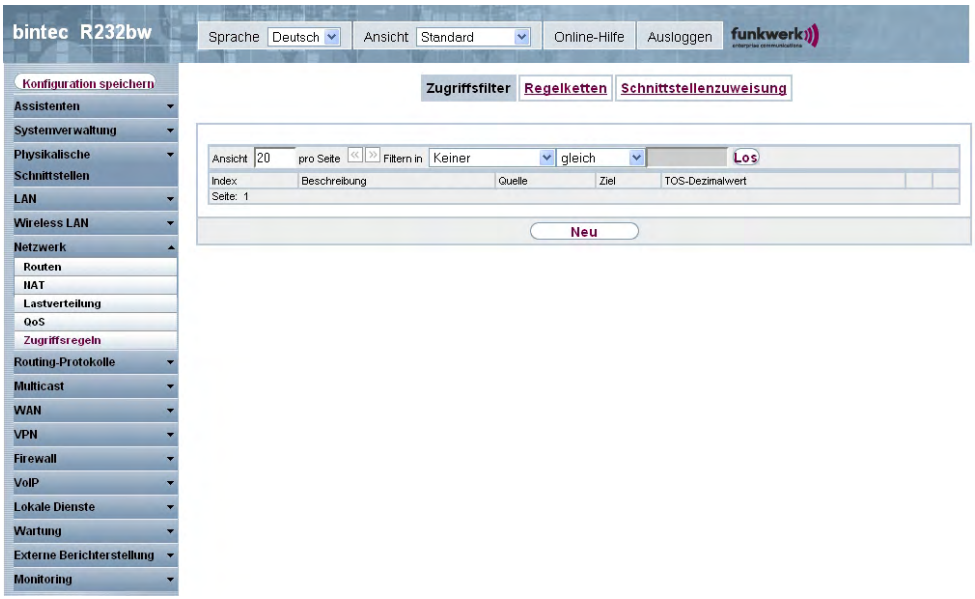


Abb. 64: **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter**

13.5.1.1 Bearbeiten oder Neu

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

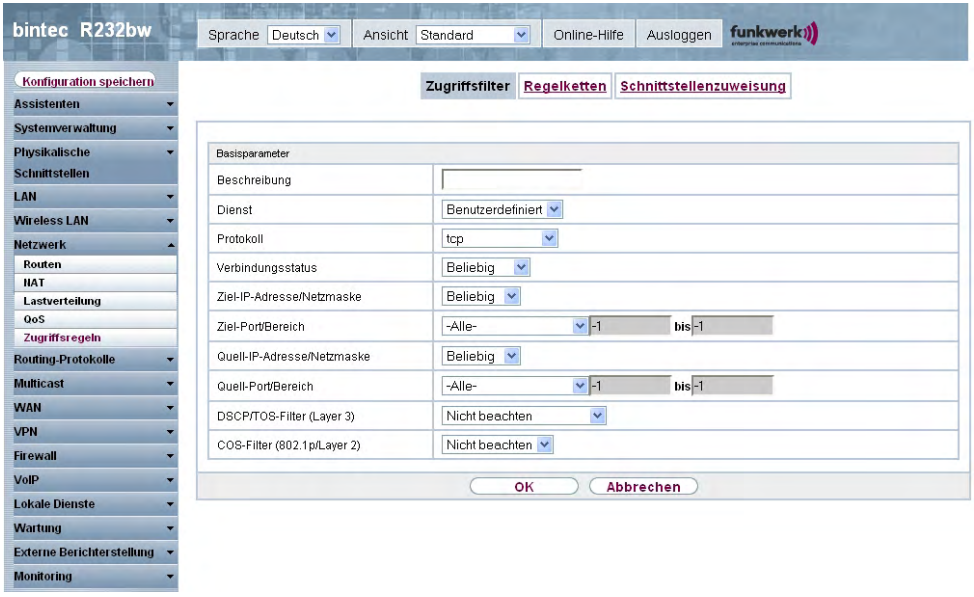


Abb. 65: **Netzwerk->Zugriffsregeln->Zugriffsfilter->Neu**

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

Felder im Menü ZugriffsfilterBasisparameter

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* Standardwert ist *Benutzerdefiniert*.

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option *nicht überprüfen* (Standardwert) passt auf jedes Protokoll.
Typ	Nur bei **Protokoll** = *icmp* Mögliche Werte: • *Any* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* . Standardwert ist *Any*. 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:

Feld	Beschreibung
	• *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	Nur bei **Protokoll** = *tcp*, *udp* Geben Sie Ziel-Port-Nummer bzw. Bereich von Ziel-Port- Nummern ein, auf den das Filter passt. Mögliche Werte: • *-Alle-* (Standardwert): Die Route 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. Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Die Route 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 Signalierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalierung der Priorität der IP-

Feld	Beschreibung
	Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalierung 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*. Standardwert ist *Nicht beachten*.

13.5.2 Regelketten

Im Menü Access Lists 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.

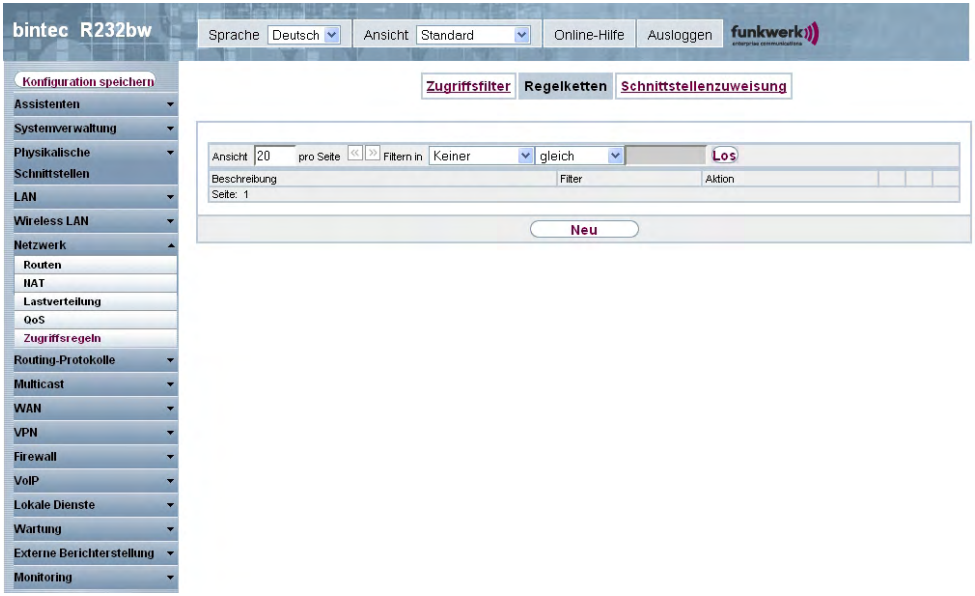


Abb. 66: **Netzwerk->Zugriffsregeln+Regelketten**

13.5.2.1 Bearbeiten oder Neu

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

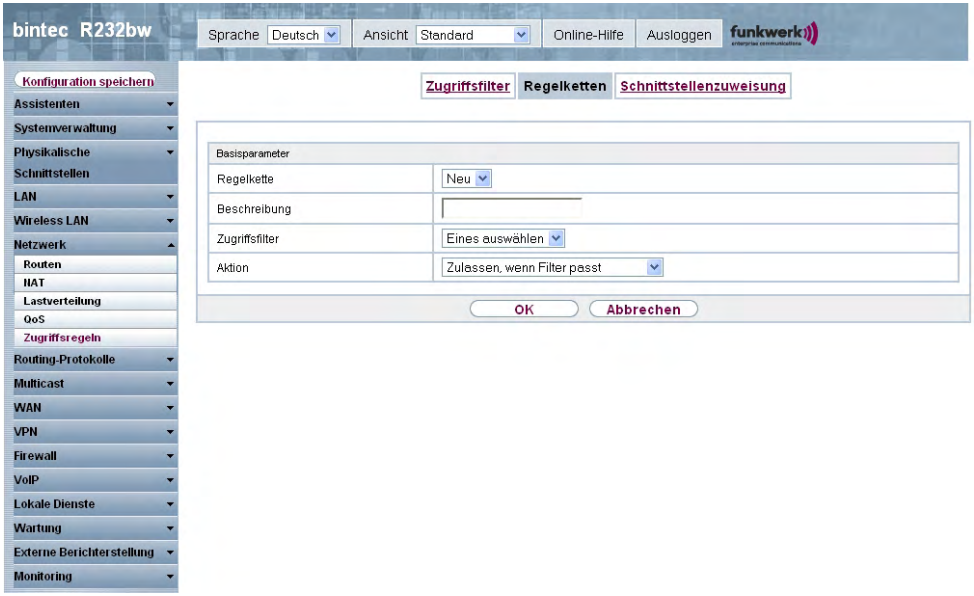


Abb. 67: **Netzwerk->Zugriffsregeln+Regelketten->Neu**

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

Felder im Menü RegelkettenBasisparameter

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 des Klassenplans>`: 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.

Feld	Beschreibung
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *Zulassen* (Standardwert): Paket annehmen, wenn das Filter passt. • *Zulassen, wenn Filter nicht passt*: Paket annehmen, wenn das Filter nicht passt. • *Verweigern, wenn Filter passt*: Paket abweisen, wenn das Filter passt. • *Verweigern, wenn Filter nicht passt*: Paket abweisen, wenn das Filter nicht passt. • *Nicht beachten*: Nächste Regel anwenden.

Um die Regeln einer Regelkette in eine andere Reihenfolge zu bringen, wählen Sie im Listenmenü bei dem Eintrag, der verschoben werden soll, die Schaltfläche . Daraufhin öffnet sich ein Dialog, bei dem Sie unter **Verschieben** entscheiden können, ob der Eintrag *unter* (Standardwert) oder *über*einer weiteren Regel dieser Regelkette verschoben wird.

13.5.3 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.

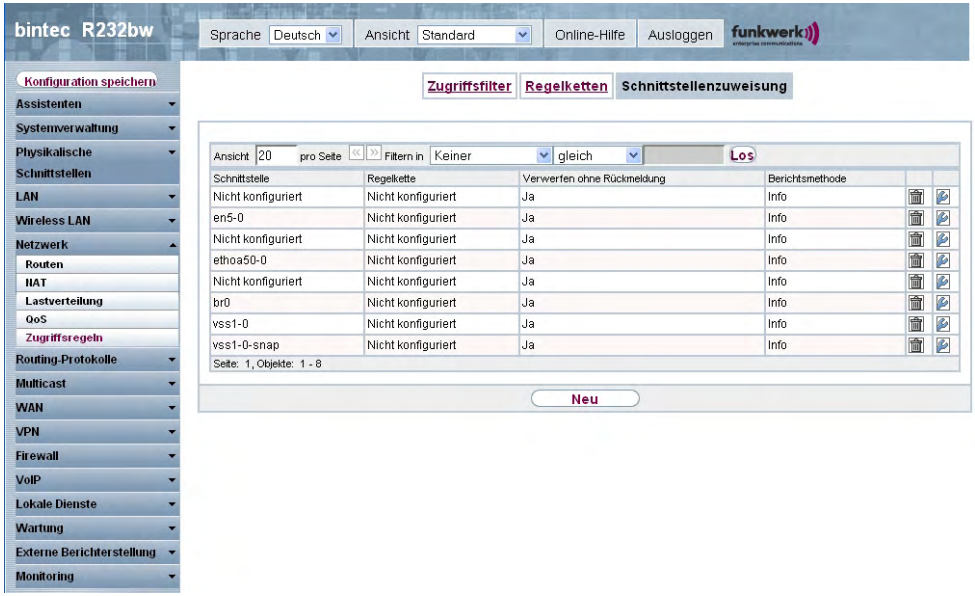


Abb. 68: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung**

13.5.3.1 Bearbeiten oder Neu

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

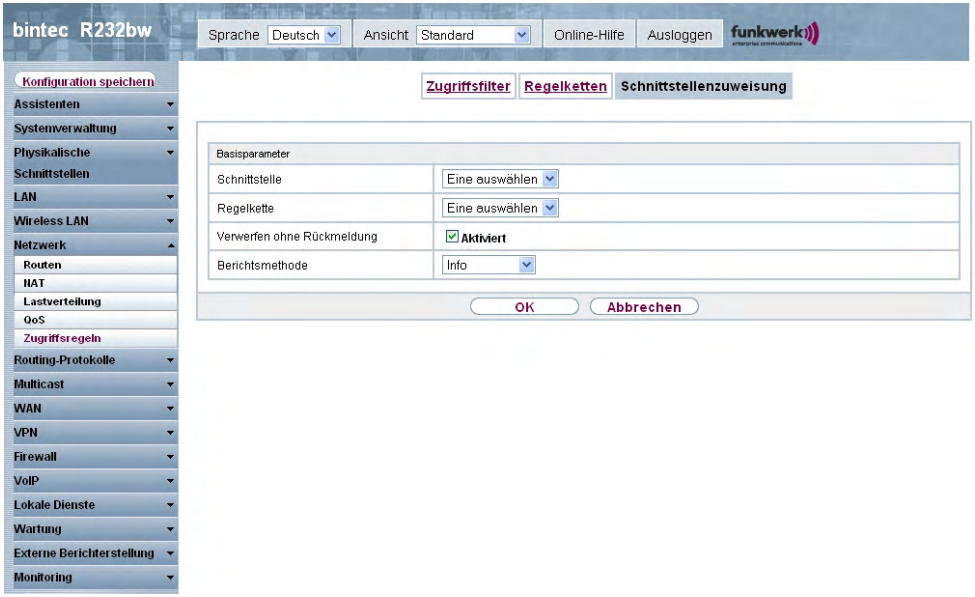


Abb. 69: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung->Neu**

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

Felder im Menü SchnittstellenzuweisungBasisparameter

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. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiviert.
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

Feld	Beschreibung
	wird generiert. • *Dump*: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

Kapitel 14 Routing-Protokolle

14.1 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.

14.1.1 RIP-Schnittstellen

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

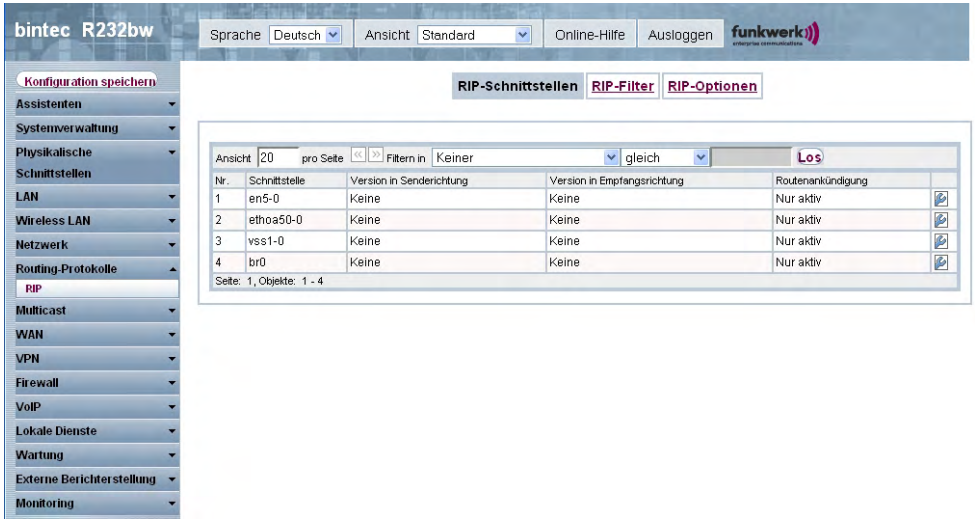


Abb. 70: **Routing-Protokolle->RIP->RIP-Schnittstellen**

14.1.1.1 Bearbeiten

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

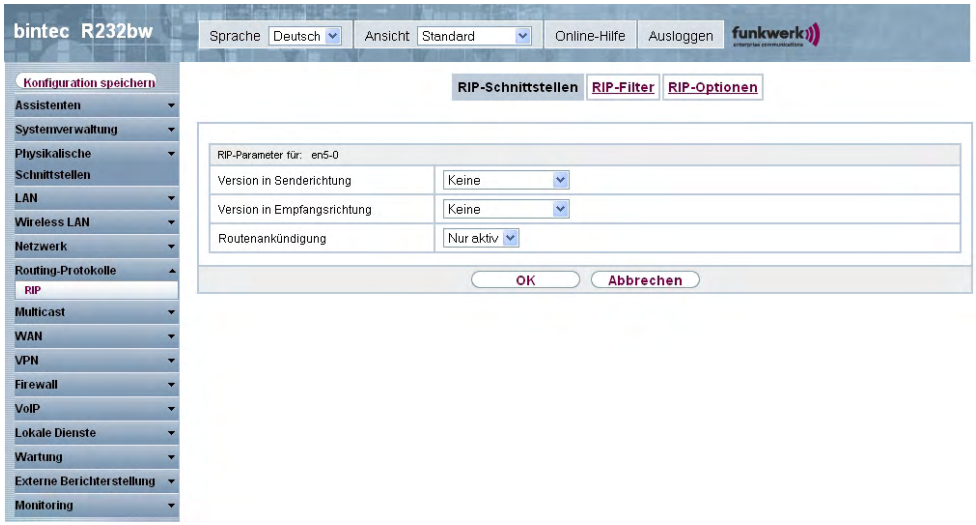


Abb. 71: **Routing-Protokolle->RIP->RIP-Schnittstellen->**

Das Menü **Routing-Protokolle->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 (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).

Feld	Beschreibung
	• *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 interface-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.

14.1.2 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.

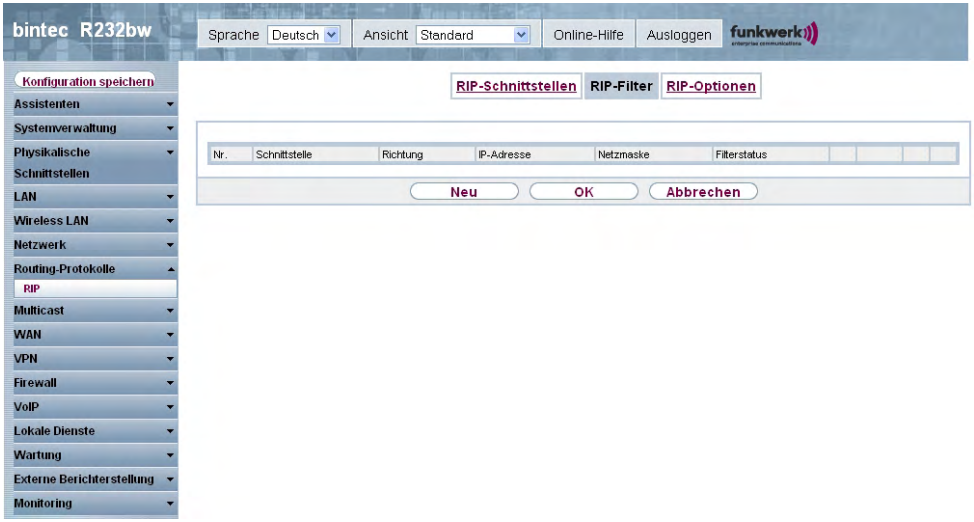


Abb. 72: **Routing-Protokolle->RIP->RIP-Filter**

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.

14.1.2.1 Neu

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

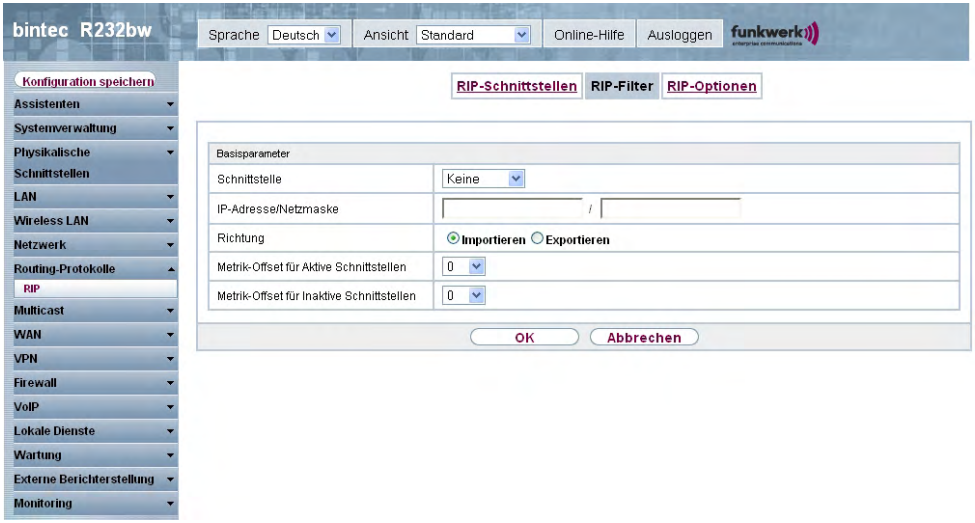


Abb. 73: **Routing-Protokolle->RIP->RIP-Filter->Neu**

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

Felder im Menü RIP-FilterBasisparameter

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*

Feld	Beschreibung
Metrik-Offset für Aktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Aktiv" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Aktiv" ist. Mögliche Werte sind *-16* bis *16*. 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*. Standardwert ist *0*.

14.1.3 RIP-Optionen

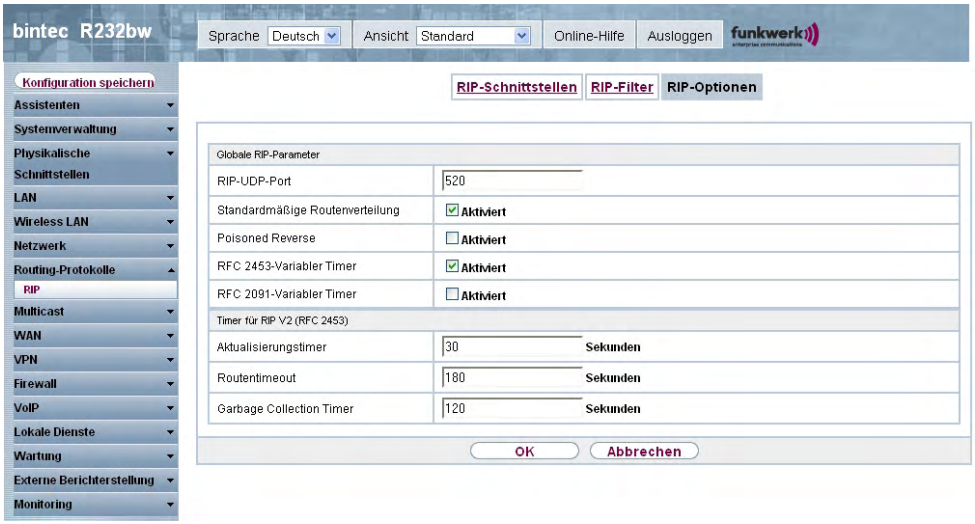


Abb. 74: **Routing-Protokolle->RIP->RIP-Optionen**

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

Felder im Menü RIP-OptionenGlobale RIP-Parameter

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

Feld	Beschreibung
	Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Felder im Menü RIP-OptionenTimer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	Nur für **RFC 2453-Variabler Timer** = *Aktiviert* Nach Ablauf dieses Zeitraums wird ein 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 RIP-OptionenTimer 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).

Feld	Beschreibung
Retransmission Timer	Nur für **RFC 2091-Variabler Timer** = *Aktiviert* Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft. Der Standardwert ist 5 (in Sekunden).

Kapitel 15 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 Emfpänger 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. Memberschip 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 benutzt. 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 eingehendem 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.

15.1 Allgemein

15.1.1 Allgemein

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

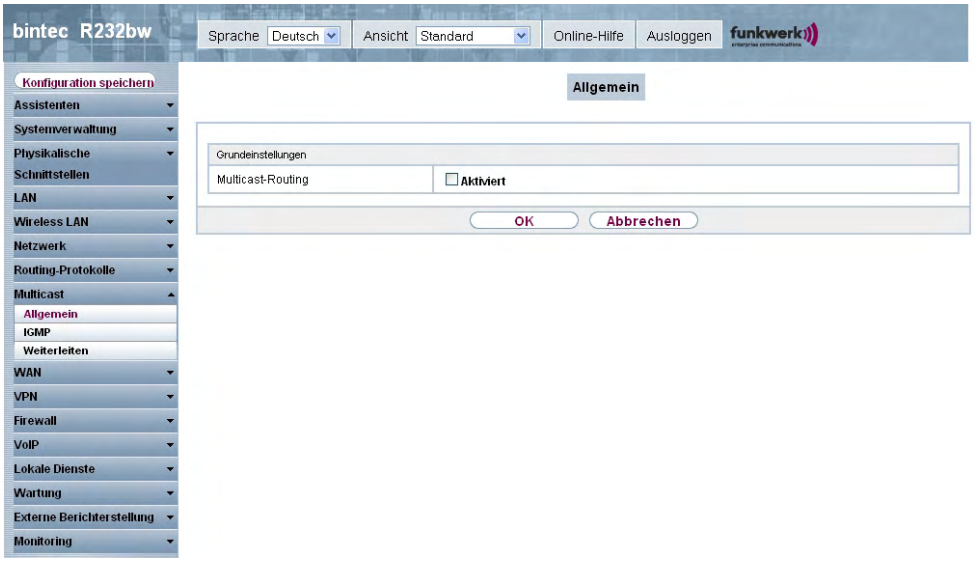


Abb. 75: **Multicast->Allgemein->Allgemein**

Das Menü **Multicast->Allgemein->Allgemein** besteht aus den folgenden Feldern:

Felder im Menü AllgemeinGrundeinstellungen

Feld	Beschreibung
Multicast-Routing	Wählen Sie aus, ob **Multicast-Routing** verwendet werden soll. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

15.2 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.

15.2.1 IGMP

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

15.2.1.1 Bearbeiten oder Neu

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

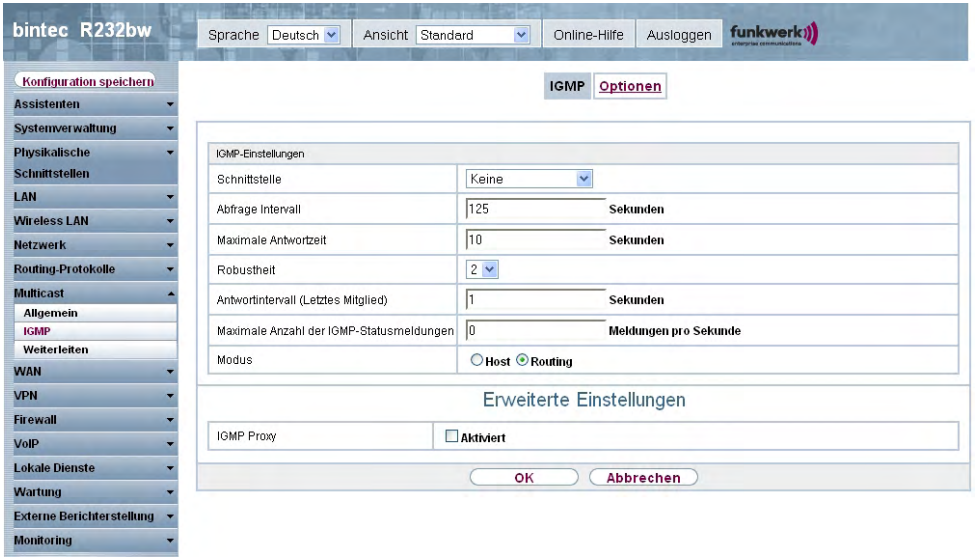


Abb. 76: **Multicast->IGMP->IGMP->Neu**

Das Menü **Multicast->IGMP->IGMP->Neu** besteht aus den folgenden Feldern:

Felder im Menü IGMPIGMP-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* bis *100*. Der Standardwert ist *100*.

Feld	Beschreibung
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 dieses Schnittstelle weitergeleitet werden müssen. Möglich Werte sind *0* bis *255*. Der Standardwert ist *10*.
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.

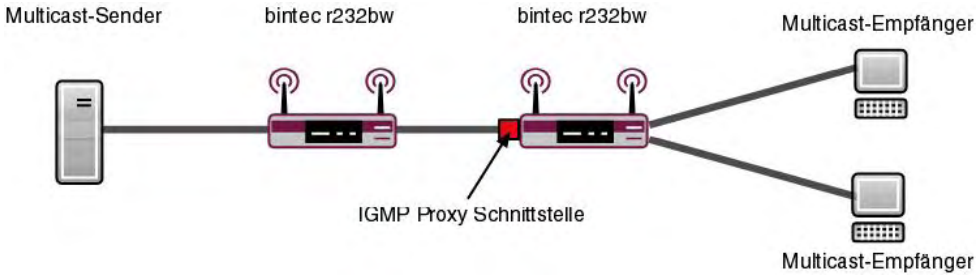


Abb. 77: IGMP Proxy

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.

15.2.2 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.

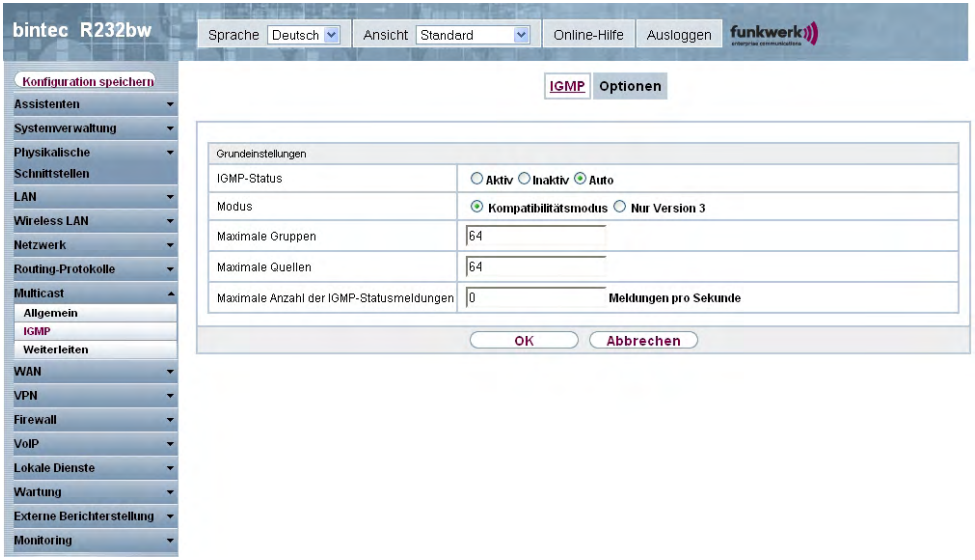


Abb. 78: **Multicast->IGMP->Optionen**

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

Felder im Menü OptionenGrundeinstellungen

Feld	Beschreibung
IGMP-Status	Wählen Sie den IGMP-Status aus. Mögliche Werte: • `Auto` (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden. • `Aktiv`: Multicast ist immer aktiv. • `Inaktiv`: Multicast ist immer inaktiv.
Modus	Nur für **IGMP-Status** = `Aktiv`oder `Auto` Wählen Sie den Multicast-Modus aus. Mögliche Werte: • `Kompatibilitätsmodus` (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen konnte. • `Nur Version 3`: Nur IGMP Version 3 wird verwendet.

Feld	Beschreibung
Maximale Gruppen	Geben Sie ein, wieviele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen.
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.
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.

15.3 Weiterleiten

15.3.1 Weiterleiten

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

15.3.1.1 Neu

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

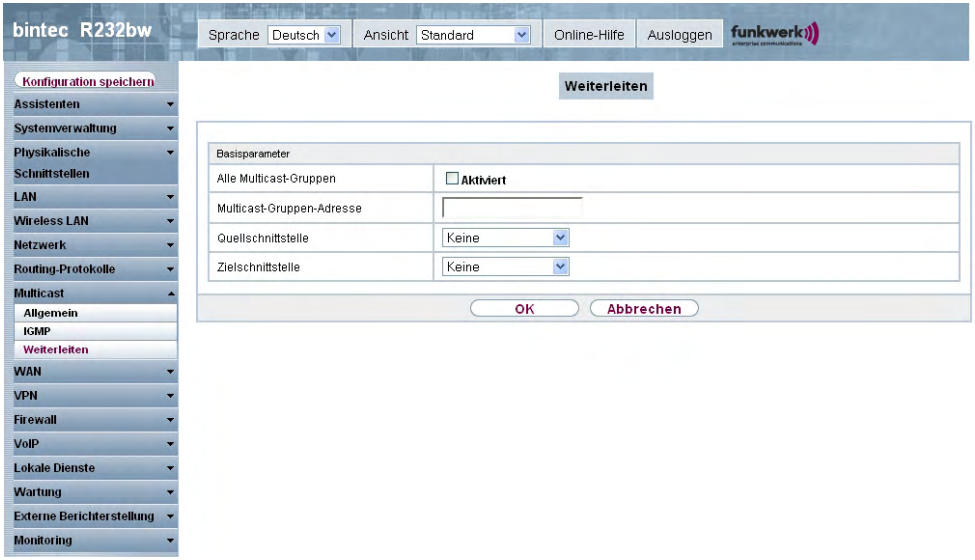


Abb. 79: **Multicast->Weiterleiten->Weiterleiten->Neu**

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

Felder im Menü WeiterleitenBasisparameter

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.

Kapitel 16 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.

16.1 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), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist ebenfalls konfigurierbar.

Hinweis

Beachten Sie die Vorgaben Ihres Providers!

Einwahl-Verbindungen über ISDN dienen dazu, zu Netzwerken oder Hosts außerhalb Ihres LANs eine Verbindung herzustellen.

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **Benutzername**, 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

Feld	Beschreibung
	einer definierten Anzahl von Sekunden möglich)
	administrativ auf inaktiv gesetzt (deaktiviert); Verbindungsaufbau nicht möglich

Standard-Route (Default Route)

Bei einer Standard-Route werden automatisch alle Daten auf eine Verbindung geleitet, wenn keine andere passende Route verfügbar ist. Ein Zugang zum Internet sollte immer als Standard-Route zum Internet-Service-Provider (ISP) eingerichtet sein. Weitergehende Informationen zum möglichen Routentyp finden Sie unter **Netzwerk**->**Routen**.

NAT aktivieren

Mit Network Address Translation (NAT) verbergen Sie Ihr gesamtes Netzwerk nach außen hinter nur einer IP-Adresse. Für die Verbindung zum Internet Service Provider (ISP) sollten Sie dies auf jeden Fall tun.

Bei aktiviertem NAT sind zunächst nur ausgehende Sessions zugelassen. Um bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen diese explizit definiert und zugelassen werden.

Timeout bei Inaktivität festlegen

Der Timeout bei Inaktivität wird festgelegt, um die Verbindung bei Nichtbenutzen, d.h. wenn keine Nutzdaten mehr gesendet werden, automatisch zu trennen und somit ggf. Gebühren zu sparen.

Blockieren nach Verbindungsfehler

Mit dieser Funktion richten Sie eine Wartezeit für ausgehende Verbindungsversuche ein, nachdem ein Verbindungsversuch durch Ihr Gerät fehlgeschlagen ist.

Authentifizierung

Wenn bei ISDN-Verbindungen ein Ruf eingeht, wird über den ISDN-D-Kanal die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann Ihr Gerät den Anrufer identifizieren (CLID), wenn dieser auf Ihrem Gerät eingetragen ist. Nach der Identifizierung mit CLID kann Ihr Gerät zusätzlich eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird.

Für alle PPP-Verbindungen benötigt Ihr Gerät Vergleichsdaten, die Sie eintragen müssen. Legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll und tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Callback

Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann der Callback-Mechanismus für jede Verbindung über eine ISDN- oder über eine AUX-Schnittstelle verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufer eindeutig identifiziert wurde. Ihr Gerät kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch von einem Verbindungspartner einen Rückruf anfordern. Die Identifizierung kann aufgrund der Calling Party Number oder aufgrund der PAP/CHAP/MS-CHAP-Authentifizierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party Number über den ISDN-D- Kanal übermittelt wird, im zweiten Fall mit Rufannahme.

Kanalbündelung

Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Kanalbündelung kann nur bei ISDN-Verbindungen für Bandbreitenerhöhung bzw. als Backup angewendet werden. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch

Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle für Verbindungen zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen.

Falls auf der Gegenstelle Geräte anderer Fabrikate verwendet werden, stellen Sie sicher, dass diese dynamische Kanalbündelung für Bandbreitenerhöhung bzw. als Backup unterstützen.

Statisch

Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät für Verbindungen nutzen soll, unabhängig von der übertragenen Datenrate.

16.1.1 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.

16.1.1.1 Neu

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

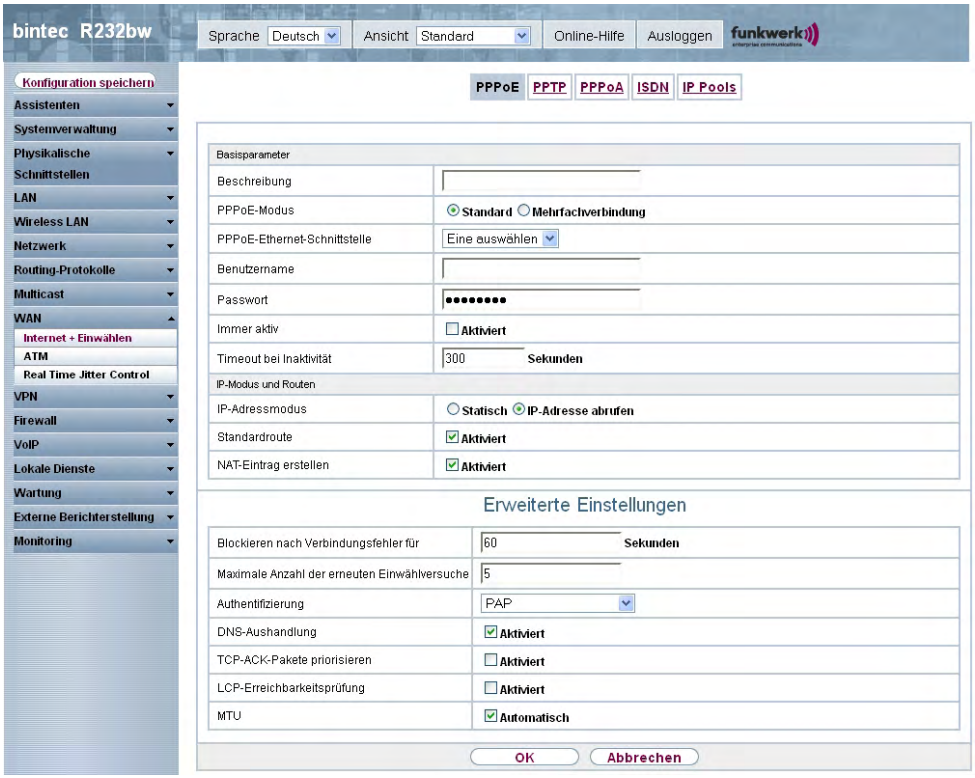


Abb. 80: **WAN**->**Internet + Einwählen**->**PPPoE**->**Neu**

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

Felder im Menü PPPoEBasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (*Standard*) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (*Mehrfachverbindung*). Wählen Sie *Mehrfachverbindung*, so können Sie mehrere DSL-Verbindungen eines Providers über PPP als statische Bündel koppeln, um mehr Bandbreite zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung. Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Port-Modus zu betreiben und für jede PPPoE-Verbindung eine eigene Ethernet-Schnittstelle zu benutzen, z. B. *en1-1*, *en1-2*.
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 **Physikalische Schnittstellen**->**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.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.

Feld	Beschreibung
	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. Standardwert ist *300* . Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü PPPoEIP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *IP-Adresse abrufen*(Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • *Statisch* : Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	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*). 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. Standardwert ist *60*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von *0* bis *100*. Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte:

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

16.1.2 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, z. B. in Österreich notwendig.

16.1.2.1 Neu

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

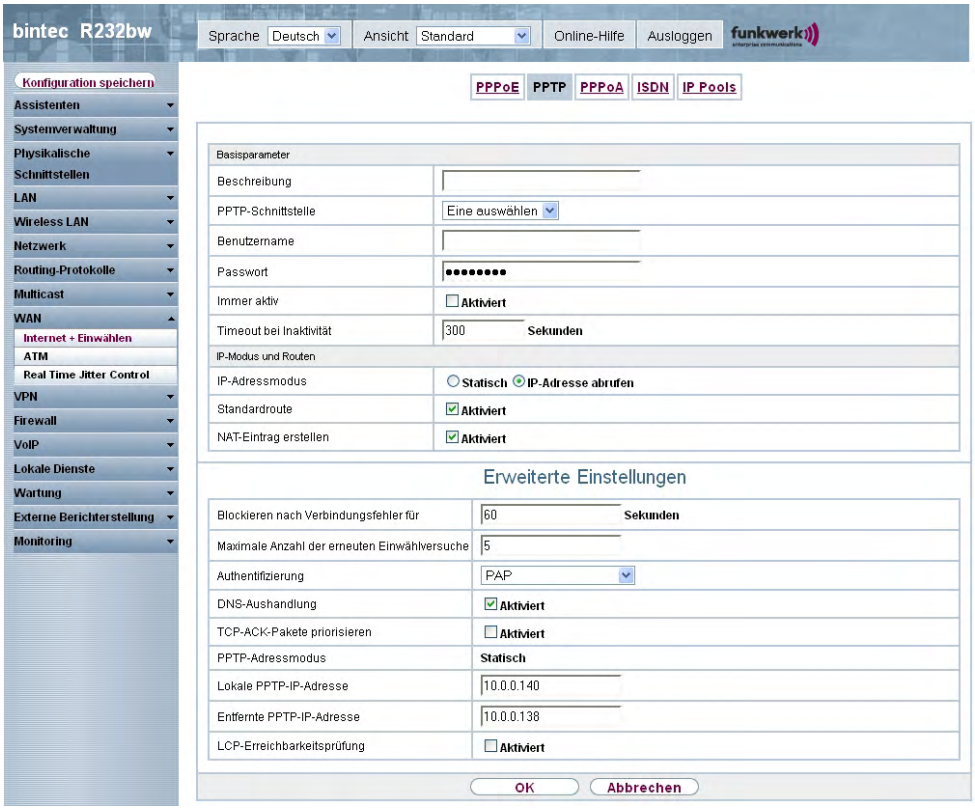


Abb. 81: **WAN->Internet + Einwählen->PPTP->Neu**

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

Felder im Menü PPTPBasisparameter

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-Schnittstelle	Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden. Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist. Bei Verwendung des internen DSL-Modems, wählen Sie hier die in **Physikalische Schnittstellen**->**ATM**->**Profile**->**Neu** für diese Verbindung konfigurierte EthoA-Schnittstellez 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, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Standardwert ist *300* . Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü PPTPIP-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. • *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*). 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. Standardwert ist *60* .
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von *0* bis *100* . 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 **DNS-Server Primär** und **DNS-Server Sekundär** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
PPTP-Adressmodus	Zeigt den Adressmodus an. Der Wert kann nicht verändert werden. Mögliche Werte: • *Statisch* : Die IP-Adresse des in **PPTP-Schnittstelle** ausgewählten Ethernet-Ports wird verwendet.
Lokale PPTP-IP-Adresse	Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird. Standardwert ist *10.0.0.140*.
Entfernte PPTP-IP-Adresse	Geben Sie die IP-Adresse des PPTP-Partners ein. 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 nicht aktiv.

16.1.3 PPPoA

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

In diesem Menü konfigurieren Sie eine xDSL-Verbindung, die zum Verbindungsaufbau PP-

PoA verwendet. Bei PPPoA wird die Verbindung so konfiguriert, dass ein PPP-Datenstrom direkt über ein ATM-Netzwerk transportiert wird (RFC 2364). Dieses ist bei manchen Providern erforderlich. Achten Sie bitte auf die Spezifikationen Ihres Providers!

Bei Verwendung des internen DSL-Modems, muss in **WAN**->**ATM**->**Profile**->**Neu** für diese Verbindung eine PPPoA-Schnittstelle mit **Client-Typ** = *Auf Anforderung* konfiguriert werden.

16.1.3.1 Neu

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

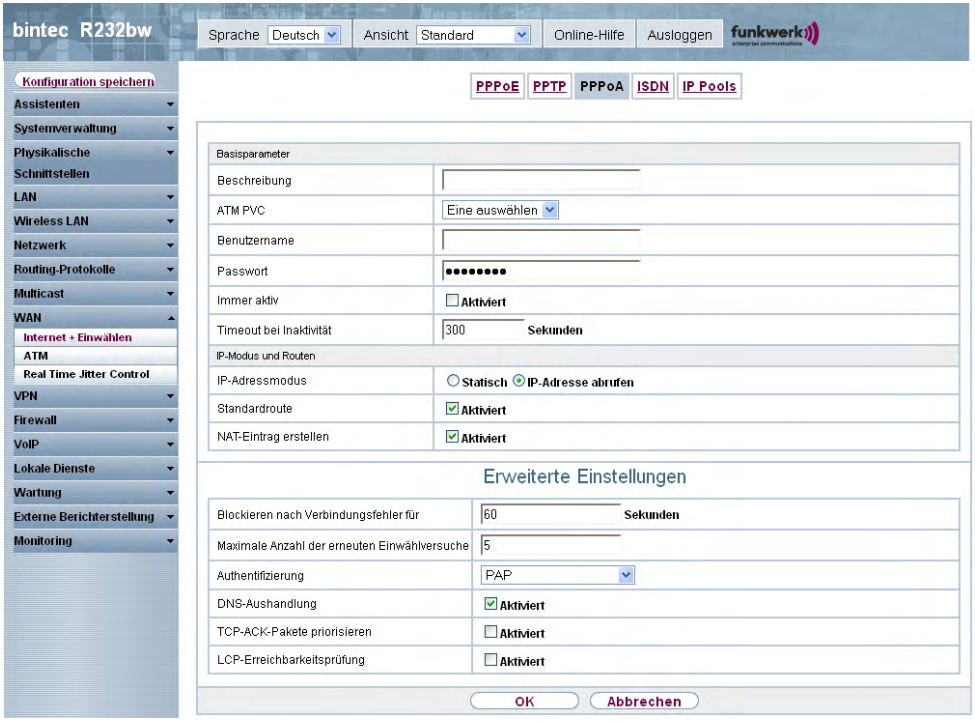


Abb. 82: **WAN**->**Internet + Einwählen**->**PPPoA**->**Neu**

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

Felder im Menü PPPoABasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen

Feld	Beschreibung
	ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü **ATM**->**Profile** angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID VPI und VCI.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort für die PPPoA-Verbindung ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen soll. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold. Standardwert ist *300* . Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü PPPoAIP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihr Gerät eine statische IP-Adresse hat oder diese dynamisch erhält. Mögliche Werte: • *IP-Adresse abrufen*(Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse.

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*. Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0* ... *15*). 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. Standardwert ist *60* .

Feld	Beschreibung
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von *0* bis *100* . 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 **DNS-Server Primär** und **DNS-Server Sekundär** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

16.1.4 ISDN

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

In diesem Menü konfigurieren Sie folgende ISDN-Verbindungen:

- Internetzugang über ISDN
- LAN-zu-LAN Kopplung über ISDN
- Remote (Mobile) Dialin
- Nutzung der Funktion ISDN Callback

16.1.4.1 Neu

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

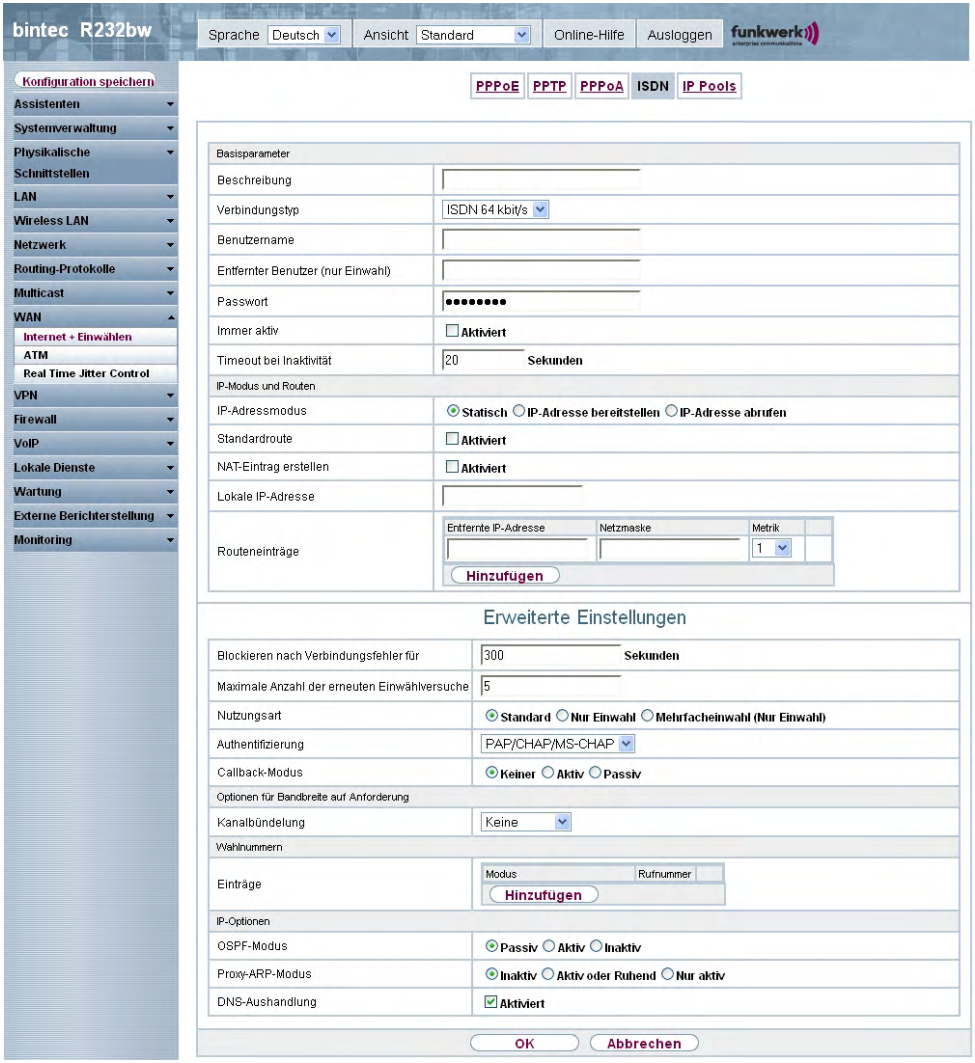


Abb. 83: **WAN->Internet + Einwählen->ISDN->Neu**

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

Felder im Menü ISDNBasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.

Feld	Beschreibung
Verbindungstyp	Wählen Sie aus, welches Layer-1-Protokoll Ihr Gerät nutzen soll. Diese Einstellung gilt für ausgehende Verbindungen zum Verbindungspartner und nur für eingehende Verbindungen vom Verbindungspartner, wenn sie anhand der Calling Party Number identifiziert werden konnten. Mögliche Werte: • *ISDN 64 kbit/s*: Für ISDN-Datenverbindungen mit 64 kBit/s • *ISDN 56 kbit/s*: Für ISDN-Datenverbindungen mit 56 kBit/s
Benutzername	Geben Sie die Kennung Ihres Geräts (lokaler PPP Benutzername) ein.
Entfernter Benutzer (nur Einwahl)	Geben Sie die Kennung der Gegenstelle (entfernter PPP Benutzername) ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Zur Verfügung stehen Werte von *-1* bis *3600* (Sekunden). Ein Wert von *-1* bedeutet, dass die Verbindung nach einem Abbruch sofort wieder aufgebaut wird, *0* deaktiviert den Shorthold. Standardwert ist *20*.

Felder im Menü ISDNIP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *Statisch* (Standardwert): Sie geben eine statische IP-Adresse ein. • *IP-Adresse bereitstellen*: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	Nur bei **IP-Adressmodus** = *Statisch* und *IP-Adresse abrufen* Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
NAT-Eintrag erstellen	Nur bei **IP-Adressmodus** = *Statisch* und *IP-Adresse abrufen* Wenn eine ISDN-Internetverbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur bei **IP-Adressmodus** = *Statisch* Weisen Sie der ISDN-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.

Feld	Beschreibung
	• *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0* ... *15*). Standardwert ist *1* .
IP-Zuordnungspool	Nur bei **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP-Pool aus.

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. Standardwert ist *300* .
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von *0* bis *100* . Standardwert ist *5* .
Nutzungsart	Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle. Mögliche Werte: • *Standard* (Standardwert): Kein spezieller Typ ist ausgewählt. • *Nur Einwahl* : Die Schnittstelle wird für eingehende Wählverbindungen und für von außen initiierten Callback verwendet. • *Mehrfacheinwahl (Nur Einwahl)* : Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort

Feld	Beschreibung
	ein.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP* : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	Nur für **Authentifizierung** = *MS-CHAPv2* Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiv ist. Wenn **Verschlüsselung** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keine* (Standardwert): Es wird keine MPP-Verschlüsselung angewendet. • *Aktiviert*: Die MPP-Verschlüsselung V2 mit 128 bit wird nach RFC 3078 angewendet. • *Windows-kompatibel*: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.

Feld	Beschreibung

Callback-Modus	Wählen Sie die Funktion Callback-Modus.
	
	Mögliche Werte:
	
	• *Keiner* (Standardwert): Ihr Gerät führt keinen Rückruf aus.
	• *Aktiv*: Wählen Sie eine der folgenden Optionen:
	  • *Keine PPP-Aushandlung*: Ihr Gerät ruft den Verbindungspartner an, um einen Rückruf anzufordern.
	  • *Windows-Clientmodus*: Ihr Gerät ruft den Verbindungspartner an, um über CBCP (Callback Control Protocol) einen Rückruf anzufordern. Wird für Windows Clients benötigt.
	• *Passiv*: Wählen Sie eine der folgenden Optionen:
	  • *PPP-Aushandlung oder CLID* : Ihr Gerät ruft sofort zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert wird.
	  • *Windows-Servermodus* : Ihr Gerät ruft nach einer vom Microsoft Client vorgeschlagenen Zeit (NT: 10 Sekunden, neuere Systeme: 12 Sekunden) zurück. Es verwendet die Rufnummer (**Einträge**->**Rufnummer**) mit dem **Modus** *Ausgehend* oder *Beide*, die für den Verbindungspartner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP Aushandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheitsgründen möglichst nicht zu verwenden. Bei der Anbindung von mobilen Microsoft-Clients über DFÜ-Netzwerk ist dies derzeit nicht vermeidbar.
	  • *Verzögert, nur CLID* : Ihr Gerät ruft nach ca. vier Sekunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID.
	  • *Windows-Servermodus, Rückruf optional* : Wie *Windows-Servermodus* mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit **Abbrechen** geschlossen wird.

Feld im Menü Erweiterte EinstellungenOptionen für Bandbreite auf Anforderung

Feld	Beschreibung
Kanalbündelung	Wählen Sie aus, ob Kanalbündelung bzw. welche Art von Kanalbündelung für ISDN-Verbindungen mit dem Verbindungspartner genutzt werden soll. Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet. Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen. Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät nutzen soll, unabhängig von der übertragenen Datenrate. Mögliche Werte: • *Keine* (Standardwert): Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. • *Statisch* : Statische Kanalbündelung. • *Dynamisch* : Dynamische Kanalbündelung.

Feld im Menü Erweiterte EinstellungenWahlnummern

Feld	Beschreibung

Einträge	Geben Sie die Rufnummern des Verbindungspartners ein.
	
	• **Modus**: Wählen Sie aus, ob **Rufnummer** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte:
	  • *Beide* (Standardwert): Für eingehende und ausgehende Rufe.
	  • *Eingehend* : Für eingehende Rufe, wenn der Verbindungspartner sich bei Ihrem Gerät einwählen soll.
	  • *Ausgehend* : Für ausgehende Rufe, wenn Sie sich beim Verbindungspartner einwählen wollen.
	
	  Die Calling Party Number des eingehenden Rufes wird mit der unter **Rufnummer** eingetragenen Nummer verglichen.
	• **Rufnummer**:

Feld	Beschreibung
	Geben Sie die Rufnummer des Verbindungspartners ein.

Felder im Menü Erweiterte EinstellungenIP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellen Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • *Aktiv* : OSPF ist für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten werden. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *aktiv* oder *Ruhend* ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *aktiv* ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **DNS-Server Primär** und **Sekundär** und **WINS-Server Primär** und **Sekundär**

Feld	Beschreibung
	vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

16.1.5 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 Address-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 Address-Pool zuweisen (falls verfügbar). Bei Address-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.

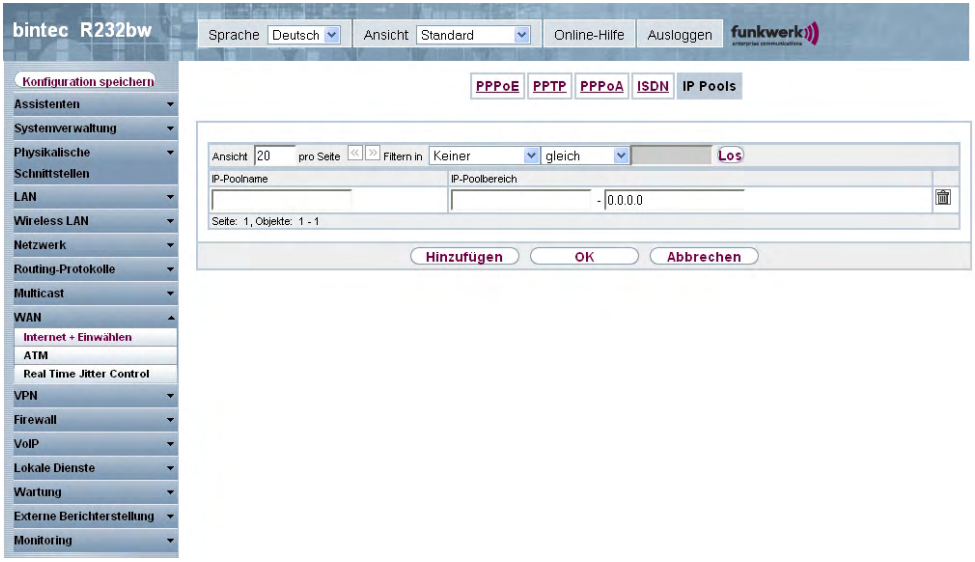


Abb. 84: **WAN->Internet + Einwählen->IP Pools->Hinzufügen**

Das Menü **WAN->Internet + Einwählen->IP Pools->Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü OptionenIP Pools

Feld	Beschreibung
IP-Poolname	Geben Sie die Bezeichnung des IP-Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein. Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.

16.2 ATM

ATM (Asynchronous Transfer Mode) ist ein Datenübertragungsverfahren, das ursprünglich für Breitband-ISDN konzipiert wurde.

Aktuell wird ATM u.a. in Hochgeschwindigkeitsnetzen verwendet. Sie benötigen ATM z. B., wenn Sie über das integrierte ADSL- bzw. SHDSL-Modem einen Hochgeschwindigkeitszugang ins Internet realisieren wollen.

In einem ATM-Netz können unterschiedliche Anwendungen wie z. B. Sprache, Video und

Daten nebeneinander im asynchronen Zeitmultiplexverfahren übertragen werden. Jedem Sender werden dabei Zeitabschnitte zum Übertragen seiner Daten zur Verfügung gestellt. Beim asynchronen Verfahren werden ungenutzte Zeitabschnitte eines Senders von einem anderen Sender verwendet.

Bei ATM handelt es sich um ein verbindungsorientiertes Paketvermittlungsverfahren. Für die Datenübertragung wird eine virtuelle Verbindung genutzt, die zwischen Sender und Empfänger ausgehandelt oder auf beiden Seiten konfiguriert wird. Es wird z. B. der Weg festgelegt, den die Daten nehmen sollen. Über eine einzige physikalische Schnittstelle können mehrere virtuelle Verbindungen eingerichtet werden.

Die Daten werden in sogenannten Zellen oder Slots konstanter Größe übermittelt. Jede Zelle besteht aus 48 Byte Nutzdaten und 5 Byte Steuerinformation. Die Steuerinformation enthält u.a. die ATM-Adresse vergleichbar der Internetadresse. Die ATM-Adresse setzt sich aus den Bestandteilen Virtual Path Identifier (VPI) und Virtual Connection Identifier (VCI) zusammen; sie identifiziert die virtuelle Verbindung.

Über ATM werden verschiedene Arten von Datenströmen transportiert. Um den unterschiedlichen Ansprüchen dieser Datenströme an das Netz, z. B. bezüglich Zellverlust und Verzögerungszeit, gerecht zu werden, können mit Hilfe der Dienstkategorien dafür geeignete Werte festgelegt werden. Für unkomprimierte Videodaten werden z. B. andere Parameter benötigt als für zeitunkritische Daten.

In ATM-Netzen steht Quality of Service (QoS) zur Verfügung, d. h. die Größe verschiedener Netzparameter wie z. B. Bitrate, Delay und Jitter kann garantiert werden.

OAM (Operation, Administration and Maintenance) dient der Überwachung der Datenübertragung bei ATM. OAM umfasst Konfigurationsmanagement, Fehlermanagement und Leistungsmessung.

16.2.1 Profile

Im Menü **WAN**->**ATM**->**Profile** wird eine Liste aller ATM-Profile angezeigt.

Wenn die Verbindung für Ihren Internetzugang über das interne Modem aufgebaut wird, müssen dafür die ATM-Verbindungsparameter eingestellt werden. Ein ATM-Profil fasst einen Satz Parameter für einen bestimmten Provider zusammen.

Standardmäßig ist ein ATM-Profil mit der Beschreibung *AUTO-CREATED* vorkonfiguriert, dessen Werte (VPI 1 und VCI 32) z.B. für eine ATM-Verbindung der Telekom geeignet sind.

Hinweis

Die ATM-Enkapsulierungen sind in den RFCs 1483 und 2684 beschrieben. Sie finden die RFCs auf den entsprechenden Seiten der IETF (*www.ietf.org/rfc.html*).

16.2.1.1 Neu

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

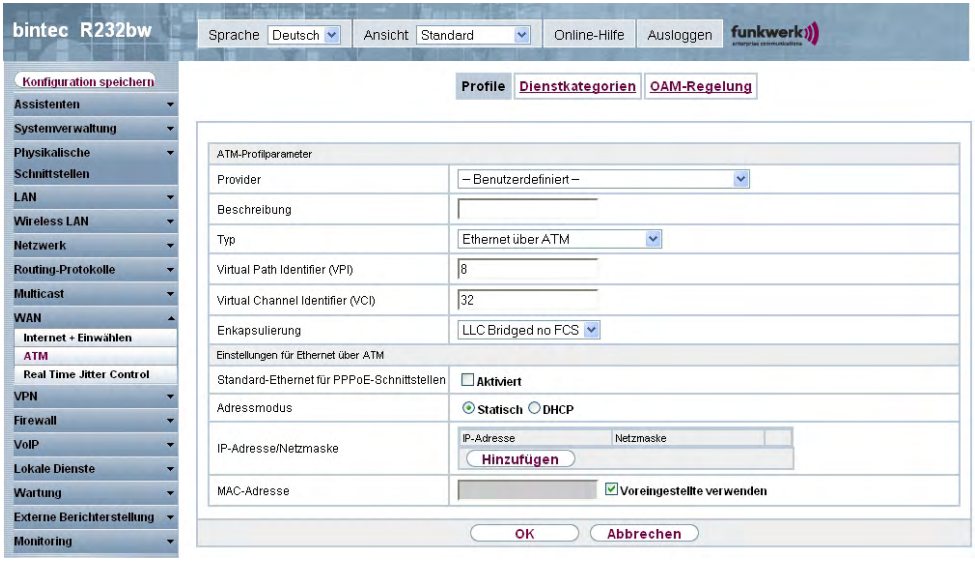


Abb. 85: **WAN->ATM->Profile->Neu**

Das Menü **WAN->ATM->Profile->Neu** besteht aus folgenden Feldern:

Felder im Menü ProfileATM-Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profile für Ihren Provider aus der Liste aus oder definieren Sie mit `-- Benutzerdefiniert --` ein Profil.
Beschreibung	Nur für **Provider** = `-- Benutzerdefiniert --` Geben Sie eine beliebige Beschreibung für die Verbindung ein.
Typ	Nur für **Provider** = `-- Benutzerdefiniert --`

Feld	Beschreibung
	Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: • *Ethernet über ATM* (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet. • *Geroutete Protokolle über ATM*: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Geroutete Protokolle über ATM (RPoA) verwendet. • *PPP über ATM*: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtual Path Identifier (VPI)	Nur für **Provider** = *-- Benutzerdefiniert --* Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind *0* bis *255*. Standardwert ist *8*.
Virtual Channel Identifier (VCI)	Nur für **Provider** = *-- Benutzerdefiniert --* Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind *32* bis *65535*. Standardwert ist 32.
Enkapsulierung	Nur für **Provider** = *-- Benutzerdefiniert --* Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte (nach RFC 2684): • *LLC Bridged no FCS* (Standardwert für Ethernet über ATM): Wird nur für **Typ** = *Ethernet über ATM* angezeigt.

Feld	Beschreibung
	Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen). • *LLC Bridged FCS*: Wird nur für **Typ** = *Ethernet über ATM* angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen). • *Nicht ISO* (Standardwert für Geroutete Protokolle über ATM): Wird nur für **Typ** = *Geroutete Protokolle über ATM* angezeigt. Enkapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing. • *LLC*: Wird nur für **Typ** = *PPP über ATM* angezeigt. Enkapsulierung mit LLC-Header. • *VC-Multiplexing* (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).

Felder im Menü Einstellungen für Ethernet über ATM (erscheint nur für Typ = Ethernet über ATM)

Feld	Beschreibung
Standard-Ethernet für PPPoE-Schnittstellen	Nur für **Typ** = *Ethernet über ATM* Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PPPoE-Verbindungen verwendet werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Adressmodus	Nur für **Typ** = *Ethernet über ATM* Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen werden soll. Mögliche Werte: • *Statisch* (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in **IP-Adresse/Netzmaske** zugewiesen. • *DHCP*: Die Schnittstelle erhält dynamisch per DHCP eine IP-

Feld	Beschreibung
	Adresse.
IP-Adresse/**Netzmaske**	Nur für **Adressmodus** = *Statisch* Geben Sie die IP-Adressen (**IP-Adresse**) und die entsprechenden Netzmasken (**Netzmaske**) der ATM-Schnittstellen ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.
MAC-Adresse	Geben Sie der routerinternen Schnittstelle der ATM-Verbindung eine MAC-Adresse, z. B. *00:a0:f9:06:bf:03*. Ein Eintrag wird nur in speziellen Fällen benötigt. Für Internetverbindungen ist es ausreichend, die Option **Voreingestellte verwenden** (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des *en1-0* abgeleitet ist.
DHCP-MAC-Adresse	Nur für **Adressmodus** = *DHCP*. Geben Sie die MAC-Adresse der routerinternen Schnittstelle der ATM-Verbindung ein, z. B. *00:e1:f9:06:bf:03*. Sollte Ihnen Ihr Provider eine MAC-Adresse für DHCP zugewiesen haben, so tragen Sie diese hier ein. Sie haben auch die Möglichkeit, die Option **Voreingestellte verwenden** (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des *en1-0* abgeleitet ist.
DHCP-Hostname	Nur für **Adressmodus** = *DHCP*. Geben Sie ggf. den beim Provider registrierten Host-Namen an, der von Ihrem Gerät für DHCP-Anfragen verwendet werden soll. Die maximale Länge des Eintrags beträgt 45 Zeichen.

Felder im Menü Einstellungen für geroutete Protokolle über ATM (erscheint nur für Typ = Geroutete Protokolle über ATM)

Feld	Beschreibung
IP-Adresse/**Netzmaske**	Geben Sie die IP-Adressen (**IP-Adresse**) und die entsprechenden Netzmasken (**Netzmaske**) der ATM-Schnittstelle ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

Feld	Beschreibung
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld im Menü Einstellungen für PPP über ATM (erscheint nur für Typ = PPP über ATM),

Feld	Beschreibung
Client-Typ	Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll. Mögliche Werte: • *Auf Anforderung* (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang. Zusätzliche Informationen zu PPP über ATM finden Sie unter *PPPoA* auf Seite 236.

16.2.2 Dienstkategorien

Im Menü **WAN**->**ATM**->**Dienstkategorien** wird eine Liste aller bereits konfigurierten ATM-Verbindungen (PVC, Permanent Virtual Circuit) angezeigt, denen spezifische Datenverkehrsparameter zugewiesen wurden.

Ihr Gerät unterstützt QoS (Quality of Service) für ATM-Schnittstellen.

Achtung

ATM QoS ist nur anzuwenden, wenn Ihr Provider eine Liste an Datenverkehrsparametern (Traffic Contract) vorgibt.

Die Konfiguration von ATM QoS erfordert umfangreiches Wissen über die ATM-Technologie und die Funktionsweise der **bintec**-Geräte. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

16.2.2.1 Neu

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

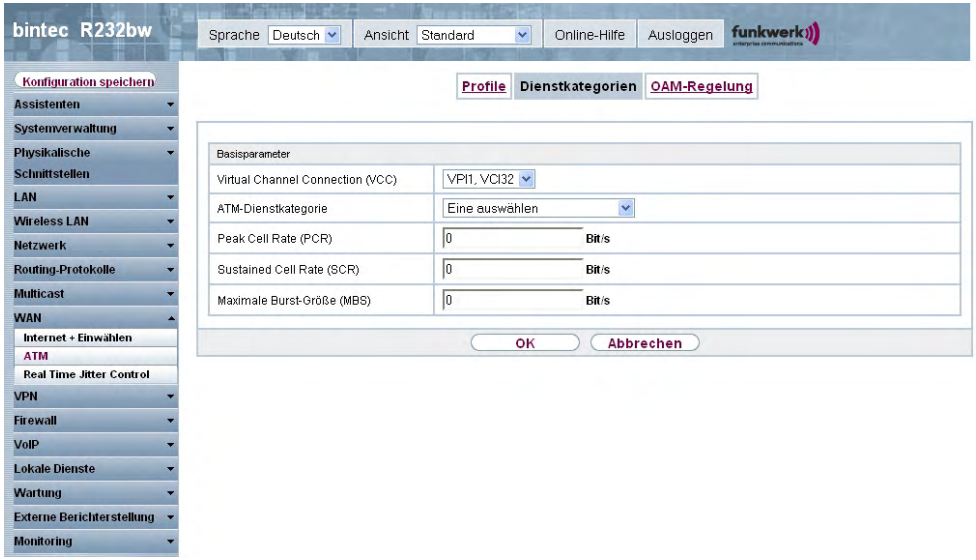


Abb. 86: **WAN->ATM->Dienstkategorien->Neu**

Das Menü **WAN->ATM->Dienstkategorien->Neu** besteht aus folgenden Feldern:

Felder im Menü DienstkategorienBasisparameter

Feld	Beschreibung
Virtual Channel Connection (VCC)	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Servicekategorie festgelegt werden soll.
ATM-Dienstkategorie	Wählen Sie aus, auf welche Art der Datenverkehr der ATM-Verbindung geregelt werden soll. Durch die Auswahl der ATM-Dienstkategorie wird implizit eine Priorität zugeordnet: von CBR (höchste Priorität) über VBR.1 /VBR.3 bis VBR (niedrigste Priorität). Zur Verfügung stehen: • *Unspecified Bit Rate (UBR)* (Standardwert): (Unspecified Bit Rate) Der Verbindung wird keine bestimmte

Feld	Beschreibung
	Datenrate garantiert. Die **Peak Cell Rate (PCR)** legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen. • *Constant Bit Rate (CBR)* : (Constant Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen, die von der **Peak Cell Rate (PCR)** bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen. • *Variable Bit Rate V.1 (VBR.1)* : (Variable Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen (**Sustained Cell Rate (SCR)**). Diese darf insgesamt um das in **Maximale Burst-Größe (MBS)** konfigurierte Volumen überschritten werden. Jeglicher weiterer ATM-Traffic wird verworfen. Die **Peak Cell Rate (PCR)** bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen. • *Variable Bit Rate V.3 (VBR.3)* : (Variable Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen (**Sustained Cell Rate (SCR)**). Diese darf insgesamt um das in **Maximale Burst-Größe (MBS)** konfigurierte Volumen überschritten werden. Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die **Peak Cell Rate (PCR)** bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.
Peak Cell Rate (PCR)	Geben Sie einen Wert für die maximale Datenrate in Bits pro Sekunde ein. Mögliche Werte: *0* bis *10000000*. Der Standardwert ist *0*.
Sustained Cell Rate (SCR)	Nur für **ATM-Dienstkategorie** = *Variable Bit Rate V.1 (VBR.1)* oder *Variable Bit Rate V.3 (VBR.3)* Geben Sie einen Wert für die mindestens zur Verfügung stehende, garantierte Datenrate in Bits pro Sekunde ein. Mögliche Werte: *0* bis *10000000*. Der Standardwert ist *0*.

Feld	Beschreibung
Maximale Burst-Größe (MBS)	Nur für **ATM-Dienstkategorie** = *Variable Bit Rate V.1 (VBR.1)* oder *Variable Bit Rate V.3 (VBR.3)* Geben Sie hier einen Wert für die maximale Anzahl in Bits pro Sekunde ein, um welche die PCR kurzzeitig überschritten werden darf. Mögliche Werte: *0* bis *100000*. Der Standardwert ist *0*.

16.2.3 OAM-Regelung

OAM ist ein Dienst zur Überwachung von ATM-Verbindungen. In OAM sind insgesamt fünf Hierarchien (Flow Level F1 bis F5) für den Informationsfluss definiert. Für eine ATM-Verbindung sind die wichtigsten Informationsflüsse F4 und F5. Der F4-Informationsfluss betrifft den virtuellen Pfad (VP), der F5-Informationsfluss den virtuellen Kanal (VC). Der VP wird durch den VPI-Wert definiert, der VC durch VPI und VCI.

Hinweis

Im Allgemeinen geht die Überwachung nicht vom Endgerät aus, sondern wird seitens des ISP initiiert. Ihr Gerät muss dann lediglich korrekt auf die empfangenen Signale reagieren. Dies ist auch ohne eine spezifische OAM-Konfiguration sowohl auf den Flow Level 4 als auch dem Flow Level 5 gewährleistet.

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: Loopback Tests und OAM Continuity Check (OAM CC). Sie können unabhängig voneinander konfiguriert werden.

Achtung

Die Konfiguration von OAM erfordert umfangreiches Wissen über die ATM-Technologie und die Funktionsweise der **bintec**-Geräte. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

Im Menü **WAN**->**ATM**->**OAM-Regelung** wird eine Liste aller überwachten OAM-Fluss-Levels angezeigt.

16.2.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Fluss-Levels einzurichten.

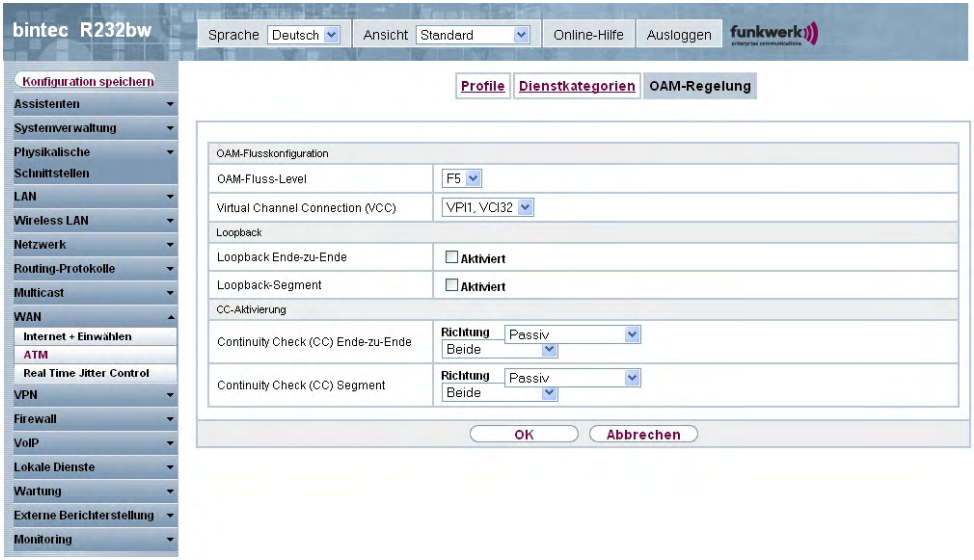


Abb. 87: **WAN->ATM->OAM-Regelung->Neu**

Das Menü **WAN->ATM->OAM-Regelung->Neu** besteht aus folgenden Feldern:

Felder im Menü OAM-RegelungOAM-Flusskonfiguration

Feld	Beschreibung
OAM-Fluss-Level	Wählen Sie den zu überwachenden OAM-Flusslevel. Mögliche Werte: • *F5* : (Virtual Channel Level) Die OAM-Einstellungen werden auf den virtuellen Kanal angewendet (Standardwert). • *F4* : (Virtual Path Level) Die OAM-Einstellungen werden auf den virtuellen Pfad angewendet.
Virtual Channel Connection (VCC)	Nur für **OAM-Fluss-Level** = *F5* Wählen Sie die zu überwachende bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus.
Virtual Path Connecti-	Nur für **OAM-Fluss-Level** = *F4*

Feld	Beschreibung
on (VPC)	Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.

Felder im Menü OAM-RegelungLoopback

Feld	Beschreibung
Loopback Ende-zu-Ende	Wählen Sie aus, ob Sie den Loopback-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Ende-zu-Ende-Sendeintervall	Nur wenn **Loopback Ende-zu-Ende** aktiviert ist. Geben Sie das Zeitintervall in Sekunden an, nach dem jeweils eine Loopback-Zelle gesendet werden soll. Mögliche Werte sind *0* bis *999*. Standardwert ist 5.
Ausstehende Ende-zu-En-de-Anforderungen	Nur wenn **Loopback Ende-zu-Ende** aktiviert ist. Geben Sie ein, wieviele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird. Mögliche Werte sind *1* bis *99*. Standardwert ist *5*.
Loopback-Segment	Wählen Sie aus, ob Sie den Loopback-Test für die Segment-Verbindung (Segment = Verbindung des lokalen Enpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Segment-Sende-intervall	Nur wenn **Loopback-Segment** aktiviert ist. Geben Sie das Zeitintervall in Sekunden an, nach dem jeweils eine Loopback-Zelle gesendet wird. Mögliche Werte sind *0* bis *999*.

Feld	Beschreibung
	Standardwert ist *5*.
Ausstehende Segment-Anforderungen	Nur wenn **Loopback-Segment** aktiviert ist. Geben Sie ein, wieviele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird. Mögliche Werte sind *1* bis *99*. Standardwert ist *5*.

Felder im Menü OAM-RegelungCC-Aktivierung

Feld	Beschreibung
Continuity Check (CC) Ende-zu-Ende	Wählen Sie aus, ob Sie den OAM-CC-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen. Mögliche Werte: • *Passiv*(Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • *Aktiv* : OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • *Beide* : OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • *Keine Aushandlung* : Je nach Einstellung im Feld **Richtung** werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt. • *Passiv*: Die Funktion ist nicht aktiv. Wählen Sie außerdem aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen. Mögliche Werte: • *Beide*(Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • *Senke*: CC-Daten werden empfangen. • *Quelle*: CC-Daten werden generiert.
Continuity Check (CC)	Wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-

Feld	Beschreibung
Segment	Verbindung (Segment=Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen. Mögliche Werte: • *Passiv*(Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • *Aktiv* : OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • *Beide* : OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • *Keine Aushandlung* : Je nach Einstellung im Feld **Richtung** werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt. • *Keiner*: Die Funktion ist nicht aktiv. Wählen Sie weiterhin aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen. Zur Verfügung stehen: • *Beide*(Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • *Senke* : CC-Daten werden empfangen. • *Quelle* : CC-Daten werden generiert.

16.3 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Spachdaten-Pakete normalerweise höchste Priorität. Trotzdem können bei geringer Bandbreite der Upload Verbindung während eines Telefongesprächs merkbare Verzögerungen bei der Sprachübertragung auftreten, wenn gleichzeitig andere Datenpakete geroutet werden.

Die Funktion Real Time Jitter Control löst dieses Problem. Um die "Leitung" für die Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

16.3.1 Regulierte Schnittstellen

Im Menü **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen** wird eine Liste der Schnittstellen angezeigt, für welche die Funktion Real Time Jitter Control konfiguriert ist.

16.3.1.1 Neu

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

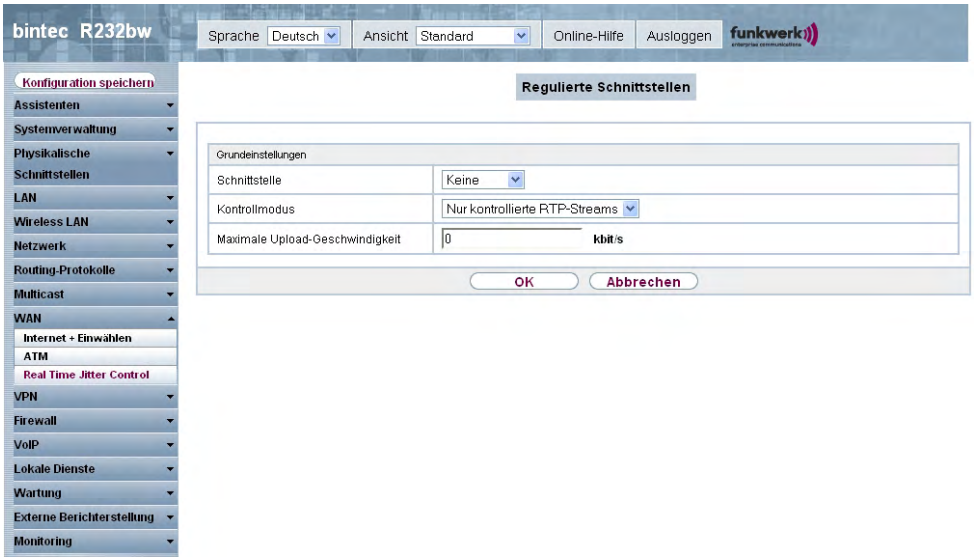


Abb. 88: **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen**->**Neu**

Das Menü **WAN**->**Real Time Jitter Control**->**Regulierte Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Regulierte SchnittstellenGrundeinstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
Kontrollmodus	Wählen Sie den Modus für die Optimierung aus. Mögliche Werte: • *Nur kontrollierte RTP-Streams*(Standardwert): An-

Feld	Beschreibung
	hand 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 17 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 verschüsselt.

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, mit Hilfe 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.

17.1 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 104) integriert werden. Die funkwerk-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.

17.1.1 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 angezeigt.

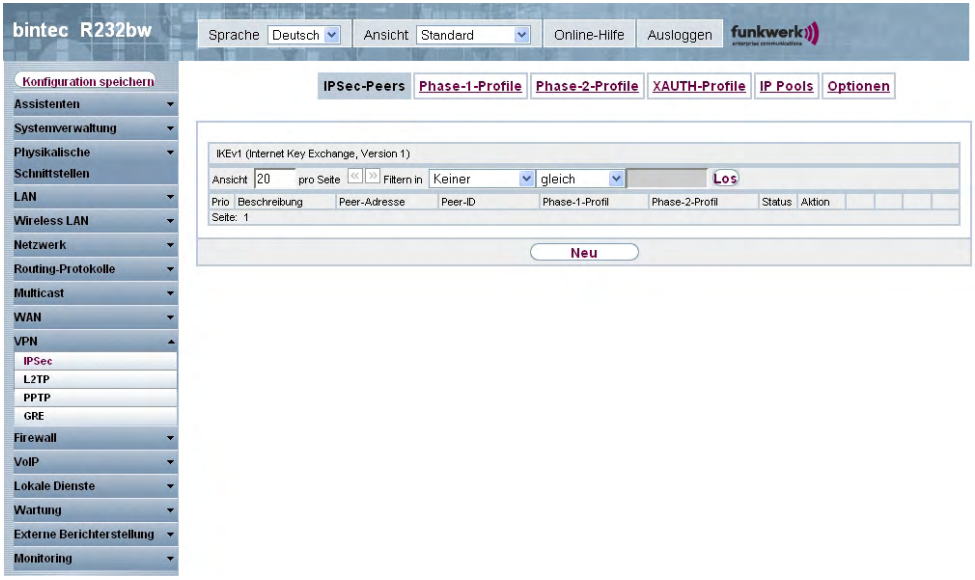


Abb. 89: **VPN->IPSec->IPSec-Peers**

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 464.

17.1.1.1 Neu

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

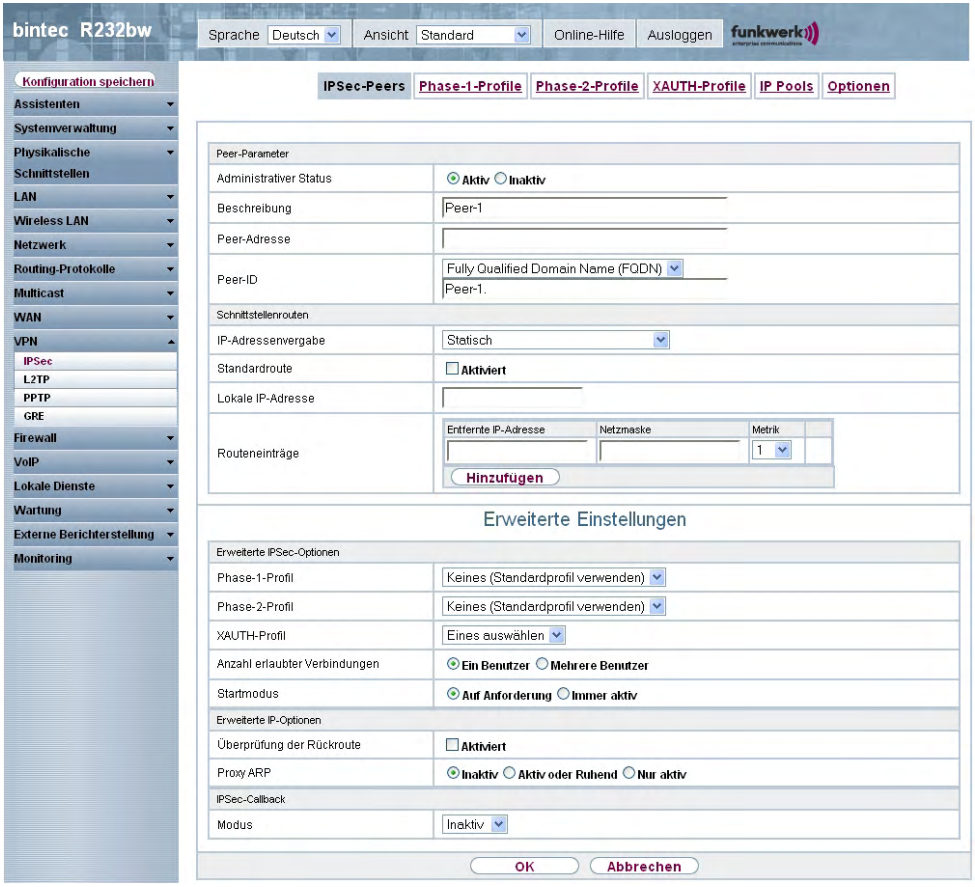


Abb. 90: **VPN->IPSec->IPSec-Peers->Neu**

Das Menü **VPN->IPSec->IPSec-Peers->Neu** besteht aus folgenden Feldern:

Felder im Menü IPSec-PeersPeer-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.

Feld	Beschreibung
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)* • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)* Auf dem Peer-Gerät entspricht diese ID dem Parameter **Lokaler ID-Wert**.
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 IPSec-PeersSchnittstellenrouten

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*: Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server ei-

Feld	Beschreibung
	ne IP-Adresse erhalten soll. • *Server im IKE-Konfigurationsmodus*: Wählen Sie diese Option, wenn Ihr Gateway als DHCP-Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten **IP-Zuordnungspool** entnommen.
IP-Zuordnungspool	Nur bei **IP-Adressenvergabe** = *Server im IKE-Konfigurationsmodus* Wählen Sie einen im Menü **VPN**->**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* und *Client im IKE-Konfigurationsmodus*Wählen Sie aus, ob die Route zu diesem IPSec Peer als Standard-Route festgelegt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur für **IP-Adressenvergabe** = *Statisch* und *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.
Routeneinträge	Nur für **IP-Adressenvergabe** = *Statisch* und *Client im IKE-Konfigurationsmodus*Definieren Sie Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -LANs. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*). Standardwert ist *1*.

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

Felder im Menü Erweiterte EinstellungenErweiterte 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 **Phase-1-Profile** als Standard markiert ist • **PSK Multiproposal*: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü **Phase-1-Profile**. • *<Profilname>*: Verwendet ein Profil, das im Menü **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 **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 **Phase-2-Profile**. • *<Profilname>*: Verwendet ein Profil, das im Menü **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 XAuthverwenden 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.

Feld	Beschreibung
	• *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.
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 EinstellungenErweiterte IP-Optionen

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

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **bintec**-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: Mit Hilfe 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.funkwerk-ec.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 Erweiterte EinstellungenIPSec-Callback* auf Seite 276 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 des gerufenen Peers die Informationen 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 IPAdresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil der 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 Erweiterte EinstellungenIPSec-Callback

Feld	Beschreibung
Modus	Wählen Sie den Callback-Modus aus. Mögliche Werte: • *Inaktiv* (Standardwert): IPSec-Callback ist deaktiviert. Das

Feld	Beschreibung
	lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • *Passiv*: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • *Aktiv*: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • *Beide*: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	Nur für **Modus** = *Passiv* oder *Beide* . Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.
Ausgehende Rufnummer	Nur für **Modus** = *Aktiv* oder *Beide* . Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.
Eigene IP-Adresse per ISDN/GSM übertragen	Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Übertragungsmodus	Nur für **Eigene IP-Adresse per ISDN/GSM übertragen** = aktiviert Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen. Mögliche Werte:

Feld	Beschreibung
	• *Automatische Erkennung des besten Modus* : Ihr Gerät bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird. (Die Verwendung des B-Kanals verursacht Kosten.) • *Nur D-Kanalmodi automatisch erkennen* : Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • *Spezifischen D-Kanalmodus verwenden* : Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. • *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen* : Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übetragen. (Dies verursacht Kosten.) • *Nur B-Kanalmodus verwenden* : Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	Nur für **Übertragungsmodus** = *Spezifischen D-Kanalmodus verwenden* oder *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen* Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen. Mögliche Werte: • *LLC* (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • *SUBADDR* : Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • *LLC und SUBADDR* : Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.

17.1.2 Phase-1-Profile

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

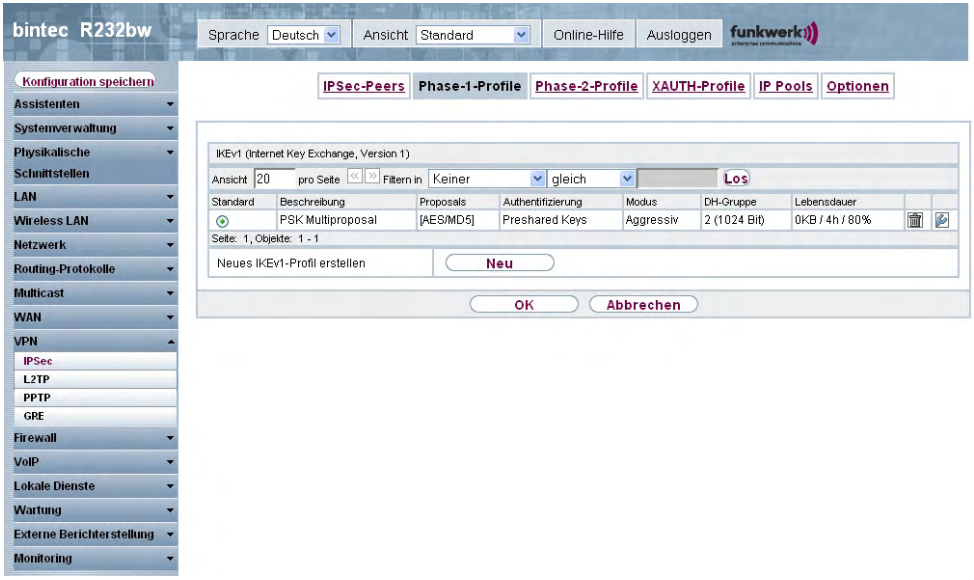


Abb. 91: **VPN->IPSec->Phase-1-Profile**

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

17.1.2.1 Neu

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

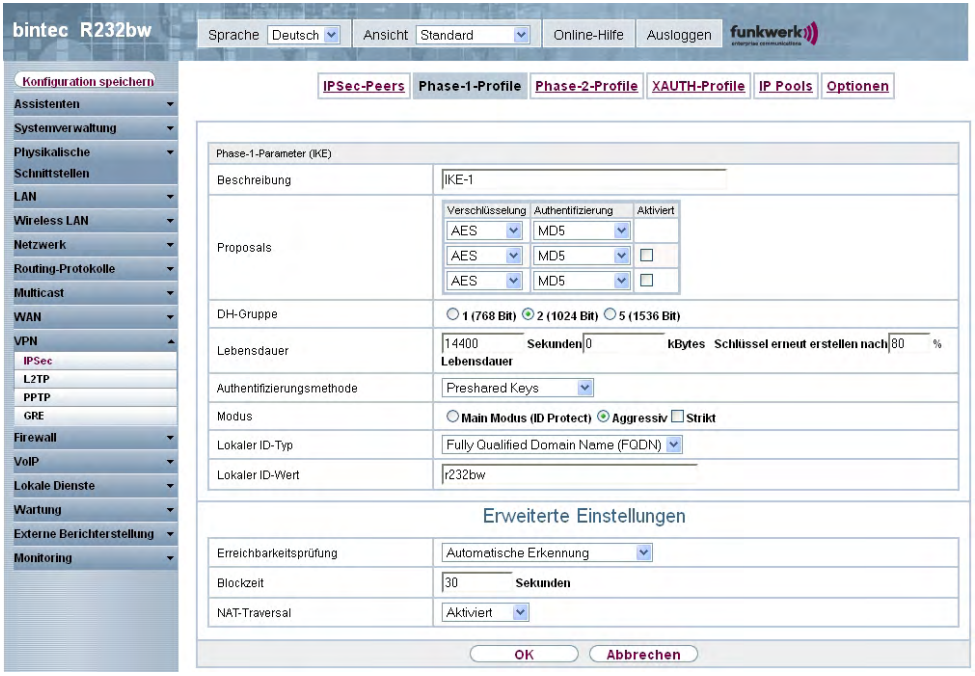


Abb. 92: **VPN->IPSec->Phase-1-Profile->Neu**

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

Felder im Menü Phase-1-ProfilePhase-1-Parameter (IKE)

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, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird.

Feld	Beschreibung
	• *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. • *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): MD 5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • *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.

Feld	Beschreibung
	• *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 Kenntnissstand 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	Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von **bintec**-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. 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-

Feld	Beschreibung
	1- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Standardwert ist *14400*. 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. Standardwert ist *0*. Der Defaultwert lt. RFC wird verwendet, wenn *0* Sekunden und *0* KBytes eingetragen werden.
Authentifizierungsmethode	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 **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 **Authentifizierungsmethode** = *DSA-Signatur*, *RSA-Signatur*oder *RSA-Verschlüsselung* Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.
Modus	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

Feld	Beschreibung
	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	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	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-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 104), 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	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. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • *Heartbeats (Nur erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • *Send*: 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 wer-

Feld	Beschreibung
	den. Mt 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.
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. 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. 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. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
CA-Zertifikate	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.

Feld	Beschreibung
	Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.

17.1.3 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.

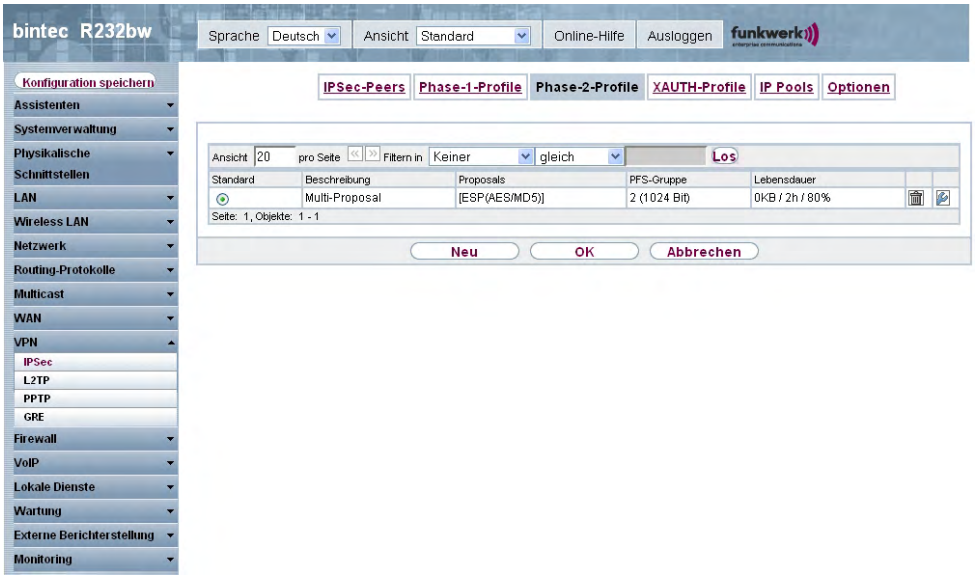


Abb. 93: **VPN**->**IPSec**->**Phase-2-Profile**

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

17.1.3.1 Neu

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

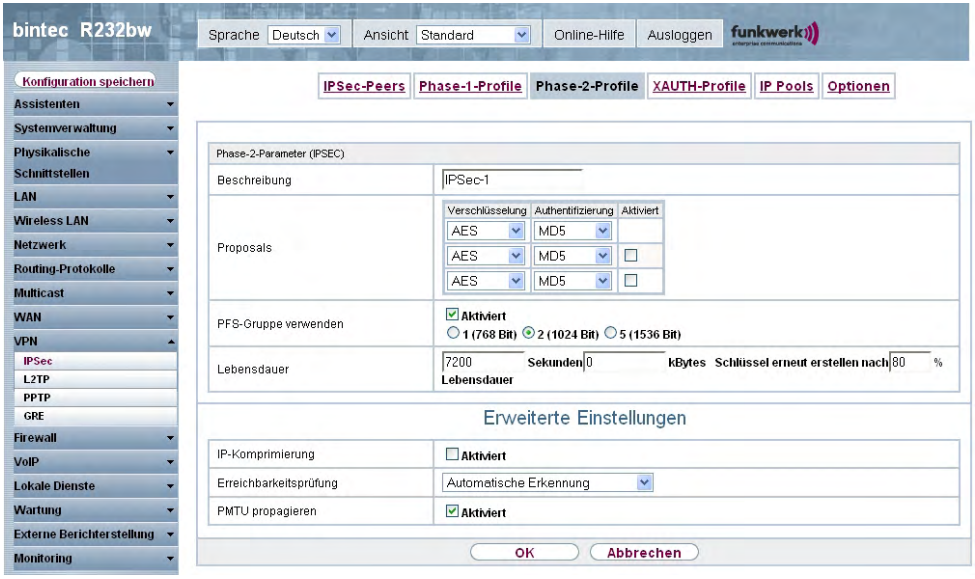


Abb. 94: **VPN->IPSec->Phase-2-Profile->Neu**

Das Menü **VPN->IPSec->Phase-2-Profile->Neu** besteht aus folgenden Feldern:

Felder im Menü Phase-2-ProfilePhase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld. Verschlüsselungsalgorithmen (**Verschlüsselung**): • *3DES* (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-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen

Feld	Beschreibung
	Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 bits angewendet. • *Twofish*: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • *Blowfish*: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • *CAST*: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • *DES*: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. Hash-Algorithmen (**Authentifizierung**): • *MD5* (Standardwert): MD 5 (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 verwen-	Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hell-

Feld	Beschreibung
den	man-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 in **Phase-1-ProfileDH-Gruppe**. PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind. Das Feld hat folgende Optionen: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)* (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen. Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäss RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind. Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung: Eingabe in *Sekunden*: Geben Sie die Lebensdauer für Phase-2- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. 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. Standardwert ist *0*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IP-Komprimierung	Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann. Mit *Aktiviert* wird die Funktion aktiv. 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** 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: • *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. • *Send*: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • *Heartbeats (Senden &Erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • *Automatische Erkennung*: Automatische Erkennung, ob die Gegenstelle ein **bintec**-Gerät ist. Wenn ja, wird Heartbeat beide (bei Gegenstelle mit **bintec**) oder keiner (bei Gegenstelle ohne **bintec**) gesetzt.
PMTU propagieren	Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll.

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

17.1.4 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 abwechsend 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.

17.1.4.1 Neu

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

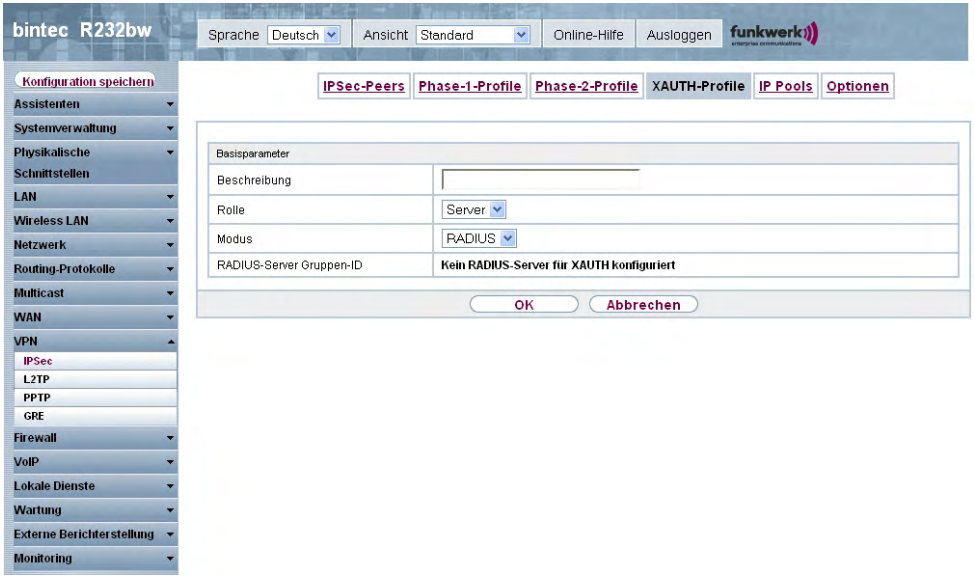


Abb. 95: **VPN**->**IPSec**->**XAUTH-Profile**->**Neu**

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

Felder im Menü XAUTH-ProfileBasisparameter

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** konfigu-

Feld	Beschreibung
	riert 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.
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** dazu.

17.1.5 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.

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

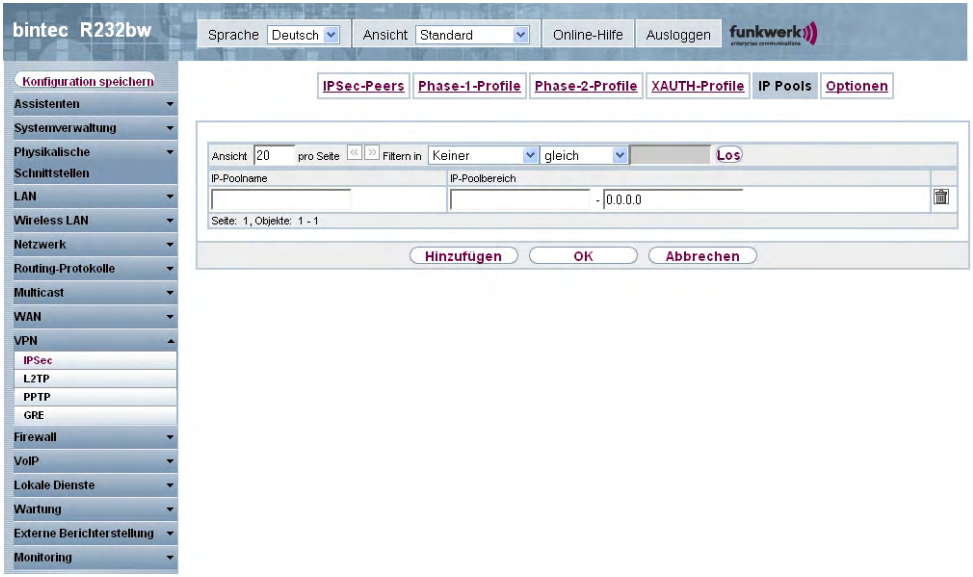


Abb. 96: **VPN->IPSec->IP Pools->Hinzufügen**

Das Menü **VPN->IPSec->IP Pools->Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü OptionenIP Pools

Feld	Beschreibung
IP-Poolname	Geben Sie die Bezeichnung des IP-Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein. Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.

17.1.6 Optionen

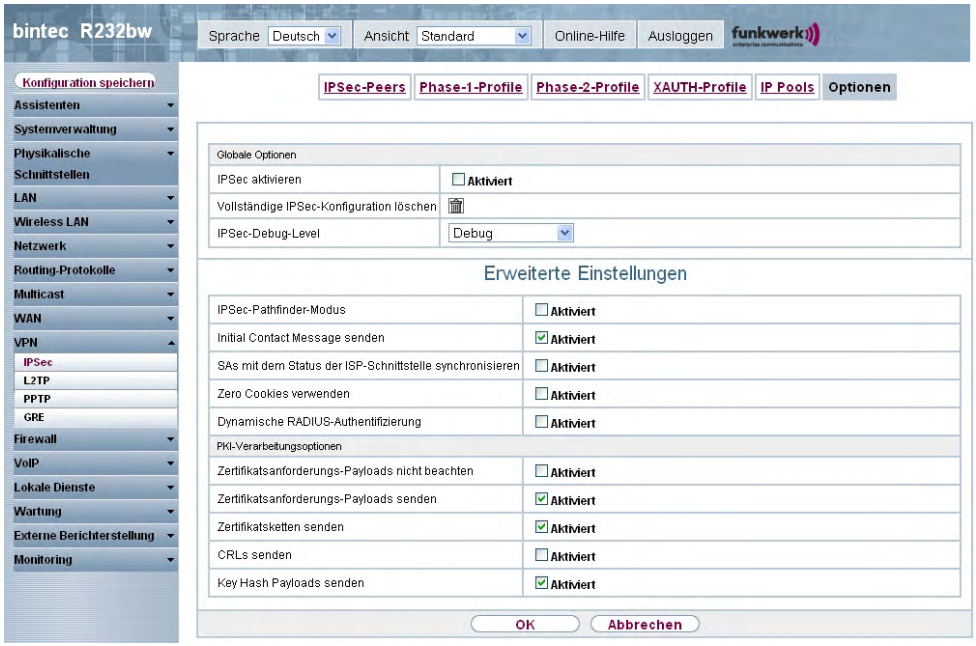


Abb. 97: **VPN->IPSec->Optionen**

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

Felder im Menü OptionenGlobale Optionen

Feld	Beschreibung
IPSec aktivieren	Wählen Sie, ob Sie IPSec aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.
Vollständige IPSec-Konfiguration löschen	Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts. Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen. Das Löschen der Konfiguration ist nur möglich mit **IPSec akti-**

Feld	Beschreibung
	vieren = 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**-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 OptionenErweiterte Einstellungen

Feld	Beschreibung
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	Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Da-

Feld	Beschreibung
der ISP-Schnittstelle synchronisieren	tenverkehr 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 zeroed (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 zeroed SPI in Bytes ein. Der Standardwert ist *32*.
Dynamische RADIUS-Authentifizierung	Wählen Sie aus, ob die RADIUS-Authentifizierung über IPSec aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Erweiterte EinstellungenPKI-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 sen-	Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen.

Feld	Beschreibung
den	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 zu unterdrücken.

17.2 L2TP

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

Ihr **bintec**-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.

17.2.1 Tunnelprofile

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

17.2.1.1 Neu

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

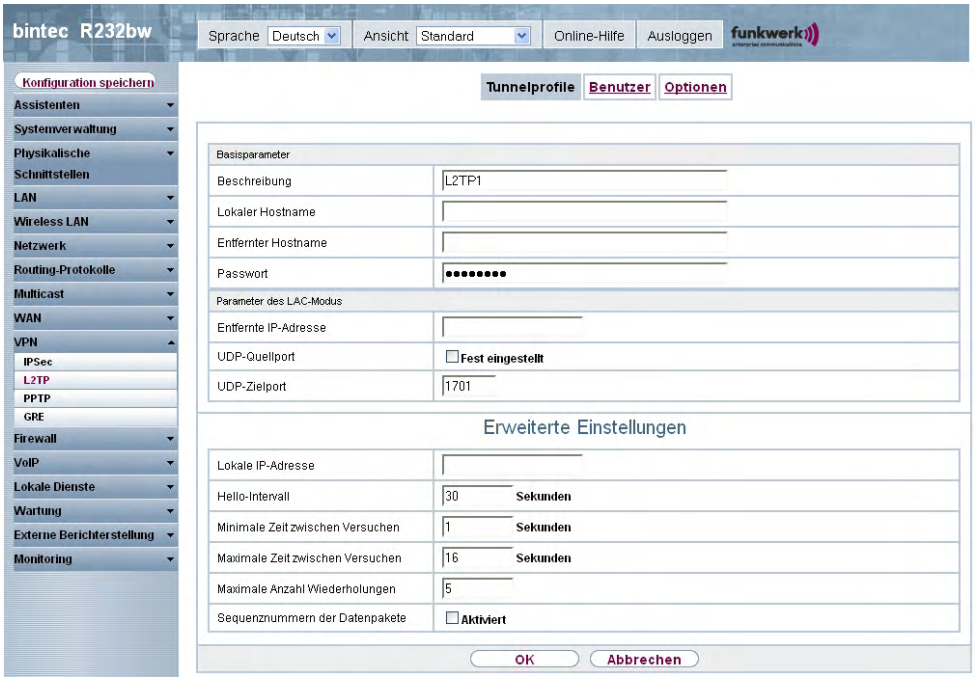


Abb. 98: **VPN**->**L2TP**->**Tunnelprofile**->**Neu**

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

Felder im Menü TunnelprofileBasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das aktuelle Profil ein. Ihr Gerät benennt die Profile automatisch mit `L2TP`

Feld	Beschreibung
	und nummeriert diese, der Wert kann jedoch geändert werden.
Lokaler Hostname	Geben Sie den Hostnamen für LNS bzw. LAC ein. • LAC: Der **Lokaler Hostname** wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem **Entfernter Hostname**n eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Reply). • LNS: Entspricht dem Wert für **Entfernter Hostname** der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	Geben Sie den Hostnamen des LNS bzw. LAC ein: • LAC: Definiert den Wert für **Lokaler Hostname** des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). 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 **Entfernter Hostname** 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 TunnelprofileParameter des LAC-Modus

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

Feld	Beschreibung
	den von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten. Verfügbare Werte sind *0* bis *255*, der Standardwert ist *30*. Der Wert *0* bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.
Minimale Zeit zwischen Versuchen	Geben Sie die Mindestzeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Die Wartezeit wird dynamisch verlängert, bis sie die **Maximale Zeit zwischen Versuchen** erreicht hat. Verfügbare Werte sind *1* bis *255*, der Standardwert ist *1*.
Maximale Zeit zwischen Versuchen	Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *16*.
Maximale Anzahl Wiederholungen	Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *5*.
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. Die Funktion wird derzeit nicht verwendet. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

17.2.2 Benutzer

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

17.2.2.1 Neu

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

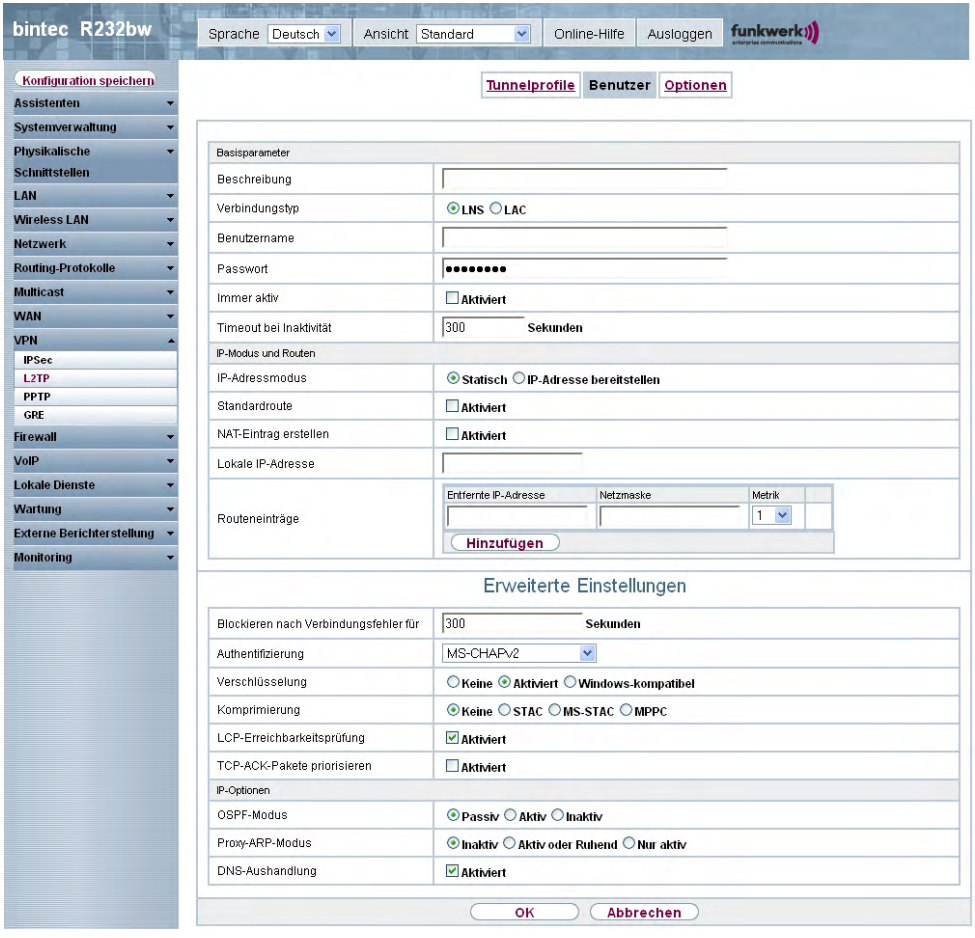


Abb. 99: **VPN->L2TP->Benutzer->Neu**

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

Felder im Menü BenutzerBasisparameter

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. Sonder-

Feld	Beschreibung
	zeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.
Verbindungstyp	Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkservers (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll. Mögliche Werte: • *LNS*(Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • *LAC* : Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.
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, wieviele 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 Shorthold. Standardwert ist *300*.

Felder im Menü BenutzerIP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *Statisch* (Standardwert): Sie geben eine statische IP-Adresse ein. • *IP-Adresse bereitstellen*: Nur für **Verbindungstyp** = *LNS* . Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Nur für **Verbindungstyp** = *LAC* . Ihr Gerät erhält dynamisch eine IP-Adresse.
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.
IP-Zuordnungspool (IPCP)	Nur für **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP Pool aus.
Lokale IP-Adresse	Nur für **IP-Adressmodus** = *Statisch* . Geben Sie die WAN IP-Adresse Ihres Geräts ein.
Routeneinträge	Nur für **IP-Adressmodus** = *Statisch* .

Feld	Beschreibung
	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 fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. 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.

Feld	Beschreibung
	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.
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 nicht 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.

Felder im Menü Erweiterte EinstellungenIP-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.

Feld	Beschreibung
Proxy-ARP-Modus	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner *aktiv* (aktiv) oder *ruhend* (ruhend) ist. Bei *ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner *aktiv* (aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **DNS-Server Primär** und **Sekundär** 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.

17.2.3 Optionen

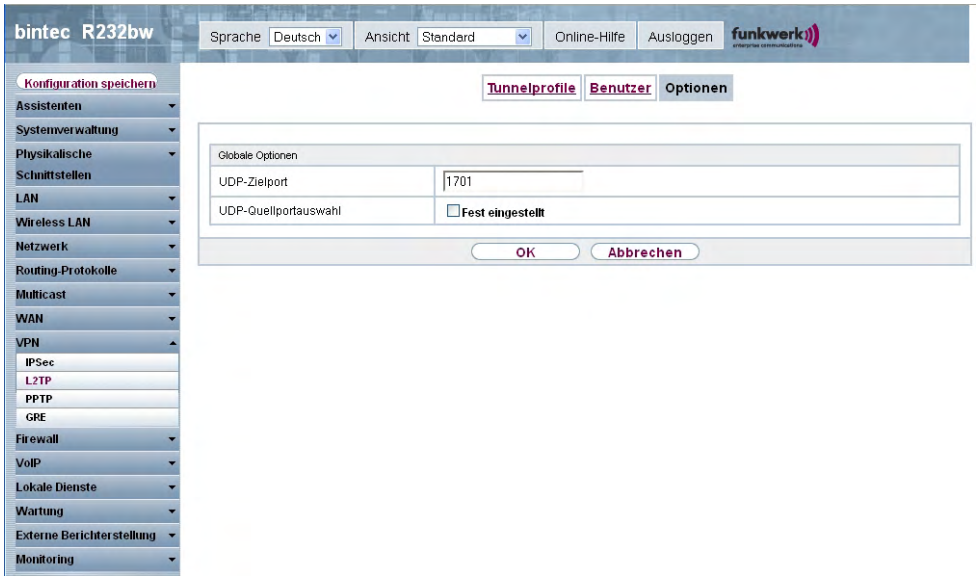


Abb. 100: **VPN->L2TP->Optionen**

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

Felder im Menü OptionenGlobale 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.

17.3 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.

17.3.1 PPTP-Tunnel

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

17.3.1.1 Neu

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

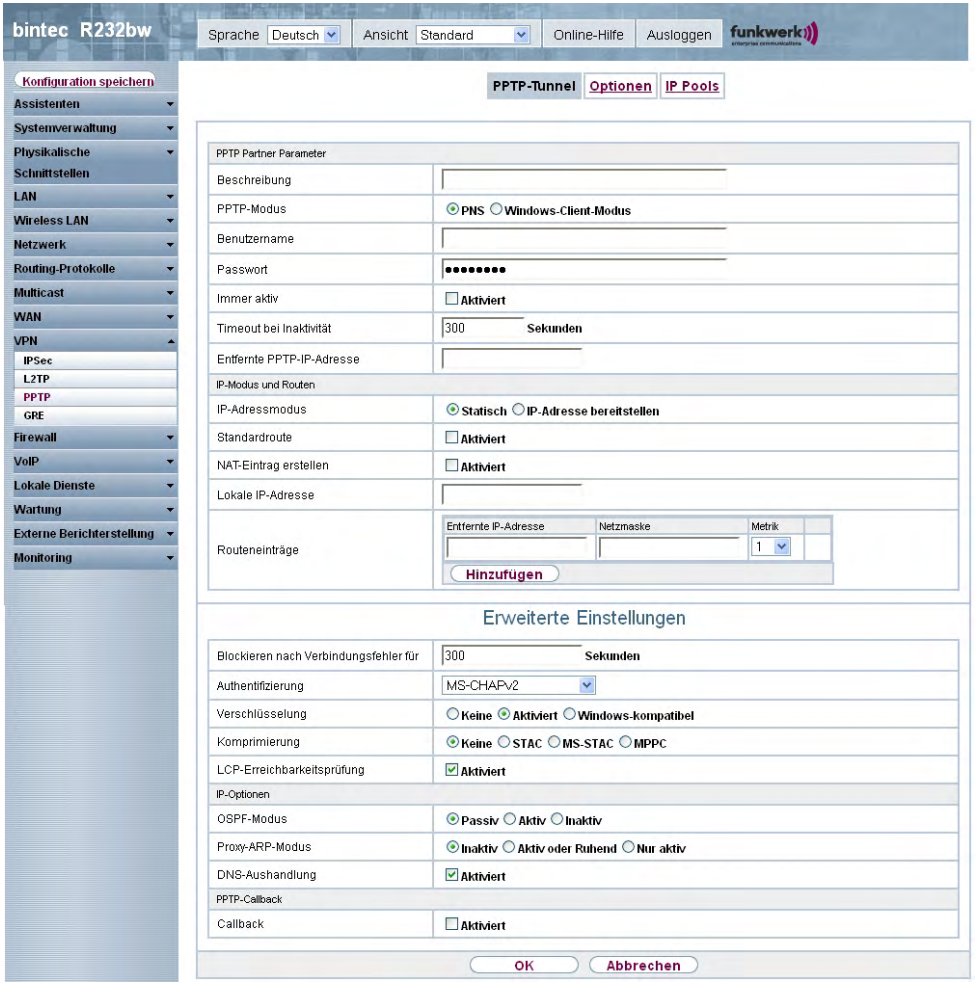


Abb. 101: **VPN->PPTP->PPTP-Tunnel->Neu**

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

Felder im Menü PPTP-TunnelPPTP 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. Sonder-

Feld	Beschreibung
	zeichen 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, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Standardwert ist *300* . Bsp. *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-AdresseHostname	Nur für **PPTP-Modus** = *Windows-Client-Modus*Geben Sie die IP-Adresse des PPTP-Partners ein.

Felder im Menü PPTP-TunnelIP-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 **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 ISDN-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 ISDN-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -LANs. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0...15*). Standardwert ist *1*.

Feld	Beschreibung
IP-Zuordnungspool (IPCP)	Nur bei **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. 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.
Verschlüsselung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll.

Feld	Beschreibung
	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 Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keiner* (Standardwert): Es wird keine Verschlüsselung angewendet. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression
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 Erweiterte EinstellungenIP-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:

Feld	Beschreibung
	• *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 **DNS-Server Primär** und **DNS-Server Sekundär** vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Folgende Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü Erweiterte EinstellungenPPTP-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).

17.3.2 Optionen

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

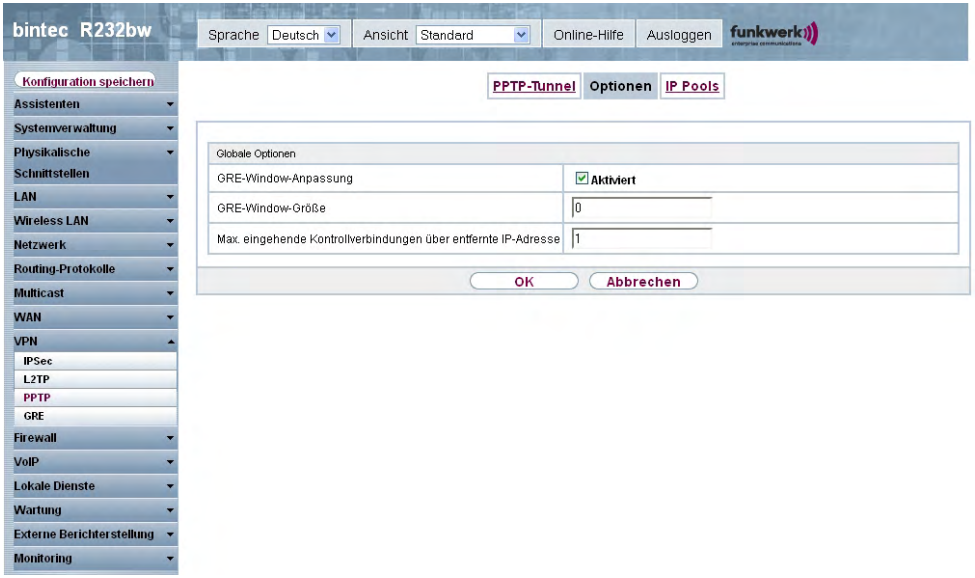


Abb. 102: **VPN->PPTP->Optionen**

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

Felder im Menü OptionenGlobale Optionen

Feld	Beschreibung
GRE-Window-Anpassung	Wählen Sie, ob Sie die GRE Window Adaption aktivieren wollen. Diese Anpassung ist erst notwendig, wenn Sie auf der Windows XP Seite das Service Pack 1 von Microsoft installiert haben. Da Microsoft mit SP 1 den Bestätigungalgorithmus innerhalb des GRE-Protokolls geändert hat, muss auf der funkwerk-Seite 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

Feld	Beschreibung
	Bestätigung geschickt werden kann. Windows XP verwendet ein höheres initiales Empfangs-Window im GRE, weshalb hier die maximale Sende-Window-Größe auf der funkwerk-Seite über den Wert **GRE-Window-Größe** angepasst werden sollte. Mögliche Werte sind `0` bis `256`. Standardwert ist `0`.
Max. eingehende Kontrollverbindungen über entfernte IP-Adresse	Geben Sie die maximale Anzahl der Kontrollverbindingen ein.

17.3.3 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.

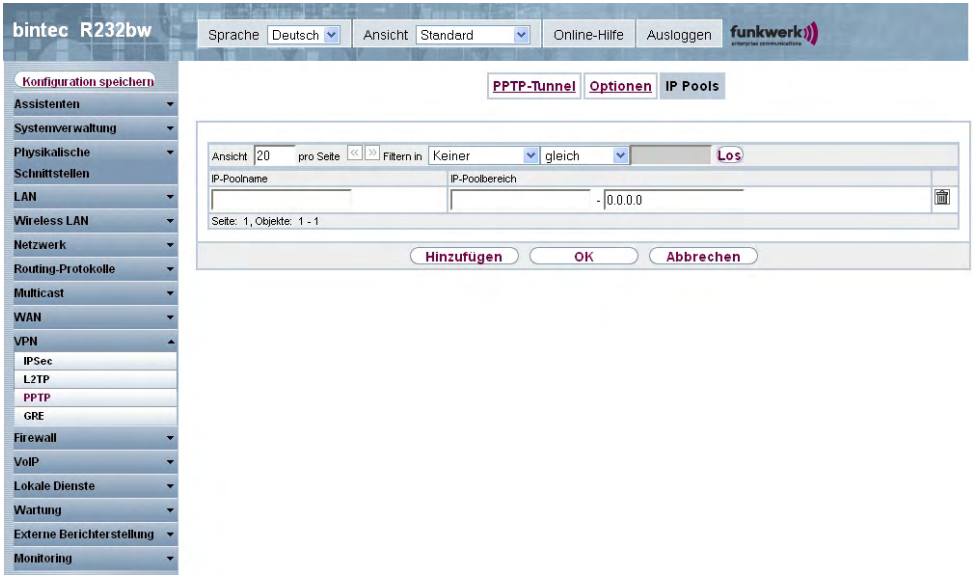


Abb. 103: **VPN->PPTP->IP Pools->Hinzufügen**

Das Menü **VPN->PPTP->IP Pools->Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü OptionenIP Pools

Feld	Beschreibung
IP-Poolname	Geben Sie die Bezeichnung des IP-Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein. Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.

17.4 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.

17.4.1 GRE-Tunnel

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

17.4.1.1 Neu

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

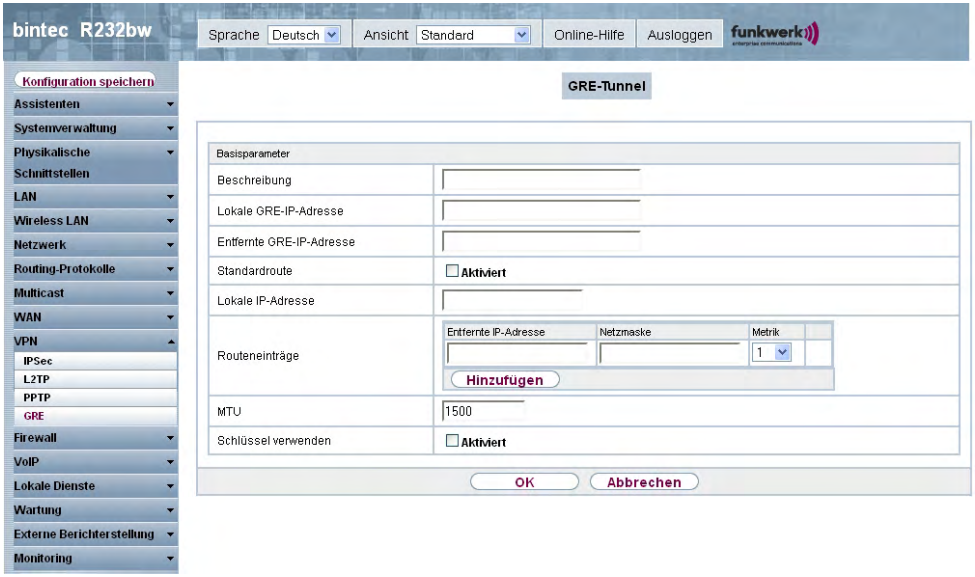


Abb. 104: **VPN->GRE->GRE-Tunnel**

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

Felder im Menü GRE-TunnelBasisparameter

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 auto-

Feld	Beschreibung
	matisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	Wenn Sie die **Standardroute** aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihre Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0* ... *15*). 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.

Feld	Beschreibung
Schlüsselwert	Nur wenn **Schlüssel verwenden** aktiviert ist. Geben Sie die GRE-Verbindungskennung ein. Mögliche Werte sind *0* bis *2147483647*. Der Standardwert ist *0*.

Kapitel 18 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen **bintec** 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

bintecs Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der **bintec**-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 ICMP Host-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).

18.1 Richtlinien

18.1.1 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 später 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.

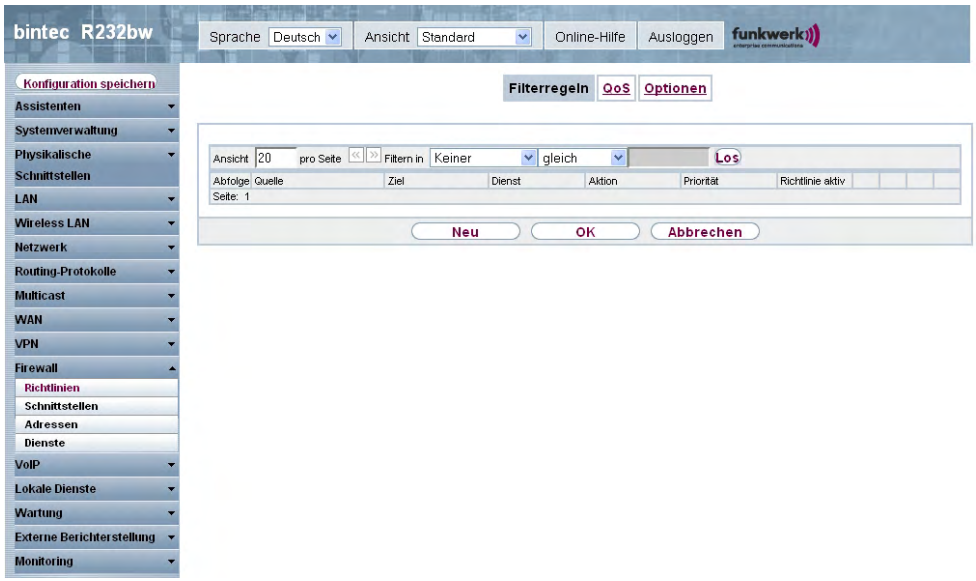


Abb. 105: **Firewall**->**Richtlinien**->**Filterregeln**

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.

18.1.1.1 Neu

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

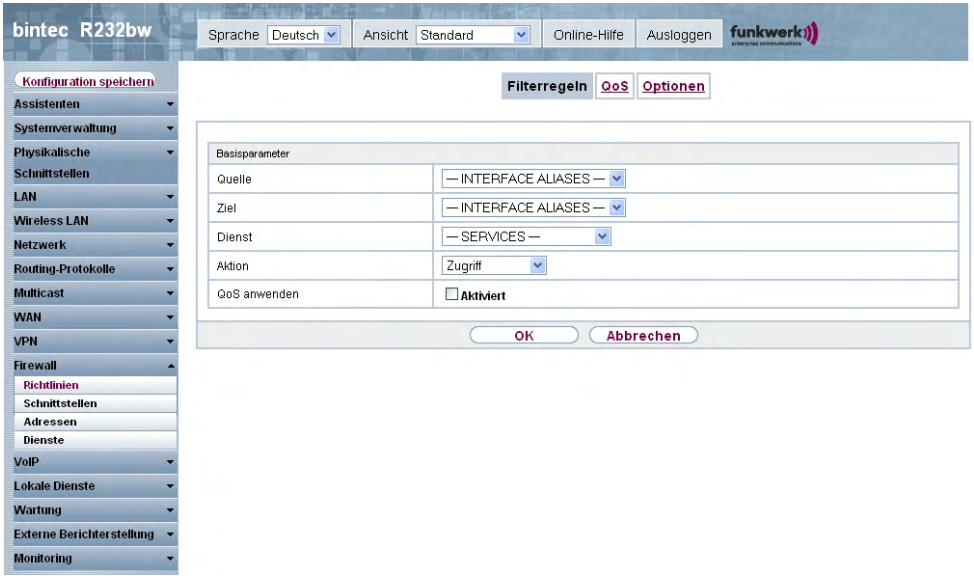


Abb. 106: **Firewall->Richtlinien->Filterregeln->Neu**

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

Felder im Menü FilterregelnBasisparameter

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 *Any* bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.

Feld	Beschreibung
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 *Any* bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* Weitere Dienste werden in **Firewall**->**Dienste**->**Diensteliste** angelegt. Außerdem stehen die in **Firewall**->**Dienste**->**Gruppen** konfigurierten Dienstegruppen zur Auswahl.
Aktion	Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll. Möglichen Werte: • *Zugriff* (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • *Verweigern* : Die Pakete werden abgewiesen. • *Zurückweisen* : Die Pakete werden abgewiesen. Eine Feh-

Feld	Beschreibung
	lermeldung 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 nicht ausdrücklich zugelassen wurde, von der Firewall geblockt wird!
Priorität	Nur für **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*

18.1.2 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 und Bandbreite für diese reserviert werden.

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

18.1.2.1 Neu

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

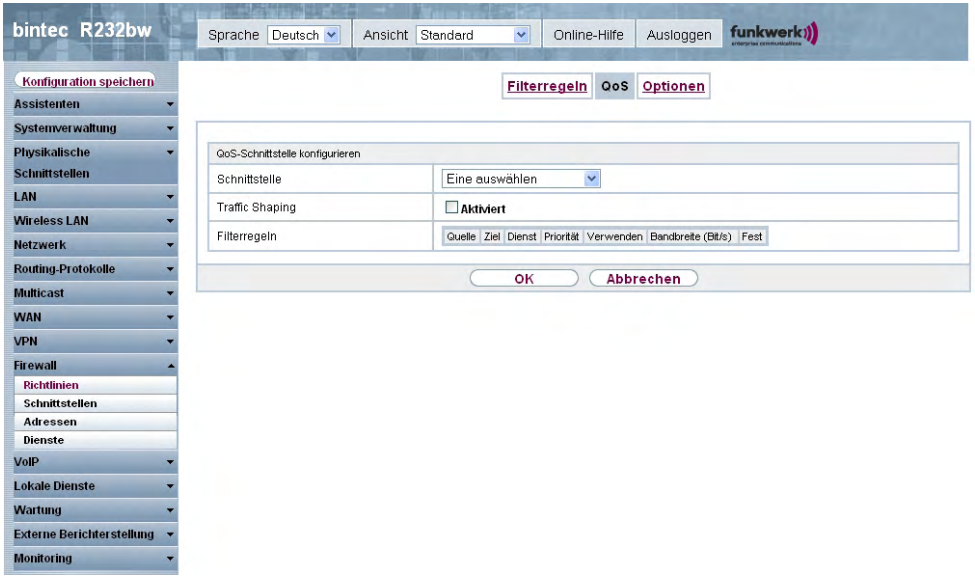


Abb. 107: **Firewall->Richtlinien->QoS->Neu**

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

Felder im Menü QoSQoS-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.

Feld	Beschreibung
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.

18.1.3 Optionen

In diesem Menü können Sie die Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wieviel Sekunden Inaktivität eine Sitzung beendet werden soll.

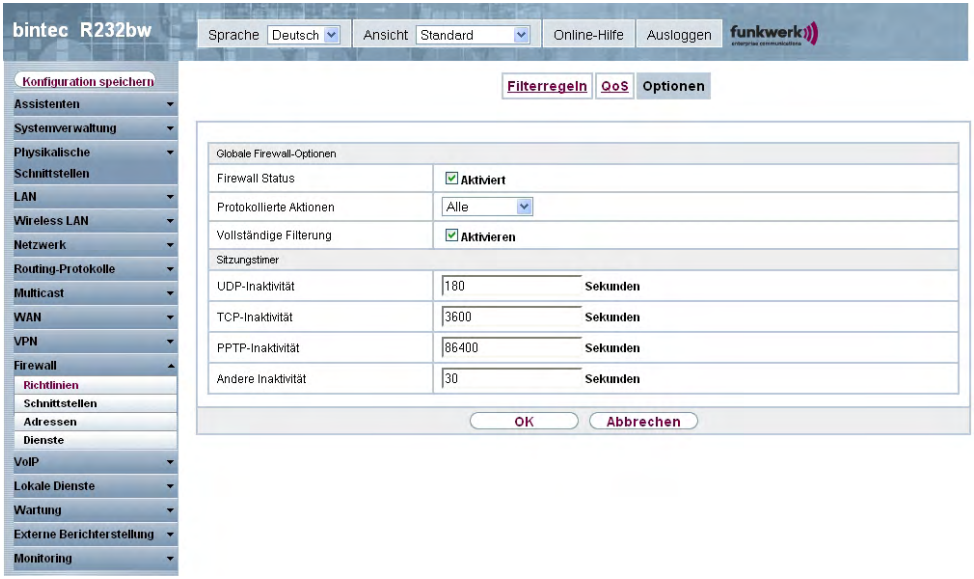


Abb. 108: **Firewall->Richtlinien->Optionen**

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

Felder im Menü OptionenGlobale 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". • *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

Feld	Beschreibung
	eine andere Schnittstelle gesendet werden als die, die die Verbindung erzeugt hat. Mit *Aktivieren*werden alle Pakete gefiltert (Standardwert).

Felder im Menü OptionenSitzungstimer

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*.

18.2 Schnittstellen

18.2.1 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.

18.2.1.1 Neu

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

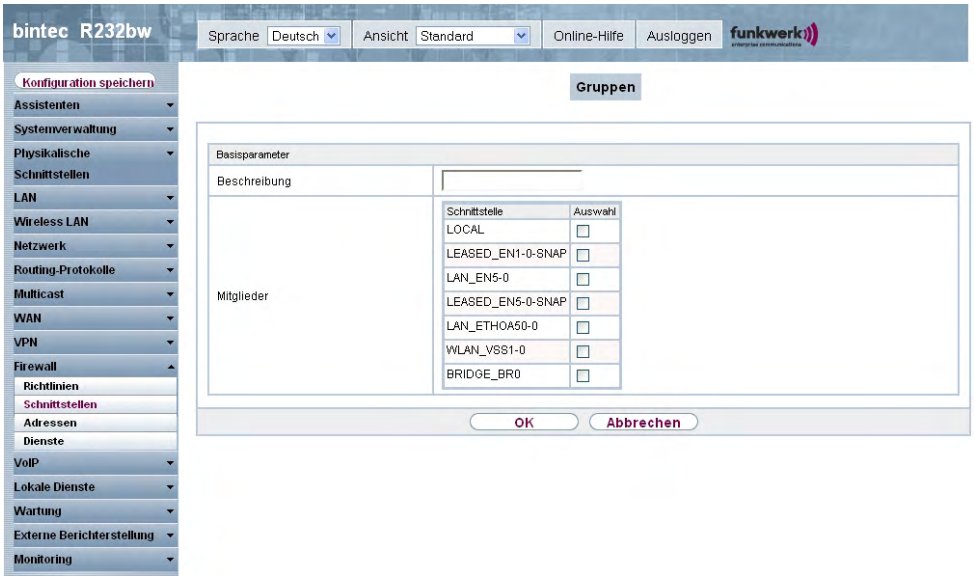


Abb. 109: **Firewall->Schnittstellen->Gruppen->Neu**

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

Felder im Menü GruppenBasisparameter

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 **Mitglieder**.

18.3 Adressen

18.3.1 Adressliste

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

18.3.1.1 Neu

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

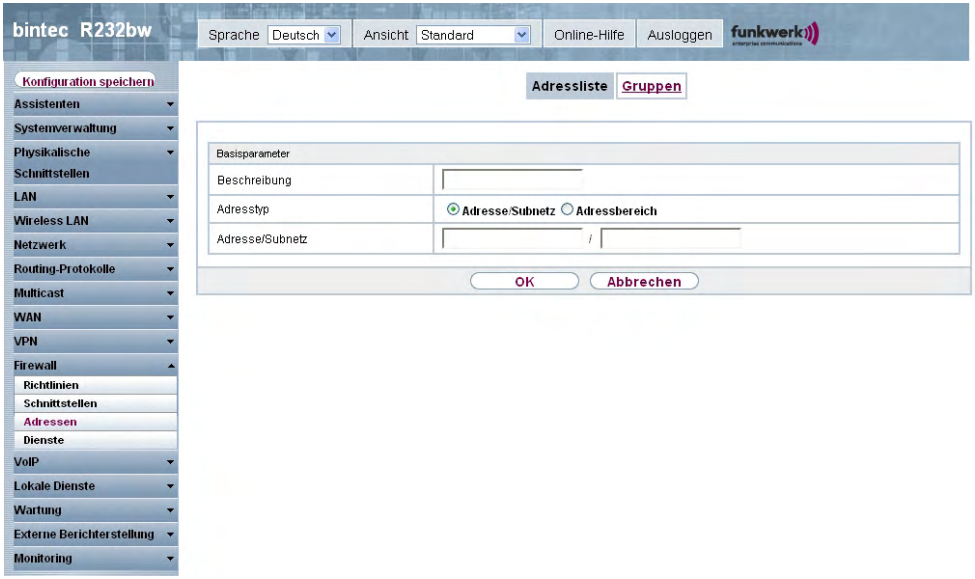


Abb. 110: **Firewall**->**Adressen**->**Adressliste**->**Neu**

Das Menü **Firewall**->**Adressen**->**Adressliste**->**Neu** besteht aus folgenden Feldern:

Felder im Menü AdresslisteBasisparameter

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 An-

Feld	Beschreibung
	fangs- 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. Standardwert ist jeweils *0.0.0.0*.
Adressbereich	Nur für **Adresstyp** = *Adressbereich* Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein.

18.3.2 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.

18.3.2.1 Neu

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

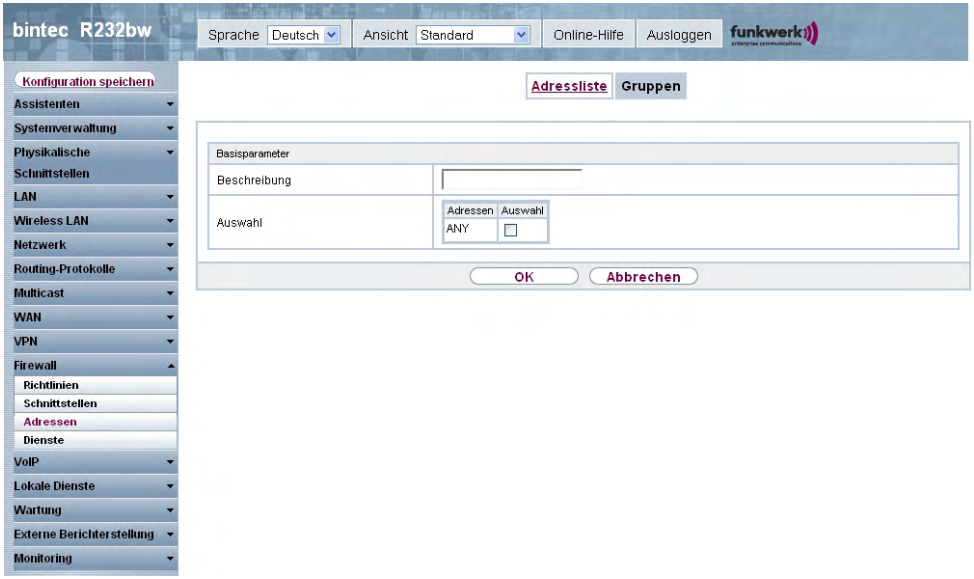


Abb. 111: **Firewall->Adressen->Gruppen->Neu**

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

Felder im Menü GruppenBasisparameter

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**.

18.4 Dienste

18.4.1 Diensteliste

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

18.4.1.1 Neu

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

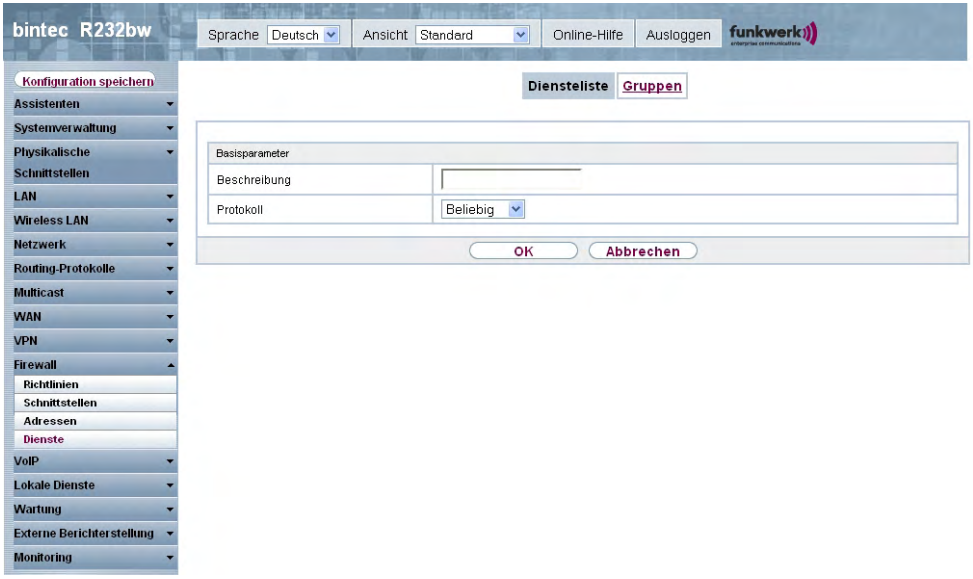


Abb. 112: **Firewall->Dienste->Diensteliste->Neu**

Das Menü **Firewall->Dienste->Diensteliste->Neu** besteht aus folgenden Feldern:

Felder im Menü DiensteListeBasisparameter

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: • *Any* (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*

18.4.2 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.

18.4.2.1 Neu

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

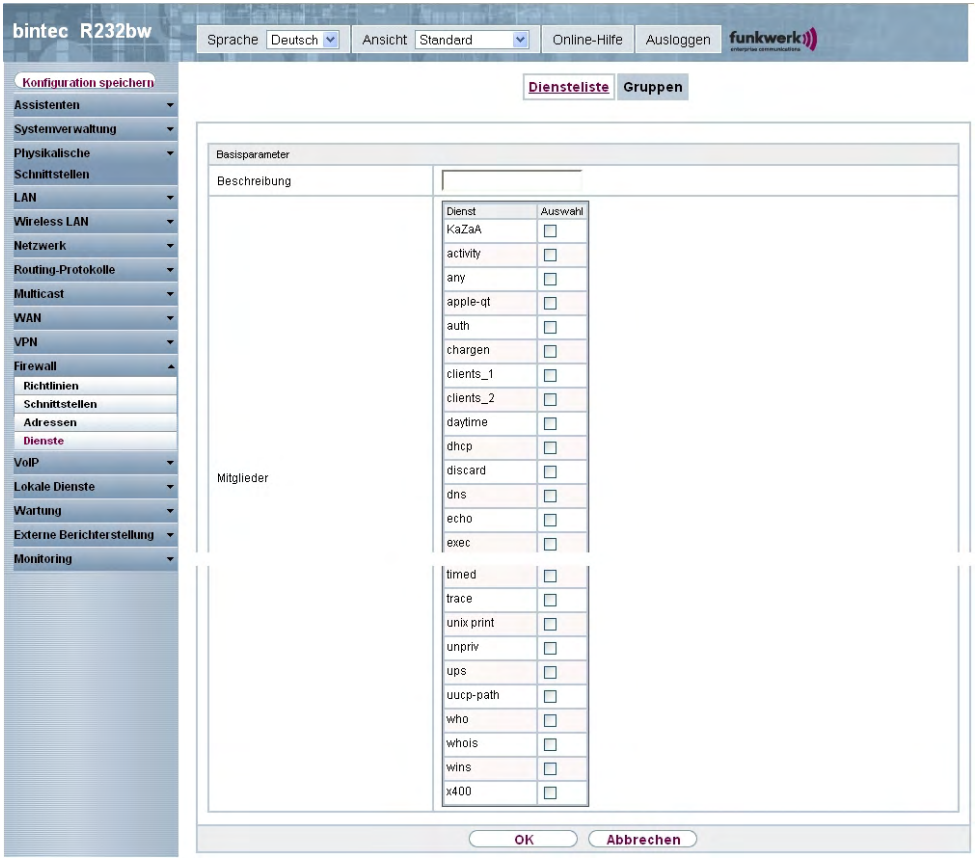


Abb. 113: **Firewall->Dienste->Gruppen->Neu**

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

Felder im Menü GruppenBasisparameter

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

Kapitel 19 VoIP

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

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

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

19.1 SIP

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

19.1.1 Optionen

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

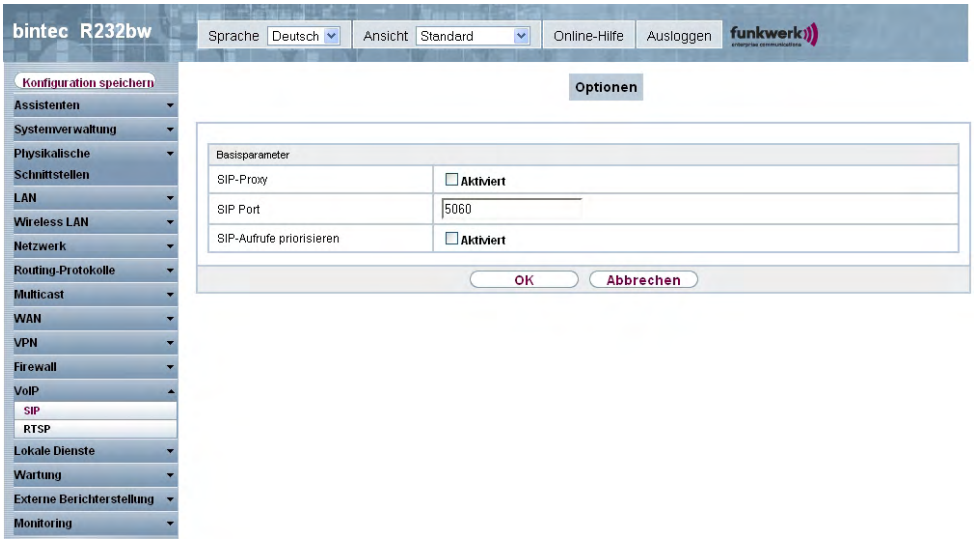


Abb. 114: **VoIP**->**SIP**->**Optionen**

Das Menü **VoIP**->**SIP**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

Feld	Beschreibung
SIP-Proxy	Wählen Sie, ob Sie den SIP-Proxy aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
SIP Port	Geben Sie den Port ein, der vom Proxy überwacht werden soll. Pro Destination Port, zu dem sich VoIP Clients aus dem LAN verbinden können, müssen Sie einen Proxy anlegen. Die Ports können Provider-spezifisch sein. Standardwert ist *5060*.
SIP-Aufrufe priorisieren	Wählen Sie, ob Sie SIP-Aufrufe priorisieren aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

19.2 RTSP

In diesem Menü konfigurieren Sie die Verwendung des RealTime Streaming Protokolls (RTSP).

RTSP ist ein Netzwerkprotokoll zur Steuerung von Multimedia-Datenströmen in IP-basierten Netzwerken. Mittels RTSP werden keine Nutzdaten übertragen. Vielmehr wird damit eine Multimedia-Session zwischen Sender und Empfänger gesteuert.

Wenn Sie RTSP nutzen möchten, müssen Firewall und NAT entsprechend konfiguriert werden. Im Menü **VoIP**->**RTSP** können Sie den RTSP-Proxy aktivieren, um bei Bedarf angefragte RTSP-Sessions über den definierten Port zu ermöglichen.

19.2.1 RTSP-Proxy

Im Menü **VoIP**->**RTSP**->**RTSP-Proxy** konfigurieren Sie die Verwendung des RealTime Streaming Protokolls.

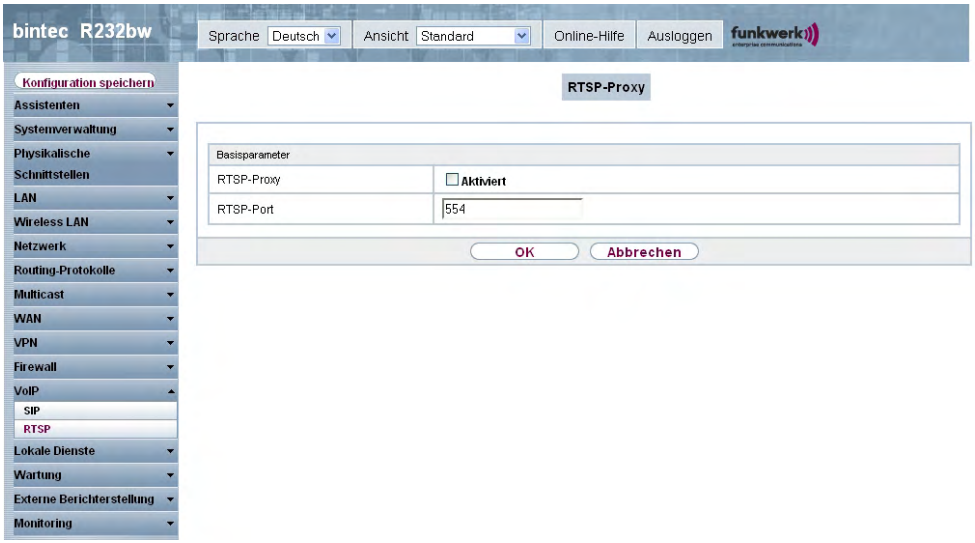


Abb. 115: **VoIP**->**RTSP**->**RTSP-Proxy**

Das Menü **VoIP**->**RTSP**->**RTSP-Proxy** besteht aus den folgenden Feldern:

Felder im Menü RTSP-ProxyBasisparameter

Feld	Beschreibung
RTSP-Proxy	Wählen Sie aus, ob Sie RTSP-Sessions zulassen möchten. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
RTSP-Port	Wählen Sie den Port aus, über den RTSP-Nachrichten ein- bzw. ausgehen sollen. Mögliche Werte sind `0` bis `65535`. Der Standardwert ist `554`.

Kapitel 20 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Zugriffsbeschränkung auf das Internet (Web-Filter)
- Zuordnung von eingehenden und ausgehenden Daten- und Sprachrufen zu authorisierten Benutzern (CAPI-Server)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Tests
- Schutz des Benutzer-LAN (Diebstahlsicherung)
- Automatische Erkennung und Konfiguration von **bintec**-Geräten
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)
- Bereitstellung öffentlicher Internetzugänge (Hotspot).
- Verwendung eines redundanten Gateways (BRRP)

20.1 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 (Forwarded Domains) 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, um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Globale Name-Server

Unter **Lokale Dienste**->**DNS**->**Globale Einstellungen**->**Basisparameter** werden die IP-Adressen von globalen Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Name-Server die IP-Adresse Ihres Geräts selbst oder die allgemeine Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch 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 globale Name-Server eingetragen sind, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Sind für lokale Anwendungen die IP-Adresse Ihres Geräts oder die Loopback-Adresse eingetragen, werden diese hier ignoriert. 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, wenn das Überschreiben der Adressen der globalen Name-Server zulässig ist (**DNS-Serverkonfiguration** = *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 werden diese als globale Name-Server eingetragen und stehen 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.

20.1.1 Globale Einstellungen

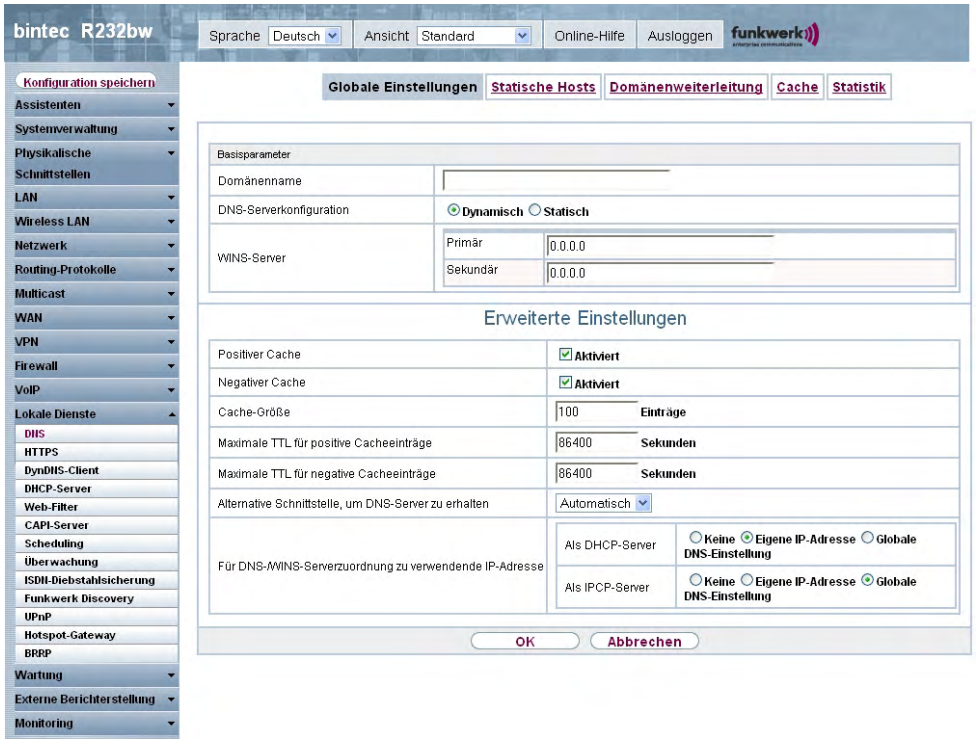


Abb. 116: **Lokale Dienste->DNS->Globale Einstellungen**

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Globale EinstellungenBasisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard Domain-Namen Ihres Geräts ein.
DNS-Serverkonfiguration	Wählen Sie aus, ob die Adressen der globalen Name-Server auf Ihrem Gerät mit übermittelten Name-Server-Adressen überschrieben werden dürfen.

Feld	Beschreibung
	Mögliche Werte: • *Dynamisch* (Standardwert): Die Name-Server-Adressen können automatisch überschrieben werden. • *Statisch* : Die Name-Server-Adressen werden nicht überschrieben.
DNS-Server **Primär** **Sekundär**	Nur für **DNS-Serverkonfiguration** = *Statisch* Geben Sie die IP-Adresse des ersten und falls erforderlich des zweiten globalen DNS-Servers ein.
WINS-Server **Primär** **Sekundär**	Geben Sie die IP-Adresse des ersten und falls erforderlich des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Negativer Cache	Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Cache-Größe	Geben Sie die maximale Gesamtanzahl der statischen und dynamischen Einträge ein. Wird dieser Wert erreicht, wird bei einem neu hinzukommenden

Feld	Beschreibung
	Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird **Cache-Größe** vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. **Cache-Größe** kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden. Mögliche Werte: *0* .. *1000* . 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. 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. Standardwert ist *86400* .
Alternative Schnittstelle, um DNS-Server zu erhalten	Nur für **DNS-Serverkonfiguration** = *Dynamisch* Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren. Standardwert ist *Automatisch* d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.
Für DNS- / WINS-Serverzuordnung zu verwendende IP-Adresse	**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.

Feld	Beschreibung
	• *Globale 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. • *Globale DNS-Einstellung* (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

20.1.2 Statische Hosts

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

20.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

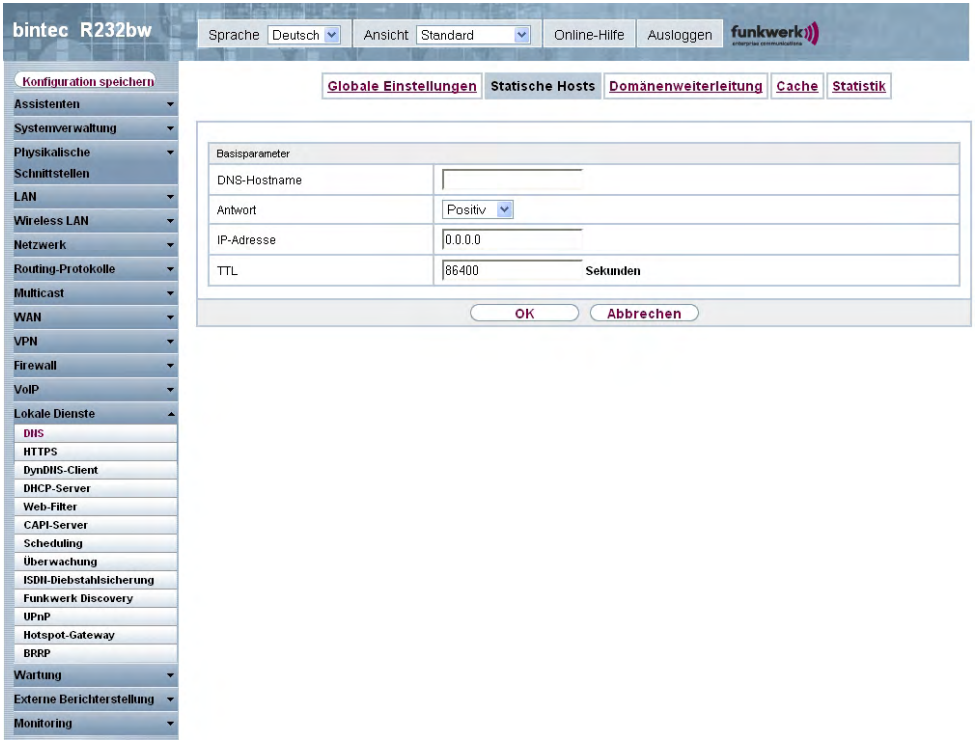


Abb. 117: **Lokale Dienste->DNS->Statische Hosts->Neu**

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Statische HostsBasisparameter

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. *.funkwerk-ec.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.

Feld	Beschreibung
	Mögliche Werte: • *Negativ* : Eine DNS-Anfrage nach **DNS-Hostname** wird negativ beantwortet. • *Positiv* (Standardwert): Eine DNS-Anfrage nach **DNS-Hostname** wird mit der dazugehörigen **IP-Adresse** beantwortet. • *Keine* : Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
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. Standardwert ist *86400* (= 24 h).

20.1.3 Domänenweiterleitung

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

20.1.3.1 Neu

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

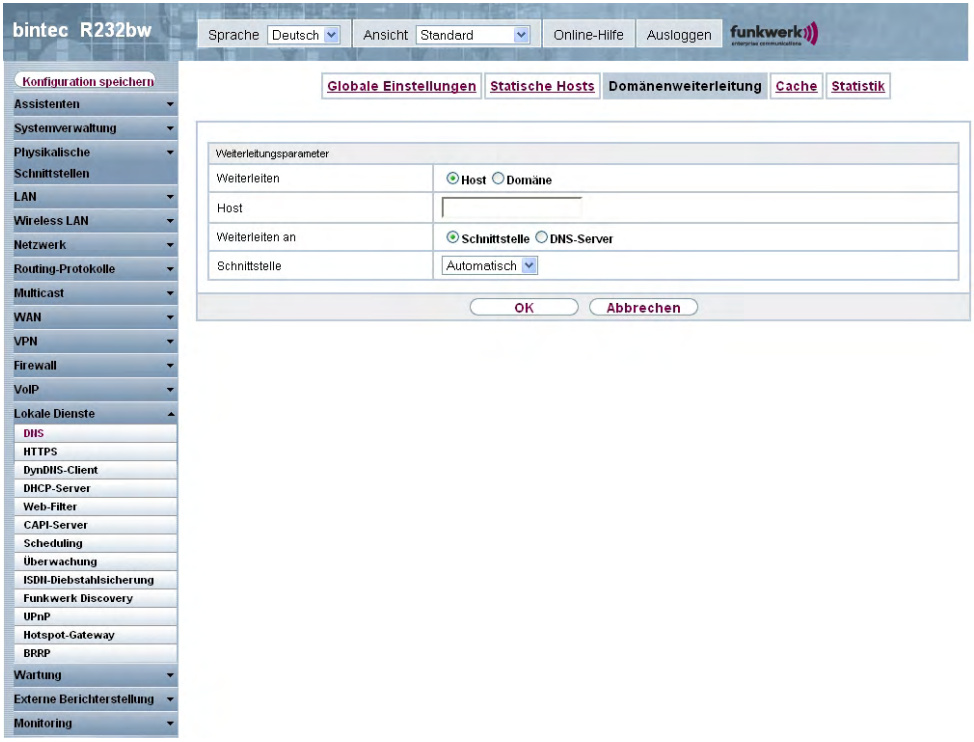


Abb. 118: **Lokale Dienste->DNS->Domänenweiterleitung->Neu**

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung->Neu** besteht aus folgenden Feldern:

Felder im Menü DomänenweiterleitungWeiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob ein Host oder eine Domäne weitergeleitet werden soll. Mögliche Werte: • `Host` (Standardwert) • `Domäne`
Host	Nur für **Weiterleiten** = `Host` Geben Sie den Namen des Hosts ein, der weitergeleitet werden soll. Der Eintrag kann auch mit dem Wildcard * beginnen, z. B.

Feld	Beschreibung
	*.funkwerk.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **OK** " **<Default Domain>.** " ergänzt.
Domäne	Nur für **Weiterleiten** = *Domäne* Geben Sie den Namen der Domäne ein, die weitergeleitet werden soll. Der Eintrag kann auch mit dem Wildcard * beginnen, z. B. *.funkwerk.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **OK** " **<Default Domain>.** " ergänzt.
Weiterleiten an	Wählen Sie aus, wohin Anfragen an den in **Host** bzw. **Domäne** definierten Namen weitergeleitet werden sollen. Mögliche Werte: • *Schnittstelle* (Standardwert): Die Anfrage wird an die definierte **Schnittstelle** weitergeleitet. • *DNS-Server*: Die Anfrage wird an den definierten **DNS-Server** weitergeleitet.
Schnittstelle	Nur für **Weiterleiten an** = *Schnittstelle* Wählen Sie die Schnittstelle aus, über die Anfragen für die definierte **Domäne** eingehen und an den DNS-Server weitergeleitet werden sollen.
DNS-Server	Nur für **Weiterleiten an** = *DNS-Server* Geben Sie IP-Adresse des primären und sekundären DNS-Servers ein.

20.1.4 Cache

Im Menü **Lokale Dienste**->**DNS**->**Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

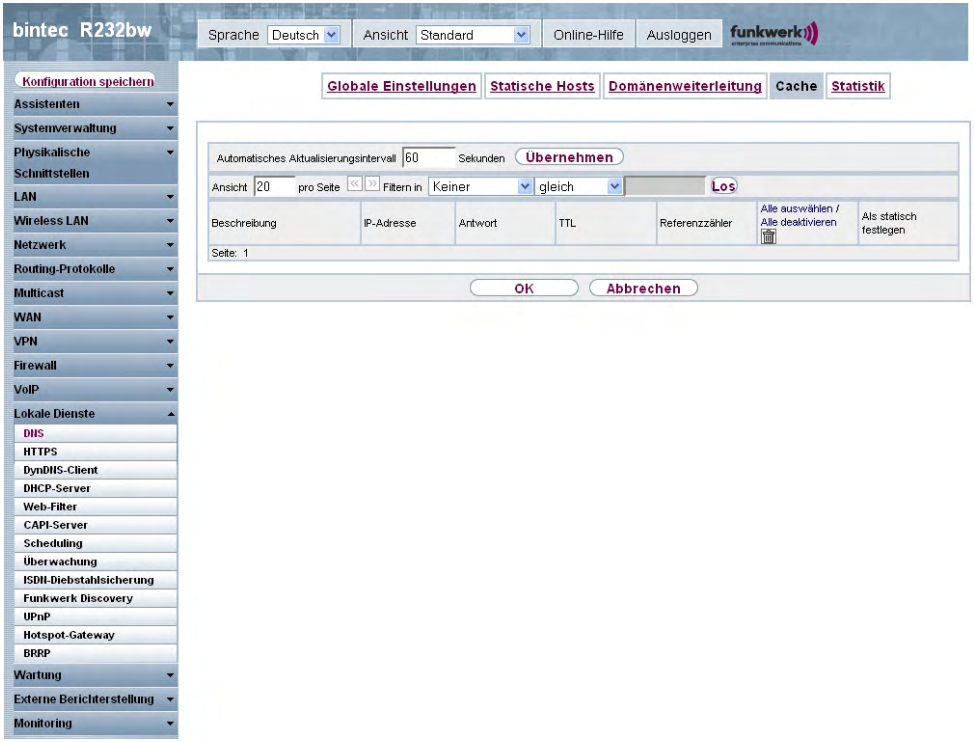


Abb. 119: **Lokale Dienste->DNS->Cache**

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 damit aus dieser Liste und wird in der Liste im Menü **Statische Hosts** aufgelistet. Die TTL wird dabei übernommen.

20.1.5 Statistik

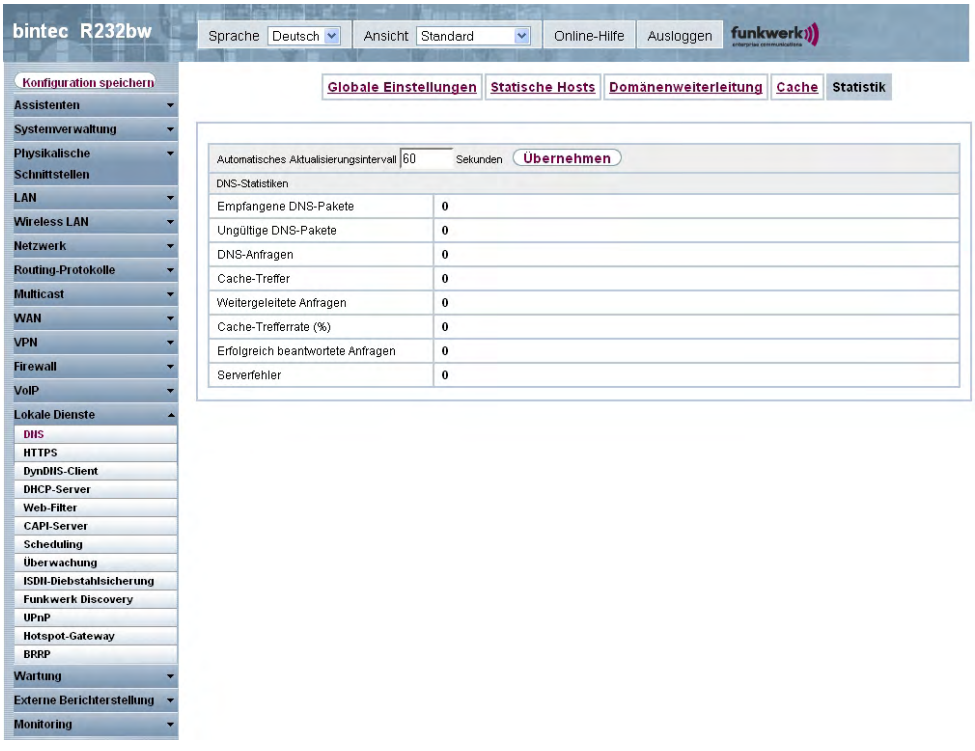


Abb. 120: **Lokale Dienste->DNS->Statistik**

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü StatistikDNS-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.

Feld	Beschreibung
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-Anfragen** 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.

20.2 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.

20.2.1 HTTPS-Server

Im Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

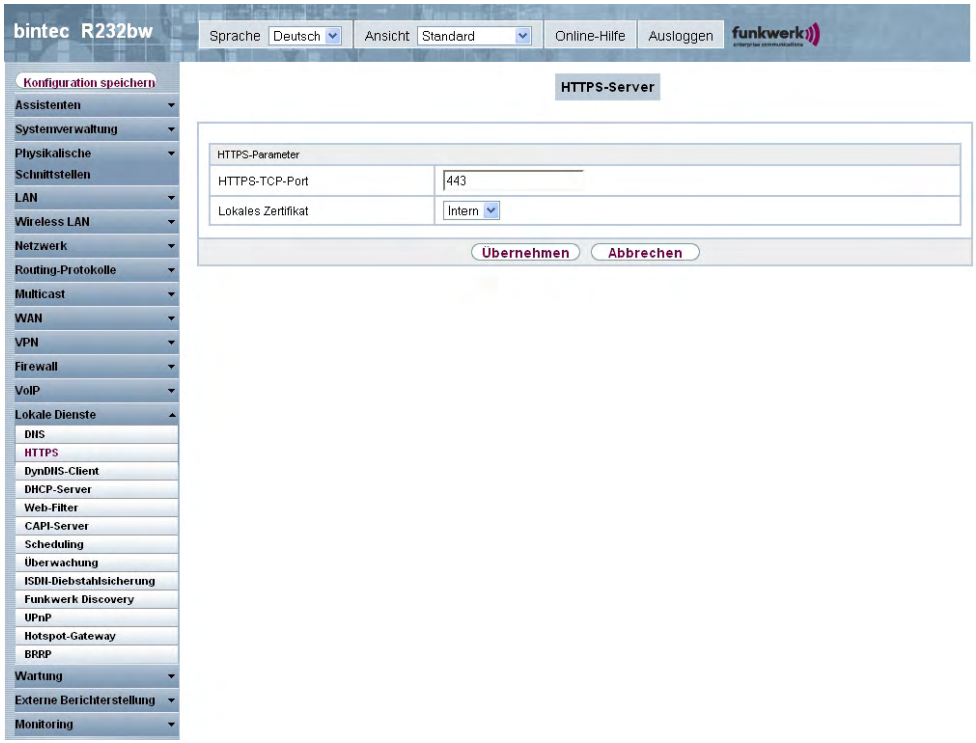


Abb. 121: **Lokale Dienste->HTTPS->HTTPS-Server**

Das Menü **Lokale Dienste->HTTPS->HTTPS-Server** besteht aus folgenden Feldern:

Felder im Menü HTTPS-ServerHTTPS-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*. Standardwert ist *443*.
Lokales Zertifikat	Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll. Mögliche Werte: • *Intern* (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möchten.

Feld	Beschreibung
	• *<Zertifikatsname>*: Wählen Sie ein unter **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** eingetragenes Zertifikat aus.

20.3 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, 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.

20.3.1 DynDNS-Aktualisierung

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

20.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

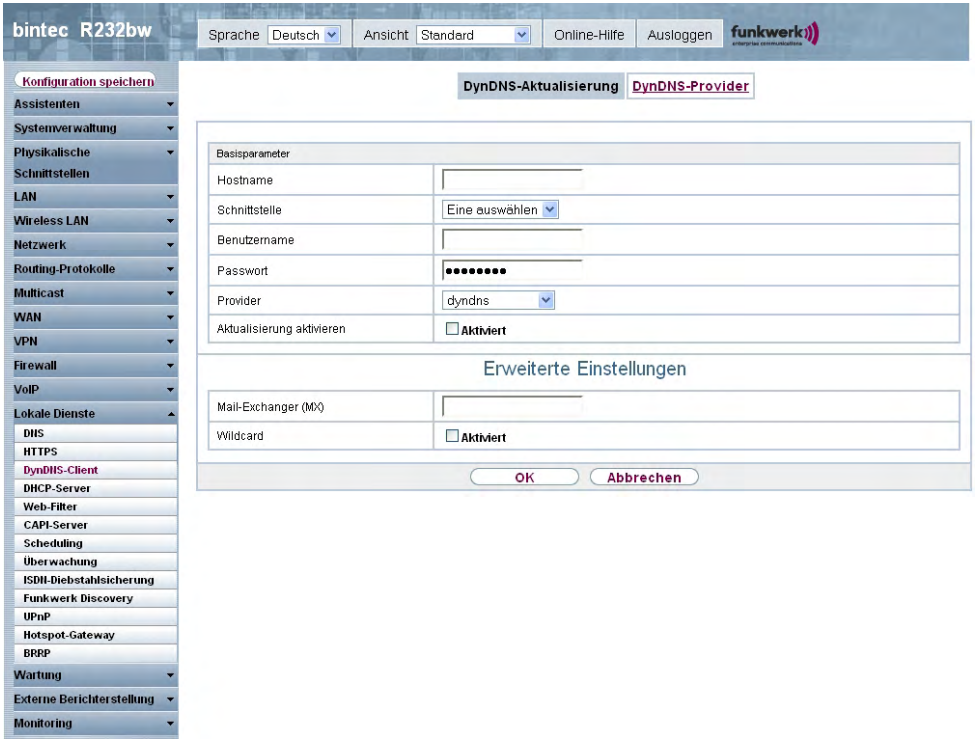


Abb. 122: **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü DynDNS-AktualisierungBasisparameter

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.

Feld	Beschreibung
Provider	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Weitere DynDNS-Provider können im Menü **Lokale Dienste**->**DynDNS-Client**->**DynDNS-Provider** konfiguriert werden. 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.

20.3.2 DynDNS-Provider

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

20.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

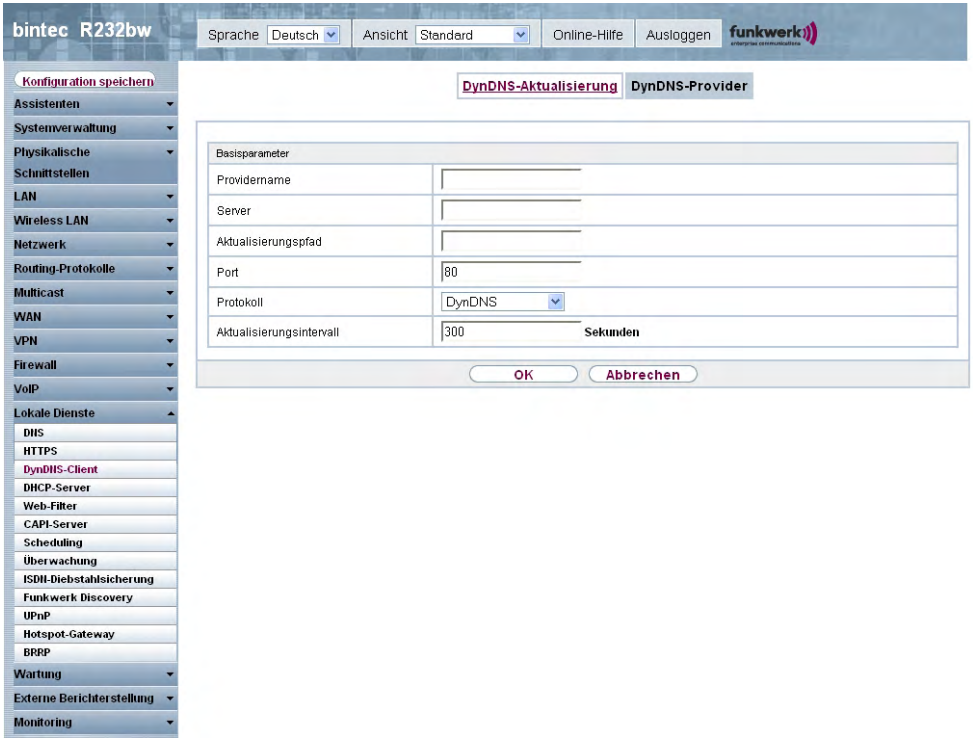


Abb. 123: **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü DynDNS-ProviderBasisparameter

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.

Feld	Beschreibung
	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. Standardwert ist *80* .
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: • *DynDNS*(Standardwert) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Aktualisierungsintervall	Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf. Standardwert ist *300* Sekunden.

20.4 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. Ein Rechner sendet einen ARP-Request aus und erhält daraufhin seine IP-Adresse von Ihrem Gerät zugewiesen. 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.

20.4.1 DHCP Pool

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 Pool** 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.

20.4.1.1 Bearbeiten oder Neu

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

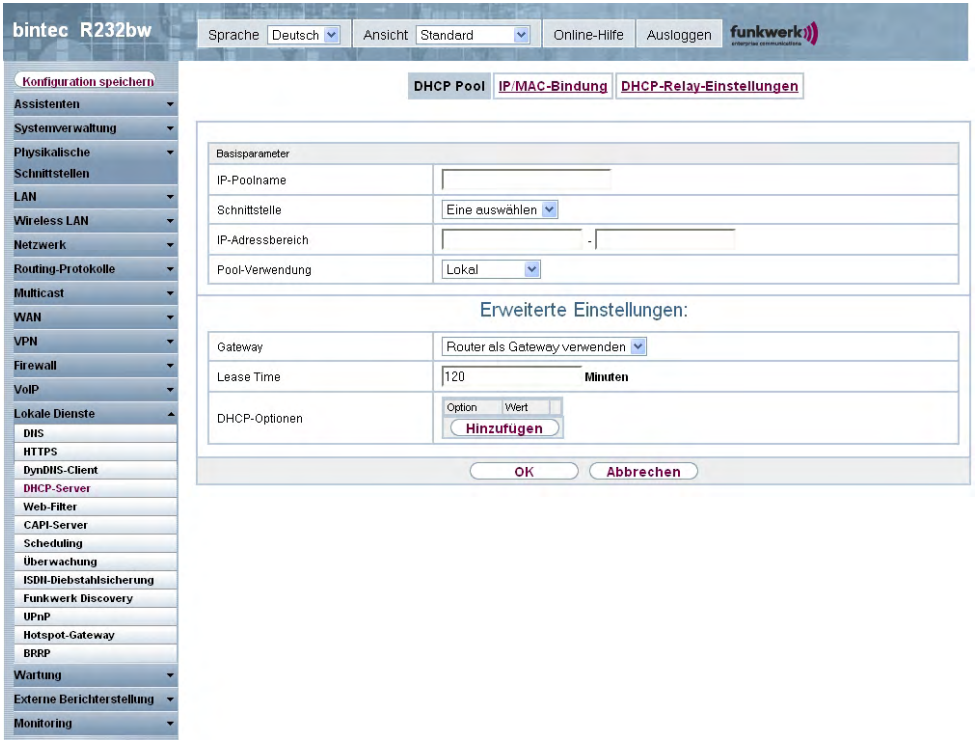


Abb. 124: **Lokale Dienste->DHCP-Server->DHCP Pool->Neu**

Das Menü **Lokale Dienste->DHCP-Server->DHCP Pool->Neu** besteht aus folgenden Feldern:

Felder im Menü DHCP PoolBasisparameter

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-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
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 an-

Feld	Beschreibung
	deren Netz zu definieren. Mögliche Werte: • *Lokal* (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • *Lokal/Relais*: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz 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: • *Kein Gateway* (Standardwert): Hier wird keine IP-Adresse übermittelt. • *Router als Gateway verwenden*: Hier wird die für die **Schnittstelle** definierte IP-Adresse übertragen. • *Angeben*: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll. Nachdem **Lease Time** abgelaufen ist, kann die Adresse durch den Server neu vergeben werden. 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

Feld	Beschreibung
	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*: Geben Sie den Typ des WINS/NBT Nodes ein, der dem Client übermittelt werden soll. • *TFTP-Server*: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche **Hinzufügen** ein.

20.4.2 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 nun 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**->**DHCP Pool** IP-Adressbereiche konfiguriert wurden.

20.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

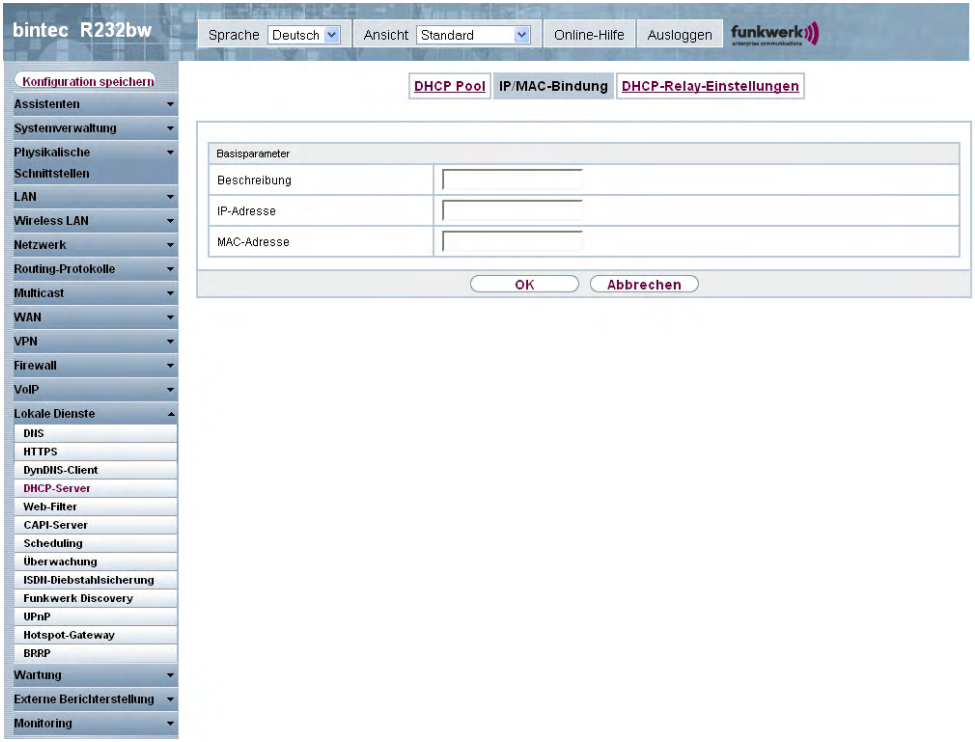


Abb. 125: **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu**

Das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu** besteht aus folgenden Feldern:

Felder im Menü IP/MAC-BindungBasisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen **MAC-Adresse** die **IP-Adresse** gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in **MAC-Adresse** angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in **IP-Adresse** angegebene IP-Adresse zugewiesen werden soll.

20.4.3 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.

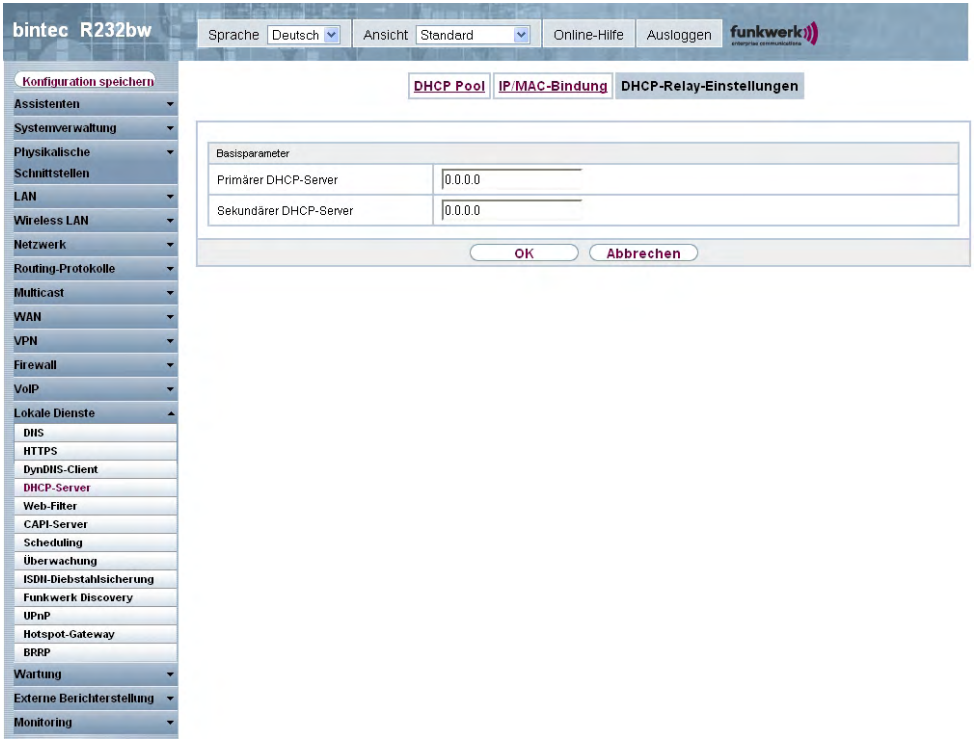


Abb. 126: **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen**

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü DHCP-Relay-EinstellungenBasisparameter

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

Feld	Beschreibung
Server	CP-Servers ein.

20.5 Web-Filter

Im Menü **Lokale Dienste**->**Web-Filter** lässt sich ein URL-basierter Web-Filter-Dienst konfigurieren, der zur Laufzeit auf das Proventia Web Filter der Firma Internet Security Systems (*www.iss.net*) zugreift und überprüft, wie eine angeforderte Internet-Seite durch das Proventia Web Filter kategorisiert worden ist. Die Aktion, die sich aus der Kategorisierung ergibt, wird auf Ihrem Gerät konfiguriert.

20.5.1 Allgemein

In diesem Menü finden Sie die Konfiguration grundlegender Parameter für die Nutzung des Proventia Web Filters.

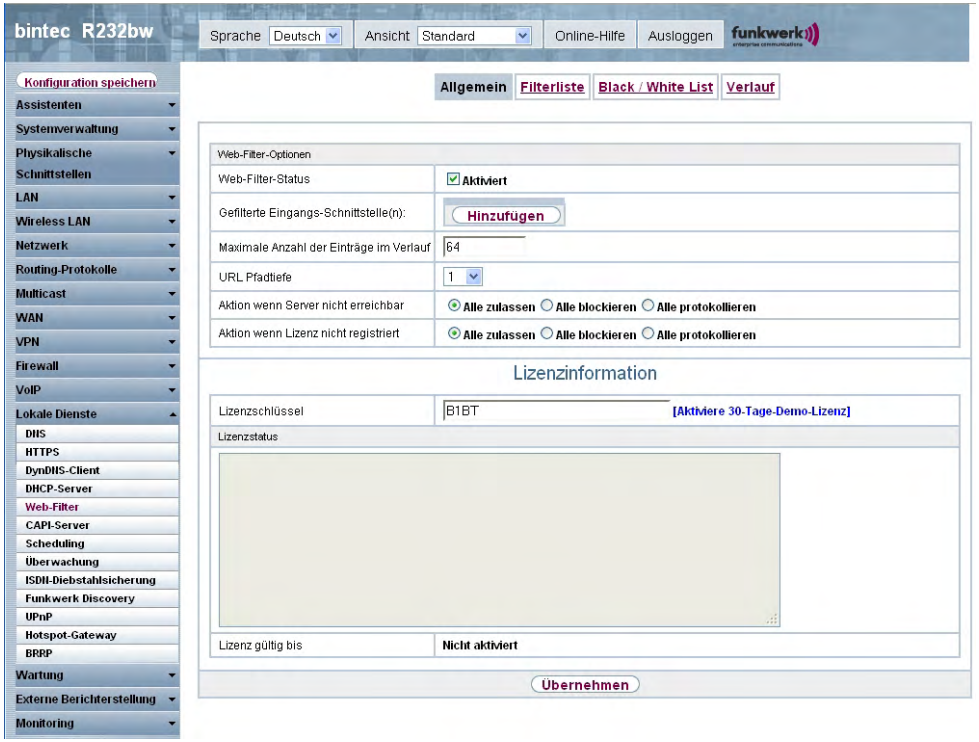


Abb. 127: **Lokale Dienste->Web-Filter+Allgemein**

Das Menü **Lokale Dienste->Web-Filter+Allgemein** besteht aus folgenden Feldern:

Felder im Menü AllgemeinWeb-Filter-Optionen

Feld	Beschreibung
Web-Filter-Status	Aktivieren oder deaktivieren Sie das Filter. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Gefilterte Eingangs-Schnittstelle(n)	Wählen Sie aus, für welche der vorhandenen Ethernet- und WLAN-Schnittstellen Web Filtering aktiviert werden soll. Drücken Sie die **Hinzufügen**-Schaltfläche, wenn Sie weitere Schnittstellen hinzufügen wollen. Die Anforderungen von http-Internetseiten, die Ihr Gerät über diese Schnittstellen erreichen, werden dann vom Web Filtering überwacht.
Maximale Anzahl der Einträge im Verlauf	Definieren Sie die Anzahl an Einträgen, die im Web Filtering Verlauf (Menü **Verlauf**) gespeichert werden sollen. Mögliche Werte sind *1* bis *512*. Standardwert ist *64*.
URL Pfadtiefe	Wählen Sie aus, bis zu welcher Pfadtiefe eine URL durch den Cobion Orange Filter geprüft werden soll.
Aktion wenn Server nicht erreichbar	Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Web-Filtering-Server nicht erreichbar ist. Mögliche Werte: • *Alle zulassen* (Standardwert): Der Aufruf wird zugelassen. • *Alle blockieren*: Der Aufruf der angeforderten Seite wird geblockt. • *Alle protokollieren*: Der Aufruf wird zugelassen, aber protokolliert.
Aktion wenn Lizenz nicht registriert	Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Lizenzschlüsselstatus *Nicht gültig* ist. Mögliche Werte: • *Alle zulassen* (Standardwert): Der Aufruf wird zugelas-

Feld	Beschreibung
	sen. • *Alle blockieren*: Der Aufruf der angeforderten Seite wird geblockt. • *Alle protokollieren*: Der Aufruf wird zugelassen, aber protokolliert.

Das Menü **Lizenzinformation** besteht aus folgenden Feldern:

Felder im Menü AllgemeinLizenzinformation

Feld	Beschreibung
Lizenzschlüssel	Tragen Sie die Nummer der erworbenen Proventia Web Filter-Lizenz ein. Die voreingestellte, von ISS vergebene Kennung bezeichnet den Gerätetyp. Im Auslieferungszustand haben Sie die Möglichkeit eine 30-Tage-Demoversion des Proventia Web Filter zu aktivieren. Klicken Sie hierzu die Verknüpfung **Aktiviere 30-Tage-Demo-Lizenz**
Lizenzstatus	Zeigt das Ergebnis der letzten Gültigkeitsprüfung der Lizenz an. Die Gültigkeit der Lizenz wird alle 23 Stunden überprüft.
Lizenz gültig bis	Zeigt das Ablaufdatum der Lizenz (relativ zur eingestellten Zeit auf Ihrem Gerät) an und kann nicht editiert werden.

20.5.2 Filterliste

Im Menü **Lokale Dienste**->**Web-Filter**->**Filterliste** konfigurieren Sie, welche Kategorien von Internetseiten auf welche Weise behandelt werden sollen.

Hierfür konfigurieren Sie entsprechende Filter. Eine Liste der bereits konfigurierten Filter wird angezeigt.

Bei der Konfiguration der Filter gibt es grundsätzlich unterschiedliche Ansätze:

- Zum einen kann man eine Filterliste anlegen, die nur Einträge für solche Adressen enthält, die blockiert werden sollen. In diesem Fall ist es notwendig, am Ende der Filterliste einen Eintrag vorzunehmen, der alle Zugriffe, auf die kein Filter zutrifft, gestattet. (Einstellung dafür: **Kategorie** = *Default behaviour*, **Aktion** = *Zulassen* oder *Zulassen und Protokollieren*)
- Wenn Sie nur Einträge für solche Adressen anlegen, die zugelassen bzw. protokolliert

werden sollen, ist eine Änderung des Standardverhaltens (=alle übrigen Aufrufe werden geblockt) nicht notwendig.

20.5.2.1 Neu

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

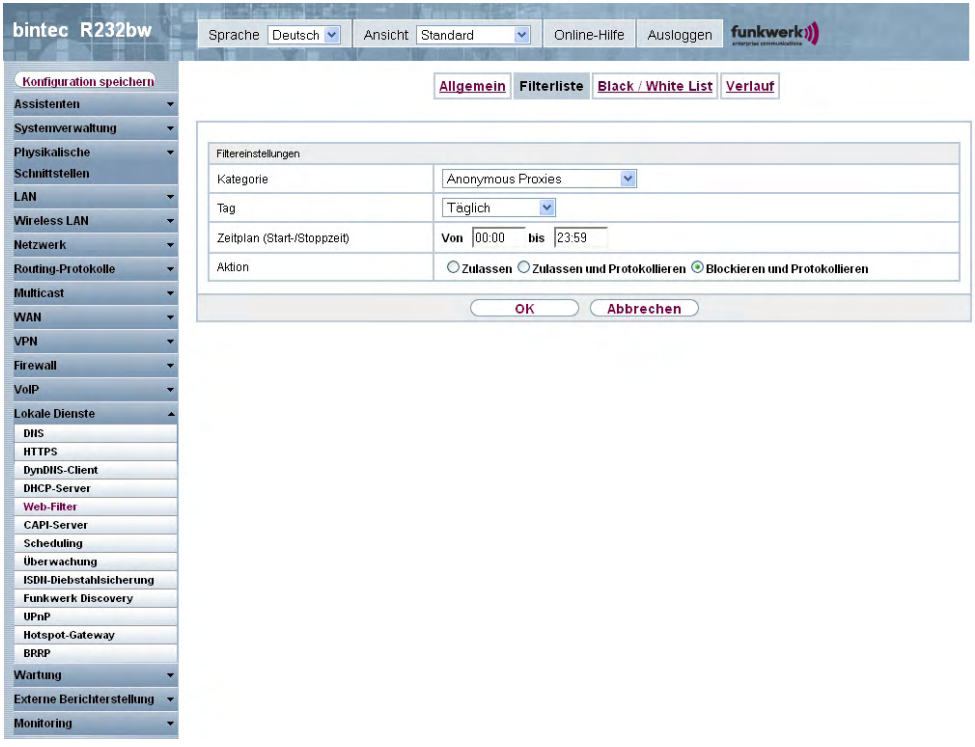


Abb. 128: **Lokale Dienste->Web-Filter->Filterliste->Neu**

Das Menü **Lokale Dienste->Web-Filter->Filterliste->Neu** besteht aus folgenden Feldern:

Felder im Menü FilterlisteFiltereinstellungen

Feld	Beschreibung
Kategorie	Wählen Sie aus, auf welche Kategorie von Adressen/URLs das Filter angewendet werden soll. Zur Auswahl stehen zum einen die Standardkategorien des Proventia Web Filters (Standardwert: `Anonymous Proxies`). Darüber hinaus können Aktionen für folgende Sonderfälle definiert werden, z. B.: • `Default behaviour`: Diese Kategorie trifft auf alle Internet-

Feld	Beschreibung
	Adressen zu. • *Other Category*: Manche Adressen sind dem Proventia Web Filter bereits bekannt, aber noch nicht kategorisiert. Für derartige Adressen wird die mit dieser Kategorie verbundene Aktion angewendet. • *Unknown URL*: Wenn eine Adresse dem Proventia Web Filter nicht bekannt ist, wird die mit dieser Kategorie verbundene Aktion angewendet.
Tag	Wählen Sie aus, an welchen Tagen das Filter aktiv sein soll. Zur Verfügung stehen: • *Täglich* (Standardwert): Das Filter gilt für jeden Tag der Woche. • *<Wochentag>*: Das Filter gilt für einen bestimmten Tag der Woche. Es kann pro Filter nur ein Tag ausgewählt werden, für mehrere einzelne Tage müssen mehrere Filter angelegt werden. • *Montag-Freitag*: Das Filter gilt montags bis freitags. Standardwert ist *Täglich*.
Zeitplan (Start-/Stoppzeit)	Geben Sie bei **Von** ein, nach welcher Uhrzeit das Filter aktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Geben Sie in das Feld nach dem **bis** ein, zu welcher Uhrzeit das Filter deaktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Standardwert ist 00:00 bis 23.59.
Aktion	Wählen Sie die Aktion, die ausgeführt werden soll, wenn das Filter auf einen Aufruf zutrifft. Mögliche Werte: • *Blockieren und Protokollieren* (Standardwert): Der Aufruf der angeforderten Seite wird unterbunden und protokolliert. • *Zulassen und Protokollieren*: Der Aufruf wird zugelassen, aber protokolliert. Einsicht in die protokollierten Ereignisse ist im Menü **Lokale Dienste**->**Web-Filter**->**Filterliste** möglich. • *Zulassen*: Der Aufruf wird zugelassen und nicht protokolliert.

20.5.3 Black / White List

Das Menü **Lokale Dienste**->**Web-Filter**->**Black / White List** enthält eine Liste mit URLs bzw. IP-Adressen. Die Adressen **Auf der White List** können auch dann aufgerufen werden, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Proventia Web Filter blockiert würden. Die Adressen **Auf der Black List** sind auch dann blockiert, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Proventia Web Filter aufgerufen werden könnten. In der Standardkonfiguration enthalten beide Listen keine Einträge.

20.5.3.1 Hinzufügen

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere URLs oder IP-Adressen der Liste hinzufügen.

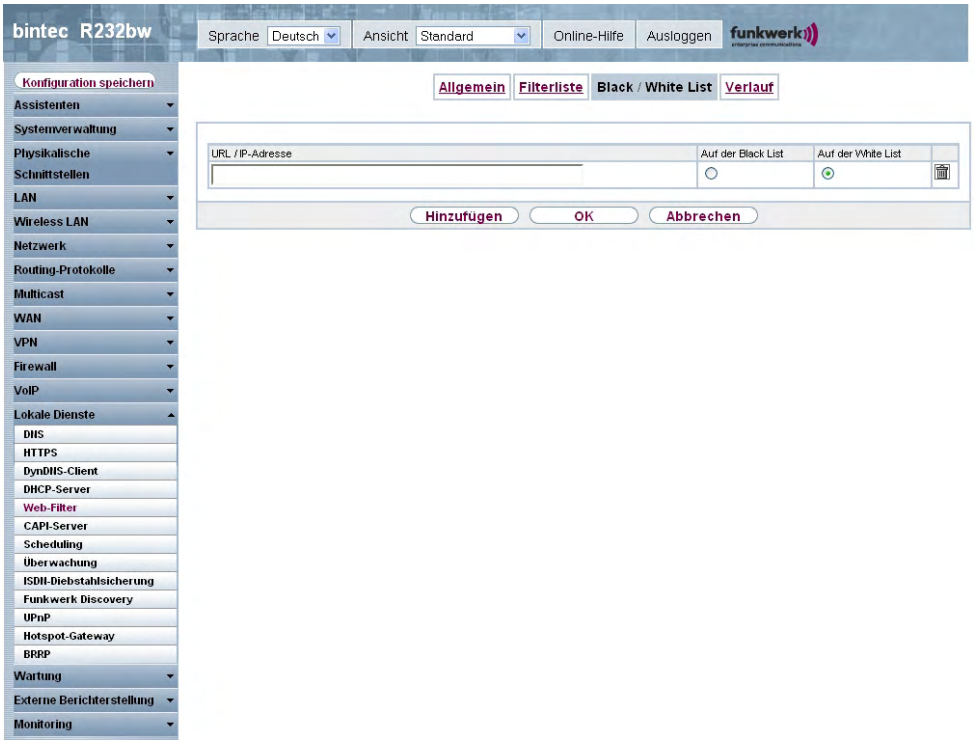


Abb. 129: **Lokale Dienste->Web-Filter->Black / White List->Hinzufügen**

Das Menü **Lokale Dienste**->**Web-Filter**->**Black / White List**->**Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Black / White List

Feld	Beschreibung
URL / IP-Adresse	Geben Sie eine URL oder IP-Adresse ein. Die Länge des Eintrags ist auf 60 Zeichen begrenzt.
Auf der Black List **Auf der White List**	Sie können wählen, ob eine URL oder IP-Adresse immer (*Auf der White List*) oder nie (*Auf der Black List*) aufgerufen werden kann. Standardmäßig ist *Auf der White List* aktiviert. Adressen, die in der White List geführt sind, werden automatisch zugelassen. Die Konfiguration eines entsprechenden Filters ist nicht notwendig.

20.5.4 Verlauf

Im Menü **Lokale Dienste**->**Web-Filter**->**Verlauf** können Sie den aufgezeichneten Verlauf des Web Filters einsehen. Es werden alle Aufrufe protokolliert, die durch einen entsprechenden Filter dafür markiert werden (**Aktion** = *Zulassen und Protokollieren* oder *Blockieren und Protokollieren*), ebenso alle abgewiesenen Aufrufe.

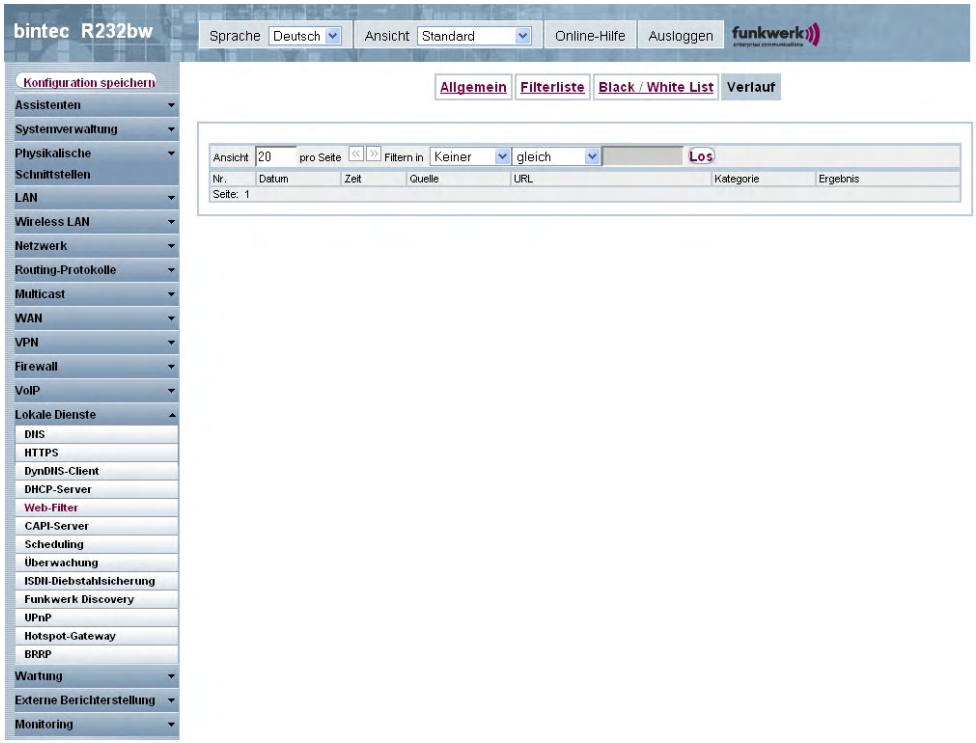


Abb. 130: **Lokale Dienste->Web-Filter->Verlauf**

20.6 CAPI-Server

Mit der Funktion CAPI-Server können Sie an Nutzer der CAPI-Anwendungen Ihres Geräts Benutzernamen und Passwörter vergeben. So stellen Sie sicher, dass nur authorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen über CAPI aufbauen können.

Der Dienst CAPI ermöglicht eingehenden und ausgehenden Daten- und Sprachrufen die Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Entfernte CAPI-Schnittstelle Ihres Geräts zugreifen. So können beispielsweise mit Ihrem Gerät verbundene Hosts Faxe empfangen und senden.

Hinweis

Alle eingehenden Rufe an die CAPI werden allen registrierten und "lauschenden" CAPI-Applikationen im LAN angeboten.

Im Auslieferungszustand ist für das Subsystem CAPI ein Benutzer mit dem Benutzer-

namen *default* ohne Passwort eingetragen.

Wenn Sie Ihre gewünschten Benutzer mit Passwort angelegt haben, sollten Sie den Benutzer *default* ohne Passwort löschen.

20.6.1 Benutzer

Im Menü **Lokale Dienste**->**CAPI-Server**->**Benutzer** wird eine Liste aller konfigurierter CAPI Benutzer angezeigt.

20.6.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

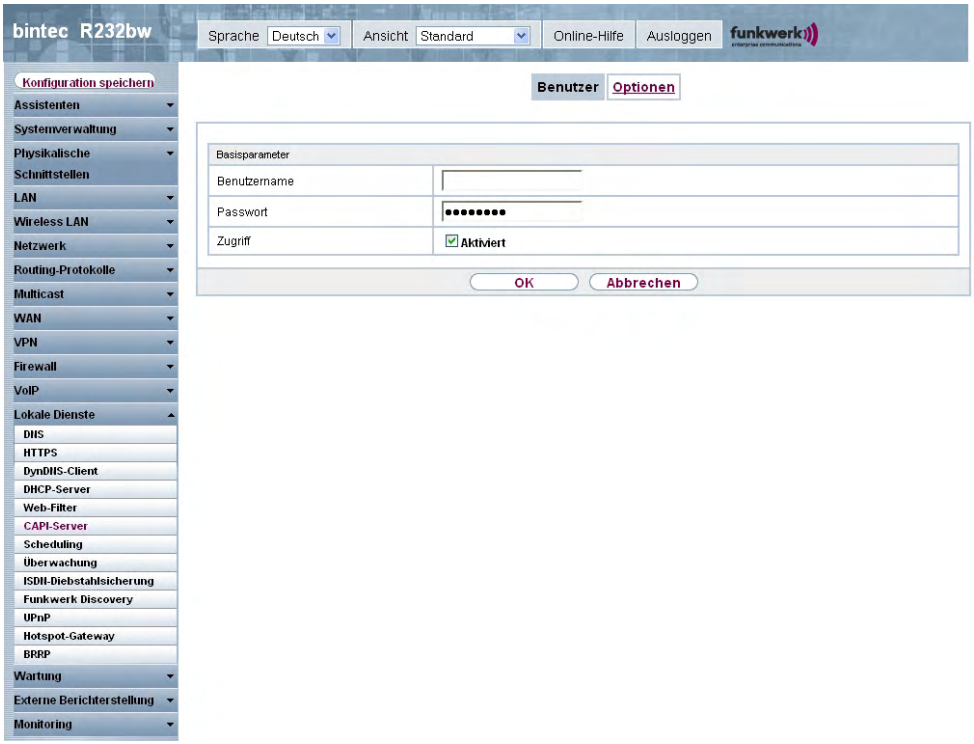


Abb. 131: **Lokale Dienste**->**CAPI-Server**->**Benutzer**->**Neu**

Das Menü **Lokale Dienste**->**CAPI-Server**->**Benutzer**->**Neu** besteht aus folgenden Feldern:

Felder im Menü BenutzerBasisparameter

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
Passwort	Geben Sie das Passwort ein, mit dem sich der Benutzer **Benutzername** identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
Zugriff	Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

20.6.2 Optionen

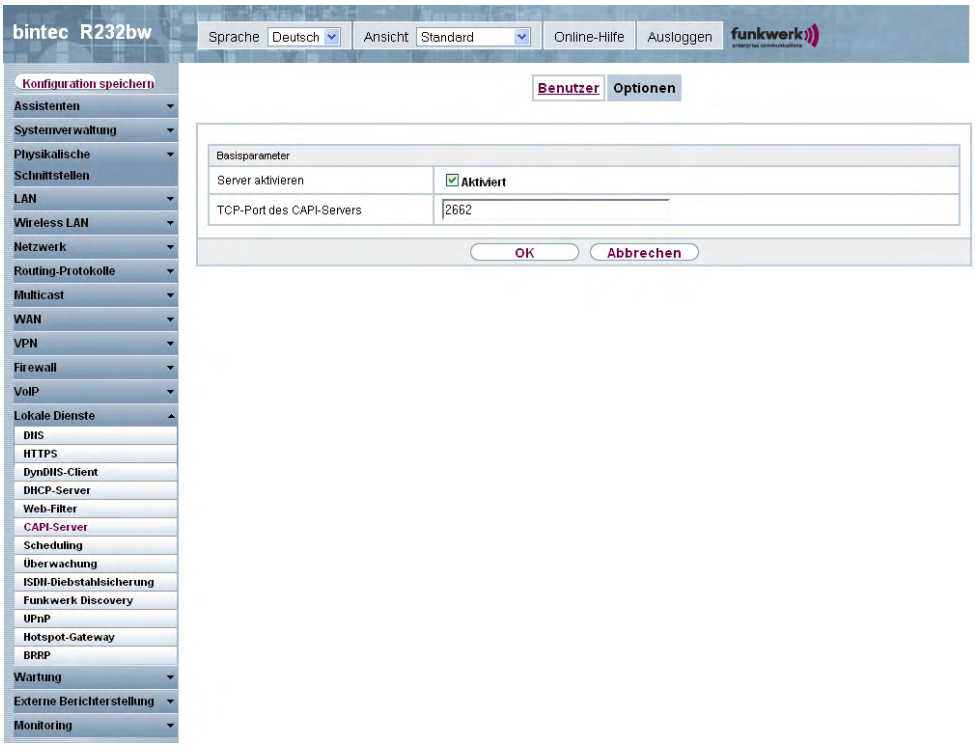


Abb. 132: **Lokale Dienste->CAPI-Server->Optionen**

Das Menü **Lokale Dienste**->**CAPI-Server**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

Feld	Beschreibung
Server aktivieren	Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-Port des CAPI-Servers	Das Feld ist nur editierbar, wenn **Server aktivieren** aktiviert ist. Geben Sie die TCP-Port-Nummer für Remote-CAPI-Verbindungen ein. Standardwert ist `2662` .

20.7 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (Aktivierung bzw. Deaktivierung von Schnittstellen) zeitabhängig durchgeführt werden können.

Hinweis

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

20.7.1 Auslöser

Im Menü **Lokale Dienste**->**Scheduling**+**Auslöser** wird eine Liste aller geplanten Aufgaben angezeigt.

20.7.1.1 Neu

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

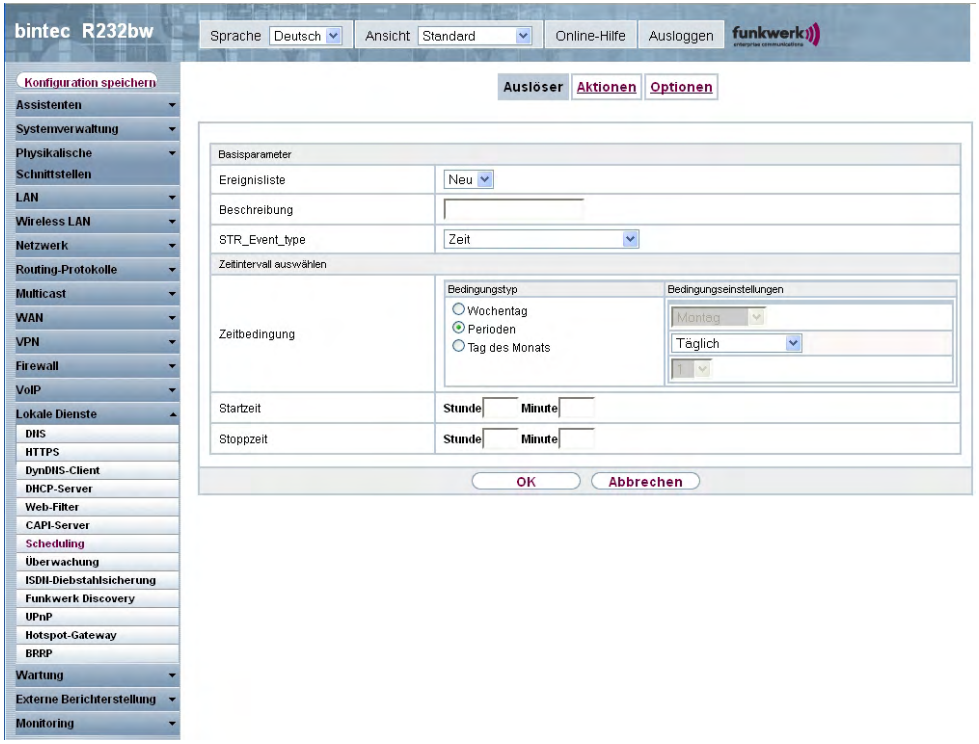


Abb. 133: **Lokale Dienste->Scheduling+Auslöser->Neu**

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

Felder im Menü AuslöserBasisparameter

Feld	Beschreibung
Ereignisliste	Geben Sie den gewünschten Index für diesen Auslöser an. Die konfigurierten Auslöser können über die Zuweisung zu einem Index zu Ereignislisten zusammengefasst werden, so dass auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden können. Die Auslöser innerhalb einer Ereignisliste werden dann in der Reihenfolge in der Liste abgearbeitet. Wenn Sie eine neue Ereignisliste hinzufügen möchten, wählen Sie `Neu` (Standardwert). Soll ein einzelnes Ereignis als Auslöser für Aktionen konfiguriert werden, erhält dieses ebenfalls einen Index.
Beschreibung	Geben Sie eine beliebige Bezeichnung für die geplante Aufgabe ein.

Feld	Beschreibung
Ereignistyp	Wählen Sie den Typ des Auslöser 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 zugewiesenene Aktionen werden ausgelöst, wenn der Datenverkehr auf den angebenen Schnittstellen den definierten Wert unter- oder überschreitet. • *Ping-Test*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die angegebenen Schnittstellen erreichbar bzw. nicht erreichbar sind. Der Status der Schnittstelle wird über einen Ping-Test überprüft. • *Lebensdauer eines Zertifikats*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist.
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*

Feld	Beschreibung
	Geben Sie den Wert der MIB-Variable ein.
Indexvariablen	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie bei Bedarf MIB-Variablen aus, die als "Index" verwendet werden sollen, um einen bestimmten Datensatz in **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** und **Indexwert** ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Überwachte Schnittstelle	Nur für **Ereignistyp** *Schnittstellenstatus* und *Schnittstellenverkehr* Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.
Schnittstellenstatus	Nur für **Ereignistyp** *Schnittstellenstatus* Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen. Mögliche Werte: • *Aktiv* (Standardwert): Die Schnittstelle ist aktiv. • *Inaktiv*: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen. Mögliche Werte: • *RX* (Standardwert): Der eingehende Datenverkehr wird überwacht. • *TX*: Der ausgehende Datenverkehr wird überwacht.
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 jeweili-

Feld	Beschreibung
	gen 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, die als "Index" verwendet werden sollen, um einen bestimmten Datensatz in **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** und **Indexwert** ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Überwachte Schnittstelle	Nur für **Ereignistyp** *Schnittstellenstatus* und *Schnittstellenverkehr* Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.
Schnittstellenstatus	Nur für **Ereignistyp** *Schnittstellenstatus* Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen. Mögliche Werte: • *Aktiv* (Standardwert): Die Schnittstelle ist aktiv. • *Inaktiv*: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen. Mögliche Werte: • *RX* (Standardwert): Der eingehende Datenverkehr wird über-

Feld	Beschreibung
	wacht. • *TX*: Der ausgehende Datenverkehr wird überwacht.
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 die noch verbleibende Gültigkeit des Zertifikats in Prozent aus.

Felder im Menü AuslöserZeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	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. • *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.

Feld	Beschreibung
	• *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.

20.7.2 Aktionen

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

20.7.2.1 Neu

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

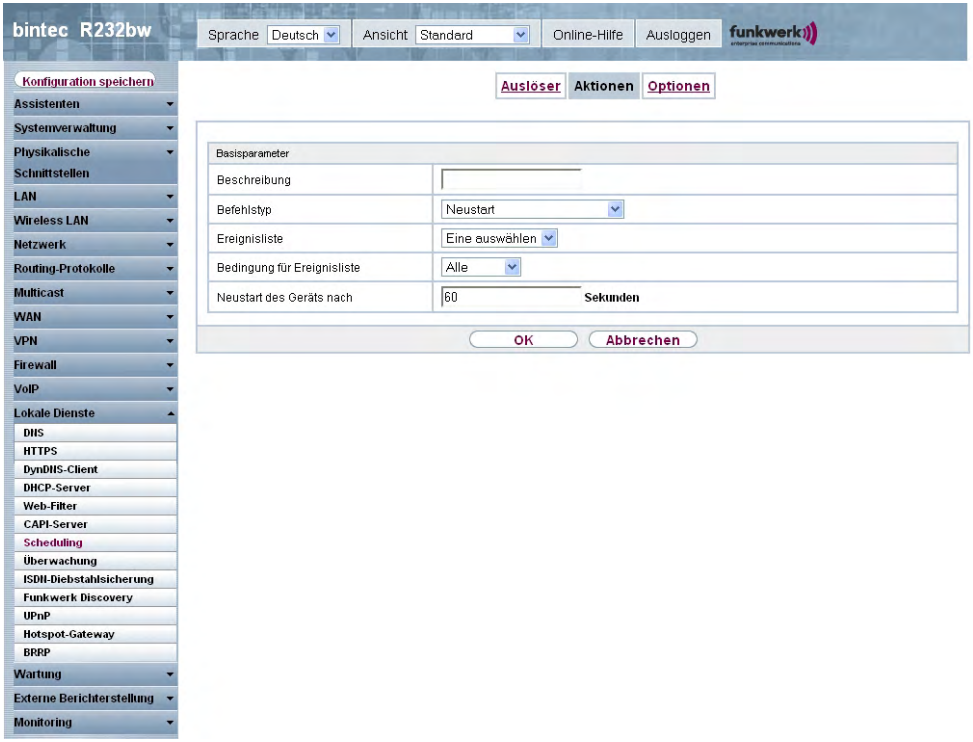


Abb. 134: **Lokale Dienste->Scheduling+Aktionen->Neu**

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

Felder im Menü AktionenBasisparameter

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. • *Softwareaktualisierung*: Es wird ein Software-Update initiiert. • *Konfigurationsmanagement*: Eine Konfigurationsdatei

Feld	Beschreibung
	wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • *Ping-Test*: Die Erreichbarkeit einer IP-Adresse wird überprüft. • *Zertifikatverwaltung*: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • *WLC: Neuer Neighbor-Scanvorgang*: In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • *WLC: VSS-Status*: Der Status eines Drahtlosnetzwerkes wird verändert.
Ereignisliste	Wählen Sie den in **Lokale Dienste**->**Scheduling**->**Auslöser**->**Ereignisliste** konfigurierten Index des Ereignisses oder der Ereignisskette aus.
Bedingung für Ereignisliste	Wählen Sie für Ereignislisten aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird. Mögliche Werte: • *all* (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • *one*: Die Aktion wird ausgelöst, wenn ein Ereigniss eintritt. • *none*: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • *one-not*: 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. Standardwert ist *60* Sekunden.
Hinzuzufügende/zu bearbeitende MIB/ SNMP-Variable	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das **System** aus und dann die **MIB-Tabelle**. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vor-

Feld	Beschreibung
	handen sind.
Befehlsmodus	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie aus, auf welche Weise der MIB-Eintrag verändert 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, die als "Index" verwendet werden sollen, um einen bestimmten Datensatz in **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** 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. • *Inactiv* : Der Wert der MIB-Variable wird verändert, wenn der Auslöser inaktiv ist. • *Beide*: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.
MIB-Variablen	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll. Ist der Auslöser aktiv (**Status des Auslösers** *Aktiv*), wird die MIB-Variable mit dem in **Aktiver Wert** eingetragenen Wert be-

Feld	Beschreibung
	schrieben. Ist der Auslöser inaktiv, **Status des Auslösers** *Inactiv*), wird die MIB-Variable mit dem in **Inaktive Variable** 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 **Inaktive Variable** 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*
Quelle	Nur bei **Befehlstyp** = *Softwareaktualisierung* Wählen Sie die gewünschte Quelle für die Software-Aktualisierung aus. Mögliche Werte: • *Aktuelle Software vom Funkwerk-Server* (Standardwert): Die aktuelle Software wird vom Funkwerk-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 HTTP-Server geladen, den Sie über die *Server-URL* festlegen.

Feld	Beschreibung
	• *TFTP-Server*: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die *Server-URL* festlegen.
Server-URL	Bei **Befehlstyp** = *Softwareaktualisierung* wenn **Quelle** nicht *Current Software from Funkwerk Server* Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* mit **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Geben Sie die URL des Servers ein, von dem eine Konfigurationsdatei geholt oder auf den die Konfigurationsdatei gesichert werden soll.
Dateiname	Bei **Befehlstyp** = *Softwareaktualisierung* Geben Sie den Dateinamen der Softwareversion ein. Bei **Befehlstyp** = *Zertifikatverwaltung* mit **Aktion** = *Zertifikat importieren* Geben Sie den Dateinamen der Zertifikatsdatei ein.
Aktion	Bei **Befehlstyp** = *Konfigurationsmanagement* Wählen Sie aus, welche Aktion Sie auf eine Konfigurationsdatei anwenden möchten. Mögliche Werte: • *Konfiguration importieren* (Standardwert) • *Konfiguration exportieren* • *Konfiguration umbenennen* • *Konfiguration löschen* • *Konfiguration kopieren* Bei **Befehlstyp** = *Zertifikatverwaltung* Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten.

Feld	Beschreibung
	Mögliche Werte: • *Zertifikat importieren* (Standardwert) • *Zertifikat löschen* • *SCEP*
Protokoll	Nur für **Befehlstyp** = *Zertifikatverwaltung* und *Konfigurationsmanagement* wenn **Aktion** = *Konfiguration importieren* Wählen Sie das Protokoll für die Dateiübertragung aus. Mögliche Werte: • *HTTP* (Standardwert) • *HTTPS* • *TFTP*
CSV-Dateiformat	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob die Datei im CSV-Format übertragen werden soll, welches problemlos gelesen und modifiziert werden kann. 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, auf den sie gespeichert werden soll, gespeichert werden soll.
Lokaler Dateiname	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren*, *Konfiguration*

Feld	Beschreibung
	umbenennen oder *Konfiguration kopieren* Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.
Dateiname in Flash	Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration exportieren* Wählen Sie die Datei aus, die exportiert werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration umbenennen* Wählen Sie die Datei aus, die umbenannt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration löschen* Wählen Sie die Datei aus, die gelöscht werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration kopieren* Wählen Sie die Datei aus, die kopiert werden soll.
Konfiguration enthält Zertifikate/Schlüssel	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen. Standardmäßig ist die Funktion nicht aktiv.
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*

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

Feld	Beschreibung
	Standardwert ist *3*.
Serveradresse	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.
Lokale Zertifikatsbeschreibung	Bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll. Bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat löschen* Wählen Sie das Zertifikat aus, das gelöscht werden soll.
Kennwort für geschütztes Zertifikat	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie ein geschütztes Zertifikat verwenden möchten, das ein Passwort benötigt, und geben Sie dieses in das Eingabefeld ein. Standardmäßig ist die Funktion nicht aktiv.
Ähnliches Zertifikat überschreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie ein auf Ihrem Gerät schon vorhandenes Zertifikat mit dem neuen überschreiben wollen. Standardmäßig ist die Funktion nicht aktiv.
Zertifikat in Konfiguration schreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
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.funkwerk.de:8080/scep/scep.dll* Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Subjektname	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie einen Subjektnamen mit Attributen ein. Beispiel: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA-Name	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows* . Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Passwort	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein 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*.

Feld	Beschreibung
Autospeichermodus	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert. Standardmäßig ist die Funktion aktiv.
CRL verwenden	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Werte: • *Auto* (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatsperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden. • *Ja*: CRLs werden grundsätzlich uberprüft. • *Nein*: Keine Überprüfung von CRLs.
WLC-SSID	Nur bei **Befehlstyp** = *WLC: VSS-Status* Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.
Status festlegen	Nur bei **Befehlstyp** = *WLC: VSS-Status* Wählen Sie den Status aus, in den das ausgewählte Drahtlosnetzwerk versetzt werden soll. Mögliche Werte: • *Aktivieren* (Standardwert) • *Deaktivieren*

20.7.3 Optionen

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

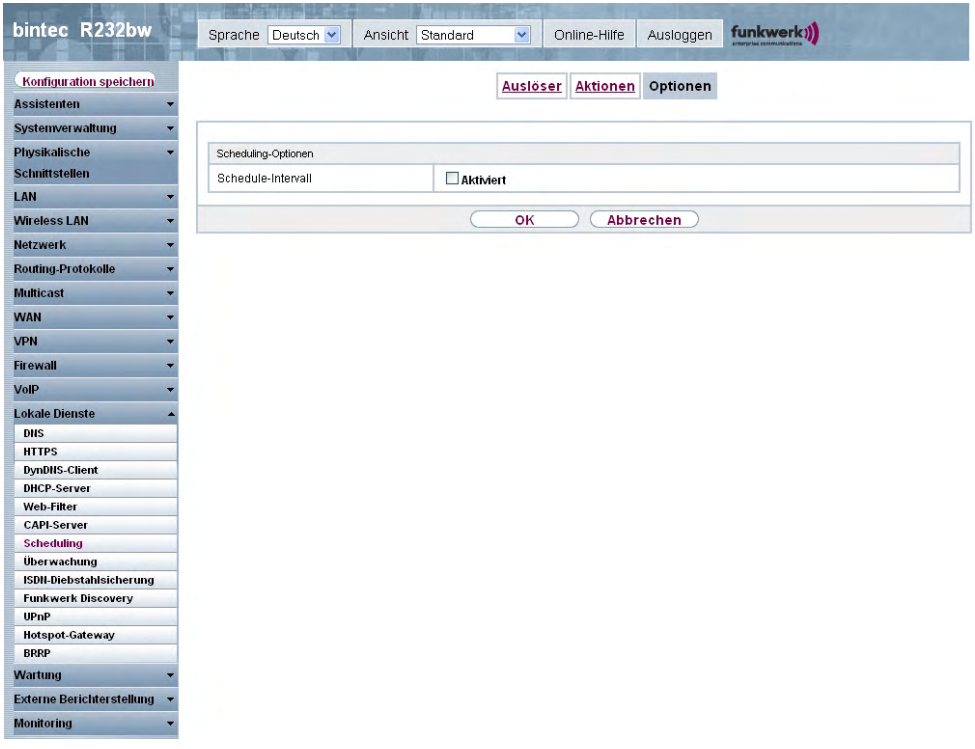


Abb. 135: **Lokale Dienste->Scheduling->Optionen**

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

Felder im Menü OptionenScheduling-Optionen

Feld	Beschreibung
Schedule-Intervall	Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll. Geben Sie das Intervall in Sekunden ein, in dem das System überprüft, ob geplante Aufgaben anstehen. Möglich sind Werte zwischen `0` und `65535`. Empfohlen wird der Wert `300` (5 Minuten Genauigkeit). Werte kleiner als 60 haben in der Regel keinen Sinn und benötigen

Feld	Beschreibung
	unnötig Systemressourcen.

20.8 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

20.8.1 Hosts

Im Menü **Lokale Dienste**->**Überwachung**->**Hosts** wird eine Liste aller überwachten Hosts angezeigt.

20.8.1.1 Bearbeiten oder Neu

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

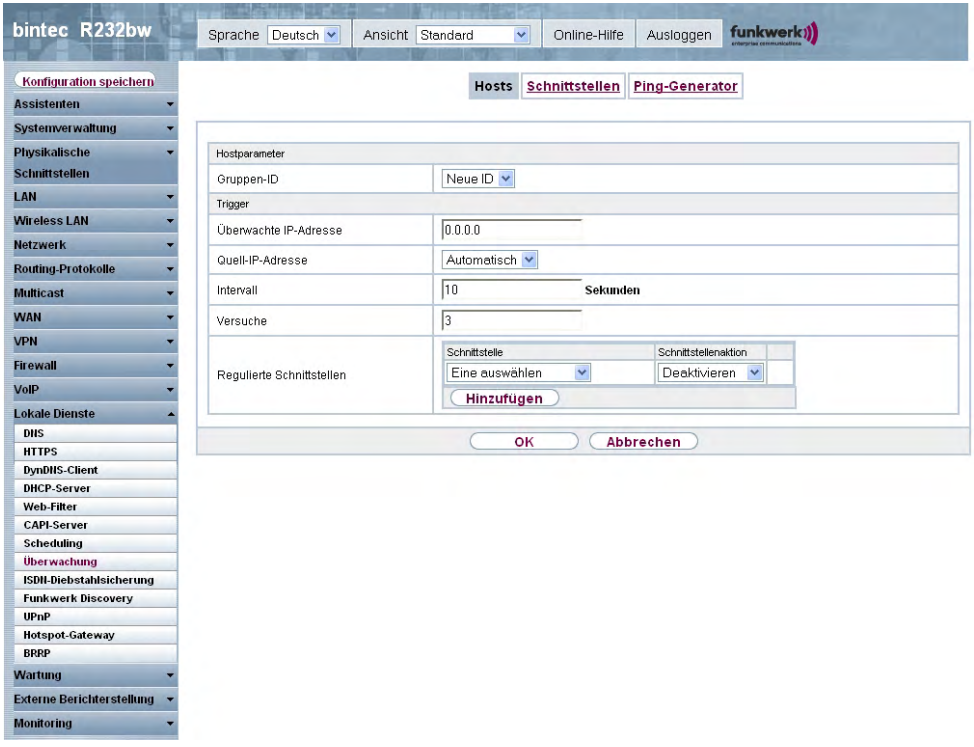


Abb. 136: **Lokale Dienste->Überwachung->Hosts->Neu**

Das Menü **Lokale Dienste->Überwachung->Hosts->Neu** besteht aus folgenden Feldern:

Feld im Menü HostsHostparameter

Feld	Beschreibung
Gruppen-ID	Wählen Sie eine ID für die Gruppe von Hosts aus, deren Erreichbarkeit von Ihrem Gerät überwacht werden soll. Die Gruppen-IDs werden automatisch von `0` bis `255` angelegt. Ist noch kein Eintrag angelegt, wird durch die Option `Neue ID` eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen. Jeder zu überwachende Host muss einer Gruppe zugeordnet werden. Die in **Schnittstellenaktion** konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied mehr erreichbar ist.

Felder im Menü HostsTrigger

Feld	Beschreibung
Überwachte IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.
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*. Standardwert ist *10* . Innerhalb einer Gruppe wird das kleinste **Intervall** der Gruppenmitglieder verwendet.
Versuche	Geben Sie die Anzahl der Pings ein, die unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Mögliche Werte sind *1* bis *65536*. Standardwert ist *3* .
Regulierte Schnittstellen	Wählen Sie aus, für welche Schnittstelle(n) die unter **Schnittstellenaktion** festgelegte Aktion ausgeführt werden soll. Auswählbar sind alle physikalischen und virtuellen Schnittstellen. Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (*Aktivieren*), deaktiviert (*Deaktivieren*, Standardwert), zurückgesetzt (*Zurücksetzen*) oder die Verbindung erneut aufgebaut (*Erneut wählen*) werden soll(en).

20.8.2 Schnittstellen

Im Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

20.8.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

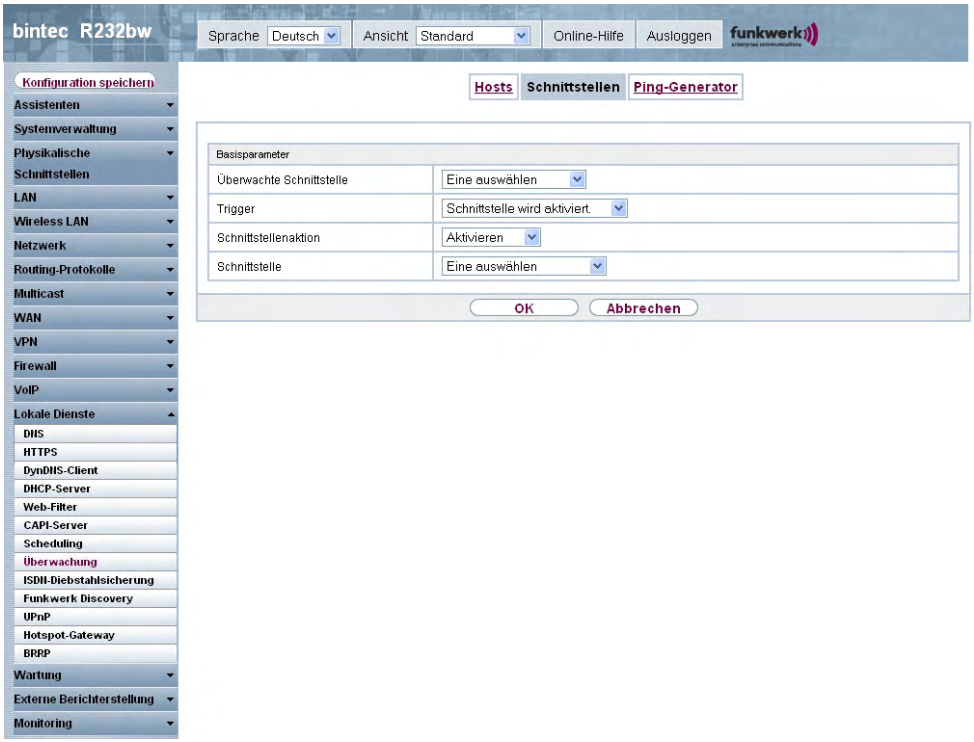


Abb. 137: **Lokale Dienste**->**Überwachung**->**Schnittstellen**->**Neu**

Das Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü SchnittstelleBasisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.

Feld	Beschreibung
Trigger	Wählen Sie den Status bzw. Statusübergang von **Überwachte Schnittstelle** aus, der eine bestimmte **Schnittstellenaktion** auslösen soll. Mögliche Werte: • *Schnittstelle wird aktiviert.* (Standardwert) • *Schnittstelle wird deaktiviert.*
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in **Trigger** definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in **Schnittstelle** ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: • *Aktivieren* (Standardwert): Aktivierung der Schnittstelle(n) • *Deaktivieren* : Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter **Schnittstelle** festgelegte Aktion ausgeführt werden soll. Auswählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen *Alle PPP-Schnittstellen* und *Alle IPSec-Schnittstellen* .

20.8.3 Ping-Generator

Im Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator** wird eine Liste aller konfigurierter Pings angezeigt, die automatisch generiert werden.

20.8.3.1 Bearbeiten oder Neu

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

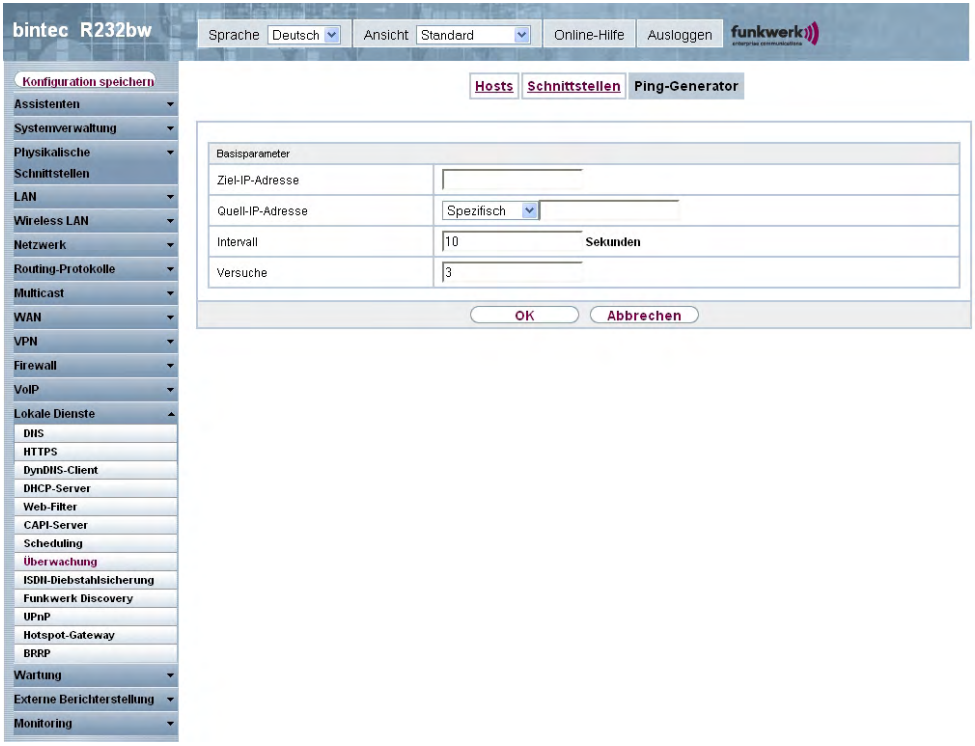


Abb. 138: **Lokale Dienste->Überwachung->Ping-Generator->Neu**

Das Menü **Lokale Dienste->Überwachung->Ping-Generator->Neu** besteht aus folgenden Feldern:

Felder im Menü Ping-GeneratorBasisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. Mögliche Werte: • *Automatisch* : Die IP-Adresse wird automatisch ermittelt. • *Spezifisch*(Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der

Feld	Beschreibung
	Ping an die in **Entfernte IP-Adresse** angegebene Adresse abgesetzt werden soll. Mögliche Werte sind *1* bis *65536*. Standardwert ist *10* .
Versuche	Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis **Ziel-IP-Adresse** als *Nicht erreichbar* gilt. Standardwert ist *3* .

20.9 ISDN-Diebstahlsicherung

Mit der Funktion ISDN-Diebstahlsicherung können Sie verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn unter **WAN**->**Internet + Einwählen**->**ISDN**->  das Feld **Immer aktiv**aktiviert ist.)

20.9.1 Optionen

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet, und die Schnittstellen werden administrativ auf "up" gesetzt.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.

Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

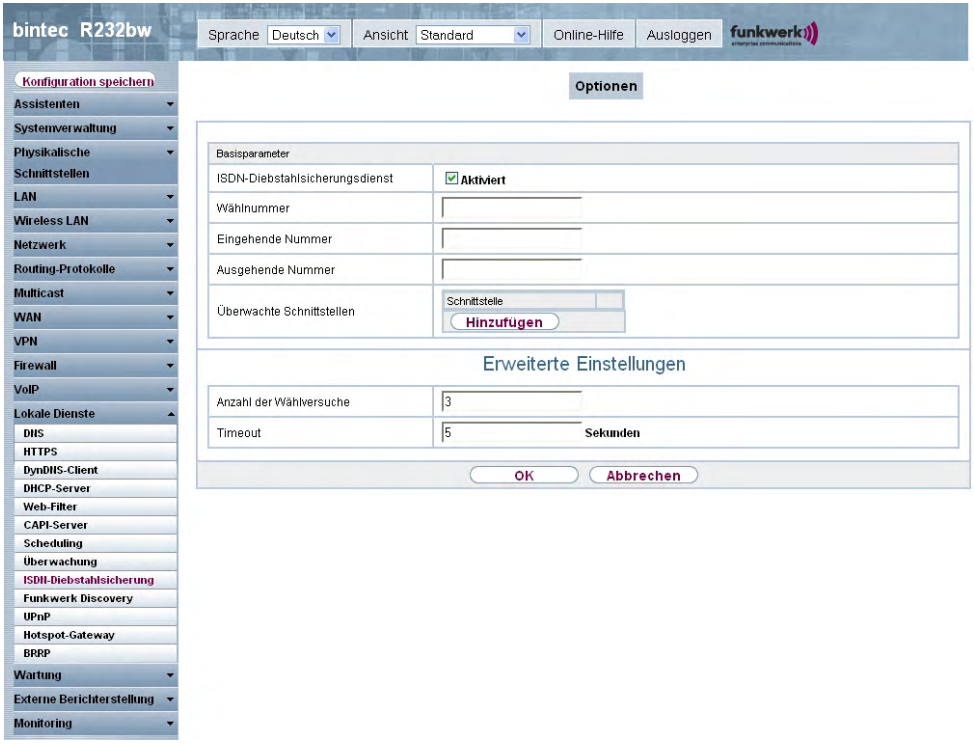


Abb. 139: **Lokale Dienste->ISDN-Diebstahlsicherung->Optionen**

Das Menü **Lokale Dienste->ISDN-Diebstahlsicherung->Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

Feld	Beschreibung
ISDN-Diebstahlsicherungs-dienst	Aktivieren oder deaktivieren Sie die Funktion ISDN-Diebstahlsicherung. Mit `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Wählnummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die das Gateway wählt, wenn es sich selbst anruft.
Eingehende Nummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die mit der aktuellen Calling

Feld	Beschreibung
	Party Number verglichen werden soll.
Ausgehende Nummer	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Geben Sie die Rufnummer ein, die als Calling Party Number gesetzt wird.
Überwachte Schnittstellen	Nur wenn **ISDN-Diebstahlsicherungsdienst** aktiviert ist. Fügen Sie mit **Hinzufügen** eine neue Schnittstelle hinzu. Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, auf welche die Funktion ISDN-Diebstahlsicherung angewendet werden soll.

Felder im Menü OptionenErweiterte Einstellungen

Feld	Beschreibung
Anzahl der Wählversuche	Geben Sie die Anzahl der Wählversuche ein, die das Gateway unternehmen soll, um sich nach einem Neustart über ISDN selbst anzurufen. Mögliche Werte sind *1* bis *255*. Standardwert ist *3*.
Timeout	Geben Sie die Zeitspanne ein, die das Gateway warten soll, bis es sich nach einem erfolglosen Versuch erneut selbst anruft. Mögliche Werte sind *2* bis *20*. Standardwert ist *5*.

20.10 Funkwerk Discovery

20.10.1 Gerätesuche

Das funkwerk Discovery Protokoll dient zur Erkennung und Konfiguration von **bintec** Geräten, die sich im gleichen kabelgebundenen Netz befinden wie Ihr Gerät. Nachdem ein **bintec** Gerät erkannt wurde, können bestimmte Basisparameter (Knotenname, IP-Adresse, Netzmaske und Geräte-Adresse) konfiguriert werden (vorausgesetzt Sie kennen das Administratorpasswort).

Hinweis

Eventuell vorhandene **bintec** Geräte werden mittels eines Multicasts ermittelt. Daher ist es unerheblich ob und welche IP-Adresse das Gerät hat.

Beachten Sie, dass erkannte **bintec** Geräte nicht im Flash gespeichert werden, d. h. die Erkennung muss nach einem Neustart Ihres Geräts wiederholt werden.

Im Menü **Lokale Dienste**->**Funkwerk Discovery**->**Gerätesuche** wird unter **Ergebnisse** eine Liste aller erkannten Access-Points im Netzwerk angezeigt. Im Feld **Schnittstelle** wählen Sie die Schnittstelle Ihres Geräts aus, über das die Access-Point Erkennung durchgeführt werden soll. Mit der Option *-Alle-* werden alle Schnittstellen abgefragt.

Unter Ermittlungsstatus wird der aktuelle Erkennungsstatus für jede einzelne Schnittstelle angezeigt. Hierbei bedeutet *Keiner*, dass keine Erkennung aktiv ist. *Suchen* wird angezeigt, wenn aktuell eine Erkennung durchgeführt wird.

Ihr Gerät kann über diese Erkennungsfunktion ebenfalls von anderen Access Points mit Discovery-Funktion erkannt und konfiguriert werden. Dieses konfigurieren Sie im Untermenü **Optionen**.

20.10.1.1 Finden

Wählen Sie die Schaltfläche **Finden**, um die Access-Point-Erkennung zu starten.

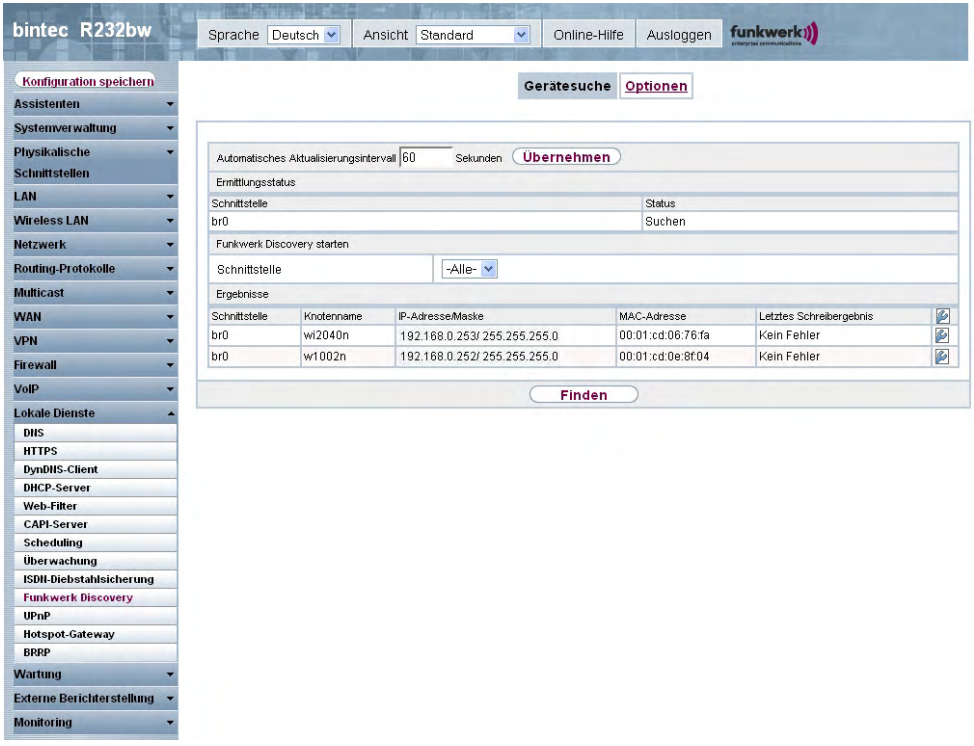


Abb. 140: **Lokale Dienste->Funkwerk Discovery->Gerätesuche**

Wurden Access-Points im Netzwerk erkannt, erscheinen diese in der Liste. Über die -Schaltfläche gelangen Sie in das Konfigurationsmenü für den jeweiligen Access-Point.

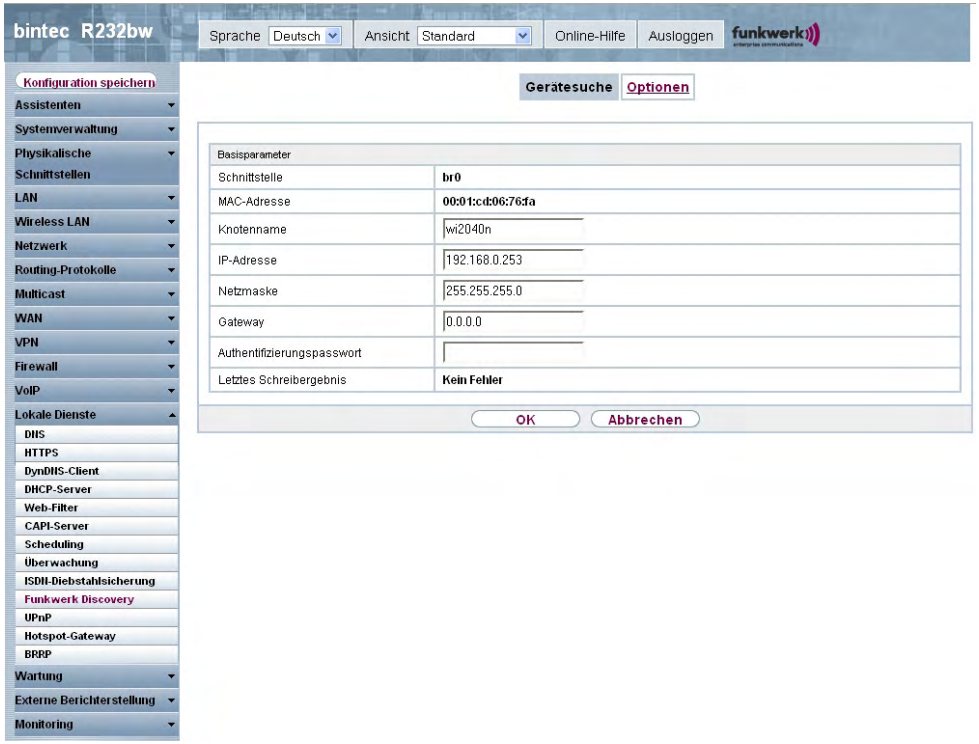


Abb. 141: **Lokale Dienste->Funkwerk Discovery->Gerätesuche->**

Das Menü **Lokale Dienste->Funkwerk Discovery->Gerätesuche->** besteht aus folgenden Feldern:

Felder im Menü GerätesucheBasisparameter

Feld	Beschreibung
Schnittstelle	Der Wert dieses Feldes kann nur gelesen werden. Zeigt die Schnittstelle Ihres Geräts an, an welchem die Erkennung durchgeführt wird.
MAC-Adresse	Der Wert dieses Feldes kann nur gelesen werden. Zeigt die MAC-Adresse des erkannten Access-Points an.
Knotenname	Sie können den Namen des erkannten Access-Points ändern.
IP-Adresse	Sie können die IP-Adresse des erkannten Access-Points ändern.

Feld	Beschreibung
Netzmaske	Sie können die dazugehörige Netzmaske ändern.
Gateway	Sie können die Gateway-Adresse des erkannten Access-Points ändern.
Authentifizierungs-passwort	Geben Sie das Administrator-Passwort des Access-Points ein. Ohne Passwort kann die Einstell-Operation nicht durchgeführt werden.
Letztes Schreibergebnis	Der Wert dieses Feldes kann nur gelesen werden. Zeigt das Ergebnis der letzten Einstell-Operation an. Mögliche Werte sind: • *Kein Fehler*: Der Access-Point hat eine erfolgreiche Operation gemeldet oder es ist noch keine Konfigurationsänderung mit **OK** durchgeführt worden. • *Timeout*: Der Access-Point hat nicht geantwortet. • *Zugriff verweigert*: Der Access-Point hat einen Autorisierungsfehler gemeldet. Bitte überprüfen Sie das Authentifizierungspasswort. • *Ungültige IP-Parameter*: Es besteht ein Problem mit den vorgesehenen IP-Parametern (IP-Adresse, Netzmaske oder Gateway-Adresse). • *Destination Unreachable*: Der Access-Point kann aus internen Gründen nicht erreicht werden (z. B. die Schnittstelle, an die der Access-Point angeschlossen ist, ist außer Betrieb). Zum Access-Point kann keine Einstellanforderung gesandt werden. • *Anderer Fehler*: Der Access-Point antwortet auf die Einstellanforderung mit einem unerwarteten oder unspezifischen Fehler. • *Interner Fehler*: Ein internes Problem Ihres Geräts hat die Einstelloperation verhindert.

20.10.2 Optionen

In diesem Menü können Sie die Erlaubnis erteilen, dass auch Ihr Gerät von anderen **bintec**-Geräten mittels funkwerk Discovery Protokoll gefunden und über dieses konfiguriert werden kann.

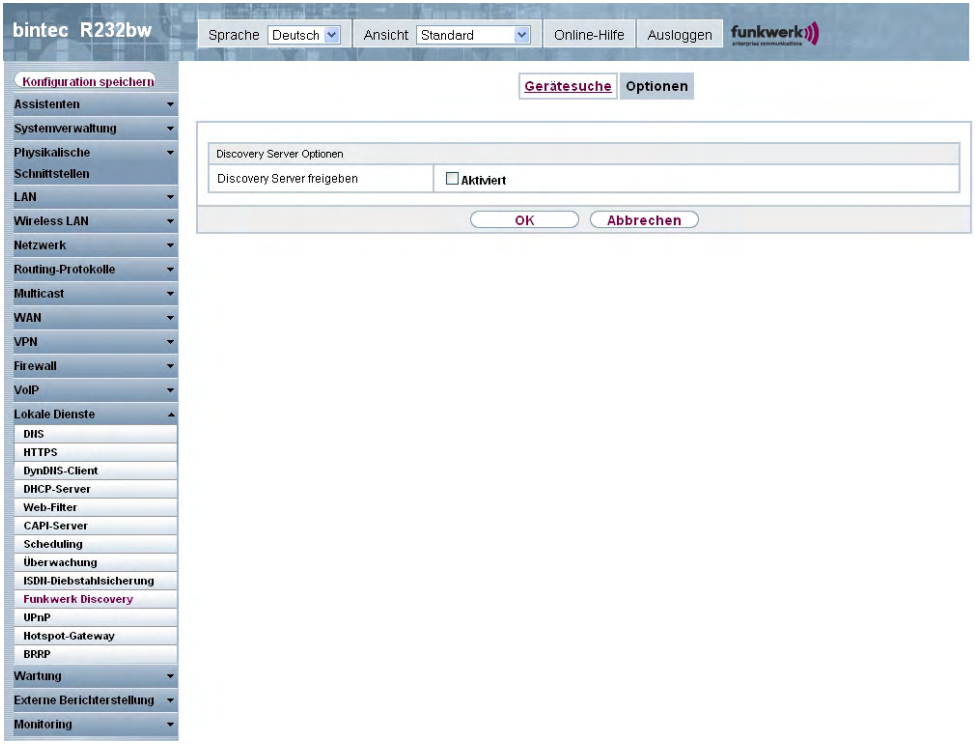


Abb. 142: **Lokale Dienste->Funkwerk Discovery->Optionen**

Das Menü **Lokale Dienste->Funkwerk Discovery->Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenDiscovery Server Optionen

Feld	Beschreibung
Discovery Server freigeben	Wählen Sie aus, ob Ihr Gerät im Netzwerk von anderen **bintec**-Geräten erkannt und konfiguriert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

20.11 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist `5678`. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch zugewesenen Ports liegen im Bereich von `5004` bis `65535`. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf *www.upnp.org* .

20.11.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

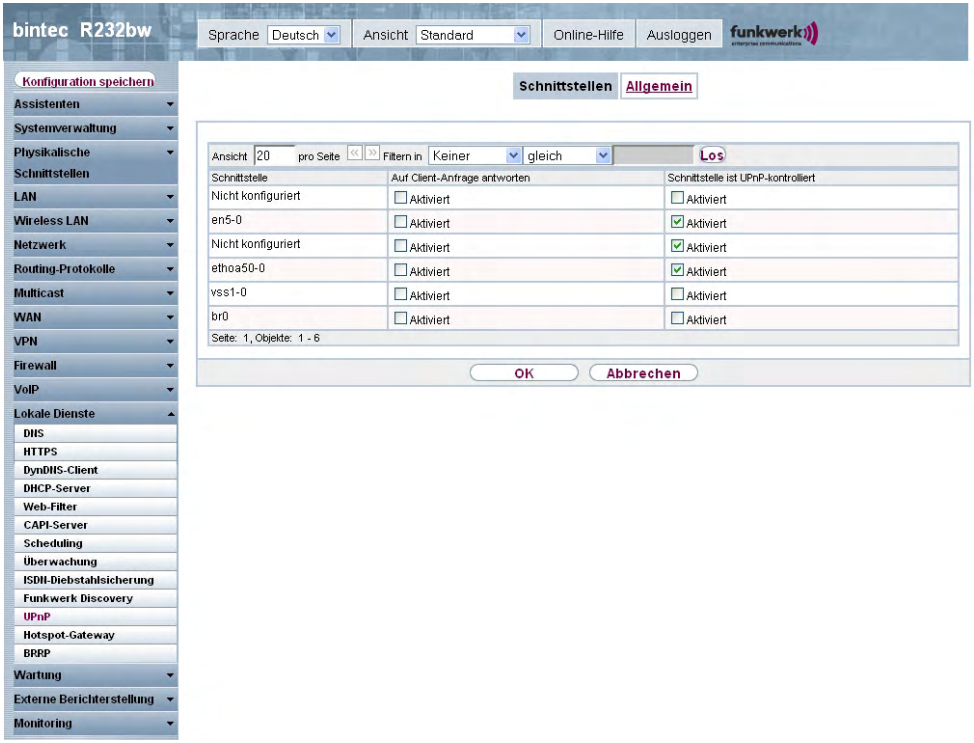


Abb. 143: **Lokale Dienste->UPnP->Schnittstellen**

Das Menü **Lokale Dienste->UPnP->Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der Schnittstelle an, für welche die UPnP-Einstellungen vorgenommen werden. Der Eintrag kann nicht verändert werden.
Auf Client-Anfrage antworten	Legen Sie fest, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle (aus dem lokalen Netzwerk) beantwortet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird.

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

20.11.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

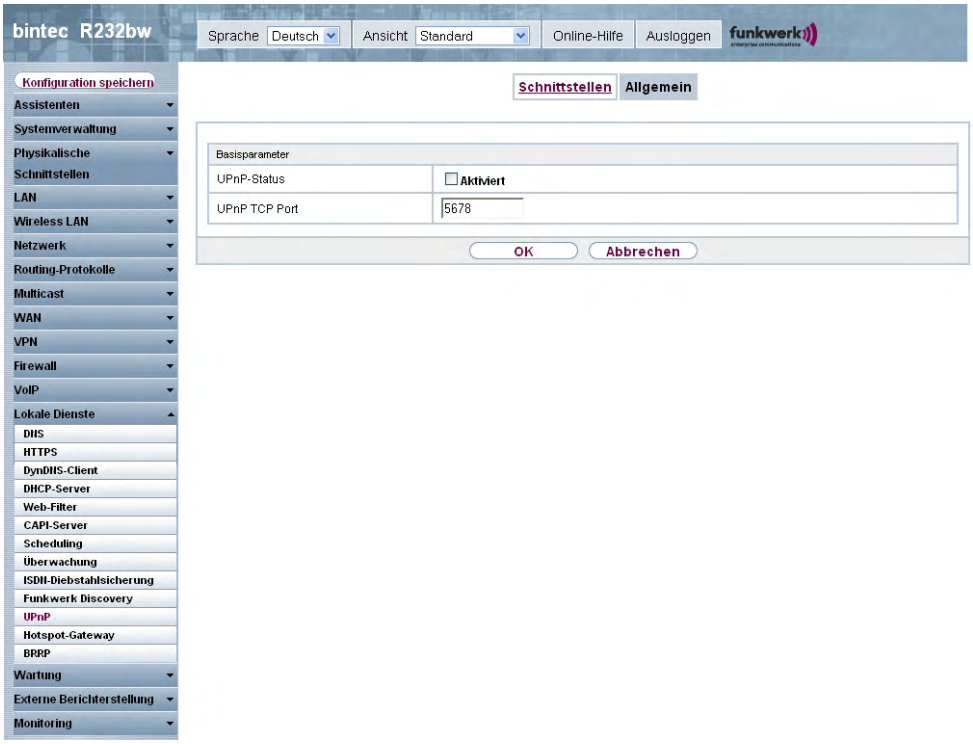


Abb. 144: **Lokale Dienste->UPnP+Allgemein**

Das Menü **Lokale Dienste->UPnP+Allgemein** besteht aus folgenden Feldern:

Felder im Menü Allgemein

Feld	Beschreibung
UPnP-Status	Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt. Mit *Aktiviert* wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Cli-

Feld	Beschreibung
	ents beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients. Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.
UPnP TCP Port	Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht. Mögliche Werte sind *1* bis *65535*, der Standardwert ist *5678*.

20.12 Hotspot-Gateway

Die **bintec 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 **bintec Hotspot Solution** besteht aus einem vor Ort installierten bintec 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 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 Hotspot Hosting (Artikelnummer 5510000198)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

  Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

  - Gehen Sie auf *www.funkwerk-ec.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 Funkwerk Enterprise Communications 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.funkwerk-ec.com/
Username	Wird durch FEC individuell festgelegt
Password	Wird durch FEC individuell festgelegt

Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf *www.funkwerk-ec.com* zum Download zur Verfügung steht.

20.12.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec Gateway für die **bintec Hotspot Solution**.

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller konfigurierter Hotspot Netzwerke angezeigt.

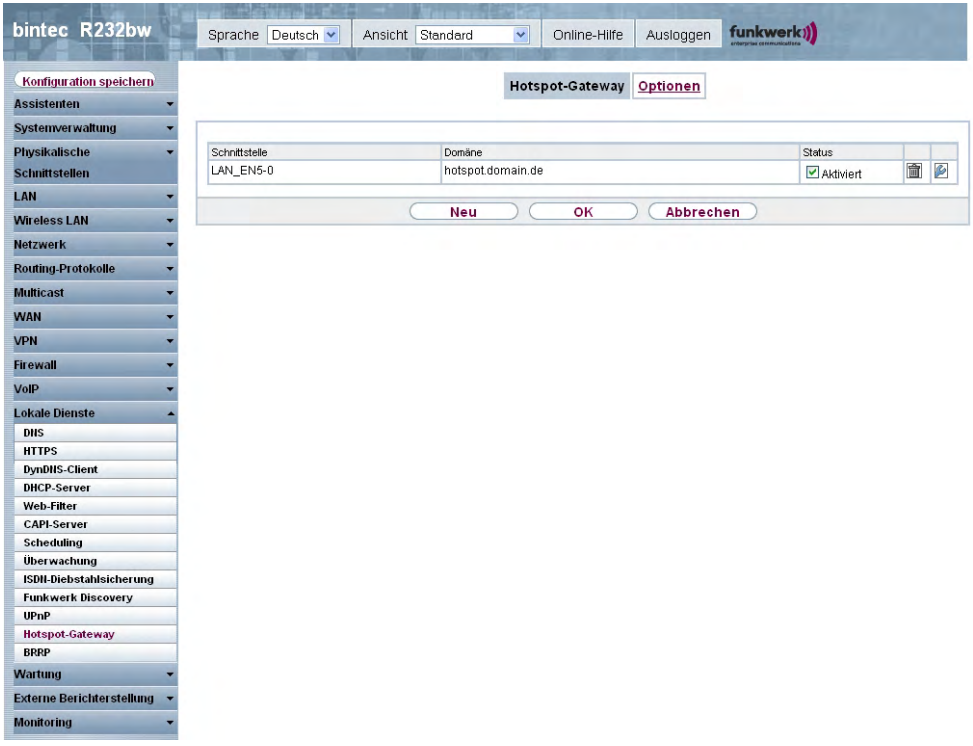


Abb. 145: **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway**

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktieren.

20.12.1.1 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.

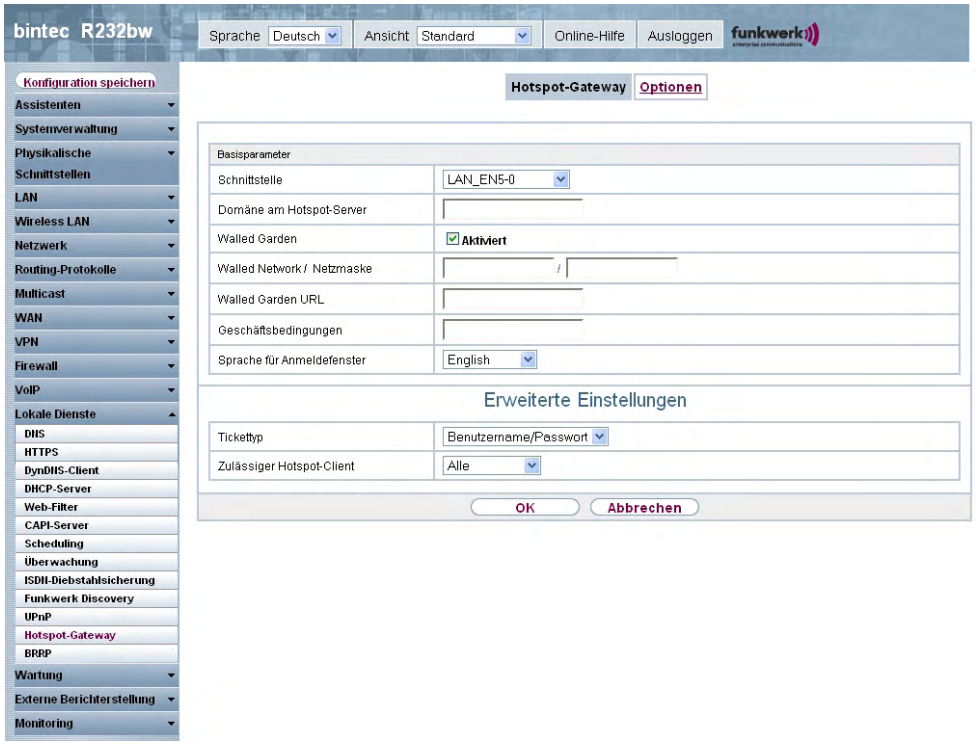


Abb. 146: **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->**

Das Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->** besteht aus folgenden Feldern:

Felder im Menü Hotspot-GatewayBasisparameter

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. **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!

Feld	Beschreibung
	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 IPAdressen 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 IPAdresse 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.
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.

Feld	Beschreibung
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. Mögliche Werte: • *Alle*: Alle Clients werden zugelassen. • *DHCP-Client*: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.

20.12.1.2 Optionen

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

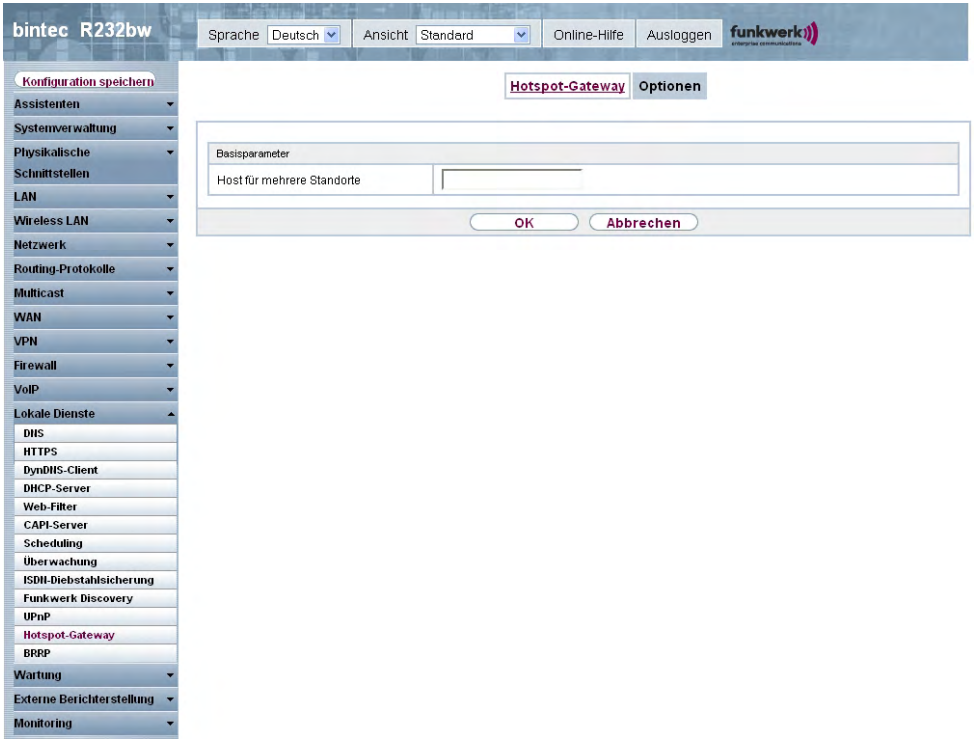


Abb. 147: **Lokale Dienste->Hotspot-Gateway->Optionen**

Das Menü **Lokale Dienste->Hotspot-Gateway->Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

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.

20.13 BRRP

Im Menü **BRRP** können Sie eine Redundanz für Ihr Gateway konfigurieren.

Hinweis

Für Geräte der R23x-Serie und der RS-Serie benötigen Sie eine Lizenz.

BRRP (Bintec Router Redundancy Protocol) ist eine bintec-spezifische Implementierung des VRRP (Virtual Router Redundancy Protocol). Ein Router-Redundanzverfahren dient hauptsächlich dazu, die Verfügbarkeit eines physikalischen Gateways im LAN oder WAN sicherzustellen.

Begriffe und Definitionen

Zur Beschreibung der Funktionalität werden einige spezielle Begriffe verwendet. Folgende Begriffe werden im entsprechenden RFC und im Internet-Entwurf definiert.

BRRP Begriffe

Feld	Beschreibung
VRRP-Router	"Ein Router, der das Virtual Router Redundancy Protocol benutzt. Er kann in einen oder in mehrere "virtuelle Router" integriert sein."
Virtueller Router	"Ein abstraktes, von VRRP gesteuertes Objekt, das als Standard-Router für Hosts eines LAN verwendet wird. Es besteht aus einem Virtual Router Identifier (**ID des virtuellen Routers**) und einer IP-Adresse bzw. einer Gruppe zugehöriger IP-Adressen innerhalb eines gemeinsamen LAN. Ein VRRP-Router kann den Datenverkehr eines einzelnen virtuellen Routers oder mehrerer virtueller Router absichern."
IP Address Owner	"Der VRRP-Router, der die IP-Adresse(n) des virtuellen Routers als echte Schnittstellen- Adresse(n) besitzt. Es handelt sich um den Router, der, wenn er aktiv ist, auf Pakete für ICMP-Pings, TCP-Verbindungen etc. an eine dieser IP-Adressen antwortet."
Primary IP Address	"Eine IP-Adresse, die aus der Gruppe der echten Schnittstellenadressen gewählt wird. Eine mögliche Algorithmusoption ist die Auswahl der ersten Adresse. VRRP Advertisements werden immer mit der Primary IP-Adresse als Quelle des IP-Pakets verschickt."
VRRP Advertisement	Ein Keepalive, das der Master zu den Backup-Gateways schickt, um seine Erreichbarkeit zu signalisieren.
Virtual Router Master	"Der VRRP-Router, der das Weiterleiten der Pakete übernimmt, die an die mit dem "virtuellen Router" verbundenen IP-Adressen geschickt wurden, und der für die Beantwortung von ARP (Address Resolution Protocol) Requests an diese IP-Adressen zuständig ist."

Feld	Beschreibung
Virtual Router Backup	"Die Gruppe der VRRP-Router, welche die Verantwortung für das Weiterleiten übernehmen, falls der Master ausfallen sollte." Im Backup-Status sind diese VRRP-Router inaktiv, d.h. beantworten keine ARP-Requests."

20.13.1 Virtuelle Router

Bei der Verwendung eines Router-Redundanzprotokolls werden mehrere Router zu einer logischen Einheit zusammengefasst. Das Router-Redundanzprotokoll BRRP verwaltet die beteiligten Router und organisiert im einzelnen Folgendes:

Es stellt sicher, dass jeweils nur ein Router innerhalb des logischen Verbunds aktiv ist.

Es gewährleistet, dass bei Ausfall des aktiven Routers ein anderer Router die Funktion des ausgefallenen Geräts übernimmt. Wann welcher Router aktiv ist, wird über eine dem Router zugeordnete Priorität bestimmt.

Nehmen wir als Beispiel ein einfaches Szenario, in dem Gateway A den Internetzugang der Hosts in einem LAN ermöglicht. Wenn dieses Gateway ausfällt, haben alle Hosts keinen Zugang zum Internet, deren Routen statisch konfiguriert sind. Um den Hosts weiterhin Zugang zum Internet zu ermöglichen, bietet Gateway B allen Hosts im LAN den Dienst an, den vorher Gateway A durchgeführt hat. Alle Aufgaben eines virtuellen Routers und das Umschalten von Diensten von einem Gateway auf das andere werden von dem BRRP-Redundanzprotokoll gesteuert.

Das BRRP folgt den Spezifikationen in RFC 2338 und dem entsprechenden Internet- Entwurf (siehe *www.ietf.org*).

Die Konfiguration des Router-Redundanzverfahrens wird in folgenden Schritten durchgeführt:

- Konfiguration der Schnittstelle, über welche die BRRP-Advertisement-Datenpakete geschickt werden.

Hinweis

Diese Schnittstelle wird zur Übertragung der BRRP-Advertisement-Datenpakete sowie eventuell zur Übertragung von Keepalive-Monitoring-Datenpaketen verwendet. Zur Übertragung der Nutzdaten muss eine andere Schnittstelle im nächsten Schritt konfiguriert werden.

Die Konfiguration der Advertisement-Schnittstelle wird im Menü **Lokale Dienste**->**BRRP**-

>**Virtueller Router**->**Neu**->**BRRP Advertisement-Schnittstelle** vorgenommen.

Nur der aktive Router des Routerverbunds sendet Advertisement-Datenpakete. Die IPv4-Multicast-Adresse 224.0.0.18 dient als Zieladresse für alle Router, die Bestandteil des Routerverbundes sind. Alle passiven Router des Verbundes müssen diese Adresse überwachen, damit sie bei Ausbleiben der Advertisement-Datenpakete entsprechend ihrer Priorität und der sonstigen BRRP-Konfiguration reagieren können.

- Konfiguration der Schnittstelle zur Übertragung von Nutzdaten (Konfiguration der virtuellen Schnittstelle).

  Eine virtuelle Schnittstelle wird über die Zuweisung zu einem virtuellen Router über das BRRP-Router-Redundanzprotokoll aktiviert bzw. deaktiviert.

  Die Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu**->**Ethernet-Schnittstelle** vorgenommen.

  In diesem Schritt konfigurieren Sie die IP-Adresseinstellungen und ordnen die Schnittstelle einem virtuellen Router zu. Darüber hinaus werden die Eigenschaften des virtuellen Routers (z. B. die Priorität) festgelegt.

Hinweis

Das System vergibt die MAC-Adresse der virtuellen Schnittstelle nach folgendem Schema automatisch: 00:00:5E:00:01:<ID des virtuellen Routers>. Die ID des virtuellen Routers bestimmt somit die MAC-Adresse der Schnittstelle, die zur Übertragung der Nutzdaten verwendet wird.

Die Konfiguration der virtuellen Schnittstelle (MAC-Adresse, IP-Adresse) sowie die Konfiguration des virtuellen Routers (Sendeintervall für Advertisements, Master down trials) muss innerhalb des logischen Verbundes auf allen Routern mit derselben Virtual Router ID identisch sein.

Sie müssen IP-Adressen aus unterschiedlichen Subnetzen für die Advertisement-Schnittstelle und für die virtuelle Schnittstelle verwenden.

Alle virtuellen Schnittstellen auf einem physikalischen Router sollten normalerweise dieselbe Priorität haben.

- Konfiguration der Synchronisation zwischen den virtuellen Routern, sowie Konfiguration der Ereignisse, die zu einem Umschalten des Betriebszustandes der virtuellen Router führen.

  Über die Steuerung des Betriebszustandes eines virtuellen Routers wird implizit auch der Betriebszustand der Schnittstelle gesteuert, die mit dem virtuellen Router verknüpft ist. Da im Fehlerfall alle Schnittstellen eines Geräts deaktiviert werden müssen, muss der

Betriebszustand aller Schnittstellen eines Geräts synchronisiert werden. Die Synchronisation ist notwendig, wenn mehrere Schnittstellen auf einem Gerät überwacht werden. Diese Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**VR-Synchronisation**->**Neu** vorgenommen.

- Einschalten des Redundanzverfahrens. Diese Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**Optionen** vorgenommen.

Im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu** konfigurieren Sie die Advertisement-Schnittstelle und die virtuelle(n) Schnittstelle(n). Sie müssen auf allen physikalischen Routern, die am Redundanzverfahren teilnehmen, dieselben virtuellen Router mit denselben Schnittstellen konfigurieren. (Die virtuellen Router haben jedoch auf den verschiedenen physikalischen Routern unterschiedliche Priorität.)

20.13.1.1 Neu

Wählen Sie die Schaltfläche **Neu** um weitere Virtuelle Router zu konfigurieren.

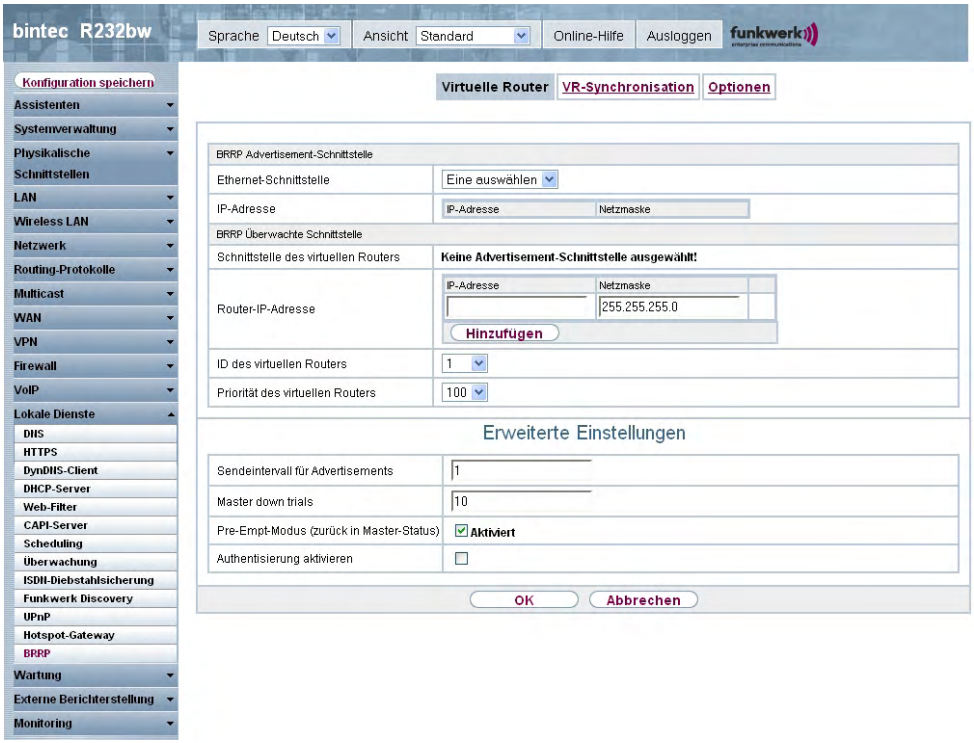


Abb. 148: **Lokale Dienste**->**BRRP**->**Virtuelle Router**->**Neu**

Das Menü **Lokale Dienste**->**BRRP**->**Virtuelle Router**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Virtuelle RouterBRRP Advertisement-Schnittstelle

Feld	Beschreibung
Ethernet-Schnittstelle	Wählen Sie die Schnittstelle aus, über die BRRP-Advertisement-Pakete versendet und erwartet werden. Wenn Sie einen virtuellen Router bearbeiten, wird die Ethernet-Schnittstelle angezeigt und kann nicht verändert werden. Hinweis: Die Ethernet-Schnittstelle zur Versendung der Advertisements ist immer up and running und kann daher nicht als **Schnittstelle des virtuellen Routers** verwendet werden.
IP-Adresse	Zeigt die IP-Adresse(n) der Schnittstelle an, über die BRRP-Advertisement-Pakete versendet und erwartet werden.

Felder im Menü Virtuelle RouterBRRP Überwachte Schnittstelle

Feld	Beschreibung
Schnittstelle des virtuellen Routers	Zeigt an, auf welcher physikalischen Schnittstelle die virtuelle Schnittstelle basiert, wenn eine neue virtuelle Schnittstelle angelegt wird. Die Bezeichnung der virtuellen Schnittstelle wird beim Anlegen automatisch vergeben. Zeigt die Bezeichnung der virtuellen Schnittstelle an, wenn eine bereits angelegte virtuelle Schnittstelle bearbeitet wird.
Router-IP-Adresse	Geben Sie die IP-Adresse und die Netzmaske des virtuellen Routers ein. Hier geben Sie die IP-Adresse ein, die Sie im lokalen Netz als eigentliche Gateway-IP-Adresse verwenden wollen.  **Hinweis** Um Probleme im LAN zu vermeiden, dürfen die **IP-Adresse** für Advertisements und die **Router-IP-Adresse** nicht aus demselben Subnetz stammen.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers. Diese ID identifiziert den "virtuellen Router" innerhalb des LAN und ist Bestandteil jedes BRRP-Advertisement-Pakets, das vom aktuellen Master gesendet wird. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*.

Feld	Beschreibung
Priorität des virtuellen Routers	Legen Sie die logische Priorität des virtuellen Routers fest. Die möglichen Werte liegen zwischen *1* und *255*. Je höher der Wert, desto höher die Priorität. Der Wert *255* bestimmt, dass dieser virtuelle Router immer als Master fungiert, sobald er aktiv ist. Standardwert ist *100*. Normalerweise übernimmt der virtuelle Router mit der höchsten Priorität die Masterrolle. Nach Eintreten eines Backup-Falles wird die weitere Rollenverteilung Master-Slave von den Parametern **Priorität des virtuellen Routers** und **Pre-Empt-Modus (zurück in Master-Status)** bestimmt.

Im Menü **Erweiterte Einstellungen** müssen Sie alle Parameter für alle virtuellen Router auf allen Geräten, die am Routerverbund teilnehmen, identisch konfigurieren. Wir empfehlen Ihnen, die Voreinstellungen zu belassen.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Sendeintervall für Advertisements	Legen Sie fest, wie oft ein BRRP-Advertisement-Paket gesendet wird, wenn der virtuelle Router als Master definiert ist. Nur der aktuelle Master sendet über Multicast BRRP-Advertisements, welche auch die ID und die Priorität des Masters enthalten. Mögliche Werte sind ganze Zahlen zwischen *1* und *255*. Der Wert wird in Sekunden angegeben, Standardwert ist *1*. Basierend auf diesem Sendeintervall für Advertisements läuft routerintern ein Advertisement Timer, nach dessen Ablauf ein Advertisement-Paket gesendet wird.
Master down trials	Legen Sie die Anzahl von BRRP Advertisements fest, die fehlschlagen darf, bevor der Backup Router mit der jeweils niedrigeren Priorität annimmt, dass der Master inaktiv ist und es die Rolle des Masters übernimmt. Basierend auf dem Parameter **Master down trials** läuft routerintern ein Master Down Timer, nach dessen Ablauf vom Backup Router angenommen wird, dass der Master nicht erreichbar ist,

Feld	Beschreibung
	falls kein Advertisment empfangen wurde. Das effektive Master Down Intervall entspricht der Zeit errechnet aus der Anzahl erwarteter, aber ausgelassener BRRP Advertisements, dem Advertisement Interval und der sogenannten Skew Time, welche einen minimalen Zeitraum abhängig von der Priorität hinzufügt. Je höher die Priorität, desto kürzer ist die hinzugefügte Zeit, so dass ein Backup-Router mit höherer Priorität früher reagiert als einer mit niedrigerer Priorität). Mögliche Werte sind ganze Zahlen zwischen *1* und *255*, Standardwert ist *10*.
Pre-Empt-Modus (zurück in Master-Status)	Legen Sie fest, ob ein Backup-Router mit höherer Priorität Vorrang hat vor einem Master-Router mit niedriger Priorität. Der Pre-Empt-Modus dient dazu, unnötige Umschaltvorgänge zu verhindern. Mit *Aktiviert* wird die Funktion aktiv. Der Router mit der höheren Priorität hat immer Vorrang. Das heißt, bei Wiedererreichbarkeit des eigentlichen Master-Routers wird dieser auch immer aktiv. Wenn die Funktion nicht aktiv ist, bleibt der aktuell aktive Backup-Router auch nach Wiedererreichbarkeit des eigentlichen Master-Routers weiterhin aktiv, obwohl die Priorität des Master-Routers höher ist als die Priorität des derzeitig aktiven Backup-Routers. Standardmäßig ist die Funktion aktiv. Beachten Sie eine Ausnahme: Wird als **Priorität des virtuellen Routers** *255* ausgewählt, erhält das Gateway mit dieser Priorität auf jeden Fall die Masterrolle, d.h. die Einstellung in **Pre-Empt-Modus (zurück in Master-Status)** wird nicht berücksichtigt. Wählen Sie daher zur Nutzung von Pre-Empt-Modus eine **Priorität des virtuellen Routers** kleiner *255*.
Authentisierung aktivieren	Aktivieren oder deaktivieren Sie die Authentisierung. Mit *Aktiviert* wird die Funktion aktiv. Wenn die Funktion aktiv ist, wird ein Eingabefeld angezeigt. Hier geben Sie den Authentisierungsschlüssel ein. Hinweis: Beachten Sie, dass der Authentisierungsschlüssel für

Feld	Beschreibung
	alle am Routerverbund teilnehmenden virtuellen Router gleich sein muss. Standardmäßig ist die Funktion nicht aktiv.

20.13.2 VR-Synchronisation

Im Menü **Lokale Dienste**->**BRRP**->**VR-Synchronisation** wird der Watchdog Daemon konfiguriert, d.h. Sie legen fest, wie Statusänderungen gehandhabt werden.

Nach Öffnen des Menüs **Lokale Dienste**->**BRRP**->**VR-Synchronisation** wird eine Liste aller Synchronisationen angezeigt. Sie können entweder virtuelle Router untereinander synchronisieren oder Schnittstellen. Neue Synchronisationen können im Menü **Neu** hinzugefügt werden.

Sie können z. B. die beiden virtuellen Router R1 und R2 über BRRP synchronisieren. Dazu müssen Sie zwei Einträge anlegen. Für den ersten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R1 und als **Synchronisations-VR/Schnittstelle** R2 verwenden. Für den zweiten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R2 und als **Synchronisations-VR/Schnittstelle** R1 konfigurieren.

20.13.2.1 Neu

Wählen Sie die Schaltfläche **Neu** um neue Synchronisationen hinzuzufügen.

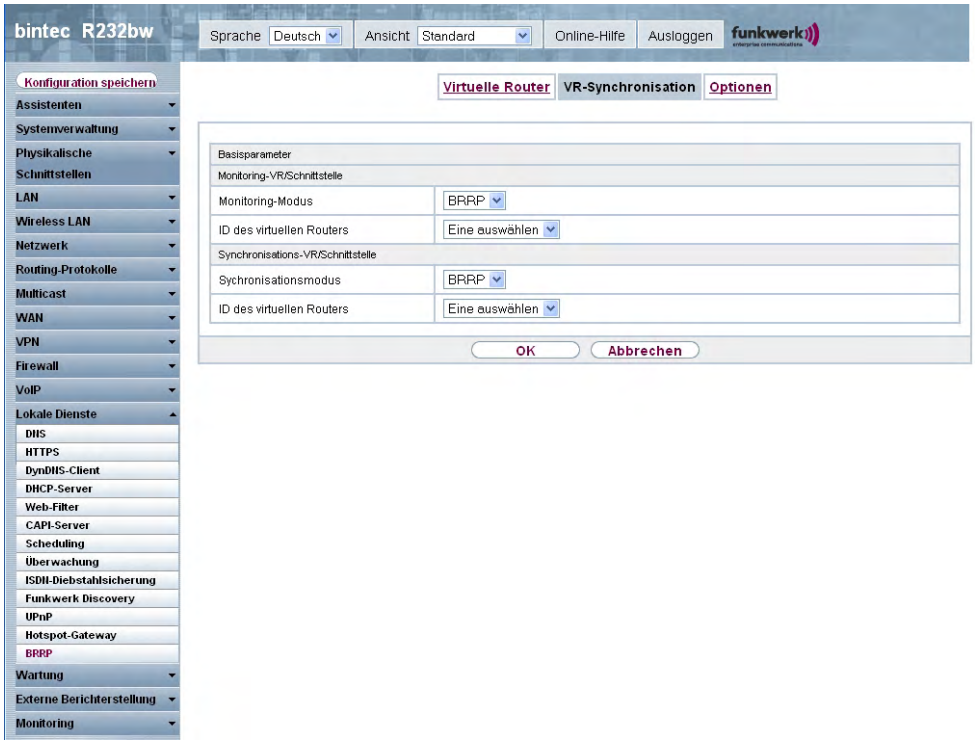


Abb. 149: **Lokale Dienste->BRRP->VR-Synchronisation->Neu**

Das Menü **Lokale Dienste->BRRP->VR-Synchronisation->Neu** besteht aus folgenden Feldern:

Felder im Menü VR-SynchronisationMonitoring-VR/Schnittstelle

Feld	Beschreibung
Monitoring-Modus	Zeigt an, welcher Mechanismus für die Überwachung eines virtuellen Routers angewendet wird. Mögliche Werte: • *BRRP* : Die BRRP-spezifischen Status-Advertisements werden zur Statusermittlung des Masters verwendet. (Der Master sendet Advertisements gemäß seiner Konfiguration im Menü **Lokale Dienste->BRRP->Virtuelle Router->Neu->Erweiterte Einstellungen**.)
ID des virtuellen Routers	Wählen Sie einen virtuellen Router über die **ID des virtuellen Routers** und legen Sie durch die Auswahl fest, welche Schnittstelle kontrolliert werden soll. Wählbar sind die vorher definier-

Feld	Beschreibung
	ten IDs (siehe **ID des virtuellen Routers** im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu**->**BRRP Überwachte Schnittstelle**). Der Watchdog Daemon fragt die in **Virtueller Router** festgelegten Detailinformationen ab.

Felder im Menü VR-SynchronisationSynchronisations-VR/Schnittstelle

Feld	Beschreibung
Sychronisationsmodus	Zeigt an, mit welchem Mechanismus virtuelle Router bzw. Schnittstellen synchronisiert werden: Mögliche Werte: • *BRRP* : BRRP wird für die Synchronisierung der virtuellen Router verwendet.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers, der synchronisiert werden soll. Über die Synchronisation des virtuellen Routers wird implizit die mit dem virtuellen Router verbundene virtuelle Schnittstelle synchronisiert.

20.13.3 Optionen

Im Menü **Lokale Dienste**->**BRRP**->**Optionen** können Sie die Funktion BRRP ein- oder ausschalten.

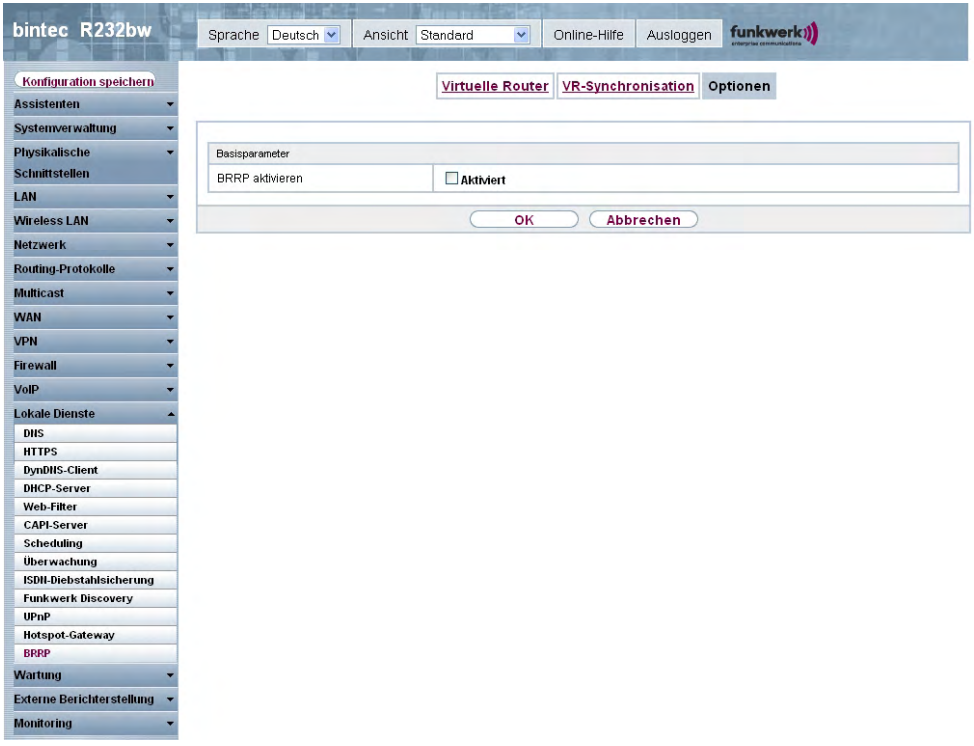


Abb. 150: **Lokale Dienste->BRRP->Optionen**

Das Menü **Lokale Dienste->BRRP->Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

Feld	Beschreibung
BRRP aktivieren	Aktivieren oder deaktivieren Sie die Funktion BRRP. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Kapitel 21 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.

21.1 Diagnose

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

21.1.1 Ping-Test

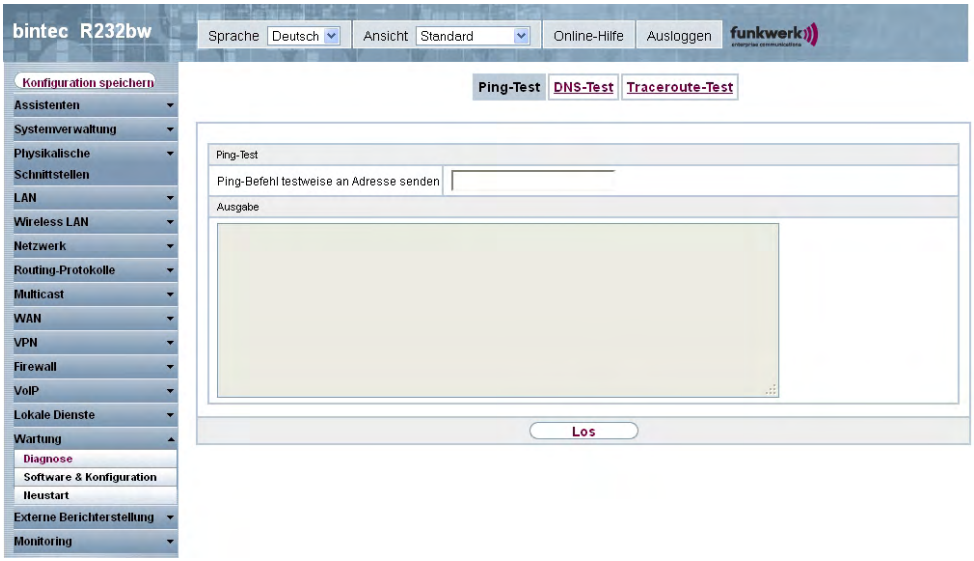


Abb. 151: **Wartung**->**Diagnose**->**Ping-Test**

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 Drücken der **Los**-Schaltfläche wird der Ping-Test gestartet.

21.1.2 DNS-Test

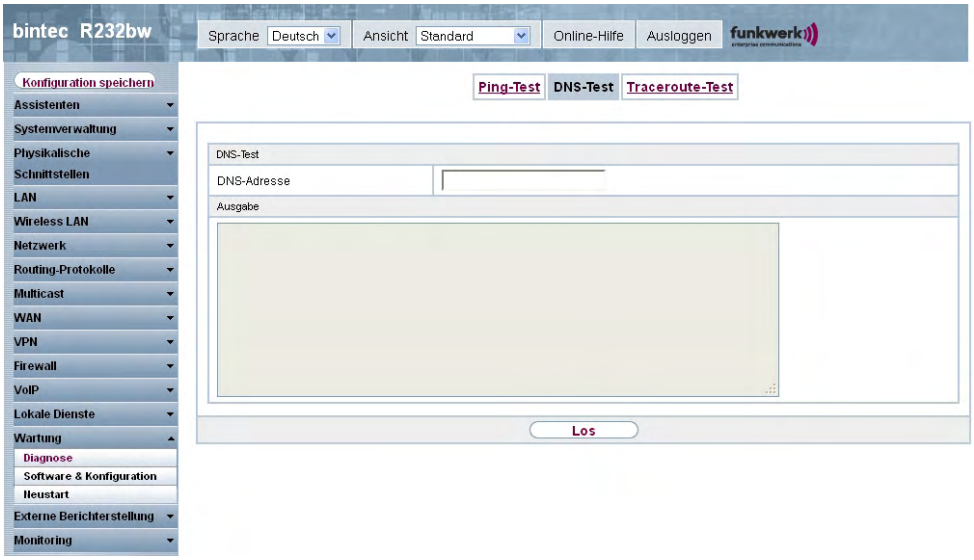


Abb. 152: **Wartung**->**Diagnose**->**DNS-Test**

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 Drücken der **Los**-Schaltfläche wird der DNS-Test gestartet.

21.1.3 Traceroute-Test

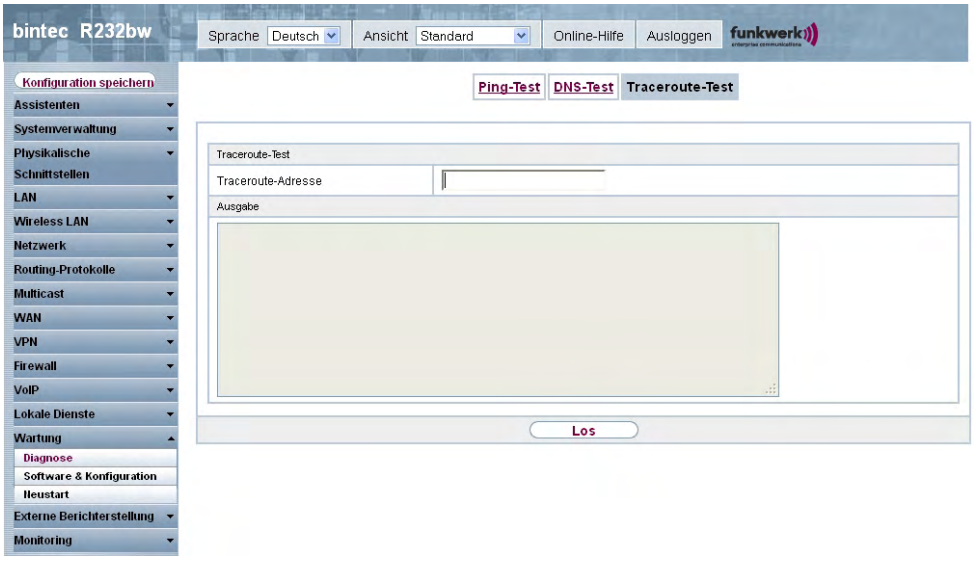


Abb. 153: **Wartung**->**Diagnose**->**Traceroute-Test**

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 Drücken der **Los**-Schaltfläche wird der Traceroute-Test gestartet.

21.2 Software &Konfiguration

21.2.1 Optionen

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

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.funkwerk-ec.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 Funkwerk Enterprise Communications 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 **Funkwerk Configuration Interfaces**. 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 Kom-

patibilität 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.

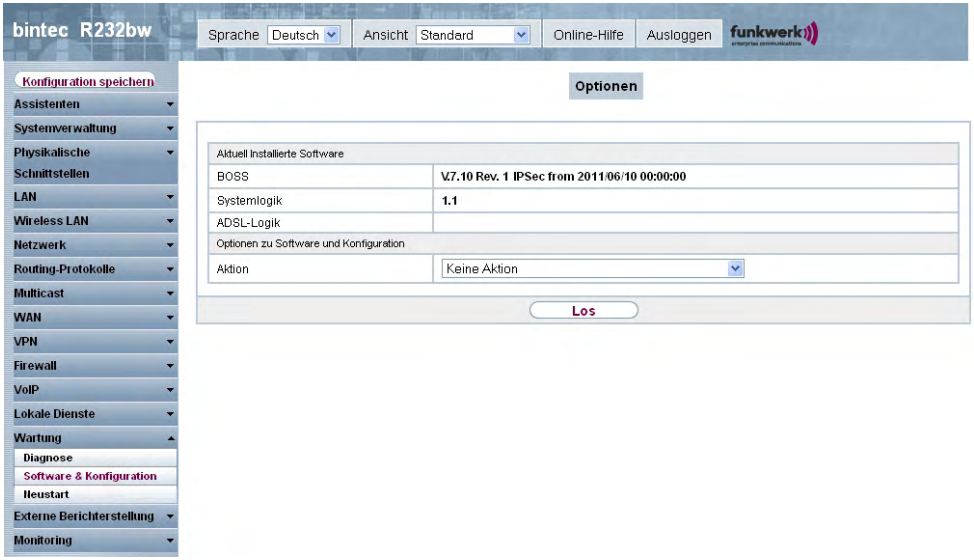


Abb. 154: **Wartung->Software &Konfiguration->Optionen**

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

Felder im Menü OptionenAktuell 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 OptionenOptionen 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 importieren*: Wählen Sie in **Dateiname** eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken von **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! • *Sprache importieren*: Sie können weitere Sprachversionen des **Funkwerk Configuration Interface** auf Ihr Gerät einspielen. Die Dateien können Sie vom Download-Bereich auf *www.funkwerk-ec.com* auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen. • *Systemsoftware aktualisieren*: Sie können eine Aktualisierung der Systemsoftware, der ADSL-Logik und des BOOTmonitors initiieren. • *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 mit Statusinformationen exportieren*: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie die **Los**-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. • *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. • *Kopieren*: Die Konfigurationsdatei im Feld **Name der Quelldatei** wird als **Name der Zieldatei** gespeichert. • *Umbenennen*: Die Konfigurationsdatei im Feld **Datei auswählen** wird zu **Neuer Dateiname** umbenannt. • *Konfiguration löschen*: Die Konfiguration im Feld **Datei auswählen** wird gelöscht. • *Datei löschen*: Die Datei im Feld **Datei auswählen** wird gelöscht.
Verschlüsselung der Konfiguration	Nur für **Aktion** = *Konfiguration importieren*, *Konfiguration exportieren*, *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.
Quelle	Nur für **Aktion** = *Systemsoftware aktualisieren* Wählen Sie die Quelle für der Aktualisierung aus.

Feld	Beschreibung
	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 Funkwerk-Server*: Die Datei liegt auf dem offiziellen Funkwerk-Update-Server.
URL	Nur für **Quelle** = *HTTP-Server* Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.
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*, *Konfiguration mit Statusinformationen 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.
Name der Quelldatei	Nur für **Aktion** = *Kopieren*Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für **Aktion** = *Kopieren*Geben Sie den Namen der Kopie ein.
Datei auswählen	Nur für **Aktion** = *Umbenennen* , *Konfiguration löschen* oder *Datei löschen*Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.
Neuer Dateiname	Nur für **Aktion** = *Umbenennen*Geben Sie den neuen Namen der Konfigurationsdatei ein.

21.3 Neustart

21.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **Funkwerk Configuration Interface** 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 der Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

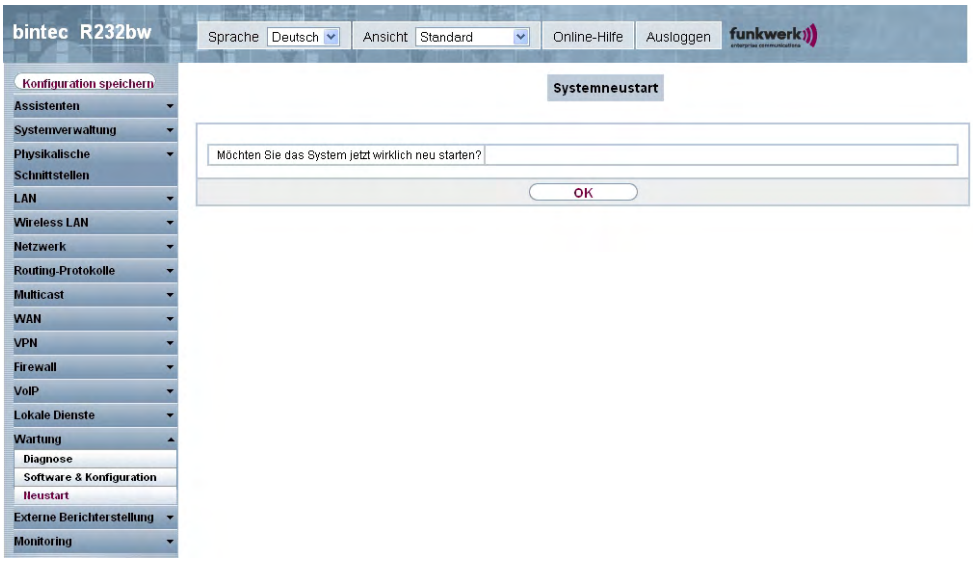


Abb. 155: **Wartung->Neustart->Systemneustart**

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

Kapitel 22 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.

22.1 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.funkwerk-ec.com*).

22.1.1 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.

22.1.1.1 Neu

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

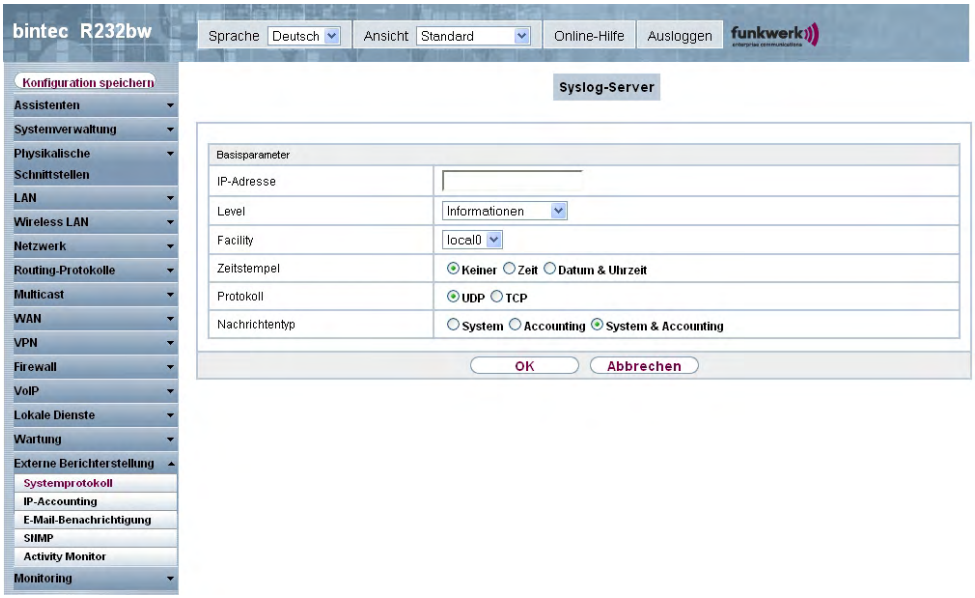


Abb. 156: **Externe Berichterstellung**->**Systemprotokoll**->**Syslog-Server**->**Neu**

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

Felder im Menü Syslog-ServerBasisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.

Feld	Beschreibung
Level	Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung* • *Benachrichtigung* • *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.

Feld	Beschreibung
	Mögliche Werte: • *UDP* (Standardwert) • *TCP*
Nachrichtentyp	Wählen Sie den Nachrichtentyp aus. Mögliche Werte: • *System &Accounting* (Standardwert) • *System* • *Accounting*

22.2 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 z.B. 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 überhaupt 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.

22.2.1 Schnittstellen

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

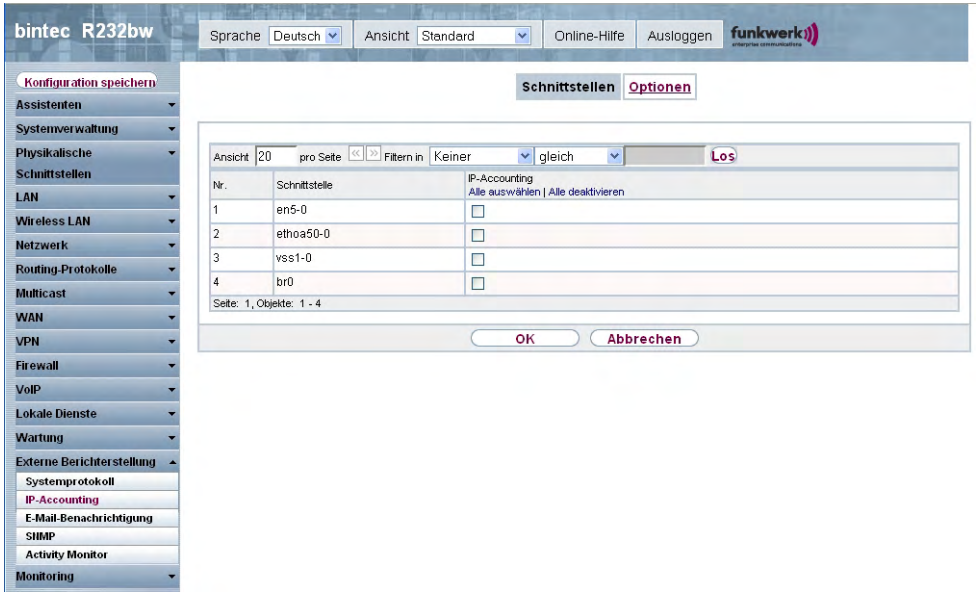


Abb. 157: **Externe Berichterstellung->IP-Accounting->Schnittstellen**

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.

22.2.2 Optionen

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

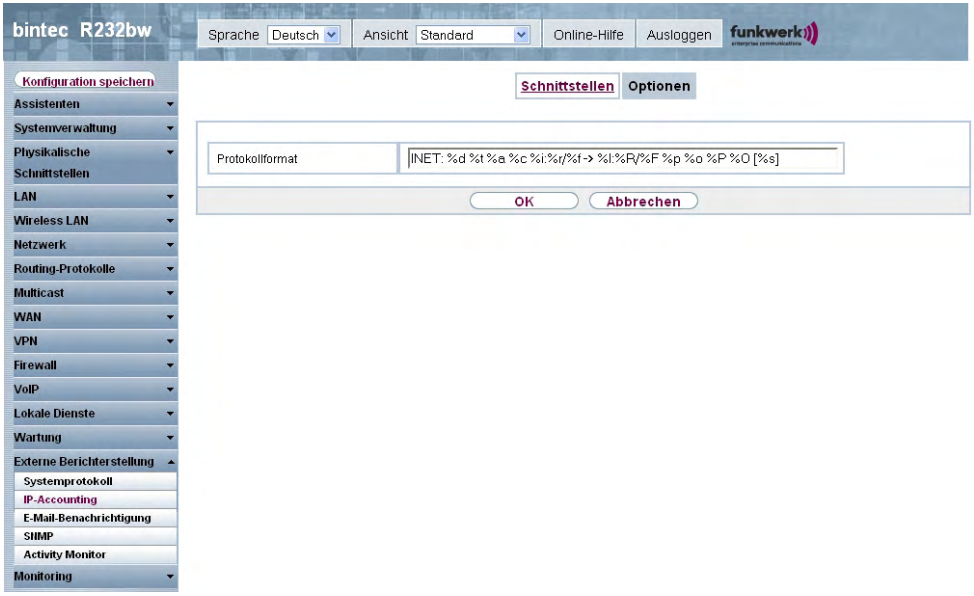


Abb. 158: **Externe Berichterstellung->IP-Accounting->Optionen**

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

Feld	Beschreibung
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

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

22.3 E-Mail-Benachrichtigung

Mit der E-Mail-Benachrichtigung werden dem Administrator je nach Konfiguration Emails gesendet, sobald relevante Syslog Meldungen auftreten.

22.3.1 E-Mail-Benachrichtigungs-Server

Das Menü **E-Mail-Benachrichtigungs-Server** besteht aus folgenden Feldern:

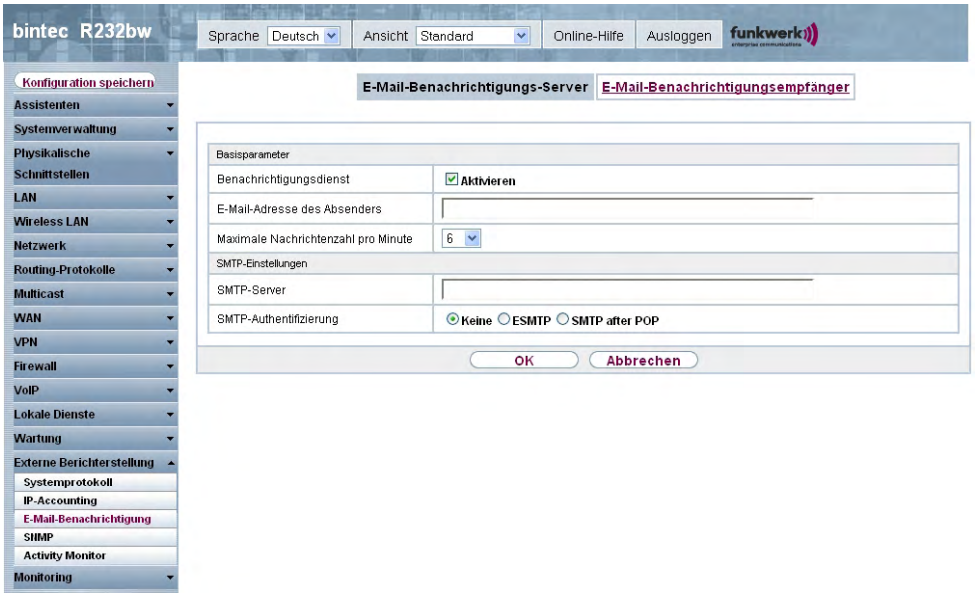


Abb. 159: **Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungs-Server**

Das Menü**Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungs-Server** besteht aus folgenden Feldern:

Felder im Menü E-Mail-Benachrichtigungs-ServerBasisparameter

Feld	Beschreibung
Benachrichtigungs-dienst	Aktivieren bzw. deaktivieren Sie die Funktion.
E-Mail-Adresse des Absenders	Geben Sie die Mailadresse ein, die in das Absenderfeld der Email eingetragen werden soll.
Maximale Nachrichten-zahl 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-Benachrichtigungs-ServerSMTP-Einstellungen

Feld	Beschreibung
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll. Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Au-thentifizierung	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.

Feld	Beschreibung
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. Standardwert ist *600* sekunden.

22.3.2 E-Mail-Benachrichtigungsempfänger

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

22.3.2.1 Neu

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

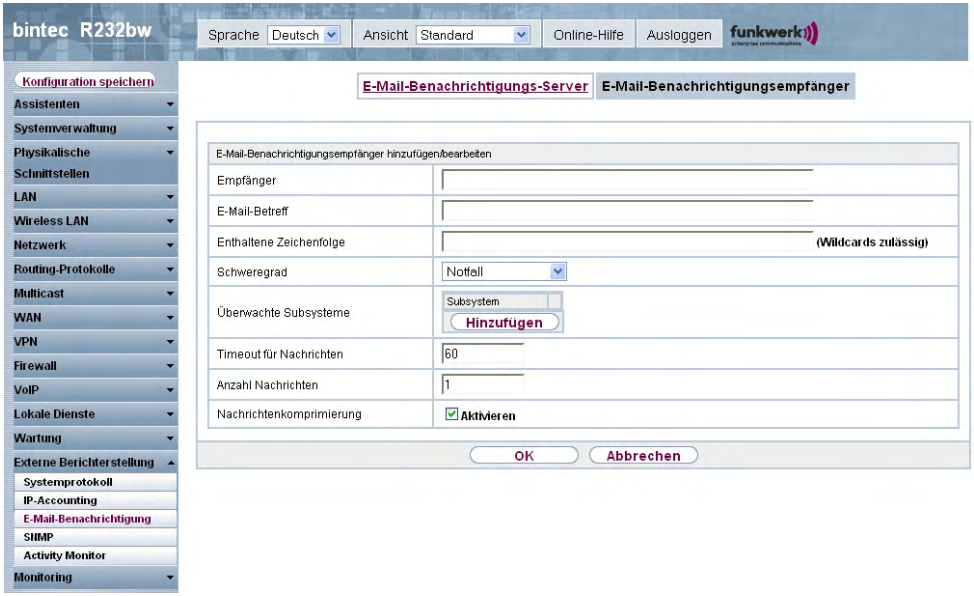


Abb. 160: **Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungsempfänger**

Das Menü **Externe Berichterstellung->E-Mail-Benachrichtigung->E-Mail-Benachrichtigungsempfänger** besteht aus folgenden Feldern:

Felder im Menü E-Mail-BenachrichtigungsempfängerE-Mail-Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Empfänger	Geben Sie die Email-Adresse des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
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 Zeichen-

Feld	Beschreibung
	folge" 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*
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 dem Timeout.
Anzahl Nachrichten	Geben Sie die Anzahl an 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*, Defaultwert ist *1*.
Nachrichtenkomprimierung	Wählen Sie aus, ob der Text des 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.

Felder im Menü E-Mail-BenachrichtigungsempfängerÜberwachte Subsysteme

Feld	Beschreibung
Subsystem	Wählen Sie die Subsysteme aus, die überwacht werden sollen. Fügen Sie mit **Hinzufügen** neue Subsysteme hinzu.

22.4 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

22.4.1 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.

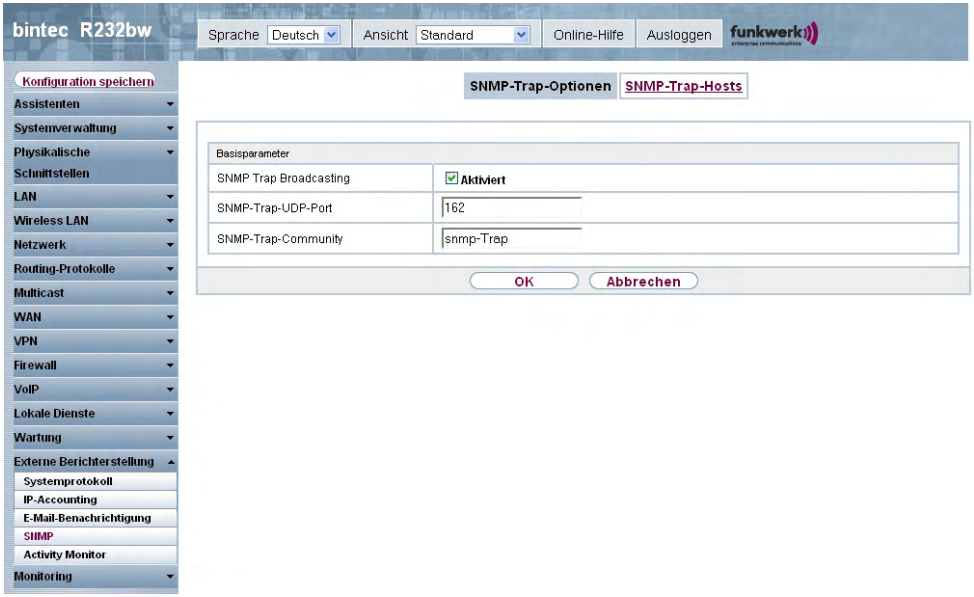


Abb. 161: **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen**

Das Menü **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen** besteht aus folgenden Feldern:

Felder im Menü SNMP-Trap-OptionenBasisparameter

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. Mögliche ist jeder ganzzahlige Wert. Standardwert ist `162` .

Feld	Beschreibung
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 hier eine Zeichenkette mit `0` bis `255` Zeichen. Standardwert ist `SNMP-Trap` .

22.4.2 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.

22.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

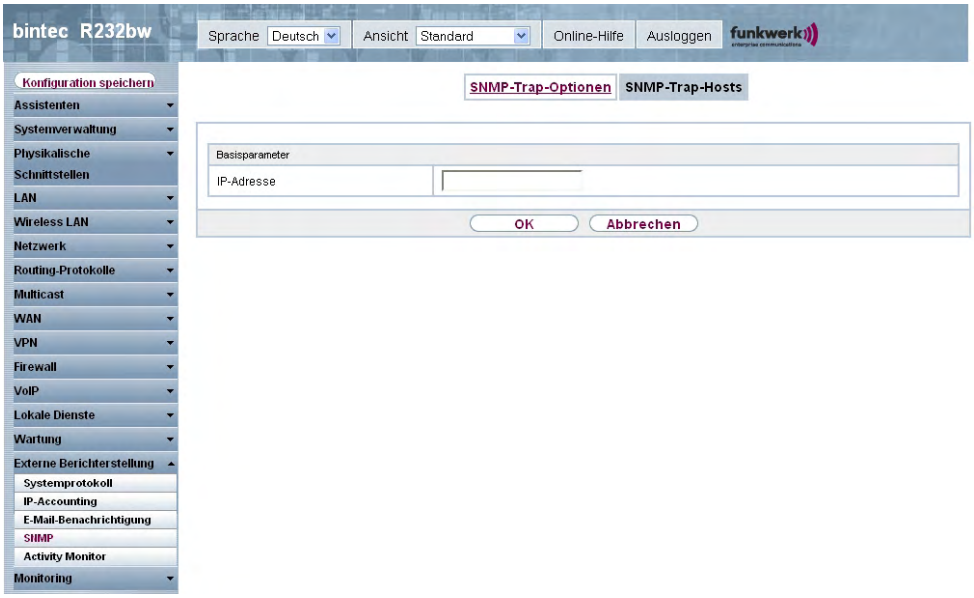


Abb. 162: **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu**

Das Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu** besteht aus folgenden Feldern:

Felder im Menü SNMP-Trap-HostsBasisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

22.5 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 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.funkwerk-ec.com* auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen).

22.5.1 Optionen

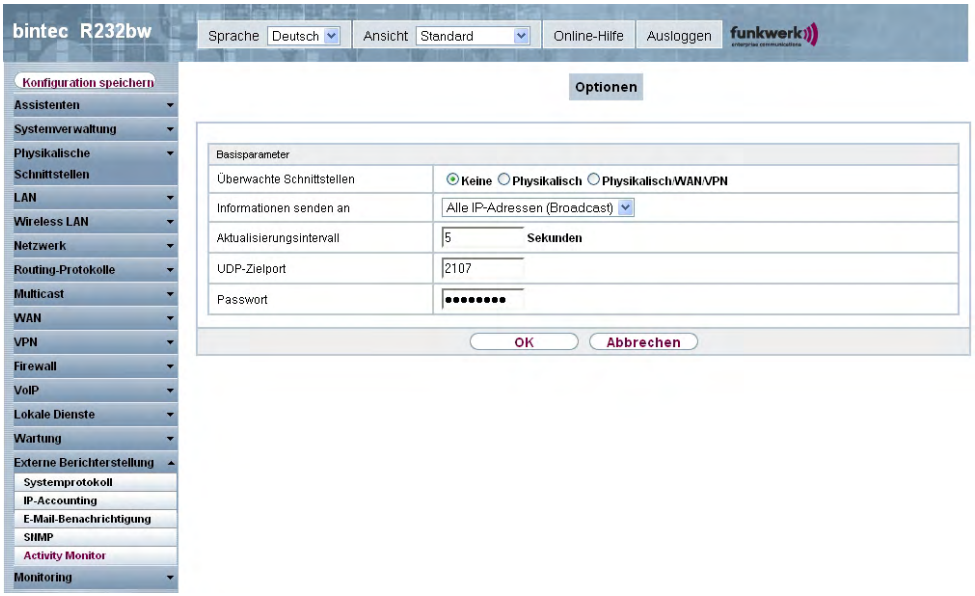


Abb. 163: **Externe Berichterstellung->Activity Monitor->Optionen**

Das Menü **Externe Berichterstellung->Activity Monitor->Optionen** besteht aus folgenden Feldern:

Felder im Menü OptionenBasisparameter

Feld	Beschreibung
Überwachte Schnittstellen	Wählen Sie die Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden sollen. 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.

Feld	Beschreibung
	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* Standardwert ist *5* .
UDP-Zielport	Geben Sie die Port-Nummer für die Windows-Anwendung **Activity Monitor** ein. Standardwert ist *2107* (registriert durch IANA - Internet Assigned Numbers Authority).
Passwort	Geben Sie das Passwort für den **Activity Monitor** ein.

Kapitel 23 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.

23.1 Internes Protokoll

23.1.1 Systemmeldungen

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

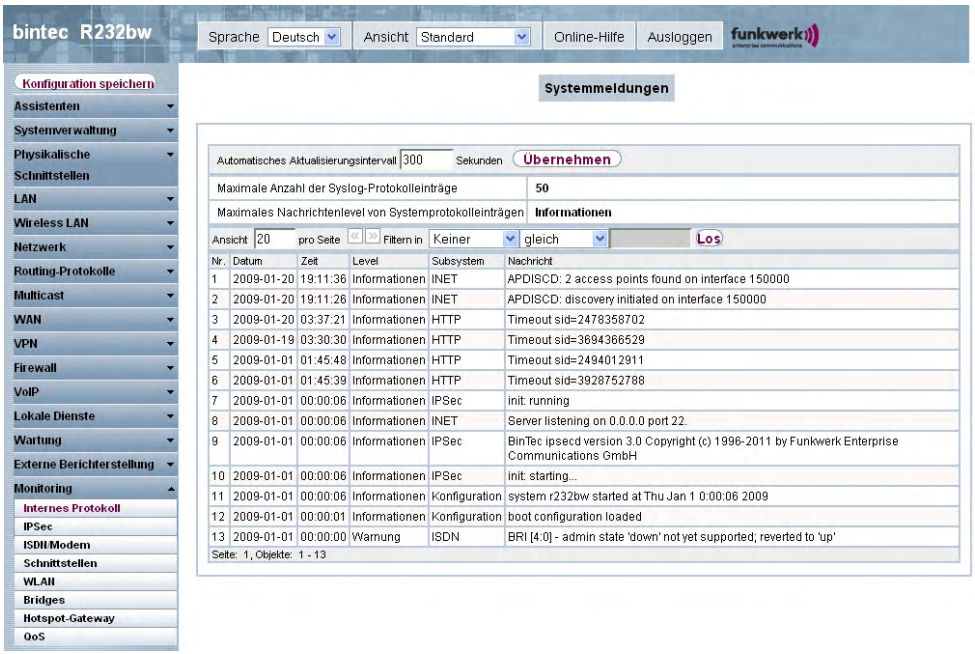


Abb. 164: **Monitoring->Internes Protokoll->Systemmeldungen**

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.

23.2 IPSec

23.2.1 IPSec-Tunnel

Im Menü **Monitoring**->**IPSec**->**IPSec-Tunnel** wird eine Liste aller konfigurierter IPSec-Tunnel angezeigt.

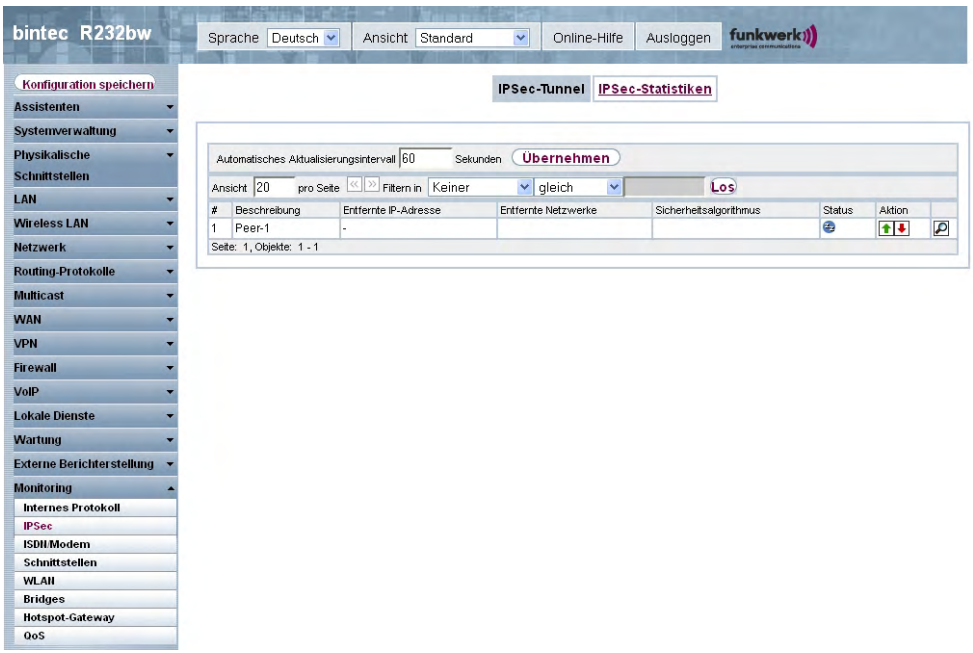


Abb. 165: **Monitoring->IPSec->IPSec-Tunnel**

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 Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der IPSec-Verbindung geändert.

Durch Drücken der -Schaltfläche wird eine ausführliche Statistik zu der jeweiligen IPSec-Verbindung angezeigt.

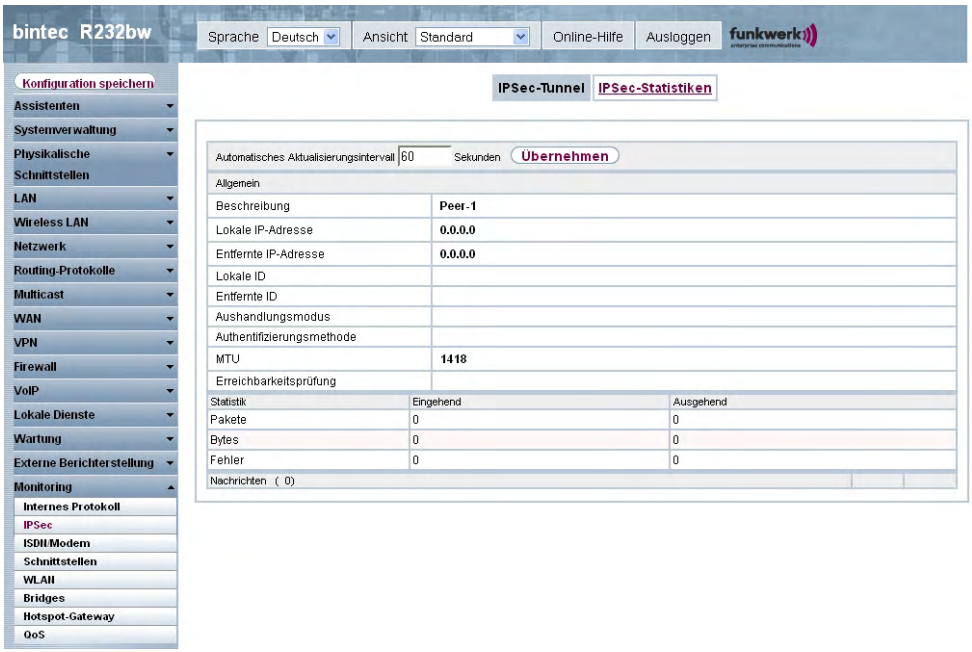


Abb. 166: **Monitoring->IPSec->IPSec-Tunnel->**

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.
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.

23.2.2 IPSec-Statistiken

Im Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

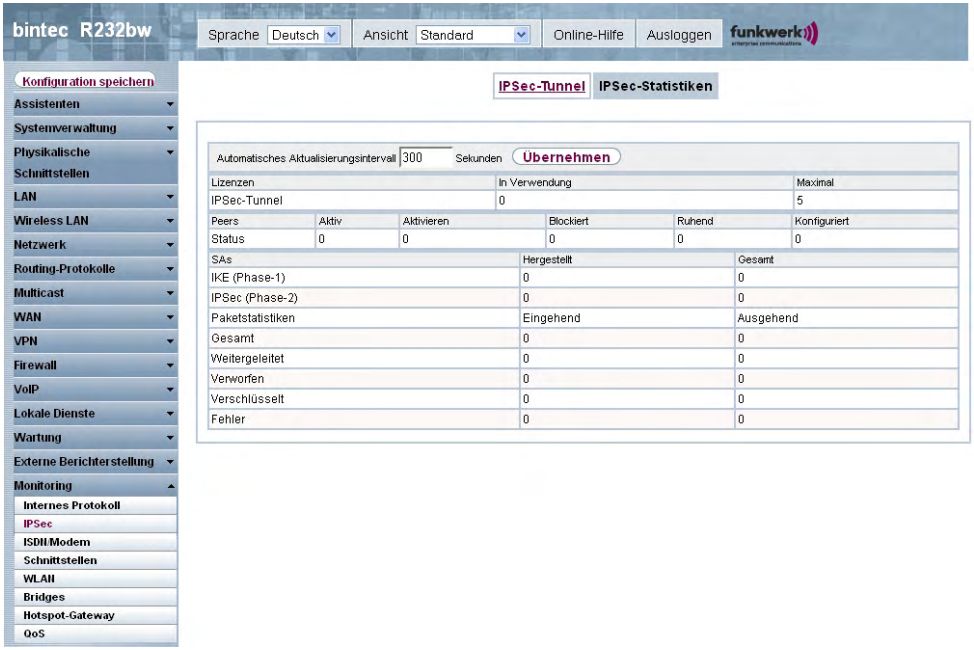


Abb. 167: **Monitoring->IPSec->IPSec-Statistiken**

Das Menü **Monitoring->IPSec->IPSec-Statistiken** besteht aus folgenden Feldern:

Feld im Menü IPSec-StatistikenLizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (**In Verwendung**) und die Anzahl der maximal verwendbaren Lizenzen (**Maximal**) an.

Feld im Menü IPSec-StatistikenPeers

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 IPSec-StatistikenSAs

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 IPSec-StatistikenPaketstatistiken

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.

23.3 ISDN/Modem

23.3.1 Aktuelle Anrufe

Im Menü **Monitoring**->**ISDN/Modem**->**Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

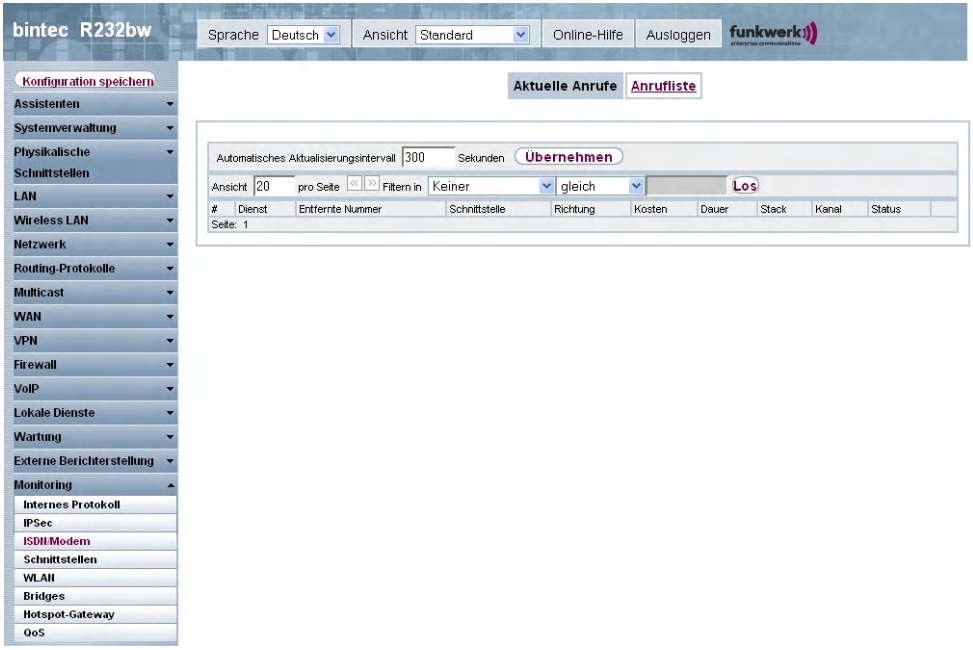


Abb. 168: **Monitoring->ISDN/Modem->Aktuelle Anrufe**

Werte in der Liste Aktuelle Anrufe

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden ist: *PPP*, *IPSec*, *X.25*, *POTS*.
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: *Eingehend*, *Ausgehend*.
Kosten	Zeigt die Kosten der laufenden Verbindung an.
Dauer	Zeigt die Dauer der laufenden Verbindung an.
Stack	Zeigt den zugehörigen ISDN-Port (STACK) an.
Kanal	Zeigt die Nummer des ISDN-B-Kanals an.
Status	Zeigt den Status der Verbindung an: *null*, *c-initiated*, *ovl-send*, *oc-procd*, *c-deliverd*, *c-present*, *c-recvd*, *ic-procd*, *aktiv*, *discon-req*, *discon-ind*, *suspd-req*, *resum-req*, *ovl-recv*.

23.3.2 Anrufliste

Im Menü **Monitoring**->**ISDN/Modem**->**Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

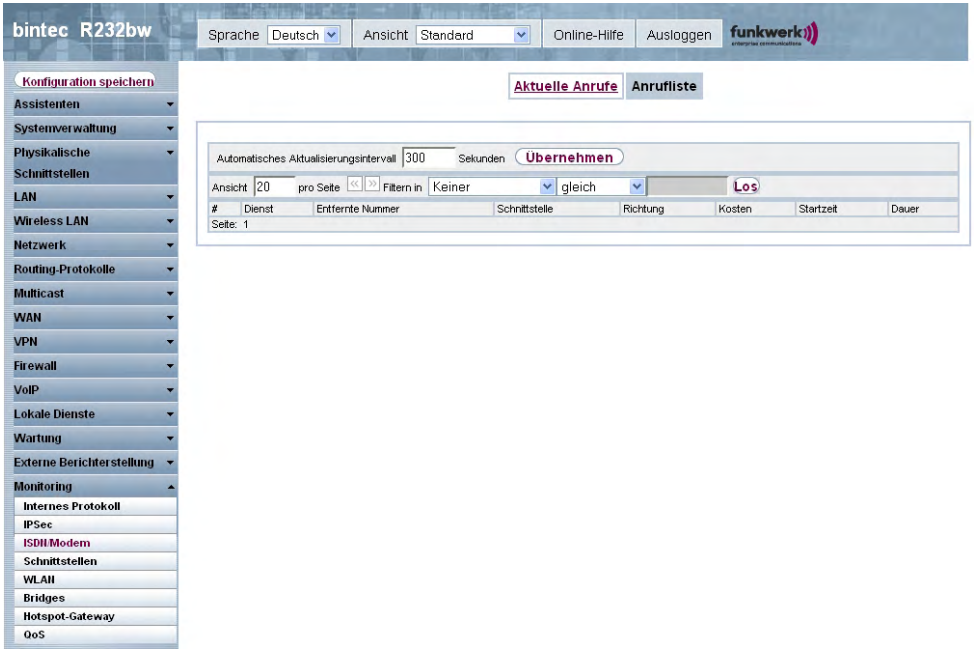


Abb. 169: **Monitoring->ISDN/Modem->Anrufliste**

Werte in der Liste Anrufliste

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden war: *PPP*, *IPSec*, *X.25*, *POTS*.
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: *Eingehend*, *Ausgehend*.
Kosten	Zeigt die Kosten der Verbindung an.
Startzeit	Zeigt die Uhrzeit an, zu welcher der Ruf aus- bzw. einging.
Dauer	Zeigt die Dauer der Verbindung an.

23.4 Schnittstellen

23.4.1 Statistik

Im Menü **Monitoring**->**Schnittstellen**->**Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

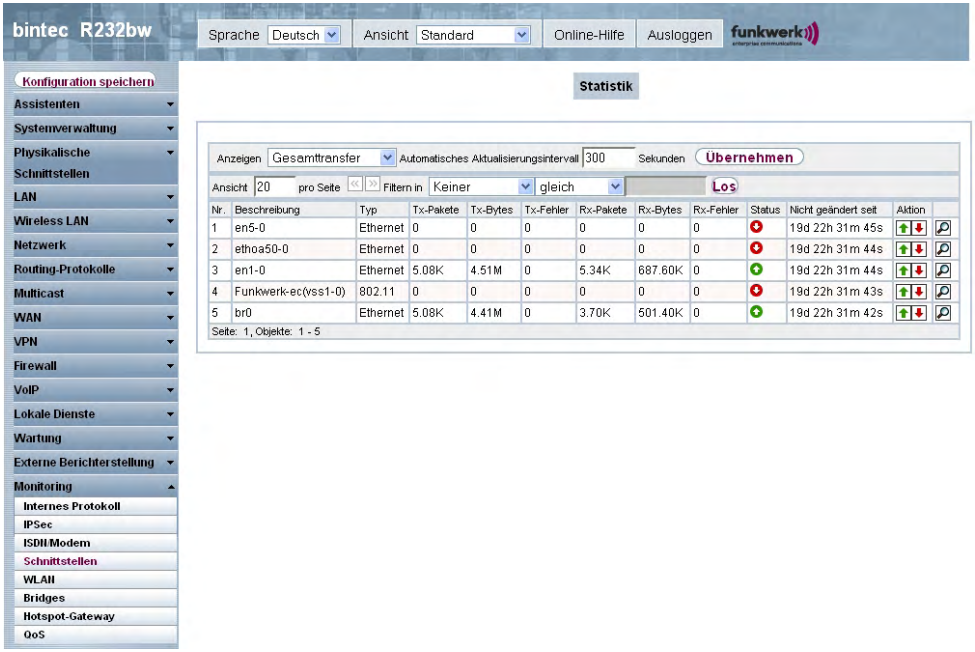


Abb. 170: **Monitoring**->**Schnittstellen**->**Statistik**

Durch Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert. Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

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.

Feld	Beschreibung
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt zu ändern.

23.5 WLAN

23.5.1 WLAN1

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

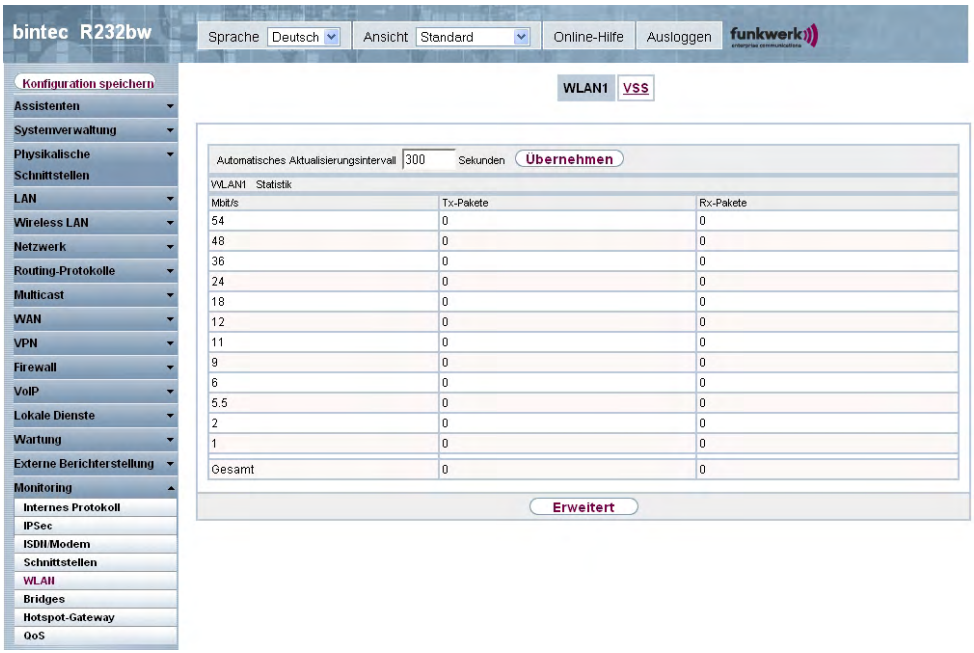


Abb. 171: **Monitoring**-> **WLAN**-> **WLAN**

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.

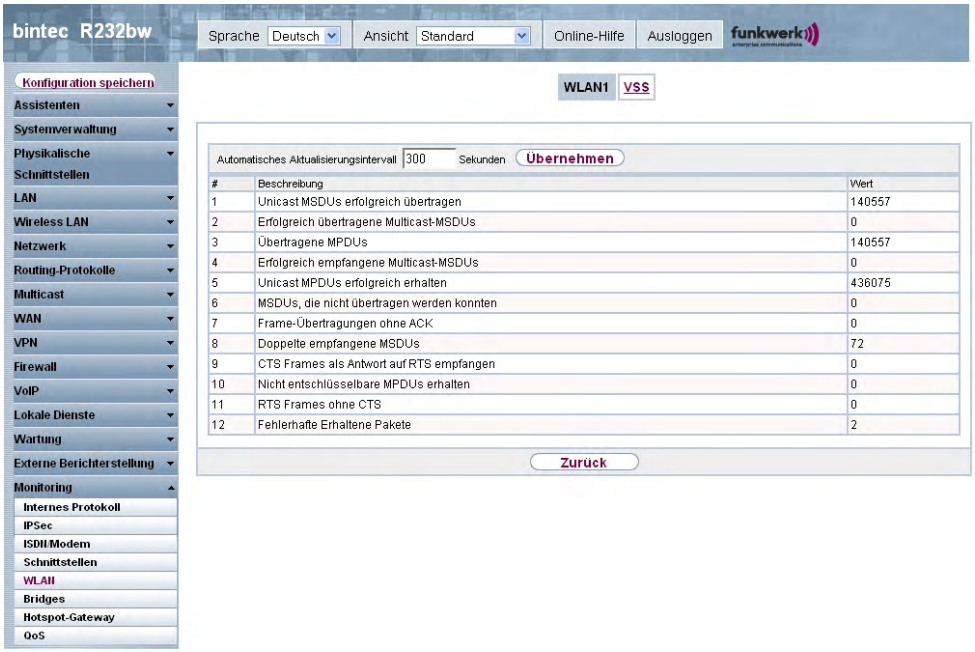


Abb. 172: **Monitoring->WLAN-> WLAN->Erweitert**

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 versandte MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wur-

Beschreibung	Bedeutung
	de 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.
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.

23.5.2 VSS

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

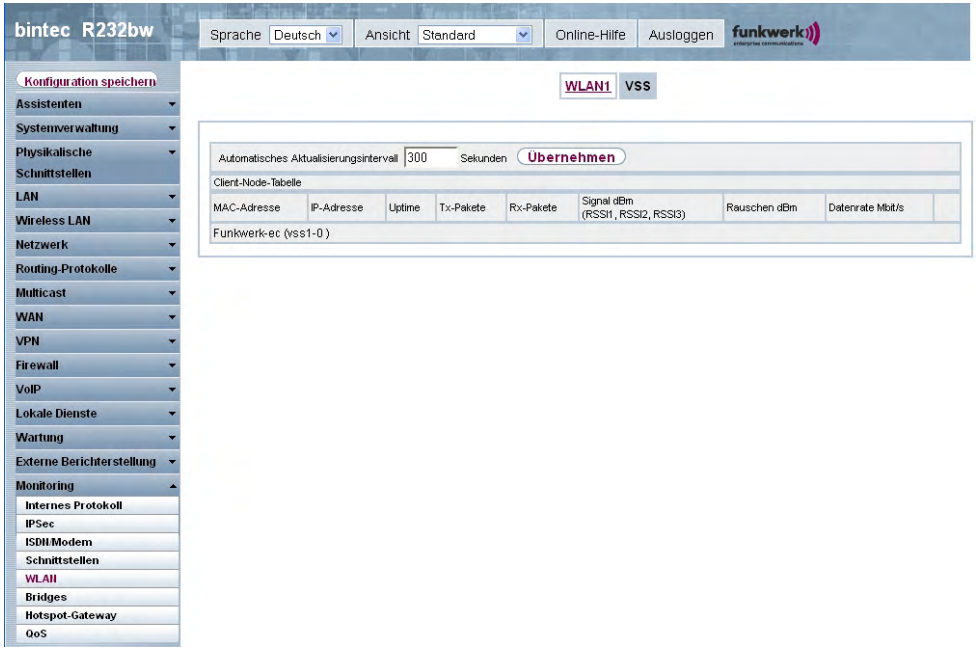


Abb. 173: **Monitoring->WLAN->VSS**

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 von diesem Client empfangener 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

Feld	Beschreibung
	von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.

VSS - Details für Verbundene Clients

Im Menü **Monitoring**->**WLAN**->**VSS**->**<Verbundener Client>**-> werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt.

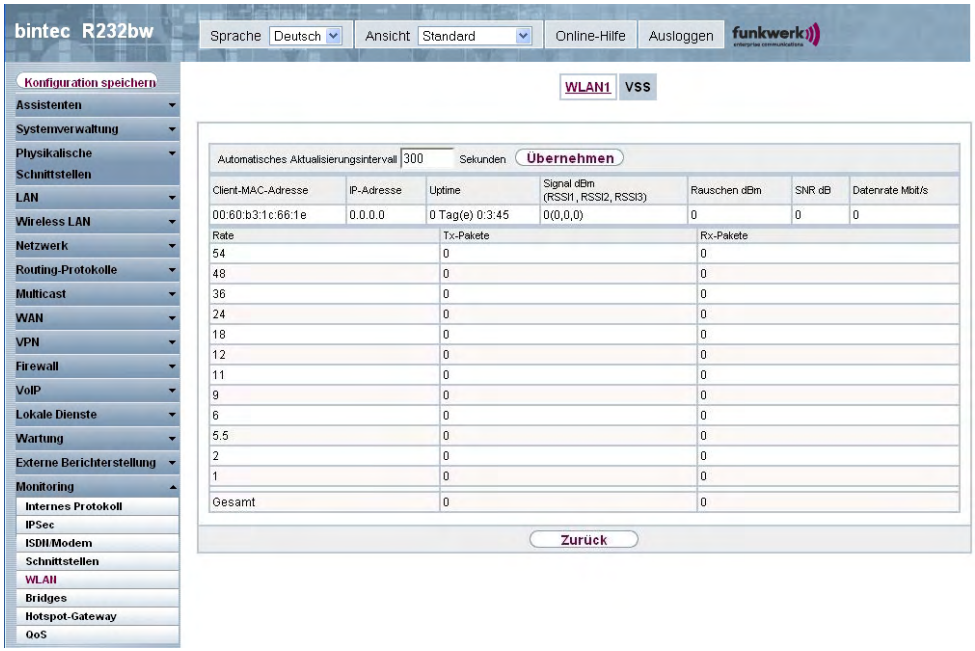


Abb. 174: **Monitoring**->**WLAN**->**VSS**->**<Verbundener Client>**->

Werte in der Liste VSS <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 von diesem Client empfangener 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.

23.6 Bridges

23.6.1 br<x>

Im Menü **Monitoring**->**Bridges**-> **br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

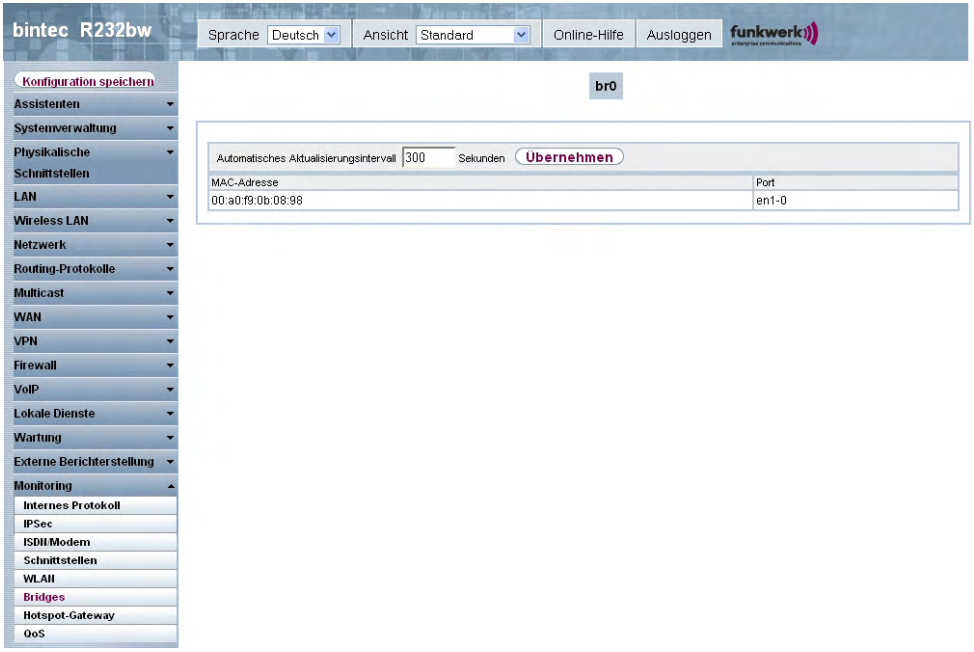


Abb. 175: **Monitoring**->**Bridges**

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.

23.7 Hotspot-Gateway

23.7.1 Hotspot-Gateway

Im Menü **Monitoring**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller verbundenen Hosts angezeigt.

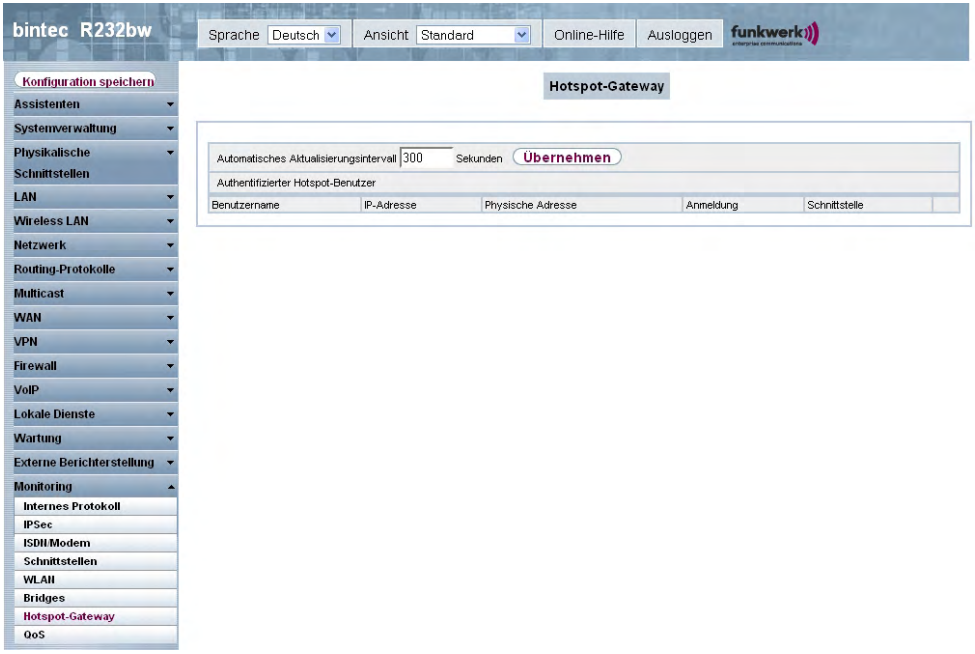


Abb. 176: **Monitoring->Hotspot-Gateway->Hotspot-Gateway**

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 die Zeit der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

23.8 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

23.8.1 QoS

Im Menü **Monitoring**->**QoS**->**QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

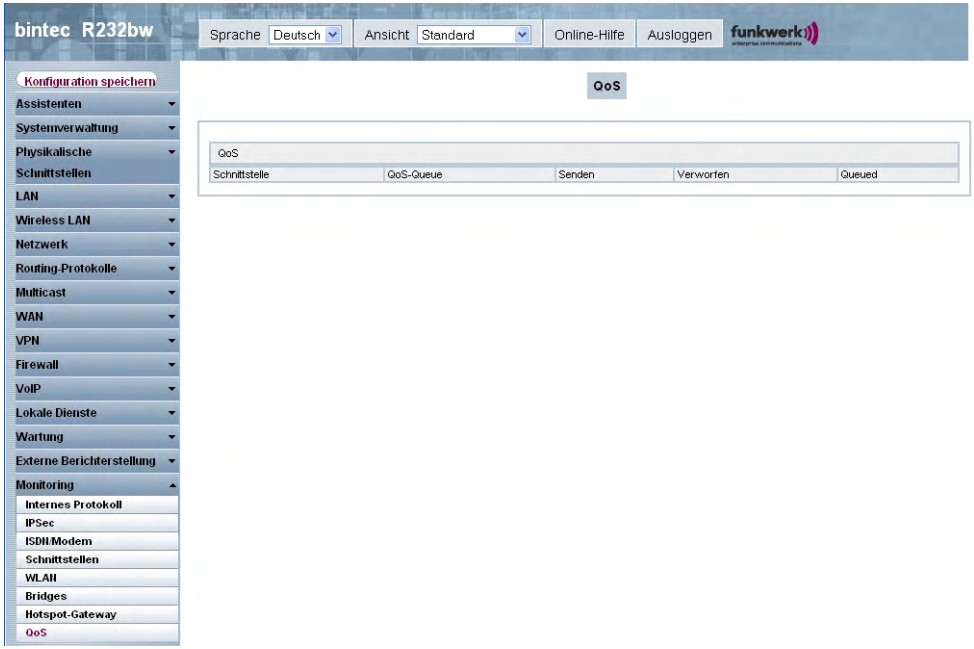


Abb. 177: **Monitoring->QoS->QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Glossar

Bit

Binary Digit. Kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.

Bündel

Die externen Anschlüsse größerer Telefonanlagen können zu Bündeln zusammengefasst werden. Bei der Einleitung eines externen Gespräches durch die Amtskennziffer oder bei automatischer Amtsholung wird beim Verbindungsaufbau ein für den Teilnehmer freigegebenes Bündel benutzt. Ist ein Teilnehmer für mehrere Bündel berechtigt, wird die Verbindung über das erste freigegebene Bündel aufgebaut. Ist ein Bündel belegt, wird das nächste freigegebene Bündel benutzt. Sind alle freigegebenen Bündel belegt, hört der Teilnehmer den Besetztton.

Busy On Busy

Anruf auf einen besetzten Team-Teilnehmer. Hat ein Teilnehmer eines Teams den Hörer abgehoben oder führt ein Gespräch, können Sie entscheiden, ob weitere Anrufe für dieses Team signalisiert werden sollen. Die Erreichbarkeit eines Teilnehmers kann zwischen "Standard" und "Busy On Busy" (Besetzt bei Besetzt) umgeschaltet werden. In der Grundeinstellung steht sie auf Standard. Ist Busy on Busy für ein Team eingerichtet, so erhalten weitere Anrufer Besetzt signalisiert.

DECT

Digital European Cordless Telecommunication. Europäischer Standard für schnurlose Telefone und schnurlose Telefonanlagen. Zwischen mehreren Handgeräten können kostenfreie interne Gespräche geführt werden. Ein weiterer Vorteil ist die erhöhte Abhörsicherheit (GAP).

Dienste

Im Euro-ISDN gibt es so genannte Dienste-Indikatoren, deren Namen festgelegt sind. Teilweise haben diese nur noch historische Bedeutung. Generell sollte man für "echte" Telefonate den Dienst "Fernsprechen" auswählen. Falls diese Auswahl nicht funktioniert (Netzbetreiberabhängig), kann man es mit "speech", "audio 3k1Hz" oder "telephony 3k1Hz" weiterversuchen. Das Gleiche gilt für den Faxbetrieb. Auch hier gibt es den Sammelbegriff Fax sowie einige Spezialunterscheidungen. Rein technisch sind die Dienste Bits in einem Datenwort, die über eine Maske ausgewertet werden. Wenn man in der Maske mehrere Bits einschaltet, werden alle diese Dienste zur Weiterschaltung zugelassen. Bei einem Bit entsprechend nur der eine ausgewählte Dienst.

Digitale Sprachübertragung

Durch die international genormte Puls Code Modulation (PCM) werden analoge Sprachsignale in einen digitalen Impulsstrom von 64

KBit/s umgewandelt. Vorteile: bessere Sprachqualität und geringere Störanfälligkeit als bei analoger Sprachübertragung.

Digitale Vermittlungsstelle

Ermöglicht durch computergesteuerte Koppelfelder den schnellen Verbindungsaufbau und die Aktivierung von Komfortleistungen wie Rückfragen, Anklopfen, Dreierkonferenz und Anrufweiterschaltung. Seit Januar 1998 sind alle Vermittlungsstellen der T-Com digitalisiert.

Direktruf

Sie befinden sich außer Haus. Es gibt jedoch jemanden bei Ihnen zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Da Sie für ein oder mehrere Telefone die Funktion Direktruf einrichten können, braucht lediglich der Hörer des entsprechenden Telefons abgehoben zu werden. Nach fünf Sekunden wählt die Telefonanlage automatisch die festgelegte Direktrufnummer, sofern Sie vorher nicht mit der Wahl einer anderen Nummer beginnen. Sie können in der Konfiguration Direktruf bis zu 12 Zielrufnummern eintragen. Eine Direktrufnummer ist jeweils nur von einem Teilnehmer nutzbar. Möchten Sie eine eingegebene Direktrufnummer ändern, können Sie die neue Direktrufnummer einfach eingeben, ohne die alte Direktrufnummer löschen zu müssen. Sie wird bei der Übertragung der geänderten Konfiguration zur Telefonanlage automatisch überschrieben.

DISA

Direct Inward System Access

Download

Datentransfer bei Online-Verbindungen, wobei Dateien von einem PC oder einem Datennetz-Server in den eigenen PC, Telefonanlage oder Endgerät “geladen” werden, um sie dort weiterzuverwenden.

Dreierkonferenz

Telefonieren zu dritt. Leistungsmerkmal im T-Net, im T-ISDN und in Ihrer Telefonanlage.

DSL- und ISDN-Verbindungen

Der Datentransfer zwischen dem Internet und Ihrer Telefonanlage erfolgt über ISDN- oder T-DSL. Die Telefonanlage ermittelt, zu welcher Gegenstelle ein Datenpaket geschickt werden soll. Damit eine Verbindung ausgewählt und aufgebaut werden kann, müssen Parameter für alle notwendigen Verbindungen festgelegt werden. Diese Parameter sind in Listen abgelegt, deren Zusammenspiel den Aufbau der richtigen Verbindung gestattet. Beim ISDN-Zugang wird von der Telefonanlage das PPP (Point-to-Point-Protocol) benutzt, beim Zugang über T-DSL das PPPoE (Point-to-Point-Protocol over Ethernet). Der Datenverkehr auf diesen beiden Internet-Verbindungen wird von der Telefonanlage getrennt überwacht.

DSL-Modem Spezielles Modem für die Datenübertragung mit Hilfe der DSL-Zugangstechnologie.

DSL-Splitter Eine Breitbandanschlusseinheit (BBAE), umgangssprachlich Splitter, ist ein Gerät, das die Daten beziehungsweise Frequenzen verschiedener Anwendungen, die über eine Teilnehmeranschlussleitung oder einen Abschlusspunkt Linientechnik laufen, aufteilt und über getrennte Anschlüsse zur Verfügung stellt.

Durchsage Sie möchten Ihre Mitarbeiter oder Ihre Familienmitglieder zu einer Besprechung oder zum Essen zusammenrufen? Sie könnten jeden einzelnen anrufen oder einfach die Durchsage-Funktion nutzen. Mit nur einem Anruf erreichen Sie alle durchsageberechtigten Telefone, ohne dass Ihre Gesprächspartner den Hörer der Telefone abheben müssen.

Durchsagefunktion Leistungsmerkmal von Telefonanlagen. An geeigneten Telefonen (z. B. Systemtelefonen) lassen sich wie bei einer Sprechanlage Durchsagen tätigen.

100Base-T Twisted-Pair-Anschluss, Fast Ethernet. Netzwerkanschluss für 100-MBit-Netze.

10Base-2 Thin-Ethernet-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp BNC. Zum Anschluss von Geräten mit BNC-Buchsen werden T-Verbindungsstücke eingesetzt.

10Base-T Twisted-Pair-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp RJ45.

1TR6 Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das DSS1.

3DES (Triple DES) Siehe DES.

802.11a/g Spezifiziert Datenraten von 54, 48, 36, 24, 18, 12, 9 und 6 Mbit/s und eine Arbeitsfrequenz im Bereich von 5 GHz (bei IEEE802.11a) bzw. 2,4 GHz (bei IEEE802.11g). IEEE802.11 g kann so konfiguriert werden, dass es zusätzlich zu 11b oder 11b und 11 kompatibel betrieben wird.

802.11b/g Einer der IEEE Standards für drahtlose Netzwerk-Hardware. Produkte, die dem gleichen IEEE Standard entsprechen, können miteinander kommunizieren, selbst wenn sie von verschiedenen Hardware- Herstellern stammen. Der IEEE802.11b Standard spezifiziert Datenraten von 1, 2, 5,5 und 11 Mbit/s, eine Arbeitsfrequenz im Be-

reich von 2,4 bis 2,4835GHz und WEP Verschlüsselung. IEEE802.11 Funknetze werden auch Wi-Fi Netzwerke genannt.

A-Teilnehmer Der A-Teilnehmer ist der Anrufer.

A-Telefonnummer unterdrücken (CLIR) CLIP/CLIR: Calling Line Identification Presentation/Calling Line Identification Restriction

a/b-Schnittstelle Zum Anschluss eines analogen Endgerätes. Bei einem ISDN-Endgerät (Terminaladapter) mit a/b-Schnittstelle wird ein angeschlossenes analoges Endgerät in die Lage versetzt, die unterstützten T-ISDN Leistungsmerkmale zu nutzen.

AAA Authentication, Authorization, Accounting

Access List Eine Regel, die eine Anzahl von Datenpaketen definiert, die vom Gateway übertragen bzw. nicht übertragen werden sollen.

Access Point Eine aktive Komponente eines Netzwerks, das aus funkbasierten und optional zusätzlich aus kabelgebundenen Bestandteilen besteht. An einem Access Point (AP) können sich viele WLAN-Clients (Endgeräte) einbuchen und gegenseitig über den AP Daten austauschen. Bei optionalem Anschluss eines kabelgebundenes Ethernet, werden die Signale zwischen den beiden physikalischen Medien, dem funkbasierten Interface und dem kabelgebundenen Interface überbrückt (Bridging).

Accounting Aufzeichnen von Verbindungsdaten, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.

Active Probing Active Probing macht sich den Umstand zu Nutze, dass Access Points dem Standard nach auf Anfragen eines Clients antworten sollen. Clients versenden so genannte Probe-Requests auf allen Kanälen und warten auf Antworten eines in der Nähe befindlichen Access Points. Im Antwortpaket steht dann die SSID des Funk-LANs und ob WEP-Verschlüsselung verwendet wird.

Ad Hoc Netzwerk Ein Ad Hoc Netzwerk bezeichnet eine Anzahl von Computern, die jeweils mit einem Wireless Adapter ein unabhängiges 802.11 WLAN bilden. Ad Hoc Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer Basis. Der Ad Hoc Modus wird auch als IBSS Modus bezeichnet (Independent Basic Service Set) und ist in kleinsten Netzen sinnvoll, z. B. wenn zwei Notebooks ohne Access Point miteinander vernetzt werden sollen.

ADSL Asymmetric Digital Subscriber Line

AH Authentication Header

Alphanumerisches Display Anzeigeeinheit z. B. beim Systemtelefon T-Concept PX722, die außer Ziffern auch Buchstaben und weitere Zeichen darstellen kann.

Amtsberechtigung Telefonanlagen unterscheiden die folgendem "Amtsberechtigungen". Diese können in der Konfiguration für jeden Teilnehmer individuell eingerichtet werden.

Analoge Anschlüsse Zum Anschluss analoger Endgeräte wie Telefon, Telefax und Anrufbeantworter.

Analoge Endgeräte Endgeräte, die Sprache oder andere Informationen analog übertragen, sind z. B. Telefon, Faxgerät, Anrufbeantworter und Modem.

Analoge Sprachübertragung Für die Übermittlung von Sprache über das Telefon werden akustische Schwingungen in kontinuierliche elektrische Signale umgewandelt, die über ein Leitungsnetz übertragen werden (digitale Sprachübertragung).

Anklopfen Mit dem Leistungsmerkmal "Anklopfen" sind Sie auch während eines Telefonats für andere erreichbar. Ruft Sie ein weiterer Teilnehmer an, während Sie telefonieren, hören Sie den Anklopfton im Hörer Ihres Telefons. Sie können dann entscheiden, ob Sie Ihr bisheriges Gespräch fortführen oder mit dem Anklopfenden sprechen wollen.

Anklopfsperre Soll das Leistungsmerkmal Anklopfen nicht genutzt werden, schalten Sie den Anklopfschutz ein. Während Sie ein Telefongespräch führen, wird dann einem weiteren Anrufer der Besetztton übermittelt.

Anlagenanschluss Point-to-Point (Punkt-zu-Punkt)

Anlagenrufnummer Zu einem Anlagenanschluss gehören eine Anlagenrufnummer und ein Rufnummernband. Mit Hilfe der Anlagenrufnummer erreichen Sie die TK-Anlage. Über eine Rufnummer des Rufnummernbands wird dann ein bestimmtes Endgerät der TK-Anlage ausgewählt.

Anruf auf einen besetzten Teilnehmer Busy on busy =Besetzt bei Besetzt

Anruf heranholen Leistungsmerkmal von Telefonanlagen. Anrufe können an einem internen Endgerät entgegengenommen werden, das sich nicht in der aktiven Rufverteilung befindet.

Anrufbeantworter Einen analogen Anrufbeantworter konfigurieren Sie unter "Endgerätetyp".

Anruferliste Komfortable Telefone wie das Sytemtelefon T-Concept PX722 bieten die Möglichkeit, Anrufwünsche während der Abwesenheit zu speichern.

Anruffilter Leistungsmerkmal, z. B. vom systemtelefon T-Concept PX722, von Komforttelefonen oder Anrufbeantwortern. Die Rufsignalisierung erfolgt nur bei bestimmten, vorher festgelegten Telefonnummern.

Anrufschutz Ausschalten der akustischen Anrufsignalisierung: Ruhe vor dem Telefon.

Anrufvariante Tag / Nacht Möglichkeit bei Telefonanlagen, die Rufverteilung über einen Kalender zu ändern. Nach Büroschluss ankommende Telefonanrufe werden zu einem personell noch besetzten Telefon oder zum Anrufbeantworter, Telefax weitergeleitet.

Anrufweiterschaltung in der Telefonanlage Die Telefonanlage gibt Ihnen mit dem Leistungsmerkmal der Anrufweiterschaltung (AWS) die Möglichkeit, erreichbar zu bleiben, auch wenn Sie nicht in der Nähe Ihres Telefons sind. Dieses erreichen Sie durch automatisches Weiterleiten von Anrufen an die gewünschte interne oder externe Telefonnummer. Mit dem Konfigurationsprogramm können Sie festlegen, ob die Anrufweiterschaltung in der Telefonanlage oder in der Vermittlungsstelle erfolgen soll. Die Anrufweiterschaltung in der Vermittlungsstelle können Sie nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie bei Ihrem Berater der T-Com.

Anrufweiterschaltung in der Vermittlungsstelle Die Möglichkeiten der Anrufweiterschaltung in der Vermittlungsstelle können Sie nur über Keypad nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie beim Berater der T-Com. Die Vermittlungsstelle verbindet den anrufenden Teilnehmer mit einem von Ihnen festgelegten externen Teilnehmer.

Anschluss analoger Endgeräte Die Leistungsmerkmale für analoge Endgeräte lassen sich nur mit Endgeräten nutzen, die mit dem MFV -Wahlverfahren wählen und eine R- bzw. eine Flash-Taste besitzen.

Anschluss von ISDN-Endgeräten In die am internen ISDN-Bus angeschlossenen ISDN-Endgeräte muss die interne Telefonnummer des jeweiligen Anschlusses als MSN eingetragen werden und nicht die externe Telefonnummer (Mehrfachrufnummer). Siehe in der Bedienungsanleitung für die ISDN-Endgeräte: MSN eintragen. Beachten Sie bitte, dass nicht alle

	im Handel angebotenen ISDN-Endgeräte die von der Telefonanlage bereitgestellten Leistungsmerkmale über ihre Tastenoberfläche nutzen können.
Anzeige der Telefonnummer des Anrufers	Voraussetzung für diese Leistung ist ein geeignetes Telefon. Die Übermittlung der Telefonnummer muss vom Anrufer freigeschaltet sein.
Anzeige und Ausgabe der Verbindungsdaten	Die Speicherung der Datensätze lässt sich über die Konfiguration für bestimmte oder auch alle Endgeräte festlegen. In der Werkseinstellung werden alle kommenden externen Verbindungen und alle von Ihnen eingeleiteten externe Gespräche gespeichert.
AOC-D	Anzeige während und am Ende der Verbindung.
AOC-D/E	Advice of Charge-During/End.
AOC-E	Anzeige nur am Ende der Verbindung.
ARP	Address Resolution Protocol
asynchron	Übertragungsverfahren, bei dem die Zeitabstände zwischen übertragenen Zeichen unterschiedlich lang sein können. Dadurch können Geräte miteinander kommunizieren, die nicht in gleichen Zeittakten arbeiten. Anfang und Ende der übertragenen Zeichen müssen durch Start- und Stop-Bits gekennzeichnet sein – im Gegensatz zu synchron.
ATM	Asynchronous Transfer Mode
Aufmerksamkeitston	Einblenden eines akustischen Signals in laufende Telefongespräche z. B. beim Anklopfen.
Aufschalten	Möglichkeit bei Telefonanlagen, sich in eine bestehende Gesprächsverbindung einzublenden. Dies wird akustisch durch einen Aufmerksamkeitston signalisiert.
Authentication	Überprüfung der Identität des Nutzers (Authentisierung).
Authorization	Auf der Basis der Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
Automatische Amtsholung	Nach Abheben des Hörers an eines Telefons kann die Telefonnummer des Externteilnehmers sofort gewählt werden.
Automatische Wahlwiederholung	Leistungsmerkmal von Endgeräten. Im Besetzfall erfolgen automatisch mehrere Anwahlversuche.

Automatischer Abbau der Internetverbindung (ShortHold) Sie haben die Möglichkeit, ShortHold einzuschalten. Dabei legen Sie eine Zeit fest, nach der eine bestehende Verbindung getrennt wird, wenn kein Datentransfer mehr stattfindet. Wenn Sie hier die Zeit 0 eintragen ist ShortHold ausgeschaltet.

Automatischer Rückruf Komfortleistung bei Telefonen: Per Tastendruck oder Kennziffer fordert der Anrufer von einem besetzten Endgerät einen Rückruf an. Ist der gewünschte Teilnehmer nicht an seinem Platz oder kann er das Gespräch nicht annehmen, wird er automatisch mit dem Anrufer verbunden, sobald er sein Telefon das nächste Mal benutzt hat und den Hörer wieder auflegt.

Automatischer Rückruf bei Besetzt Diese Funktion ist nur mit Telefonen nutzbar, die Nachwahl erlauben! Ein automatischer Rückruf ist aus einer Rückfrageverbindung nicht möglich.

Automatischer Rückruf bei Besetzt (CCBS) Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie jedoch immer den Besetztton. Wenn Sie eine Mitteilung erhielten, dass der gewünschte Teilnehmer das Gespräch beendet hat, wären Ihre Chance, ihn zu erreichen sehr gut. Mit dem "Rückruf bei Besetzt" können Sie den besetzten Gesprächspartner sofort erreichen, wenn dieser am Ende seines Gespräches den Hörer auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut. Ein interner "Rückruf bei Besetzt" wird automatisch nach 30 Minuten gelöscht. Der externe "Rückruf bei Besetzt" wird nach einer von der Vermittlungsstelle vorgegebenen Zeit gelöscht (ca. 45 Minuten). Manuelles Löschen vor Ablauf der Zeit ist ebenfalls möglich.

Automatischer Rückruf bei Nichtmelden (CCNR) Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie zwar immer den Freiton, Ihr Partner ist jedoch nicht in der Nähe seines Telefons und hebt nicht ab. Mit dem "Rückruf bei Nichtmelden" können Sie den Teilnehmer sofort erreichen, wenn dieser ein Gespräch beendet hat oder den Hörer seines Telefons abhebt und wieder auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut.

AUX Auxiliary

B-Kanal Basiskanal eines ISDN-Basisanschlusses bzw. Primärmultiplex-anschlusses zur Übertragung von Nutzinformationen (Sprache, Daten). Ein ISDN-Basisanschluss besitzt zwei B-Kanäle und einen D-Kanal. Ein B-Kanal hat eine Datenübertragungsrate von 64 kBit/s.

Durch Kanalbündelung kann mit Ihrem Gateway die Datenübertragungsrate bei einem ISDN-Basisanschluss auf bis zu 128 kBit/s gesteigert werden.

B-Telefonnummer unterdrücken (COLR) COLP/COLR: Connected Line Identification Presentation/Connected Line Identification Restriction = Übermittlung der Telefonnummer des Anrufenden zum Angerufenen einschalten/unterdrücken. Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers unterdrückt. Wird die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt.

Back Route Verify Überprüfung der Rückroute

BACP/BAP Bandwidth Allocation Control Protocols (BACP/BAP nach RFC 2125)

Basisanschluss ISDN-Anschluss, der zwei Nutzkanäle (B-Kanäle) von je 64 KBit/s und einen Steuerkanal (D-Kanal) mit 16 KBit/s umfasst. Die beiden Nutzkanäle können unabhängig voneinander für jeden im T-ISDN angebotenen Dienst genutzt werden. Man kann also z. B. telefonieren und zur gleichen Zeit faxen. Die T-Com bietet den Basisanschluss als Mehrgeräte- oder Anlagenanschluss an.

Bedienerführung Elektronische Bedienungsanleitung, die den Anwender per Display Schritt für Schritt zu gewünschten Funktionen eines Endgeräts wie z. B. Telefon, Anrufbeantworter oder Faxgerät führt (menügeführte Bedienung).

Block Cipher Modes Blockorientierter Verschlüsselungsalgorithmus

Blowfish Ein von Bruce Schneier entwickelter Algorithmus. Es handelt sich um eine block cipher mit einer Blockgrösse von 64 Bit und einem Schlüssel mit variabler Länge (bis 448 Bits).

Bluetooth Bluetooth ist eine drahtlose Übertragungstechnik, die verschiedene Geräte miteinander verbinden kann. Bluetooth ist dabei ein Kabelersatz zum Anschluss verschiedener Geräte, z. B. Notebook, PC, PDA, etc.. Diese Geräte können dank Bluetooth ohne eine feste Verbindung miteinander Daten austauschen. Zum Beispiel können PCs, Notebooks oder PDA Zugang zum Internet oder einem lokalen Netzwerk erlangen. Die Termine eines PDA können mit den Terminen auf dem PC synchronisiert werden, ohne dass hierfür eine Kabelverbindung erforderlich ist. Aufgrund der vielfältigen Anwendungsmöglichkeiten der Bluetooth-Technik werden die einzelnen Verbindungsarten zwischen den Geräten in Profiles unterteilt. Durch

	ein Profile wird der Dienst (die Funktion) festgelegt, den die einzelnen Bluetooth-Clients untereinander nutzen können.
BOD	Bandwith on Demand
BootP	Bootstrap Protocol
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Basic Rate Interface
Bridge	Netzwerkkomponente zum Verbinden gleichartiger Netze. Im Gegensatz zu einem Gateway arbeiten Bridges auf Schicht 2 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.
Broadcast	Broadcasts sind Rundrufe (Datenpakete), die an alle im Netz angeschlossenen Geräte gesendet werden, um Informationen im Netz auszutauschen. Normalerweise gibt es im Netz eine bestimmte Adresse (Broadcast-Adresse), die es allen Geräten ermöglicht, eine Nachricht als Broadcast zu interpretieren.
Browser	Programm zur Darstellung von Inhalten im Internet bzw. WorldWide-Web.
Bus	Ein Medium zur Datenübertragung für alle Geräte im Netz. Die Daten werden über den gesamten Bus verbreitet und von allen Geräten am Bus empfangen.
CA	Certificate Authority
Call Through	Unter Call Through versteht man die Einwahl über einen externen Anschluss in die Telefonanlage und die Weiterwahl aus der Telefonanlage über einen anderen externen Anschluss.
Called Party's Number	Nummer des Angerufenen.
Calling Party's Number	Nummer des Anrufers.
CAPI	Common ISDN Application Programming Interface
CAST	Ein 128-bit Verschlüsselungsalgorithmus mit ähnlicher Funktionalität wie DES. Siehe Block Cipher Modes.

CBC Cipher Block Chaining

CCITT Commite Consultatif International Telegraphique et Telephonique

CD (Call Deflection) Weiterleiten von Anrufen. Mit diesem Leistungsmerkmal haben Sie die Möglichkeit, einen Anruf weiterzuleiten, ohne diesen selbst annehmen zu müssen. Leiten Sie einen Anruf zu einem externen Teilnehmer weiter, tragen Sie die anfallenden Verbindungskosten von Ihrem Anschluss zu dem Ziel der Anrufweiterleitung. Sie können dieses Leistungsmerkmal vom Systemtelefon nutzen, oder von ISDN-Telefonen, die diese Funktion unterstützen (siehe Bedienungsanleitung der Endgeräte). Weitere Hinweise zur Ausführung dieses Leistungsmerkmal mit dem Telefon entnehmen Sie bitte der Bedienungsanleitung.

Certificate Zertifikat

CHAP Challenge Handshake Authentication Protocol

CLID Calling Line Identification (Rufnummernüberprüfung)

Client Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.

CLIP Abkürzung für Calling Line Identification Presentation. Telefonnummernanzeige des Anrufenden.

CLIR Abkürzung für Calling Line Identification Restriction. Zeitweise Unterdrückung der Übermittlung der Telefonnummer des Anrufenden.

COLR Connected Line Identification Restriction (B-Telefonnummer unterdrücken). Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers ermöglicht oder unterdrückt. Ist die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt. Beispiel: Sie haben eine Rufumleitung zu einem anderen Endgerät eingerichtet. Hat dieses Endgerät das Unterdrücken der B-Telefonnummer eingeschaltet, sieht der Anrufende keine Telefonnummer im Display seines Endgerätes.

Configuration Manager Windows-Applikation (ähnlich dem Windows-Explorer), die SNMP-Kommandos benutzt, um die Einstellungen Ihres Gateways abzufragen und vorzunehmen. Die Applikation wurde vor der BRICKware, Version 5.1.3, als DIME Browser bezeichnet.

CRC Cyclic Redundancy Check

CRL	Zertifikatssperrliste, ermöglicht es festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.
CTI	Computer-Telephony Integration. Begriff für die Verbindung zwischen Telefonanlage und Server. Durch CTI können Funktionen der Telefonanlage von einem PC gesteuert bzw. ausgewertet werden.
D-Kanal	Steuerkanal eines ISDN-Basisanschlusses bzw. Primärmultiplexanschlusses. Der D-Kanal hat eine Datenübertragungsrate von 16 kBit/s. Außer dem D-Kanal besitzt jeder ISDN-Basisanschluss zwei B-Kanäle.
Daemon	Programm das im Hintergrund abläuft.
Datagramm	Ein in sich abgeschlossenes Datenpaket, das mit einem Minimum an Protokoll-Overhead im Netz weitergeleitet wird – ohne Quittierungsmechanismus.
Datenkompression	Methode, um übertragene Datenmengen zu verringern. Bei gleicher Übertragungsdauer kann so der Durchsatz erhöht werden. Bekannte Verfahren sind z. B. STAC, VJHC, MPPC.
Datenpaket	Ein Datenpaket dient der Übermittlung von Informationen. Jedes Datenpaket enthält eine vorgeschriebene Anzahl von Zeichen (Informationen und Steuerzeichen).
Datenübertragungsrate	Die Datenübertragungsrate gibt die Anzahl der Informationseinheiten pro Zeitabschnitt an, die zwischen Sender und Empfänger übertragen werden.
Datex-J	Abkürzung für Data Exchange Jedermann. Die Zugangsplattform zu T-Online. Lokale Einwahlknoten in jedem Ortsnetz. In einigen deutschen Großstädten gibt es zusätzliche Hochgeschwindigkeitszugänge über T-Net/T-Net-ISDN.
DCE	Data Circuit-Terminating Equipment
Default Gateway	Bezeichnet die Adresse des Routers, an den sämtlicher Verkehr gesendet wird, der nicht für das eigene Netzwerk bestimmt ist.
Denial-Of-Service Attack	Ein Denial-of-Service (DoS) Angriff ist ein Versuch, ein Gateway oder einen Host in einem LAN mit gefälschten Requests zu überfluten, so dass diese völlig überlastet sind. Das bedeutet das System oder ein bestimmter Dienst kann nicht mehr betrieben werden.
DES	Data Encryption Standard

DFÜ	Datenfernübertragung
DHCP	Dynamic Host Configuration Protocol
DIME	Desktop Internetworking Management Environment
DIME Browser	Alte Bezeichnung für Configuration Manager.
DLCI	In einem Frame Relay Netzwerk bezeichnet ein DLCI eine vituelle Verbindung eindeutig. Beachten Sie, dass ein DLCI nur für das lokale Ende der Punkt-zu-Punkt-Verbindung von Bedeutung ist.
DMZ	DeMilitarized Zone
DNS	Domain Name System
DOI	Domain Of Interpretation
Domäne	Ein Domäne ist ein logischer Zusammenschluss von Geräten in einem Netzwerk. Im Internet Teil einer Namenshierarchie (z. B. bintec.de).
Dotted Decimal Notation	Die syntaktische Repräsentation für eine 32-Bit-Ganzzahl, die in vier 8-Bit-Zahlen in dezimaler Schreibweise geschrieben ist und durch Punkt unterteilt ist. Sie wird zur Darstellung von IP-Adressen im Internet verwendet, z. B. 192.67.67.20
Downstream	Datenübertragungsrate vom ISP zum Kunden.
DSA (DSS)	Digital Signature Algorithm (Digital Signature Standard).
DSL/xDSL	Digital Subscriber Line
DSS1	Digital Subscriber Signalling System
DSSS	Direct Sequence Spread Spectrum ist eine Funktechnologie, die ursprünglich für den militärischen Bereich entwickelt wurde und eine hohe Störsicherheit bietet, weil das Nutzsignal auf einen breiten Bereich gespreizt wird. Das Signal wird mittels einer Spreizsequenz oder Chipping Code, bestehend aus 11 Chips auf 22MHz Breite gespreizt. Selbst wenn ein oder mehr Chips in der Übertragung gestört sind, kann aus den restlichen Chips die Information zuverlässig zurückgewonnen werden.
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi Frequency (Tonfrequenzwahlsystem)

Durchwahl Leistungsmerkmal von größeren Telefonanlagen am Anlagenanschluss: Die Nebenstellen können gezielt von Extern angerufen werden.

Durchwahlbereich Siehe Rufnummernband

Durchwahlnummer Eine Durchwahlnummer (Extension) ist eine interne Rufnummer für ein Endgerät oder ein Subsystem. Bei Anlagenanschlüssen ist die Durchwahlnummer in der Regel eine Rufnummer aus dem vom Telefonanbieter zugeteilten Rufnummernband. Bei Mehrgeräteanschlüssen kann es die MSN oder ein Teil der MSN sein.

Dynamische IP Adresse Im Gegensatz zu einer statischen IP Adresse wird die dynamische IP Adresse temporär per DHCP zugeordnet. Netzwerk Komponenten wie Web-Server oder Drucker besitzen in der Regel statische IP Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP Adressen.

E-Mail Electronic Mail

E1/T1 E1: Europäische Variante des ISDN-Primärmultiplexanschlussesmit 2,048 MBit/s, die auch als E1-System bezeichnet wird.

EAZ Endgeräteauswahlziffer

ECB Electronic Code Book mode

ECT Explizit Call Transfer = Externes Vermitteln.Mit diesem Leistungsmerkmal können zwei externe Verbindungen vermittelt werden, ohne die beiden B-Kanäle des Amtsanschlusses zu blockieren.

Eigene Telefonnummer für das nächste Gespräch festlegen Falls Sie z. B. am späten Abend aus Ihrem privaten Bereich - vielleicht dem Wohnzimmer - noch geschäftlich telefonieren wollen, können Sie Ihre geschäftliche Telefonnummer für dieses Gespräch als gehende Mehrfachrufnummer (MSN) definieren. Der Vorteil liegt zum einen darin, dass die Verbindung unter der ausgewählten MSN kostenmäßig erfasst wird und zum anderen kann Ihr Gesprächspartner Sie an der übermittelten MSN erkennen. Bevor Sie eine externe Wahl beginnen, können Sie festlegen, welche Ihrer Telefonnummern zur Vermittlungsstelle und zum externen Gesprächspartner mitgesendet werden soll. Die Auswahl erfolgt über den Telefonnummern-Index.

Eigene Telefonnummer unterdrücken Temporäres Ausschalten der Übermittlung der eigenen Telefonnummer.

Einstellungen zu- Ein Reset der Geräte ermöglicht es Ihnen, Ihre Anlage wieder in

rücksetzen (Reset) einen definierten Ausgangszustand zu bringen. Dieses kann nötig sein, wenn unerwünschte Konfigurationen zurückgenommen oder das Gerät neu programmiert werden soll.

Einwahlparameter Legen Sie die Einwahlparameter fest, d.h. Sie geben die Einwahlrufnummer des Providers ein und legen fest:

Empfangsabruf Funktion von Faxgeräten, um bei anderen Faxgeräten oder von Faxdatenbanken bereitgestellte Dokumente "abzuholen".

Encapsulation Enkapsulierung von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete über ein Netzwerk zu übertragen, das den ursprünglichen Protokolltyp nicht direkt unterstützt (z. B. NetBIOS über TCP/IP).

Encryption Bezeichnet die Verschlüsselung von Daten, z. B. MPPE.

Erfassen der externen Verbindungsdaten In derWerkseinstellung werden alle, sowohl gehende als auch kommende über Ihre Telefonanlage geführten externen Verbindungen erfasst und in Form von Verbindungsdatensätzen gespeichert.

Erweiterte Wahlwiederholung Eine gewählte Telefonnummer wird in einem Speicher des Telefons “geparkt”. Sie kann später wieder gewählt werden, auch wenn zwischendurch mit anderen Telefonnummern telefoniert worden ist.

ESP Encapsulating Security Payload

ESS Der Extended Service Set bezeichnet mehrere BSS (mehrere Access Points) die ein einzelnes logisches Funknetz bilden.

Ethernet Ein lokales Netzwerk, das alle Geräte im Netz (Rechner, Drucker, etc.) über ein Twisted-Pair- oder Koaxialkabel verbindet.

Ethernet-Anschlüsse Die 4 Anschlüsse sind gleichberechtigt über einen internen Switch herausgeführt. An die Anschlussbuchsen können Netzwerkclients direkt angeschlossen werden. Die Ports sind als 100/BaseT vollduplex, autosensing, auto MDIX abwärtskompatibel zu 10/Base T realisiert. Hier können IP-Softclients mit SIP-Standard auf PCs mit Netzwerkkarte oder bis zu 4 SIP-Telefone direkt angeschlossen werden.

Eumex Recovery Sollte während des Ladens einer neuen Firmware die Stromversorgung der Telefonanlage unterbrochen werden, sind alle Funktionen der Telefonanlage gelöscht.

Euro-ISDN Harmonisiertes, in Europa standardisiertes ISDN, beruhend auf dem Signalisierungsprotokoll DSS1, zu dessen Einführung sich Netzbe-

treiber in über 20 europäischen Staaten verpflichtet haben. In Deutschland ist das Euro-ISDN - nach dem nationalen Vorläufersystem 1 TR6 - inzwischen eingeführt.

Eurofile-Transfer Kommunikationsprotokoll für den Austausch von Dateien zwischen zwei PCs über ISDN mittels ISDN-Karte (File-Transfer) oder über dafür vorbereitete Telefone oder Telefonanlagen.

Fall Back: Priorität der Internet-Provider-Einträge Die Priorität der Internet-Provider-Einträge wird nach der Reihenfolge festgelegt, in der sie in die Liste eingetragen werden. Der erste Eintrag einer DSL-Verbindung ist der Standardzugang. Sollte über den Standardzugang nach einer vorgegebenen Anzahl von Versuchen, kein Verbindungsaufbau möglich sein, wird die Verbindung über den zweiten Eintrag und die folgenden Einträge versucht. Wenn auch der letzte Eintrag auf der Liste nicht zu einem erfolgreichen Verbindungsaufbau führt, wird der Vorgang bis zu einer erneuten Anfrage abgebrochen. Wenn der Fall Back eintritt, und alle übrigen ISP's nur durch Wahlverbindungen zu erreichen sind, können beide B-Kanäle belegt sein. Im Falle einer Kanalbündelung sind Sie dann für die Dauer dieser Verbindung nicht zu erreichen.

Fax Kurzform für Telefax.

Fernabfrage Anrufbeantworterfunktion. Aus der Ferne Nachrichten abhören, meist in Verbindung mit Möglichkeiten wie Nachrichten löschen oder Ansagen ändern.

Ferndiagnose/Fernwartung Einige Endgeräte und Telefonanlagen werden komfortabel von T-Service Stützpunkten aus über die Telefonleitung betreut bzw. gewartet. Spart in vielen Fällen den Einsatz eines Servicetechnikers vor Ort.

Feststation Zentraleinheit von schnurlosen Telefongeräten. Es gibt zwei verschiedene Ausführungen: Die einfache Feststation dient zum Aufladen der Handgeräte. Bei den so genannten Komforttelefonen ist die Feststation gleichzeitig als Telefon nutzbar, die Handgeräte werden über separate Ladestationen aufgeladen.

Feststellen böswilliger Anrufer (Fangen) Dieses Leistungsmerkmal müssen Sie bei der T-Com beauftragen. Dort wird man Sie auch über die weitere Vorgehensweise informieren. Wenn Sie während eines Gespräches oder nach Beendigung des Gespräches durch den Anrufer (Sie hören den Besetzt-Ton aus der Vermittlungsstelle) die Kennziffer 77 wählen, wird die Telefonnummer des Anrufers in der Vermittlungsstelle gespeichert. ISDN-Telefone können für dieses Leistungsmerkmal auch eigene Funktionen nutzen. Weitere Hinweise zur Ausführung dieser Funktion ent-

	nehmen Sie bitte der Bedienungsanleitung.
Festverbindung	Standleitung (leased line)
FHSS, Frequency Hopping Spread Spectrum	Frequenzspreizung wird in einem FHSS System durch ständig nach bestimmten Sprungmustern wechselnde Frequenzen erreicht. Im Gegensatz zu DSSS Systemen gibt es hier keine fest eingestellte Frequenz, sondern einstellbare Sprungmuster (hopping patterns). Die Frequenz wird innerhalb einer Sekunde sehr häufig gewechselt.
File-Transfer	Datenübertragung von einem Computer zu einem anderen, z. B. nach dem Eurofile-Transfer-Standard.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Anhand dieser Kriterien wird ein Paket aus dem Datenstrom ausgesondert. Mit einem so bestimmten Paket kann dann in spezifischer Weise verfahren werden. Zu diesem Zweck wird mit dem Filter eine bestimmte Aktion verbunden. Dadurch entsteht eine Filterregel.
Firewall	Bezeichnet die Summe der Schutzmechanismen für das lokale Netzwerk gegen Zugriffe von außen. Mit Ihrem Gateway stehen Schutzmechanismen wie NAT, CLID, PAP/CHAP, Access-Listen etc. zur Verfügung.
Firmware	Software Code, der alle Funktionen eines Gerätes beinhaltet. Dieser Code wird in einen PROM (Programmable Read Only Memory) geschrieben und bleibt dort auch nach Abschalten des Gerätes erhalten. Firmware kann durch den Benutzer erneuert werden, wenn eine neue Software Version verfügbar ist (Firmware Upgrade).
First-Level Domain	Englische Bezeichnung für den letzten Teil eines Namens im Internet. Bei www.t-com.de lautet die First-Level Domain de und bezeichnet in diesem Fall Deutschland.
Flash-Taste	Die Flash-Taste bei Telefonen entspricht der R-Taste. R ist die Abkürzung für Rückfrage. Die Taste unterbricht die Leitung für einen kurzen Moment, um bestimmte Funktionen wie z. B. Rückfrage über die Telefonanlage einzuleiten.
Follow-me	Leistungsmerkmal von Telefonanlagen zur Rufumleitung von Gesprächen am Zieltelefon.
Fragmentierung	Prozess, durch den ein IP-Datagramm in kleiner Teile getrennt wird, um die Bedingungen eines physikalischen Netzes zu erfüllen. Der umgekehrte Prozess wird Reassembly genannt.

Frame	Einheit der Information, die über eine Datenverbindung gesendet wird.
Frame Relay	Eine Packet Switching Methode, die kleinere Pakete und weniger Fehlerprüfung beinhaltet als das traditionelle Packet Switching wie X.25. Aufgrund seiner Eigenschaften wird Frame Relay für schnelle WAN-Verbindungen mit dichtem Traffic verwendet.
Freecall	Telefonnummer. Bisher Service 0130. Seit dem 1. Januar 1998 werden diese Telefonnummern auf freecall 0800 umgestellt.
Freisprechen	Ermöglicht freihändiges Telefonieren bei Telefonen mit eingebautem Mikrofon und Lautsprecher. Weitere Personen im Raum können so am Gespräch teilnehmen.
FTP	File Transfer Protocol
Full Duplex	Betriebsart, bei der beide Kommunikationspartner gleichzeitig bidirektional kommunizieren können.
Funktionstasten	Mit Telefonnummern oder Netzfunktionen belegbare Tasten an Telefonen.
G.991.1	Datenübertragungsempfehlung für HDSL
G.991.2	Datenübertragungsempfehlung für SHDSL
G.992.1	Datenübertragungsempfehlung für ADSL Siehe auch G.992.1 Annex A und G.992.1 Annex B.
G.992.1 Annex A	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex A
G.992.1 Annex B	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex B
G.SHDSL	Siehe G.991.2.
Gateway	Aus-/Einfahrt, Übergangspunkt
Gehende Durchwahlsignalisierung	Die "gehende Durchwahlsignalisierung" ist für interne Anschlüsse am Anlagenanschluss vorgesehen, denen keine explizite Durchwahl zugeordnet wurde. Bei einem Anruf nach extern wird die unter gehende Durchwahlsignalisierung eingetragene Durchwahlnummer mit gesendet.
Gehende Telefonnummer	Sofern Sie die Übermittlung Ihrer Telefonnummern nicht unterdrückt haben und das Telefon Ihres Gesprächspartners die CLIP-Funktion unterstützt, kann Ihr Gesprächspartner die Telefonnummer des An-

schlusses, von dem aus Sie telefonieren, im Display seines Telefons sehen. Diese bei einem Ruf nach extern übermittelte Telefonnummer wird als gehende Telefonnummer bezeichnet.

Gesprächskostenkonto Sie können hier für einen Teilnehmer ein "Gesprächskostenkonto" einrichten. Jedem Teilnehmer kann damit auf seinem persönlichen "Gesprächskostenkonto" eine maximal zur Verfügung stehende Anzahl von Einheiten in Form eines Limits zugeteilt werden. Damit Einheiten abgebucht werden, ist "Kostenlimit" aktiv zu schalten. Sind die Einheiten verbraucht, sind keine Gespräche nach extern mehr möglich. Interne Gespräche können jederzeit weiter geführt werden. Die Abbuchung des Kontos erfolgt jeweils nach Beendigung eines Gespräches.

GRE Generic Routing Encapsulation

Half Duplex Bidirektionale Kommunikationmethode, bei der zu einem Zeitpunkt nur gesendet oder empfangen werden kann. Wird auch Simplex genannt.

Halten einer Verbindung Ein Telefongespräch auf Wartestellung schalten, ohne die Verbindung zu verlieren (Rückfragen/Makeln).

Halten in der Telefonanlage Bei den Leistungsmerkmalen "Während eines Gespräches einen weiteren Gesprächspartner anrufen" und "Mit zwei Gesprächspartnern abwechselnd sprechen" (Makeln) werden beide B-Kanäle des ISDN-Anschlusses benötigt. Über den zweiten B-Kanal Ihrer Telefonanlage sind Sie dann von extern nicht erreichbar und können selbst nicht extern telefonieren. In dieser Einstellung hört ein gehaltener externer Gesprächspartner dieWartemusik der Telefonanlage.

Handgerät Mobile Komponente bei schnurlosen Telefongeräten. Bei digitaler Übertragung kann auch zwischen den Handgeräten telefoniert werden (DECT).

hashing Der Vorgang des Ableitens einer Nummer, hash genannt, von einer Zeichenfolge. Ein Hash ist im allgemeinen viel kürzer als der Textfluss, von dem er abgeleitet wurde. Der Hashing-Algorithmus ist so gestaltet, dass mit ziemlich geringer Wahrscheinlichkeit ein Hash generiert wird, der mit einem anderen Hash, der aus einer Textfolge mit unterschiedlicher Bedeutung generiert wurde, übereinstimmt. Verschlüsselungsvorrichtungen benutzen Hashing, um sicherzustellen, dass Eindringlinge übermittelte Nachrichten nicht verändern können.

HDLC High Level Data Link Conrol

HDSL	High Bit Rate DSL
HDSL2	High Bit Rate DSL, Version 2
Headset	Kombination aus Kopfhörer und Mikrofon als nützliche Hilfe für alle, die viel telefonieren müssen und dabei die Hände für Notizen frei haben wollen.
Heranholen von Rufen (Pick up)	Ein externer Anruf wird nur bei Ihrem Kollegen signalisiert. Da Sie sich in verschiedenen Teams befinden, ist das nicht verwunderlich. Sie können nun verschiedene Gruppen von Teilnehmern bilden, in denen das Heranholen Rufen möglich ist. Ein Ruf kann nur von Teilnehmern/Endgeräten der gleichen Pick up Gruppe herangeholt werden. Das Zuordnen der Teilnehmer in Pick up Gruppen ist unabhängig von den jeweiligen Einstellungen in der Team-Anrufzuordnung Tag und Nacht.
HMAC	Hashed Message Authentication Code
HMAC-MD5	Hashed Message Authentication Code - benutzt den Message - Digest-Algorithmus Version 5.
HMAC-SHA1	Hashed Message Authentication Code - benutzt den Secure-Hash-Algorithm Version 1.
Hook-Flash	Die Nutzung der Komfortleistungen Rückfragen, Makeln, Dreierkonferenz im T-Net und bestimmter Leistungsmerkmale einiger Telefonanlagen sind nur mit der Hook-Flash-Funktion (langer Flash) der Signaltaste am Telefon möglich. Bei modernen Telefonen ist diese Taste mit "R" bezeichnet.
Hörerlautstärke	Regelung der Lautstärke im Telefonhörer.
Host	Computer, der Dienste in einem Rechnernetz zur Verfügung stellt.
Host-Name	Bezeichnet in IP-Netzen einen Namen, der anstelle einer zugehörigen Adresse benutzt wird. Ein Host-Name besteht aus einer ASCII-Zeichenfolge, die den Host eindeutig kennzeichnet.
Host-Route	Route zum einen einzelnen Host.
HSDPA	High Speed Downlink Packet Access (Datenübertragungsverfahren des Mobilfunkstandards UMTS).
HTTP	HyperText Transfer Protocol
Hub	Netzwerkkomponente, mit der mehrere Netzwerkkomponenten zu

	einem lokalen Netz zusammengeschlossen werden (sternförmig).
IAE	ISDN-Anschlusseinheit ISDN-Anschlussdosen.
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Das Institute of Electrical and Electronics Engineers (IEEE). Ein großer weltweiter Zusammenschluss von Ingenieuren. Arbeitet ständig an Standards und Normen, um das Zusammenspiel verschiedenster Geräte zu gewährleisten.
IETF	Internet Engineering Task Force
IGMP	Internet-Group-Management-Protokoll, dient zur Organisation von Multicast-Gruppen.
IKE	Internet-Key-Exchange-Protokoll dient der automatischen Schlüsselverwaltung für IPsec.
Index	Der Index von 0...9 ist fest vorgegeben. Jede eingetragene externe Mehrfachrufnummer wird einem Index zugeordnet. Diesen Index benötigen Sie beim Einrichten von Leistungsmerkmalen über die Kennziffern eines Telefons, z. B. Einrichten einer "Anrufweiterschaltung in der Vermittlungsstelle" oder "Telefonnummer für das nächste externe Gespräch festlegen".
Infrastruktur Modus	Ein Netzwerk im Infrastruktur Modus ist ein Netzwerk, das mindestens einen Access Point als zentrale Kommunikations- und Steuerstelle beinhaltet. 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 solches Netzwerk wird auch BSS (Basic Service Set) genannt, ein Netzwerk, das aus mehreren BSS besteht wird ESS (Extended Service Set) genannt. Die meisten Funknetze arbeiten im Infrastruktur Modus, um Verbindung mit dem verkabelten Netz herzustellen.
Interne Telefonnummern	Ihre Telefonanlage verfügt über einen festen internen Telefonrufnummernplan.
Internet	Das Internet besteht aus einer Reihe von regionalen, lokalen und Universitätsnetzen. Für Datenübertragung im Internet wird das Protokoll IP verwendet.
Internet Time Sha-	Ermöglicht mehreren Nutzern gleichzeitig über eine ISDN-

ring	Verbindung im Internet zu surfen. Die Informationen werden zeitversetzt von den einzelnen Computern abgefragt.
Interngespräche	Kostenfreie Verbindung zwischen Endgeräten einer Telefonanlage.
Internkennziffer übertragen	Erhalten Sie bei Abwesenheit an Ihrem Anschluss einen internen Anruf z. B. vom Teilnehmermit der internen Telefonnummer 22, wird seine interne Telefonnummer in der Anruferliste Ihres Telefons gespeichert. Da Ihr Anschluss aber werkseitig auf automatische Amtsholung eingestellt ist, müssten Sie für einem Rückruf zunächst ** wählen, um den internen Wählton zu erhalten, und dann die 22. Ist "Internkennziffer übertragen" aktiv, wird ** vor die 22 gesetzt und der Rückruf kann automatisch aus der Anruferliste heraus erfolgen.
Internrufton	Besondere Signalisierung an Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.
Intranet	Lokales, unternehmensinternes Computernetz auf der Basis von Internettechnologien, das die gleichen Internetdienste bereitstellt, wie z. B. E-Mail-Versand und Homepages.
IP	Internet Protocol
IP-Adresse	In einem IP-Netzwerk der erste Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 192.168.1.254. Siehe auch Netzmaske.
IPComP	IP payload compression
IPCONFIG	Ein Hilfsmittel, das unter Windows Computern verwendet wird, um die eigenen IP Einstellungen zu überprüfen oder zu ändern.
IPoA	IP over ATM
ISDN	Integrated Services Digital Network
ISDN-Adresse	Die Adresse eines ISDN-Gerätes, welche aus einer ISDN-Nummer besteht gefolgt von weiteren Ziffern, die sich auf ein spezifisches Endgerät beziehen, z. B. 47117.
ISDN-Basisanschluss	Teilnehmeranschluss beim ISDN. Der Basisanschluss besteht aus zwei B-Kanälen und einem D-Kanal. Außer dem Basisanschluss gibt es noch den Primärmultiplexanschluss. Die Schnittstelle zum Teilnehmer wird über den sogenannten So-Bus geschaffen.
ISDN-BRI	ISDN Basic Rate Interface

ISDN-Dynamic Dieses Leistungsmerkmal setzt die Installation des T-ISDN Speedmanagers voraus! Wenn Sie gerade im Internet surfen, und zum Download zwei B-Kanäle nutzen, sind Sie telefonisch von Extern nicht mehr erreichbar. Da die Signalisierung eines weiteren Anrufes über den D-Kanal erfolgt, hat Ihre Telefonanlage, je nach Einstellung, die Möglichkeit, einen B-Kanal gezielt abzuschalten und Sie können das Gespräch annehmen.

ISDN-Intern/-Extern Alternative Bezeichnung für den S0-Bus.

ISDN-Karte Adapter für den Anschluss eines PCs an den ISDN-Basisanschluss. Technisch unterscheidet man aktive und passive Karten. Aktive ISDN-Karten verfügen über einen eigenen Prozessor, der Kommunikationsvorgänge unabhängig vom PC-Prozessor abwickelt und somit keine Ressourcen benötigt. Eine passive ISDN-Karte hingegen nutzt Ressourcen des PCs.

ISDN-Login Funktion Ihres Gateways. Über ISDN-Login ist Ihr Gateway fernkonfigurier- und wartbar. ISDN-Login funktioniert bereits bei Gateways im Auslieferungszustand, sobald sie mit einem ISDN-Anschluss verbunden und so über eine Rufnummer erreichbar sind.

ISDN-Nummer Die Netzwerkadresse der ISDN-Schnittstelle, z. B. 4711.

ISDN-PRI ISDN Primary Rate Interface

ISDN-Router Ein Router, der nicht über Netzwerkanschlüsse verfügt, aber gleiche Funktionen zwischen PC, ISDN und dem Internet bereitstellt.

ISO International Standardization Organization

ISP Internet Service Provider

ITU International Telecommunication Union

IWV Abkürzung für Impulswahlverfahren. Herkömmliches Wahlverfahren im Telefonnetz. Wählziffern werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Das Impulswahlverfahren wird durch das Mehrfrequenzwahlverfahren (MFV) abgelöst.

Kalender Mit der Zuweisung eines Kalender erfolgt die Umschaltung zwischen den Anrufzuordnungen Tag und Nacht. Für jeden Wochentag kann eine beliebige Tag-/ Nachtumschaltzeit gewählt werden. Ein Kalender verfügt über jeweils vier Schaltzeiten, die jedem einzelnen Wochentag gezielt zugewiesen werden können.

Kanalbündelung Channel Bundling

Key Escrow Hinterlegte Schlüssel können von der Regierung eingesehen werden. Besonders die U.S.-Regierung schreibt Schlüsselhinterlegung vor, um zu verhindern, dass Verbrechen durch Datenverschlüsselung getarnt werden.

Kombigerät Ist ein analoger Endgeräteanschluss der Telefonanlage als „Multifunktionsport“ für Kombigeräte eingerichtet, werden alle Anrufe unabhängig vom Dienst angenommen. Bei einer Amtsholung über Kennziffern können unabhängig von der Konfigurierung des analogen Anschlusses die Dienstekennungen „analoge Telefonie“ oder „Telefax Gruppe 3“ mit gesendet werden. Bei Wahl der 0 wird die Dienstekennung „analoge Telefonie“ mit gesendet.

Komfortanschluss T-ISDN Basisanschluss mit umfangreichem Leistungsangebot: Anklopfen, Anrufweiterschaltung, Dreierkonferenz, Gesprächskostenanzeige am Ende der Verbindung, Rückfragen/Makeln, Telefonnummernübermittlung. Im Komfortanschluss sind als Standard drei Mehrfachrufnummern enthalten.

Komfortleistungen Leistungsmerkmale der Netze T-Net und T-ISDN wie Anzeige der Telefonnummer des Anrufers, Rückruf bei Besetzt, Anrufweiterschaltung, veränderbare Anschluss-Sperre, veränderbare Telefonnummernsperre, Verbindung ohne Wahl und Übermittlung von Tarifinformationen. Die Verfügbarkeit ist abhängig vom Standard der angeschlossenen Endgeräte.

Konferenzschaltung Leistungsmerkmal von Telefonanlagen: Mehrere interne Gesprächsteilnehmer können gleichzeitig telefonieren. Es sind auch mit externen Gesprächspartnern, Dreierkonferenzen möglich.

Konfiguration der Telefonanlage mit dem PC Eine wichtige Voraussetzung für die erfolgreiche Übertragung Ihrer Konfiguration zur Telefonanlage ist, dass Sie eine Verbindung zwischen PC und Telefonanlage eingerichtet haben. Sie haben die Möglichkeit über die Ethernet-Verbindung LAN.

Konfiguration der Telefonanlage mit dem Telefon Sie können Ihre Telefonanlage - allerdings eingeschränkt - auch mit einem Telefon programmieren. Hinweise zur Programmierung Ihrer Telefonanlage mit dem Telefon entnehmen Sie bitte der beiliegenden Bedienungsanleitung.

Kurzwahl Jeder der bis zu 300 Telefonnummern des Telefonbuches kann ein Kurzwahl-Index (000...299) zugeordnet werden. Diesen Kurzwahl-Index wählen Sie dann anstelle der langen Telefonnummer. Beachten Sie dass über die Kurzwahl gewählte Telefonnummern ebenfalls der Wahlregel unterliegen.

L2TP	Ermöglicht das Tunneln von PPP-Verbindungen.
LAN	Local Area Network (Lokales Netzwerk)
LAPB	Link Access Procedure Balanced
Lauthören	Funktion bei Telefonen mit eingebauten Lautsprechern: Per Tastendruck können im Raum anwesende Personen ein Telefongespräch mithören.
Layer 1	Schicht 1 des ISO-OSI-Modells, die Bitübertragungsschicht.
LCD	Liquid-Crystal Display (Flüssigkristallbildschirm), ist ein Bildschirm, bei dem spezielle Flüssigkristalle zur Bilddarstellung genutzt werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
Lease Time	Unter "Lease Time“ versteht man die Zeit, in der ein Rechner seine ihm zugewiesene IP-Adresse behält, ohne mit dem DHCP-Server ”Rücksprache” halten zu müssen.
Leased Line	Standleitung, eine permanente (stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetzwerk.
Letzter Zugriff	Der letzte Zugriff durch den T-Service wird gespeichert und in der Konfigurierung angezeigt.
LLC	Link Layer Control
MAC-Adresse	Jedes Gerät im Netz ist über eine feste Hardware-Adresse (MAC-Adresse) definiert. Die Netzwerkkarte eines Geräts bestimmt diese weltweit eindeutige Adresse.
Makeln	Makeln erlaubt es, zwischen zwei externen bzw. internen Gesprächspartnern hin- und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
Man-in-the-Middle Attack	Die Verschlüsselung mittels öffentlicher Schlüssel setzt den Austausch der öffentlichen Schlüssel voraus. Während des Austausches kann der ungeschützte Schlüssel leicht abgefangen werden und eröffnet so die Möglichkeit eines "man-in-the-middle"-Angriffs. Der Angreifer kann früh seinen eigenen Schlüssel setzen, so dass ein Schlüssel, der dem "man-in-the-middle" bekannt ist, anstelle des eigentlich gewollten Schlüssels des richtigen Kommunikationspart-

	ners verwendet wird.
MD5	Siehe HMAC-MD5
Mehrfachrufnummer (MSN)	Multiple Subscriber Number
Mehrgeräteanschluss	Point-to-Multipoint (Punkt-zu-Mehrpunkt)
Mehrgeräteanschluss	Basisanschluss im T-ISDN mit standardmäßig drei Telefonnummern und zwei Leitungen. Der Anschluss der ISDN-Endgeräte erfolgt direkt am Netzabschluss (NTBA) oder am ISDN-Internanschluss einer Telefonanlage.
Mehrgeräteanschluss für die Telefonanlage	Ihre von der T-Com mit der Auftragsbestätigung erhaltenen Mehrfachrufnummern tragen Sie in der Konfiguration in die dort vorgesehenen Tabellenfelder ein. In der Regel erhalten Sie drei Mehrfachrufnummern, können jedoch bis zu zehn Telefonnummern je Anschluss beantragen. Mit der Eintragung der Telefonnummern erfolgt neben der Zuordnung zu einem "Index" gleichzeitig die Zuordnung zu einem Team. Beachten Sie bitte, dass alle Telefonnummern zunächst dem Team 00 zugeordnet werden. In das Team 00 wiederum sind werkseitig die internen Telefonnummern 10, 11 und 20 eingetragen. Anrufe von extern werden somit an den in Team00 eingetragenen Anschlüssen mit den internen Telefonnummern 10, 11 und 20 signalisiert.
MFV	Mehrfrequenzwahlverfahren
MIB	Management Information Base
Mikrofonstummschaltung	Taste zum Abschalten des Mikrofons. Der Gesprächspartner am Telefon kann dann die im Raum geführten Rückfragen nicht mithören.
Mitschneiden von Telefongesprächen	Leistungsmerkmal eines Anrufbeantworters. Erlaubt die Aufnahme eines Gespräches auch während des Telefonats.
Mixed Mode	Der Access Point akzeptiert WPA sowie WPA2.
MLPPP	Multilink-PPP
Modem	Modulator/Demodulator
MPDU	MAC Protocol Data Unit - jedes Informationspaket, das auf dem Funkmedium ausgetauscht wird inclusive Management-Frames und fragmentierten MSDUs.

MPPC	Microsoft Point-to-Point Compression
MPPE	Microsoft Point-to-Point Encryption
MSDU	MAC Service Data Unit - ein Datenpaket, ohne Berücksichtigung von Fragmentierung im WLAN.
MSN	Multiple Subscriber Number
MSSID	Siehe SSID
MTU	Maximum Transmission Unit
Multicast	Eine spezifische Form des Broadcasts, bei dem gleichzeitig eine Nachricht an eine definierte Benutzergruppe übertragen wird.
Multiprotokollgateway	Gateway, der mehrere Protokolle routen kann, z. B. IP, X.25 etc.
Music On Hold (MOH,Wartemusik)	Ihre Telefonanlage verfügt über zwei interne Wartemusik-Melodien Bei Auslieferung ist die interne Melodie 1 aktiv. Sie können zwischen den Melodien 1 und 2 wählen oder die Wartemusik inaktiv schalten.
MWI	Übermittlung einer vorliegenden Sprachnachricht aus einer Nachrichtenbox, z. B. T-NetBox oder MailBox an ein entsprechendes Endgerät. Der Nachrichteneingang am Endgerät wird z. B. durch eine Leuchtdiode signalisiert.
NAT	Network Address Translation
NDIS WAN	NDIS WAN ist eine Microsoft-Erweiterung dieses Standards in Bezug auf Wide Area Networking (WAN). Der NDIS WAN CAPI-Treiber erlaubt die Nutzung des ISDN-Controllers als WAN-Karte. Der NDIS WAN Treiber ermöglicht die Nutzung eines DFÜ-Netzwerkes unter Windows. NDIS ist die Abkürzung für Network Device Interface Specification und stellt einen Standard für die Anbindung von Netzwerkkarten (Hardware) an Netzprotokolle (Software) dar.
Nebenstelle	Bezeichnet bei Telefonanlagen das mit der Anlage verbundenen Endgerät (z. B. Telefon). Jede Nebenstelle kann auf die Anlagenleistungen zugreifen und mit anderen Nebenstellen kommunizieren.
NetBIOS	Network Basic Input Output System
Netsurfen	"Entdeckungsreise" auf der Suche nach interessanten Angeboten in weit verzweigten Datennetzen wie T-Online. Vor allem bekannt aus

der Welt des Internets.

Netz-Direkt (Keypad-Funktionen) Mit Hilfe der Funktion "Netz-Direkt" (Keypad) können Sie durch die Eingabe einer Tastenfolge auch von Ihrem ISDN- oder analogen Telefon aus aktuelle T-ISDN Funktionen nutzen. Fragen Sie hierzu beim Kundenberater der T-Com nach und lassen Sie sich die entsprechenden Kennziffern geben (z. B. Anrufweiterschaltung in der Vermittlungsstelle).

Netzabschluss (NTBA) Mit Netzabschluss bezeichnet man in der Telekommunikation den Punkt, an dem einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt wird.

Netzadresse Eine Netzadresse bezeichnet die Adresse eines gesamten lokalen Netzwerks.

Netzmaske In einem IP-Netzwerk der zweite Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 255.255.255.0. Siehe auch IP-Adresse.

Netzwerk Ihre Telefonanlage verfügt über einen DSL-Router, damit ein oder mehrere PCs schnell im Internet surfen und downloaden können.

NMS Network Management Station

Notizbuchfunktion Während eines Telefonats kann eine Telefonnummer in den Zwischenspeicher des Telefons eingegeben werden, um sie später anzuwählen.

Notrufnummern Der Fall der Fälle tritt ein und Sie müssen dringend Polizei, Feuerwehr oder eine andere Telefonnummer telefonisch erreichen. Zu allem Überfluss sind alle Anschlüsse belegt. Sie haben jedoch Ihrer Telefonanlage die Telefonnummern mitgeteilt, die im Notfall erreichbar sein müssen. Wählen Sie nun eine dieser Notrufnummern, wird dies von der Telefonanlage erkannt und automatisch ein B-Kanal des T-ISDN für Ihren Notruf freigeschaltet. Notrufe unterliegen keinen Einschränkungen durch Konfigurationen. Ist für einen Anschluss "Telefonieren mit Vorwahlziffer eingestellt", wird der interne Anschluss belegt. Wählen Sie, um nach extern telefonieren zu können, vorab die 0 und dann die gewünschte Notrufnummer.

NT Network Termination

NTBA Network Termination for Basic Access

NTP Network Time Protocol

Nutzkanal Entspricht einer Telefonleitung im T-Net. Beim T-ISDN sind im Basisanschluss zwei Nutzkanäle mit je 64 KBit/s Datenübertragungsrate enthalten.

OAM Operations and Maintenance

Offline Vom englischen "off-line" (ohne Verbindung). Verbindungsloser Betriebszustand, z. B. des PCs.

Online Vom englischen “on-line” (in Verbindung). Zum Beispiel der Zustand der Verbindung eines PCs mit Datennetzen oder beim Datenaustausch von PC zu PC.

Online Pass Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis für das Internet. Mit dem OnlinePass kann sich ein Internetnutzer als Kunde bei einem Unternehmen ausweisen.

Online-Banking Begriff für die elektronische Kontoführung z. B. über T-Online.

Online-Dienste Leistungen, die über Kommunikationsdienste wie T-Online und Internet rund um die Uhr verfügbar sind.

Ortsvermittlungsstelle (OVst) Vermittlungsknoten eines öffentlichen Telefon-Ortsnetzes, der den Anschluss von Endsystemen unterstützt.

OSI-Modell OSI = Open System Interconnection (offene Kommunikationssysteme)

OSPF Open Shortest Path First

PABX Private Automatic Branch Exchange (Nebenstellenanlage)

Paketvermittlung Packet Switching

PAP Password Authentication Protocol

Parken Das Gespräch wird in der Vermittlungsstelle vorübergehend gehalten. Prinzipieller Unterschied zum Halten: Das Gespräch wird unterbrochen, der Hörer kann z. B. aufgelegt werden. Anwendbar für Makeln. Möglich im T-Net, im T-ISDN und bei Telefonanlagen. Das Endgerät muss mit MFV und R-Taste ausgestattet sein.

PBX Private Branch Exchange

PCMCIA Die PCMCIA (Personal Computer Memory Card International Association) ist eine 1989 gegründete Industrievereinigung, die Kreditkartengroße I/O Karten vertritt, wie z. B. WLAN Karten.

Peer	Endpunkt einer Kommunikation in einem Computernetzwerk.
PGP	Pretty Good Privacy
PH	Packet Handler
PIN	Persönliche Identifikationsnummer
Ping	Packet Internet Groper
PKCS	Public-Key Cryptography Standards
Port	Ein-/Ausgang
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPP-Authentisierung	Sicherheitsmechanismus. Authentisierung durch ein Passwort im PPP.
PPPoA	Point to Point Protocol over ATM
PPPoE	Point to Point Protocol over Ethernet
PRI	Primary Rate Interface
Primärmultiplexanschluss	Teilnehmeranschluss beim ISDN. Der Primärmultiplexanschluss besteht aus einem D-Kanal und 30 B-Kanälen (Europa). (In Amerika: 23 B-Kanäle und ein D-Kanal.) Außer dem Primärmultiplexanschluss gibt es noch den ISDN-Basisanschluss.
Protokoll	Protokolle werden verwendet, um Art und Weise eines Informationsaustausches zwischen zwei Systemen zu definieren. Protokolle steuern und regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen (Decodierung, Adressierung, Wegwahl im Netz, Kontrollmechanismen, etc.).
Proxy ARP	ARP = Address Resolution Protocol
Prüfsummenfeld	Frame Check Sequence (FCS)
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
Punkt-zu-Mehrpunkt	Point-to-Multipoint

Punkt-zu-Punkt Point-to-Point

PVID Port VLAN ID

QoS Quality of Service ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen.

R-Taste Telefone, die mit der R-Taste (Rückfragetaste) ausgestattet sind, eignen sich auch für den Anschluss an Telefonanlagen. Bei modernen Telefonen löst die R-Taste die Hook-Flash-Funktion aus. Sie ist für die Nutzung der Leistungsmerkmale im T-Net wie Rückfragen/Makeln und Dreierkonferenz erforderlich.

RADIUS Remote Authentication Dial-In User Service

RADSL Rate-adaptive Digital Subscriber Line

RAS Remote Access Service

Raumüberwachung (akustisch) Um das Leistungsmerkmal "Raumüberwachung" nutzen zu können, muss in dem zu überwachenden Raum das Telefon über eine Kennziffer zur Raumüberwachung freigegeben und der Hörer abgehoben oder Freisprechen eingeschaltet sein. Legen Sie den Hörer des Telefons im zu überwachenden Raum auf oder schalten Sie das Freisprechen aus, ist die Raumüberwachung beendet und das Leistungsmerkmal wieder ausgeschaltet.

Raumüberwachung von externen Telefonen Mit dieser Funktion kann eine Raumüberwachung von einem externen Telefon aus erfolgen.

Raumüberwachung von internen Telefonen Sie können von einem internen Telefon Ihrer Telefonanlage einen Raum akustisch überwachen. Die Einrichtung erfolgt mit den in der Bedienungsanleitung beschriebenen Telefonprozeduren. Lesen Sie bitte zu den hier beschriebenen Funktionen auch die entsprechenden Hinweise in der Bedienungsanleitung.

Real Time Clock (RTC) Hardware-Uhr mit Pufferbatterie

Real Time Jitter Control Hier können Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert werden, damit die Sprachpakete nicht blockiert werden.

Remote Entfernt, nicht lokal.

Remote Access Nicht lokaler Zugriff, siehe Remote.

Remote-CAPI bintec-eigene Schnittelle für CAPI.

Repeater Ein Gerät, das elektische Signale von einer Kabelverbindung zur anderen überträgt, ohne Routing-Entscheidungen zu treffen oder Paketfilterung vorzunehmen. Vergleiche Bridge und Router.

RFC Spezifikationen, Vorschläge, Ideen und Richtlinien, das Internet betreffend, werden in Form von so genannten RFCs (Request For Comments) veröffentlicht.

Rijndael (AES) Rijndael (AES) wurde als AES ausgewählt aufgrund der schnellen Schlüsselgenerierung, der niedrigen Speichererfordernisse und der hohen Sicherheit gegenüber Angriffen. Weitere Informationen zu AES, siehe http://csrc.nist.gov/encryption/aes.

RIP Routing Information Protocol

RipeMD 160 RipeMD 160 ist eine kryptographische Hash-Funktion mit 160 Bit. Es gilt als sichereren Ersatz für MD5 und RipeMD.

RJ45 Stecker bzw. Buchse für maximal acht Adern. Anschluss für digitale Endgeräte.

Roaming In einem mehrzelligen WLAN können sich Clients frei bewegen und sich bei der Bewegung durch Funkzellen von einem Access Point abmelden und neu auf einem anderen Access Point anmelden, ohne dass der Benutzer dies bemerkt. Diese Fähigkeit wird Roaming genannt.

Round-Robin Rundlauf-Verfahren

Router Geräte, die unterschiedliche Netze auf der Schicht 3 des OSI-Modells verbinden und Informationen von einem Netz in das andere weiterleiten (routen).

Routing Bezeichnet das Festlegen von Wegen bei der Nachrichtenübermittlung.

RSA Der RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) basiert auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Daher benötigt man eine sehr hohe Datenverarbeitungskapazität und viel Zeit, um einen RSA Schlüssel abzuleiten.

RTSP Real-Time Streaming Protocol

Rückfrage Bietet die Möglichkeit, nach dem Anklopfen das erste Gespräch zu halten und ein neues Gespräch entgegenzunehmen.

Rückruf bei Besetzt Leistungsmerkmal im T-ISDN, in Telefonanlagen und im T-Net. Eine Verbindung wird automatisch hergestellt, sobald der Besetztstatus am Zielanschluss aufgehoben ist. Nach Freiwerden des Anschlusses erfolgt die Signalisierung beim Anrufer. Sobald dieser dann seinen Hörer abhebt, wird die Verbindung automatisch hergestellt. Zuvor muss jedoch der Rückruf vom Anrufer an seinem Endgerät aktiviert werden.

Rückruf bei Nichtmelden Sie rufen bei einem gewünschten Gesprächspartner an und der Angerufene meldet sich nicht. Mit "Rückruf bei Nichtmelden" ist das für Sie in Zukunft kein Problem. Denn durch diese Komfortleistung stellen Sie die Verbindung jetzt ohne erneute Wahl her. Immer, wenn Sie nicht selbst telefonieren, erfolgt ein erneuter Verbindungsaufbau zum gewünschten Gesprächspartner - maximal 180 Minuten lang.

Rufnummernband (Durchwahlbereich)

Rufumleitung Auch: Anrufweiterleitung oder Anrufweiterschaltung. Ein ankommender Anruf wird an einen vorgegebenen Telefon-, Internet- oder Mobilfunkanschluss weitergeleitet.

Rufverteilung Bei Telefonanlagen Anrufe bestimmten Endgeräten zugeordnet werden.

Rufzustellung bei Besetzt Ablehnen

Ruhe vor dem Telefon Anrufschutz

S0-Anschluss Siehe ISDN-Basisanschluss.

S0-Bus Sämtliche ISDN-Anschlussdosen und der NTBA beim ISDN-Mehrgeräteanschluss. Jeder So-Bus besteht aus einem vieradrigen Kabel. Die Leitungen/ Kabel übertragen die digitalen ISDN-Signale. Hinter der letzten ISDN-Anschlussdose wird der So-Bus mit einem Abschlusswiderstand terminiert. Der So beginnt beim NTBA und kann bis zu 150 m lang sein. Es lassen sich beliebige ISDN-Geräte daran betreiben. Gleichzeitig können allerdings immer nur zwei Geräte den So verwenden, da nur zwei B-Kanäle zur Verfügung stehen.

S0-Schnittstelle International standardisierte Schnittstelle für ISDN-Einrichtungen. Diese Schnittstelle wird netzseitig vom NTBA bereitgestellt. Nutzerseitig ist die Schnittstelle sowohl für den Anschluss einer Telefonanlage (Anlagenanschluss) als auch für den Anschluss von bis zu acht

ISDN-Endgeräten (Mehrgeräteanschluss) vorgesehen.

S2M-Anschluss Siehe Primärmultiplexanschluss.

SAD Die SAD (=Security Association Database) enthält Informationen über die Sicherheitsvereinbarungen, wie z. B. AH oder ESP Algorithmen und Schlüssel, Sequenznummern, Protokollmodi und SA-Lebensdauer. Für ausgehende IPSec- Verbindungen weist ein SPD-Eintrag auf einen Eintrag im SAD hin, d.h. die SPD legt fest, welche SA angewendet werden muss. Für eingehende IPSec-Verbindungen wird in der SAD abgerufen, wie das Paket weiterverarbeitet werden soll.

Scheduling Zeitablaufsteuerung

SDSL Symmetric Digital Subscriber Line

Server Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden. Oft versteht man unter Server einen bestimmten Rechner im LAN, z. B. DHCP-Server.

ServerPass Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis eines Unternehmens. Mit dem ServerPass bestätigt die T-Com, dass ein Server im Internet zu einem bestimmten Unternehmen gehört und dies durch die Vorlage des Handelsregisterauszugs belegt wurde.

Service 0190 Sprachmehrwertdienst der T-Com zur gewerblichen Verbreitung privater Informationsdienstleistungen. Die Leistungen der T-Com beschränken sich auf die Bereitstellung der technischen Infrastruktur und auf die Abwicklung des Inkassos für die Informationsanbieter. Der Zugang zu den bereitgestellten Informationen erfolgt über die bundesweit einheitliche Telefonnummer 0190 und über eine 6-stellige Telefonnummer. Informationsangebote: Unterhaltung, Wetter, Finanzen, Sport, Gesundheit, Support- und Service-Hotlines.

Service 0700 Sprachmehrwertdienst der T-Com. Ermöglicht die Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Telefonnummer, die mit den Ziffern 0700 beginnt. Kostenfreie Weiterleitung im nationalen Festnetz. Erweiterung mit Vanity möglich.

Service 0900 Sprachmehrwertdienst der T-Com. Löst den Service 0190 ab.

Servicenummer 0180 Sprachmehrwertdienst 0180call der T-Com zur Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Te-

	lefonnummer, beginnend mit den Ziffern 0180.
Setup Tool	Menügesteuertes Tool zur Konfiguration Ihres Gateways. Das Setup Tool kann verwendet werden, sobald ein Zugang zum Gateway (seriell, ISDN-Login, LAN) besteht.
SFP	Small Form-factor Pluggable (kleine Module für Netzwerkverbindungen).
SHA1	Siehe HMAC-SHA.
SHDSL	Single-Pair High-Speed
Shell	Eingabeschnittstelle zwischen Computer und Benutzer.
Shorthold	Bezeichnet die definierte Zeit, nach der eine Verbindung abgebaut wird, wenn keine Daten mehr übertragen werden. Der Shorthold lässt sich statisch (feste Zeit) und dynamisch (in Abhängigkeit von Gebühreninformationen) einrichten.
Sicherungsschicht	Data Link Layer (DLL)
SIF	Stateful Inspection Firewall
Signalisierung	ignalisierung gleichzeitig: Alle zugeordneten Endgeräte werden gleichzeitig gerufen. Ist ein Telefon besetzt, kann angeklopft werden.
SIP	Session Initiation Protocol
SMS	Short Message Service
SMS Server Telefonnummern	An Ihre Telefonanlage können Sie SMS-fähige Telefone anschließen und damit das Leistungsmerkmal SMS im Festnetz der T-Com nutzen. SMS werden über den SMS Server der T-Com an den jeweiligen Empfänger weitergeleitet. Um eine SMS mit einem SMS-fähigen Endgerät versenden zu können, muss die Telefonnummer 0193010 des SMS Servers der Empfängernummer vorangestellt werden. Diese Telefonnummer ist bereits in Ihrer Telefonanlage gespeichert, so dass sich eine manuelle Eingabe der Server Telefonnummer erübrigt bzw. vom Telefon nicht mitgesendet werden muss. Damit Sie SMS an Ihrem SMS-fähigen Festnetztelefon empfangen können, müssen Sie sich einmalig beim SMS Service der Deutschen Telekom registrieren lassen. Das Senden von SMS ist kostenpflichtig. Das Empfangen von SMS ist kostenfrei.
SMS-Empfang	Haben Sie ein SMS-fähiges Endgerät angeschlossen, können Sie

entscheiden, ob für den betreffenden Anschluss der SMS-Empfang erlaubt sein soll. Werkseitig ist kein SMS-Empfang eingerichtet. Damit Sie mit Ihrem SMS-fähigen Endgerät SMS empfangen können, müssen Sie sich einmalig beim SMS Service der T-Com registrieren. Die einmalige Registrierung ist kostenfrei. Sie schicken einfach eine SMS mit dem Inhalt ANMELD an die Zielrufnummer 8888. Anschließend erhalten Sie vom SMS-Dienst der T-Com eine kostenlose Bestätigung der Registrierung. Mit einer SMS mit dem Inhalt ABMELD an die Zielrufnummer 8888 können Sie Ihr Gerät bzw. Ihre Telefonnummer auch wieder abmelden. Eingehende SMS werden dann vorgelesen. Welche Telefone SMS-fähig sind, erfahren Sie im nächsten T-Punkt, unserer Kundenhotline 0800 330 1000 oder im Internet unter http://www.t-com.de.

SNMP Simple Network Management Protocol

SNMP-Shell Eingabeebene für SNMP-Kommandos.

SOHO Small Offices and Home Offices

SPD Die SPD (=Security Policy Database) definiert die Sicherheitsdienste, die für den IP-Traffic zur Verfügung stehen. Diese Sicherheitsdienste sind abhängig von Parametern wie Quelle und Ziel des Pakets, etc.

Sperrliste (Wahlbereiche) Sie können für einzelne Teilnehmer eine Einschränkung der externen Wahl festlegen. Die in der Sperrwerk-Tabelle eingetragenen Telefonnummern können von den Endgeräten, die der Wahlkontrolle unterliegen, nicht gewählt werden. z. B. würde der Eintrag 0190 alle Verbindungen zu kostenintensiven Diensteanbietern verhindern.

SPID Service Profile Identifier

Splitter Der Splitter trennt am DSL-Anschluss Daten und Sprachsignale.

Spoofing Technik zur Reduktion des Datenverkehrs (und damit zur Kostenersparnis) insbesondere in WANs.

SSH Verschlüsselter Zugang zur Shell

SSID Als Service Set Identifier (SSID) oder auch Network Name bezeichnet man die Kennung eines Funknetzwerkes, das auf IEEE 802.11 basiert.

SSL Secure Sockets Layer Eine von Netscape entwickelte, heute standardisierte Technologie, die im allgemeinen dazu verwendet wird, HTTP-Traffic zwischen einem Web Browser und einem Web Server

zu sichern.

STAC Datenkomprimierungsverfahren.

Standardanschluss T-ISDN Basisanschluss mit den Leistungsmerkmalen Dreierkonferenz, Rückfragen/Makeln und Telefonnummernübermittlung. Im Standardanschluss sind drei Mehrfachrufnummern enthalten.

Statische IP Adresse Im Gegensatz zu einer dynamischen IP Adresse eine fest eingestellte IP Adresse.

Subadressierung Neben der Übertragung der ISDN-Telefonnummer können zusätzliche Informationen im Form einer Subadresse bereits beim Verbindungsaufbau über den D-Kanal vom Anrufer zum Angerufenen übertragen werden. Eine über die reine MSN hinausgehenden Adressierung, mit der z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt für einen Dienst angesprochen werden können. In dem angerufenen Endgerät - z.B einem PC - können auch verschiedene Applikationen angesprochen und ggf. ausgeführt werden. Das Leistungsmerkmal ist kostenpflichtig und muss beim Netzbetreiber gesondert beauftragt werden.

Subnetz Ein Netzwerkschema, das einzelne logische Netzwerke in kleinere physikalische Einheiten teilt.

Subnetz Maske Eine Methode um mehrere IP Netze in eine Reihe von Untergruppen oder Subnetze zu teilen. Die Maske ist ein Binärmuster, welches mit den IP Adressen im Netz passen muss. Standardmäßig ist die Subnet Mask 255.255.255.0. In diesem Fall können in einem Subnetz 254 verschiedene IP Adressen auftreten, von x.x.x.1 bis x.x.x.254.

Switch LAN-Switches sind Netzwerkkomponenten, die der Funktion von Bridges oder sogar von Gateways ähnlich sind. Sie vermitteln Datenpakete zwischen Ein- und Ausgangs-Port. Im Gegensatz zu Bridges haben Switches allerdings mehrere Ein- und Ausgangs-Ports. Dadurch erhöht sich die Bandbreite im Netz. Switches können auch eingesetzt werden, um zwischen verschieden schnellen Netzen (z. B. 100MBit- und 10MBit-Netzen) zu übersetzen.

Swyx Ware Softwarelösung für die IP-Telefonie

synchron Übertragungsverfahren, bei dem Sender und Empfänger in genau gleichen Zeittakten arbeiten – im Gegensatz zu asynchron. Leerzeichen werden durch eine Pausencodierung überbrückt.

Syslog Syslog dient als De-facto-Standard zur Übermittlung von Log-Meldungen in einem IP-Netzwerk. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP Port 514 gesendet und zentral gesammelt. Sie werden meist zum Überwachen von Computersystemen benutzt.

Systemtelefone Zu modernen Telefonanlagen gehörendes Telefon, das – je nach Telefonanlage – mit einer Reihe von Komfortfunktionen und Sondertasten ausgestattet ist z. B. das T-Concept PX722.

T-DSL Produktname der Deutschen Telekom AG für ihre DSL-Dienstleistungen und Produkte.

T-Fax Produktbezeichnung für die Telefaxgeräte der T-Com.

T-ISDN Telefonieren, Faxen, Datenübertragung, Online-Dienste - alles über ein Netz und über einen einzigen Anschluss: T-ISDN erschließt Ihnen faszinierende Leistungen mit vielen Vorteilen. Zum Beispiel mit einem Mehrgeräteanschluss - genau die passende Lösung für Familien oder kleine Firmen. Diese Anschlussvariante, bei der bereits die vorhandenen Telefonkabel genutzt werden können, kostet weniger als zwei Telefonanschlüsse, bringt Ihnen aber viel mehr an Qualität und Komfort. Zwei voneinander unabhängige Leitungen, damit Sie auch dann noch telefonieren, ein Fax empfangen oder im Internet surfen können, wenn gerade ein anderes Familienmitglied etwas länger plaudert. Drei oder mehr Telefonnummern, die Sie individuell Ihren Geräten zuordnen und bei Bedarf durch einfache Programmierung wieder anders verteilen können. Wobei man wissen muss, dass die meisten ISDN-Telefone mehrere Telefonnummern "verwalten" können. So lässt sich z. B. ein "zentrales" Telefon im Haushalt einrichten, damit Sie dort auf die Anrufe unter allen ISDN-Telefonnummern reagieren können. Zusätzlich bekommen Fax und Telefon im Arbeitszimmer je eine Telefonnummer - das Telefon für Tochter oder Sohn nicht zu vergessen. So ist jedes Familienmitglied ganz gezielt erreichbar. Ein feiner Komfort, der bestimmt so manchen "Reibungseffekt" beseitigt! Und was die Kosten betrifft, können Sie auf Wunsch in Ihrer Rechnung getrennt ausweisen lassen, welche Tarifeinheiten sich auf welcher ISDN-Telefonnummer summiert haben.

T-Net Das digitale Telefonnetz der T-Com zum Anschluss analoger Endgeräte.

T-NetBox Der Anrufbeantworter im T-Net und im T-ISDN. Die T-NetBox speichert bis zu 30 Nachrichten.

T-NetBox Telefonnummer Tragen Sie hier die aktuelle T-NetBox-Telefonnummer ein, falls diese von der werkseitig eingetragenen 08003302424 abweicht. Sobald eine Sprach- oder Faxnachricht in Ihrer T-NetBox eingegangen ist, wird eine Benachrichtigung an Ihre Telefonanlage gesendet.

T-Online Oberbegriff für die Online-Plattform der T-Com. Mit Leistungen wie E-Mail und Zugang zum Internet.

T-Online Software Softwaredecoder der T-Com für alle gängigen Computersysteme, der den Zugang zu T-Online ermöglicht. Unterstützt alle Funktionen wie KIT, E-Mail und Internet mit einem Browser. Diese Software erhalten alle T-Online Nutzer kostenlos.

T-Service Der T-Service führt sämtliche Installationsarbeiten und Konfigurationen der Telefonanlagen im Auftrag des Kunden aus. Durch Instandhaltungs- und Instandsetzungsarbeiten sorgt er jederzeit für eine optimale Gesprächs- und Datenübertragung.

T-Service Zugang Der T-Service Zugang bietet Ihnen die Möglichkeit, Ihre Telefonanlage vom T-Service konfigurieren zu lassen. Rufen Sie den T-Service an! Lassen Sie sich beraten und geben Sie Ihre Konfigurationswünsche an. Der T-Service konfiguriert dann Ihre Telefonanlage aus der Ferne ohne Ihr weiteres Zutun.

TA Terminal Adapter

TACACS+ Terminal Access Controller Access Control System

TAE Telekommunikationsanschlusseinheit

Tag/Nacht/Kalender Sie legen fest, wie die Umschaltung der Anrufvariante Tag/Nacht erfolgen soll.

TAPI Telephony Applications Programming Interface

TAPI-Konfiguration Mit der TAPI-Konfiguration können Sie den TAPI-Treiber dem Programm, das diesen Treiber nutzt, anpassen. Sie können überprüfen, welche MSN einem Endgerät zugeordnet ist, können einen neuen Leitungsnamen festlegen und die Wählparameter einstellen. Konfigurieren Sie zuerst Ihre Telefonanlage. Anschließend müssen Sie die TAPI-Schnittstelle konfigurieren. Benutzen Sie das Programm "TAPI-Konfiguration".

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TE Terminal Equipment

TEI Terminal Endpoint Identifier

Teilnehmer Name Um Anschlüsse einfacher zu unterscheiden, können Sie für jeden internen Teilnehmer einen Teilnehmer-Namen vergeben.

Telefax Bezeichnung für Fernkopieren zur originalgetreuen Übertragung von Texten, Grafiken und Dokumenten über das Telefonnetz.

Telefonanlage Der Leistungsumfang einer Telefonanlage ist herstellerspezifisch und ermöglicht unter anderem den Betrieb von Nebenstellen, kostenlose Interngespräche, Rückruf bei Besetzt und Konferenzschaltungen. Telefonanlagen übernehmen z. B. die Bürokommunikation (Sprach-, Textund Datenübertragung).

Telefonbuch Die Telefonanlage verfügt über ein internes Telefonbuch. Sie können bis zu 300 Telefonnummern mit den dazugehörigen Namen speichern. Auf das Telefonbuch der Telefonanlage können Sie mit einem funkwerk-Gerät (z. B. CS 410) zugreifen. Über die Konfigurationsoberfläche fügen Sie dem Telefonbuch Einträge hinzu.

Telematik Telematik bezeichnet eine Kombination aus Telekommunikation und Computertechnik und beschreibt die Datenkommunikation zwischen Systemen und Geräten.

Telnet Protokoll aus der TCP/IP-Protokollfamilie. Telnet ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk.

Terminaladapter Gerät zur Schnittstellenanpassung. Hierdurch wird der Anschluss von unterschiedlichem Equipment an das T-ISDN ermöglicht. So dient der Terminaladapter a/b zum Anschluss analoger Endgeräte an die S0-Schnittstelle des ISDN-Basisanschlusses. Bereits vorhandene analoge Endgeräte mit Tonwahl können weiter betrieben werden.

TFE Türfreisprecheinrichtung. Sie lässt sich an verschiedene Telefonanlagen anschalten. Über ein Telefon kann ein Türgespräch geführt und die Tür geöffnet werden.

TFE am analogen Anschluss Ein analoger Anschluss kann für die Anschaltung eines Funktionsmoduls M06, zur Anschaltung einer Türfreisprecheinrichtung DoorLine eingerichtet werden.

TFE-Adapter Das Funktionsmodul kann an einem analogen Anschluss Ihrer Telefonanlage installiert werden. Ist an Ihre Telefonanlage eine TFE (DoorLine) über ein Funktionsmodul angeschaltet, können Sie von

	jedem berechtigten Telefon aus mit einem Besucher an der Tür sprechen. Jedem Klingeltaster können Sie bestimmte Telefone zuordnen, die dann beim Betätigen des Klingeltasters klingeln. Die Signalisierung erfolgt bei analogen Telefonen im Takt des Türstellenrufes. Anstelle der internen Telefone kann auch ein externes Telefon für den Klingeltaster als Rufziel konfiguriert werden. Ihre Türsprechstelle kann bis zu 4 Klingeltaster besitzen. Der Türöffner kann während eines Türgespräches betätigt werden. Eine Betätigung ohne Türgespräch ist nicht möglich.
TFTP	Trivial File Transfer Protocol
Tiger 192	Tiger 192 ist ein relativ neuer und sehr schneller Hash-Algorithmus.
TK-Anlage	Telekommunikationsanlage
TLS	Transport Layer Security
Tonwahl	Mehrfrequenzwahlverfahren (MFV)
Trap	Unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.
Trap-Paket	Nachricht im Fehlerfall.
Trigger	Auslöseimpuls
Trunk	Bündelung
TTL	TTL bedeutet Time to Live und beschreibt die Zeit, in der ein Datenpaket zwischen den einzelnen Servern hin und her geschickt wird, bevor es verworfen wird.
Twofish	Twofish war ein möglicher Kandidat für AES (Advanced Encryption Standard). Er wird als ebenso sicher wie Rijndael (AES) angesehen, ist jedoch langsamer.
U-ADSL	Universal Asymmetric Digital Subscriber Line
Übertragungsrate	Die Anzahl der Bits pro Sekunde, die im T-Net oder im T-ISDN vom PC oder Faxgerät aus übertragen werden. Faxgeräte erreichen bis zu 14,4 KBit/s, Modems bis zu 56 KBit/s. Im ISDN ist Daten- und Faxaustausch mit 64 KBit/s möglich. Bei T-DSL können bis zu 8 MBit/s empfangen und bis zu 768 KBit/s gesendet werden.
UDP	User Datagram Protocol

Umschaltbares Wahlverfahren	Möglichkeit, durch Schalter oder Tasteneingabe an Endgeräten wie Telefon oder Faxgerät zwischen Impulswahlverfahren und Mehrfrequenzwahlverfahren zu wechseln.
Umstecken am Bus (Parken)	Ermöglicht beim Mehrgeräteanschluss während des Telefongespräches das Umstecken der Endgeräteverbindung in eine andere ISDN-Anschlussdose.
UMTS	Universal Mobile Telecommunications System (Mobilfunkstandard der dritten Generation, 3G)
Unterdrückung der Telefonnummer	Leistungsmerkmal in Telefonanlagen. Die Anzeige der Telefonnummer lässt sich fallweise ausschalten.
Update	Aktualisierung eines Softwareprogramms (Firmware der Telefonanlage). Ein Update ist die aktualisierte Version eines vorhandenen Softwareproduktes; man erkennt es an der geänderten Versionsnummer.
Upload	Datentransfer bei Online-Verbindungen, wobei Dateien von dem eigenen PC auf einen anderen PC oder zu einem Datennetzserver übertragen werden.
UPnP	Universal Plug and Play
Upstream	Datenübertragungsrate vom Kunden zum ISP.
URL	Universal/Uniform Resource Locator
USB	Universal Serial Bus
UUS1 (User to User Signalling 1)	Diese Funktion ist nur für Systemtelefone und ISDN-Telefone möglich.
V.11	ITU-T-Empfehlung für symmetrische Doppelstrom-Schnittstellenleitungen (bis zu 10 MBit/s).
V.24	CCITT- und ITU-T-Empfehlung, die die Schnittstelle zwischen einem Computer oder Terminal als Datenendeinrichtung (DTE) und einem Modem als Datenübertragungseinrichtung (DCE) definiert.
V.28	TU-T-Empfehlung für unsymmetrische Doppelstrom-Schnittstellenleitung.
V.35	ITU-T-Empfehlung für Datenübertragung mit 48 kBit/s im Bereich von 60 bis 108 kHz.

V.36 Modem für V.35.

V.42bis Datenkomprimierungsverfahren.

V.90 ITU-Standard für 56 kBit-Analogmodems. Im Gegensatz zu den älteren V.34-Modems werden mit dem V.90-Standard Daten digital zum Kunden weitergesendet und müssen auf einer Modemseite (Provider) nicht zuerst von digital in analog umgewandelt werden, wie es bei V.34-Modems und früheren der Fall ist. Dadurch sind höhere Übertragungsraten möglich. Eine maximale Geschwindigkeit von 56 kBit/s kann nur unter optimalen Umständen erreicht werden.

Vanity Buchstabenwahl

Variante Tag - Nacht Sie möchten wichtige Anrufe für Ihr Home-Office nach Feierabend automatisch auf einen Anrufbeantworter umleiten, damit Sie nicht gestört werden? Dieses können Sie mit der Anrufzuordnung realisieren. Sie können jedem Teilnehmer zwei verschiedene Rufverteilungen (Anrufzuordnung Tag und Anrufzuordnung Nacht) zuweisen. In den Anrufzuordnungen ist auch eine Anrufweiterschaltung zu einem externen Teilnehmer einrichtbar, so dass Sie jederzeit erreichbar sein können.In der Anrufzuordnung Tag und Nacht wird also festgelegt, welche internen Endgeräte bei einem Anruf von extern klingeln sollen. Die Anrufzuordnung Tag und Nacht ist eine Tabelle, in der die ankommenden Rufe internen Teilnehmern zugeordnet werden.

VDSL Very High Bit Rate Digital Subscriber Line (auch als VADSL oder BDSL bezeichnet)

Vermittlungsstelle Knotenpunkt im öffentlichen Telekommunikationsnetz. Man unterscheidet zwischen Ortsvermittlungsstellen und Fernvermittlungsstellen.

VID VLAN ID

VJHC Van-Jacobsen-Header-Komprimierung

VLAN Virtual LAN

VoIP Voice over IP

VPN Virtual Private Network

VSS Virtual Service Set

Wahlkontrolle Sie können in der Konfiguration für bestimmte Endgeräte eine Einschränkung der externen Wahl festlegen.

Wählverbindung Eine Verbindung wird bei Bedarf durch Wählen einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung.

Wahlvorbereitung Bei einigen Telefonen mit Display kann man eine Telefonnummer zuerst eingeben, noch einmal kontrollieren und danach wählen.

WAN Wide Area Network

WAN-Interface WAN-Schnittstelle.

WAN-Partner Gegenstelle, die über das WAN, z. B. ISDN, erreicht wird.

Wartemusik (Music On Hold, MOH) Leistungsmerkmal bei Telefonanlagen. Während der Rückfrage oder des Weiterverbindens wird eine Melodie eingespielt, die der Wartende hört. Ihre Telefonanlage verfügt über zwei interne Melodien zur Auswahl.

Web-Filter Filter der das Aufrufen unerwünschter Webseiten unterbindet.

Webmail Dienst von T-Online, mit dem über einen Browser im Internet weltweit E-Mails versendet und empfangen werden können.

Webserver Server, der Dokumente im HTML-Format zum Abruf über das Internet bereithält (WWW).

Wechselsprechen (nur ISDN-Teilnehmer) Dieser Anschluss ist für ein ISDN-Telefon (nur Systemtelefone T-Concept PX722) mit Wechselsprechfunktion nutzbar. Rufen Sie ein ISDN-Telefon mit Wechselsprechfunktion an, schaltet dieses automatisch die Funktion Lauthören ein, damit sofort ein Gespräch erfolgen kann. Bitte beachten Sie die Hinweise in der Bedienungsanleitung des Telefons zur Funktion Wechselsprechen.

WEP Wired Equivalent Privacy

Westernstecker (auch RJ-45-Stecker) Für ISDN-Endgeräte verwendeter Stecker mit acht Kontakten. Von der US-Telefongesellschaft Western Bell entwickelt. Westerntelefonstecker für analoge Telefone haben vier oder sechs Kontakte.

WINIPCFG Ein grafisches Tool unter Windows 95, 98 und Millennium, das die Win32 API verwendet, um IP Adresskonfiguration von Rechnern anzusehen und zu konfigurieren.

WLAN Eine Gruppe von Computern, die drahtlos miteinander vernetzt sind (FunkLAN).

WMM Wireless Multimedia

WPA	Wi-Fi-Protected Access
WPA - Enterprise	Wendet sich v. a. an die Bedürfnisse von Unternehmen und bietet sichere Verschlüsselung und Authentisierung. Verwendet 802.1x und das Extensible Authentication Protocol (EAP) und bietet damit eine effektive Möglichkeit der Anwender-Authentisierung.
WPA - PSK	Wendet sich an Privat-Anwender oder kleine Unternehmen, die keinen zentralen Authentisierungsserver betreiben. PSK steht für Pre-Shared Key und bedeutet, dass AP und Client eine feste, allen Teilnehmern bekannte beliebige Zeichenfolge (8 bis 63 Zeichen) als Basis für die Schlüsselberechnung im Funkverkehr verwenden.
WWW	World Wide Web
X.21	Die Empfehlungen aus X.21 definieren die physikalische Schnittstelle zwischen zwei Netzwerkomponenten in einem Paketvermittlungsnetz (z. B. Datex-P).
X.21bis	Die Empfehlungen aus X.21bis definieren die DTE/ DCE-Schnittstelle zu synchronen Modems der V-Serie.
X.25	Protokoll, das die Schnittstelle von Netzwerkkomponenten zu einem Paketvermittlungsnetz definiert.
X.31	ITU-T-Empfehlung zur Integration von X.25-fähigen DTEs in ISDN (D-Kanal).
X.500	ITU-T Standards, die Benutzerverzeichnisdienste abdecken, vergleiche: LDAP. Beispiel: Das Telefonbuch ist das Verzeichnis, in dem man Personen anhand des Namens findet (anhand der Übereinstimmung mit dem Telefonverzeichnis). Das Internet unterstützt mehrere Datenbanken mit Informationen über Anwender, wie z. B. Email-Adressen, Telefonnummern und Postanschrift. Diese Datenbanken können durchsucht werden, um Informationen über einzelne Personen zu erhalten.
X.509	ITU-T Standards, die das Format der Zertifikate und Zertifikatanfragen und deren Verwendung definieren.
XAuth	Extended Authentication (Authentifizierungsmethode)
Zentraler Kurzwahlspeicher	Leistungsmerkmal von Telefonanlagen. Telefonnummern werden in der Telefonanlage gespeichert und können dann mit einer Tastenkombination von jedem angeschlossenen Telefon aus aufgerufen werden.

Zielwahlspeicher Kurzwahlspeicher

Zugangscode PIN oder Passwort

Zugriffsschutz Über Filter kann verhindert werden, dass Außenstehende AUF die Daten der Rechnern Ihres LAN zugreifen können. Diese Filter stellen eine Basisfunktion einer Firewall dar.

Zuordnung Ein externer Anruf kann bei internen Teilnehmern signalisiert werden. Die Einträge in der Variante "Tag" und der "Variante Nacht" können unterschiedlich sein.

Index

L

M

N

O

P

W

X

Z